Infor Enterprise Server Single Sign On User Guide

Copyright © 2012 Infor

Important Notices

The material contained in this publication (including any supplementary information) constitutes and contains confidential and proprietary information of Infor.

By gaining access to the attached, you acknowledge and agree that the material (including any modification, translation or adaptation of the material) and all copyright, trade secrets and all other right, title and interest therein, are the sole property of Infor and that you shall not gain right, title or interest in the material (including any modification, translation or adaptation of the material) by virtue of your review thereof other than the non-exclusive right to use the material solely in connection with and the furtherance of your license and use of software made available to your company from Infor pursuant to a separate agreement, the terms of which separate agreement shall govern your use of this material and all supplemental related materials ("Purpose").

In addition, by accessing the enclosed material, you acknowledge and agree that you are required to maintain such material in strict confidence and that your use of such material is limited to the Purpose described above. Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Although Infor has taken due care to ensure that the material included in this publication is accurate and complete, Infor cannot warrant that the information contained in this publication is complete, does not contain typographical or other errors, or will meet your specific requirements. As such, Infor does not assume and hereby disclaims all liability, consequential or otherwise, for any loss or damage to any person or entity which is caused by or relates to errors or omissions in this publication (including any supplementary information), whether such errors or omissions result from negligence, accident or any other cause.

Without limitation, U.S. export control laws and other applicable export and import laws govern your use of this material and you will neither export or re-export, directly or indirectly, this material nor any related materials or supplemental information in violation of such laws, or use such materials for any purpose prohibited by such laws.

Trademark Acknowledgements

The word and design marks set forth herein are trademarks and/or registered trademarks of Infor and/or related affiliates and subsidiaries. All rights reserved. All other company, product, trade or service names referenced may be registered trademarks or trademarks of their respective owners.

Publication Information

Document code	U9559E US
Release	10.6
Publication date	November 2012

Table of Contents

About this document

Chapter 1 Introduction....9

Introduction....9

Infor Federation Services (IFS)....9

Integrated Windows Authentication (IWA)....10

Infor Web UI....10

Chapter 2 Prerequisites for using Single Sign On....11

Prerequisites....11

Chapter 3 Configuring SSO in LN....13

Overview....13

SSO Related Procedures....14

Configuring SSO in LN (Windows)....14

Update session SSO Parameters (ttams0100m000)....15

Update session User Data (ttams1100s000)....15

Create/Update Permissions file....16

Restart ES Logic Service....16

Configuring SSO in LN (non Windows)....18

Update session SSO Parameters (ttams0100m000)....18

Update session User Data (ttams1100s000)....18

Create/Update Permissions file....19

Activate Changes....19

Advanced topics....21

Non-Windows: Using a generic system user....21

Non-Windows: Case-insensitive permission check of SSO user....22

Non-Windows: Permission check when application user and SSO user are different....22

Windows: Dedicated SSO permission check....22

Non-Windows: Dedicated SSO permission check....23

Chapter 4 Configuring Infor Federation Services.....25
Single Sign On, Web UI and Active Directory Federation Services (AD FS).....25
Prerequisites.....25
Single Sign On with IFS.....25
Configuring Infor Federation Services for LN with Web UI.....26
Procedure.....27

Chapter 5 Configuring Integrated Windows Authentication.....31
Single Sign On, Web UI and Integrated Windows Authentication (IWA).....31
Prerequisites.....31
Single Sign On with IWA.....32
Configuring Integrated Windows Authentication for LN with Web UI.....33
Procedure.....33

Appendix A Trouble Shooting.....37
Trouble Shooting Single Sign On.....37
Error: Connect failed with host.....37
Error: Connection broken during login.....38
No permission for SSO.....49
Could not find OS user.....51
Could not impersonate user.....52
AD FS login failed.....53
Importing sp.xml in AD FS fails.....54
Single Sign On failed.....54
No identity passed.....55
Trouble shooting Single Sign Out.....56
Logout request not signed.....56
Failed to create logout request.....57
Error pages.....59
Symptom: Error Page “GSSException: Defective token detected”.....59
Symptom: Error Page “GSSException: Defective token detected.....59
Symptom: Error Page “GSSException: Failure unspecified (…)”.....60

Symptom: Blank Page.....61

Index

About this document

Document summary

This guide is intended for application and system administrators familiar with the system administration of Windows and UNIX systems.

To use this document effectively, you require knowledge of:

- The operating system on which you run Infor LN.
- The Relational Database Management System (RDBMS) that you use and the relational database concepts.
- Microsoft Active Directory Federation Services (AD FS).
- Infor Federation Services (IFS)
- Integrated Windows Authentication (IWA)
- Infor LN Tools
- Web UI

Comments?

We continually review and improve our documentation. Any remarks/requests for information concerning this document or topic are appreciated. Please e-mail your comments to documentation@infor.com .

In your e-mail, refer to the document number and title. More specific information will enable us to process feedback efficiently.

Contacting Infor

If you have questions about Infor products, go to the Infor Xtreme Support portal at www.infor.com/inforxtreme .

If we update this document after the product release, we will post the new version on this Web site. We recommend that you check this Web site periodically for updated documentation.

Chapter 1
Introduction

1

This chapter provides information on the products you need if you want to use Single Sign On (SSO) based on either Infor Federation Services (IFS) or Integrated Windows Authentication (IWA).

Introduction

The goal of the SSO solution is to offer a globally secured software environment, which allows users to provide their credentials once to access multiple applications.

Depending on configuration settings users can be signed on automatically based on their OS credentials. After signing on once, users can navigate from one application to another without having to sign on again. For example, after signing on, a user can drill back from Key Performance Indicators (KPIs) to details in LN. During the drill back actions, the relevant LN sessions start directly; the user does not have to sign on to LN.

Infor Federation Services (IFS)

The purpose of IFS application is to provide central authentication and authorization for multiple applications. The IFS application provides the feature to assign security roles and accounting entities to users. IFS incorporates Active Directory Federation Services (AD FS), a service which can be configured in Windows Server.

The IFS installer will take care of the AD FS configuration for the IFS setup. Infor specific claim types are configured and the integration with the IFS application database is configured. The IFS application will be registered as a Relying Party in AD FS, including the required claim rules.

The registration of other Infor applications in AD FS will be arranged through the IFS application. Infor applications that are prepared for IFS describe in their installation and configuration documentation what information is required to register the application in IFS and AD FS.

For more information about IFS see:

- *Infor Federation Services Installation Guide (U9661 US)*.
- *Infor Federation Services Administration Guide (U9663 US)*.

Integrated Windows Authentication (IWA)

To create automatically authenticated connections IWA uses the security features of Windows clients and servers . The Kerberos v5 protocol is used to exchange authentication information. IWA is suited for intranet environments where all users have a Windows domain account.

Infor Web UI

Infor Web UI is a browser-based user interface client on top of LN.

For more information about Web UI see:

- *Infor Web UI - Installation and Configuration Guide (U8715 US)*.

To obtain the latest version of the Web UI software download solution 22881482 from Infor's support site.

Chapter 2
Prerequisites for using Single Sign On

2

This chapter provides information about the Single Sign On requirements that must be met.

Prerequisites

To ensure users can log on using IFS or IWA SSO authentication, some requirements must be met:

- In the User Data (ttaad2500m000) session, the LN user must be linked to an Infor Security user. See chapter "Configure SSO in LN ".
- The correct SSO type (IFS or IWA) must be configured.
- An environment that uses the BaanLogin SSL protocol must be available. For details, see chapter "Configuring Infor Federation Services " and chapter "Configuring Integrated Windows Authentication ".
- The users must connect to the SSO URL. This URL has this format:

  http(s)://[hostname]:[port]/[webui-root]/servlet/fslogin
- The users must select a Web UI user profile that is linked to an environment that uses the BaanLogin SSL protocol.

For Infor Federation Services SSO, these requirements must be met:

- SSO user data must be defined in IFS. See the *Infor Federation Services Administration Guide (U9663 US)*

For details, see:

- *Infor Enterprise Server – Technical Manual (U8172 US)*.
- *The Web UI online Help*.

Chapter 3
Configuring SSO in LN

3

This chapter provides information on the user identity in LN and user access to LN in order to enable SSO in LN.

Overview

This section describes how to configure LN to allow Single Sign-On (SSO) with Web UI.

When an end user uses Web UI and SSO to access LN, Web UI and LN must complete some tasks before the end user can use the application:

- Web UI obtains the end user's identity from the security domain and requests a secure connection from the selected LN system.
- LN validates the connection request and credentials, and runs the bshell on behalf of the end user.

The required Web UI configuration is described in chapter 4 and 5. The required LN configuration is the scope of this chapter and facilitates connecting, mapping, (permission) checking and impersonation.

- *Connecting* means that the Web UI 's request for the secure connection is acknowledged and that the data exchange between Web UI and LN can start.
- *Mapping* is needed because the security domain may have identified the end user with an account name that is different than the LN account. In addition, the system account which will later be used to run the bshell must be derived.
- *Permission* checking is needed because the mapping information is not sufficiently secured.
- *Impersonation* is about the LN operating system account which will run the bshell binaries on behalf of the end user.

The LN configuration steps that are required to successfully achieve these steps are described later. This table lists the used terminology:

End User	The person using LN
Application User	An LN account for an end user
System User	The operating system account which runs the bshell on behalf of the end user
SSO User	The end user's username within the security domain (Active Directory, Infor Federation Services)
Generic System User	A (non-personal) operating system account which runs the bshell on behalf of multiple end users

SSO Related Procedures

This section describes how to create or change the LN configuration to support SSO. The procedures for Windows and non-Windows platforms are described separately.

Prerequisites

The LN system administrator must have completed the procedures to create LN users.

For details on LN user management, see the *Infor Enterprise Server Administration Guide (U8854 US)* and the session help.

For all end users which need SSO access, the SSO User must be known in Active Directory. When specifying the SSO User value in the described procedures, the SAM account name (pre-Windows 2000 logon name) for that user must be specified normally. Only when multiple domain support is used, the User Principal Name (UPN) for that user must be specified.

When LN is running on a Windows platform, a Generic System User must be present. Its username and password need to be supplied during the procedure.

When LN is running on a Windows platform, the reader must be familiar with the ES Service Manager. For details on Enterprise Server Service Manager, see the *Infor Enterprise Server Administration Guide (U8854 US)*.

Configuring SSO in LN (Windows)

This procedure applies to LN running on a Windows platform.

Update session SSO Parameters (ttams0100m000)

To activate Single Sign On:

1. Log on to LN by using Web UI.
2. Select LN Tools > Application Configuration > Parameters.
3. Start session SSO Parameters (ttams0100m000)
4. Select the SSO Active checkbox.
5. Specify this information:
   - In field Infor SSO Service Location, specify ‘N/A’ or similar. This field is not relevant but must contain info.
   - Specify the windows domain of the Generic System User, for example, “<company name>,” or, for a local account, the machine name.
   - Specify the user name of the Generic System User in the Generic System User field.
   - Specify the password of the Generic System User in the Password field.
6. Click **Dump** to place the information in the file:

   `$BSE/lib/sso_config`

See the online help of this session for more specific field information.

Update session User Data (ttams1100s000)

To SSO enable LN users:

1. Select User Management > General User Data.
2. Start the User Data (ttaad2500m000) session.
3. Open the User Data details for the Application user which needs SSO access.
4. Specify the SSO User (pre-Windows 2000 login name or User Principal Name) in the Infor Security User field.
5. Repeat steps 3 and 4 for other Application Users that need SSO access.
6. Save and Close the **User Data (ttams1100s000)** session. You will return to the Main **User Data (ttaad1100m000)** session.
7. On the specific menu in the User Data (ttaad2500m000) session, click **Convert Changes To Runtime DD**. The Convert Changes to Runtime DD (ttams2200m000) session appears.
8. Enter the required data in the Convert Changes to Runtime DD (ttams2200m000) session. See the session help for details.
9. Click **Convert** to convert the user data to an encoded s[SSO User] file in the directory:

   `$BSE/lib/user/sso/`

Create/Update Permissions file

1. Ensure that a directory with the name security exists within the BSE directory of the ES Logic Service. You can find the BSE path under Start > Administrative Tools > Services > ES Logic Services > Properties.
2. Assume the path to the ES Logic Service executable is:

   `C:\Infor\ERPLN\commonx64\bin\rexecd.exe`

   Then the path of the directory *security* must be:

   `C:\Infor\ERPLN\commonx64\security`
3. Use the Windows Domain and Generic System User as specified in the SSO parameters session, to create file sso_permissions.xml as shown in the example (replace ‘domain’ and ‘username’ with the actual values).
4. Save file sso_permissions.xml in directory *security*.
5. To avoid unauthorized changes or deletions, ensure that file sso_permissions.xml and the containing directories are sufficiently secure.

Example

```
<?xml version="1.0"?>
<SingleSignOn>
   <impersonations sso_location="STS">
      <impersonation os_user="domain\username">
         <sso_user name="*"/>
      </impersonation>
   </impersonations>
</SingleSignOn>
```

Restart ES Logic Service

1. Start the ES Service Manager.
2. Navigate to ES Logic Service > Properties > Protocol Configuration

   Ensure that the connection protocol ‘Federation Services’ is selected.
3. Restart the ES Logic Service using the ES Service Manager.

   The default SSL properties file security/ssl.properties will be used (relative to the BSE directory of the ES Logic Service). Additional arguments can be specified when starting the ES Logic Service from the command line, for example:

   `rexecd -start -d -ssl security/myssl.properties`

   The meaning of these two arguments is:

   - -d for logging additional information. An event will be logged in the Event Viewer to announce the file name to which the additional information will be logged.

- -ssl <ssl properties file> for specifying a non-default SSL properties file. Prefix the file name with an @-sign to indicate that it must not be interpreted relative to the BSE directory of the ES Logic Service. For example use: -ssl @local_file or -ssl @/etc/absolute_path.

The additional arguments provided to -start|-stop|-install are saved in the registry and used when the ES Logic Service is started (from the command line) without additional arguments or when it is started by the ES Service Manager snap-in.

This table summarizes how data from session SSO Parameters is used:

SSO parameters		
Field	Usage	Remarks
Windows Domain	Impersonation: System User domain	
Generic System User	Impersonation: System User username	
Password	Impersonation: System User password	
Overrule System User Allowed	Impersonation	Disabled: always unchecked

This table summarizes how data from session User data is used:

User data		
Field	Usage	Remarks
User	Mapping: Application User	
Infor Security User	Mapping: SSO User	
Use Generic System User	Impersonation	Disabled: always checked
System Login	Not used for SSO	

Configuring SSO in LN (non Windows)

This procedure applies to LN running on a non-Windows platform.

Update session SSO Parameters (ttams0100m000)

To activate Single Sign On:

1. Log on to LN using the Web UI.
2. Select LN Tools > Application Configuration > Parameters.
3. Start session SSO Parameters (ttams0100m000)
4. Select the SSO Active checkbox.
5. Specify this information:
   - In the Infor SSO Service Location field specify ‘N/A’ or similar This field must contain data.
   - In the Generic System User field specify a username.
   - Select the Overrule System User Allowed checkbox.
6. Click **Dump** to place the information in the directory:
   `$BSE/lib/sso_config`

See the online help of this session for more specific field information.

Update session User Data (ttams1100s000)

To SSO enable LN users:

1. Select User Management > General User Data.
2. Start the User Data (ttaad2500m000) session.

3. Open the User Data details for the Application user which needs SSO access.
4. Specify the SSO User (pre-Windows 2000 login name or User Principal Name) in the Infor Security User field.
5. Repeat steps 3 and 4 for other Application Users that need SSO access.
6. Save and Close the **User Data (ttams1100s000)** session. You will return to the Main **User Data (ttaad1100m000)** session.
7. On the specific menu in the User Data (ttaad2500m000) session, click **Convert Changes To Runtime DD**. The Convert Changes to Runtime DD (ttams2200m000) session appears.
8. Specify the required data in the Convert Changes to Runtime DD (ttams2200m000) session. See the session help for details.
9. Click **Convert** to convert the user data to an encoded s[SSO User] file in the directory:

   `$BSE/lib/user/sso/`

Create/Update Permissions file

To create/update the permissions file:

1. Ensure that a directory with the name security exists within the BSE directory of the BaanLogin daemon ($BSE/security).
2. Create the file sso_permissions.xml as shown in the example section.

   This example sso_permissions.xml file assumes that all involved combinations of Application User and SSO User are pairs of identical strings. See ‘Advanced Topics’ if the strings within one or more pairs are different.
3. Save file sso_permissions.xml in directory security.
4. To avoid unauthorized changes or deletions, ensure that file sso_permissions.xml and the containing directories are sufficiently secure.

Example

```
<?xml version="1.0"?>
<SingleSignOn>
   <impersonations sso_location="STS">
      <impersonation os_user="*">
         <sso_user name="+"/>
      </impersonation>
   </impersonations>
</SingleSignOn>
```

Activate Changes

To activate changes:

1. Stop the BaanLogin daemon with this command:

```
blogind6.2 -k
```

2. Start the BaanLogin daemon with this command:

   ```
   blogind6.2 -p 7150 -ssl security/ssl.properties
   ```

   The option –p <port number> specifies the port number used by the daemon. When this option is omitted, the default port number is 7150.

   The option –ssl <ssl properties file> specifies the SSL properties file to be used, relative to the BSE directory of the BaanLogin daemon. When this option is omitted, the default SSL properties file is security/ssl.properties

   Prefix the file name with a @-sign so it will not be interpreted relative to the BSE directory of the BaanLogin daemon. For example use –ssl @local_file or –ssl @/etc/absolute_path. To start this daemon for problem tracing use:

   ```
   blogin6.2 -p 7150 -ssl security/ssl.properties -d > ${BSE}/log/blogin.
   log 2>&1
   ```

   The trace output will be sent to the file ${BSE}/log/blogin.log

This table summarizes how data from session SSO Parameters is used:

SSO parameters		
Field	Usage	Remarks
Generic System User	Not used	
Overrule System User Allowed	Impersonation	Normally selected

This table summarizes how data from session User data is used:

User data		
Field	Usage	Remarks
User	Mapping: Application User	
Infor Security User	Mapping: SSO User	
Use Generic System Login	Impersonation	Normally not selected
System Login	Impersonation: System User username	

Advanced topics

This section describes some procedures which can be used to deviate from the standard/default procedures.

Non-Windows: Using a generic system user

The described configuration procedure (non-Windows) assumes that any bshell is started using the system user defined for the application user. To have all LN users run the binaries impersonated as the Generic System User, deviate from the described procedure.

To use a generic system user:

1. Create an account to be used as the Generic System User
2. When updating session SSO Parameters, specify the Generic System User username.
3. When updating session User Data, ensure that the 'Use Generic System User' checkbox is selected.
4. Create the file sso_permissions.xml as shown here (replace ‘username’ with the Generic System User username):

```
<?xml version="1.0"?>
<SingleSignOn>
   <impersonations sso_location="STS">
      <impersonation os_user="username">
         <sso_user name="*"/>
      </impersonation>
```

```
   </impersonations>
</SingleSignOn>
```

Non-Windows: Case-insensitive permission check of SSO user

The described Configuration Procedure (non-Windows) yields file sso_permissions.xml implementing a case-sensitive permission check; this is desired when all involved Application User/ SSO User pairs consist of identical strings. However, if the case is different for one or more end users, the permission check must be case-insensitive. To achieve this in file sso_permissions.xml, specify this information:

```
<sso_user name="#"/>
```

instead of

```
<sso_user name="+"/>
```

Non-Windows: Permission check when application user and SSO user are different

The described Configuration Procedure (non-Windows) yields file sso_permissions.xml implementing a case-sensitive permission check; this is desired when all involved Application User/ SSO User pairs consist of identical strings. However, if for one or more of the end users the SSO user differs from the application user, file sso_permissions.xml must be extended with a specific entry for each such user.

For example, if application user ‘jdoe’ is associated to SSO user ‘JRDoe’, file sso_permissions.xml must have the contents as shown here:

```
<?xml version="1.0"?>
<SingleSignOn>
   <impersonations sso_location="STS">
      <impersonation os_user="*">
         <sso_user name="+"/>
      </impersonation>
      <impersonation os_user="jdoe">
         <sso_user name="JRDoe"/>
      </impersonation>
   </impersonations>
</SingleSignOn>
```

Additional entries such as the one for ‘jdoe’ must be specified as needed.

Windows: Dedicated SSO permission check

File sso_permissions.xml can be used to allow access for one or more dedicated application users, denying SSO access to any other users. For example, if SSO access must be allowed for application users ‘jdoe’ and ‘jroe’, specify these contents in the sso_permissions.xml file:

```
<?xml version="1.0"?>
<SingleSignOn>
   <impersonations sso_location="STS">
      <impersonation os_user="domain\username">
         <sso_user name="jdoe"/>
         <sso_user name="jroe"/>
      </impersonation>
   </impersonations>
</SingleSignOn>
```

(‘domain’ and ‘username’ must be replaced with the corresponding fields of the SSO Parameters session.)

Non-Windows: Dedicated SSO permission check

File sso_permissions.xml can be used to allow access for one or more dedicated Application Users, denying SSO access to all other users. For example, if SSO access must be allowed for application users ‘jdoe’ and ‘jroe’, specify these contents in the sso_permissions.xml file:

```
<?xml version="1.0"?>
<SingleSignOn>
   <impersonations sso_location="STS">
      <impersonation os_user="jdoe">
         <sso_user name="jdoe"/>
      </impersonation>
      <impersonation os_user="jroe">
         <sso_user name="jroe"/>
      </impersonation>
   </impersonations>
</SingleSignOn>
```

Chapter 4
Configuring Infor Federation Services

4

This Chapter explains how to establish a Single Sign On connection between Web UI and LN, using IFS.

Single Sign On, Web UI and Active Directory Federation Services (AD FS)

Prerequisites

AD FS 2.0 must be installed and the basic configuration must be performed. For details, see the *AD FS and IFS Installation guide (U9661 US)*.

Enterprise Server 8.7 and Web UI 8.7 or later must be installed.

These files must be available in the 'security' directory:

- `<path>\security\keystore.p12`
- `<path>\security\ssl.properties`
- `<path>\security\sso_permissions.xml`

You can find the security folder on UNIX in:

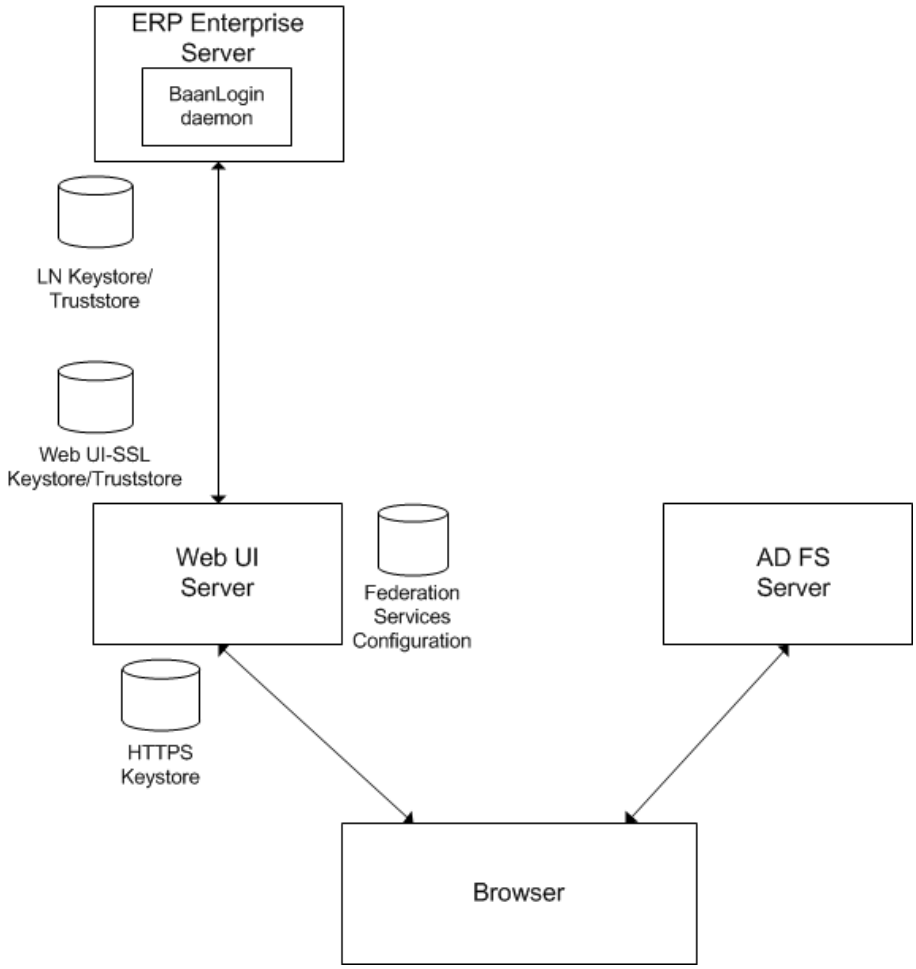
- `${BSE}/security`

On Windows for example in:

- `C:\Infor\LN\commonx86\security (32-bit porting set)`
- `C:\Infor\LN\commonx64\security (64-bit porting set)`

Single Sign On with IFS

This diagram shows the components which play a role in Single Sign On for Web UI using IFS.



The BaanLogin (Blogin) daemon is a secure alternative for the rexec protocol. For details, see the *Enterprise Server Technical Manual (U8172 US)*.

To configure Web UI for SSO using IFS, three keystores are required. See the previous diagram. Two keystores are used to establish a trust relation between the LN server and the Web UI server. The third keystore enables https on the Web UI server.

For details on how to create these keystores, see the following section.

Configuring Infor Federation Services for LN with Web UI

This section describes the procedure to configure Web UI and IFS to authenticate LN users through IFS.

LN/ Web UI is used in an environment with Infor Federation Services (IFS). This is required for a setup with Workspace. IFS is used to configure AD FS. Upon completion of the procedure that is described in this chapter, you must complete the procedure described in the LN (Manufacturing) to Workspace Integration chapter of the *Infor Web UI - Installation and Configuration Guide (U8715 US)*.

For details on IFS, see:

- *Infor Federation Services Administration Guide (U9663 US)*
- *Infor Federation Services AD FS and IFS Installation Guide (U9661 US)*

See the procedure section for details.

Procedure

To configure IFS for LN with Web UI:

Step 1: If LN runs on a Windows platform.

Select the **Federation Services** check box in the Infor ES Service Manager.

Step 2: If you use Enterprise Server 8.7, install solution 22943754 on the LN server.

Step 3: Download policy files.

Download 'Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files' for the Java version which is used on the webserver.

To download the files:

1. Open this URL:
   `http://www.oracle.com/technetwork/java/javase/downloads/index.html`
2. Scroll to Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the Java version which is used on the webserver. Select Download and download the zip archive file.
3. Extract the zip file and copy the content of the jce folder to the [JRE_HOME]/lib/security directory on the Web UI Web server.

   Note: If there are multiple JREs on the Web UI Web server, ensure you install the files in the JRE that belongs to Web UI. To check which JRE belongs to Web UI:

   a. Start the Web UI Administration Console.
   b. Select **Infor Web UI Administration > Diagnostics** to open the Diagnostics page.
   c. Check the Java system property `java.home`.
4. Restart the webserver to use the new policy files.

If you do not install the policy files, an error message can be displayed because the keystore file generation is using long key sizes for the keys.

Step 4: Create Login Configuration for Infor Federation Services

1. Start the Web UI Administration Console

2. Select Infor Web UI Administration > Login Configuration to open the Login Configuration Page
3. Verify the HTTPS Port Number value which will be used for secure communication between the user's browser and the Web UI. If needed, adapt the value and select Submit.
4. Select the Support Multiple Domain SSO checkbox when using Infor Federation Services to authenticate users from multiple domains. Click Submit.
5. Select Federation Services as the Single Sign On type and select Configure SSO.
6. Supply the correct IFS Webservice URL and click OK.

   When the process is finished, write down the Relying Party Identifier that was generated by the IFS Webservice. You will need this ID when you activate the application in IFS later in this procedure.
7. Use the following steps to configure secure communications (HTTPS) between the user's browser and the Web UI:
   - Select Configure HTTPS and enter Organizational Unit, Organisation, Locality (or City), State (or Province) and Country Name of your organisation; select OK to create a new certificate
   - Close and reopen the Login Configuration page.
   - Select Generate Certificate Request and use Copy to Clipboard to submit a request for a signed certificate toward a trusted party (Certificate Authority)
   - Use Import CA Reply and/or Import Trusted Certificate to process the response from the Certificate Authority

Step 5: Generate/Update Keystores.

1. Start the Web UI Administration Console.
2. Select **Infor LN > Infor LN Environments** to open the Manage Infor LN Environments page.
3. Select an environment that uses the BaanLogin SSL Protocol and click **Generate/Update Keystores** to display the corresponding dialog box.
4. Specify the required information. For details, see the online help of the **Generate/Update Keystores** dialog box.
5. Click **OK** in the **Generate/Update Keystores** dialog box.

   This question is displayed: `Are you sure? Existing keystores will be modified.`
6. Click **Yes** in the question window. A dialog showing the progress is displayed.

   During this process, the keystore file and the `ssl_properties` file are updated on the LN server. When you run this process multiple times, the SSO parameters are not overwritten.
7. When the process is finished, click **Close** in the **Progress** dialog.

Important!

- If a step fails, view the generated error message and try to solve the error.

Step 6: Restart Tomcat.

Step 7: Restart Baan Login Daemon

You must restart the Baan Login Daemon on the LN back-end. Otherwise the BaanLogin daemon will not pick up the new certificates that were generated in the "Generate/Update Keystores" step in this procedure. See the procedure to stop or start the daemon mentioned earlier.

Step 8: Activate the Web UI Relying Party Trust in the IFS application

To activate the Web UI Relying Party Trust in the IFS application:

1. Open the following URL and sign in to the IFS application with a user account that is assigned to the Application Admin security role.

   `https://[IFS server]:[port]/IFS/`

   See the IFS documentation for additional details.
2. Select **Configure > Applications**.
3. On the Applications page, select the Application entry with the value that matches the **Relying Party Identifier** generated in the SettingsLogin Configuration dialog box for SSO type IFS. This application has the Pending status.
4. Click **Activate** to display the Administrator Credentials dialog.
5. Specify the password for the local administrator for the server. The user ID of this administrator is "Administrator". If necessary, see the IFS documentation for account requirements for this step.
6. Click **OK** to activate the application. The Administrator Credentials dialog is closed. On the Applications page, the status of the selected application changes to Active.

Step 9: Test HTTPS connection

Now that you have a trusted HTTPS connection, you can verify that the HTTPS connection to the Web UI server is trusted by your browser.

To verify the connection:

1. Open this URL: `https://[hostname].[domain]:[HTTPS port number]`

   A Login page must be displayed.
2. Verify that a yellow padlock is displayed in the browser’s address bar.

Step 10: Test SSO connection between Web UI and LN

To test if the SSO connection between the Web UI server and the LN server is configured correctly:

1. Start the Web UI Administration Console.
2. Select **Infor LN > Diagnostics**.

3. On the **Diagnostics** page, click on the LN Environment which has just been enabled for Federation Services.
   - In the Username field, specify a valid SSO username (Infor Security User: pre-Windows 2000 login name or User Principal Name) and then click **Test connection**.
   - When the configuration is correct, a screen with the massage "Connection successfully established" is displayed.

Step 11: Test Infor Federation Services for Web UI

To verify that IFS for Web UI is correctly configured, open this URL: `https://[hostname].[domain]:[HTTPS port number]/webui/servlet/fslogin`.

A Login page must now be shown:

You can now proceed as usual, creating a new user profile for this Web UI environment.

Step 12: Optionally, perform additional steps for a setup with Workspace

For a setup with Workspace, you must complete the procedure described in the LN (Manufacturing) to Workspace Integration chapter.

Chapter 5
Configuring Integrated Windows Authentication

5

This Chapter explains how to establish a Single Sign On connection between Web UI and LN using Integrated Windows Authentication (IWA).

Single Sign On, Web UI and Integrated Windows Authentication (IWA)

Before the required configuration can be created, it must be clear which communication security between the user's browser and the Web UI will be used:

- If secure communication using the HTTPS protocol is needed, a HTTPS port number must be chosen. The default port number is 8443. The chosen HTTPS port number is needed during some of the configuration steps. The Web UI will be accessible at URL:
  - https://[hostname].[domain]:[HTTPS port number]/[webui-root]/servlet/fslogin
- Otherwise, default (unsecure) communication using the HTTP protocol is used and the Web UI will be accessible at URL:
  - http://[hostname] .[domain]:[HTTP port number]/[webui-root]/servlet/fslogin

Prerequisites

Enterprise Server and Web UI must be installed.

If Web UI is running on a Windows platform, an SPN that maps to the built-in computer account of the Web UI server is sufficient. To check the presence of the SPN run this command:

- setspn –Q HOST/[hostname].[domain]

If Web UI is running on a non-Windows platform, a pre-authentication domain account must exist.

Note

Use the Domain Controller's Active Directory Users and Computers dialog box to select the proper option of the pre-authentication account.

Select the checkbox "Password never expires" .

Clear the checkbox “Use Kerberos DES encryption types for this account”.

if Web UI is running on a non-Windows platform, an SPN mapping to the pre-authentication domain account must exist. The SPN must be created for the HTTP service class (which is valid for HTTP and HTTPS communications). To add a Service Principal Name use this setspn command:

- setspn –A HTTP/[hostname].[domain] <pre-authentication account name>

This command can be used to check the presence of the SPN:

- setspn –Q HTTP/[hostname].[domain]

On the Enterprise Server these files must be available in the ‘security’ directory:

- <path>\security\keystore.p12
- <path>\security\ssl.properties
- <path>\security\sso_permissions.xml

You can find the security folder on UNIX in:

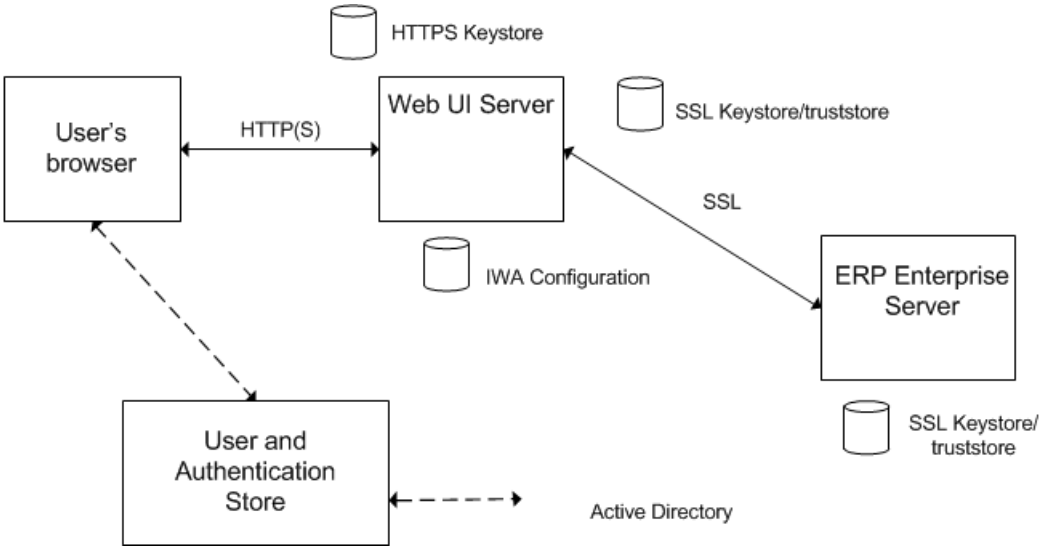
- ${BSE}/security

You can find the security folder on Windows in:

- C:\Infor\LN\commonx86\security (32-bit porting set)
- C:\Infor\LN\commonx64\security (64-bit porting set)

Single Sign On with IWA

This diagram shows the components which play a role in SSO for Web UI using IWA.



To configure Web UI for SSO using IWA, two or three keystores are required. Two keystores are used to establish a trust relation between the LN server and the Web UI server. Only if secure communication is used between the user's browser and Web UI, the third keystore to enable HTTPS on the Web UI server is needed.

Configuring Integrated Windows Authentication for LN with Web UI

The following procedure describes how to configure Web UI to authenticate LN users through IWA.

Procedure

Ensure that your software is licensed, otherwise this procedure will fail.

To configure IWA for LN with Web UI:

Step 1: If LN runs on a Windows platform.

Select the **Federation Services** check box in the Infor ES Service Manager.

Step 2: If you use Enterprise Server 8.7, install solution 22943754 on the LN server.

Step 3: Download policy files.

Download 'Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files' for the Java version which is used on the webserver.

To download the files:

1. Open this URL:
   `http://www.oracle.com/technetwork/java/javase/downloads/index.html`
2. Scroll to 'Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for the Java version which is used on the webserver. Select Download and download the zip archive file.
3. Extract the zip file and copy the content of the jce folder to the [JRE_HOME]/lib/security directory on the Web UI Web server.

   Note: If there are multiple JREs on the Web UI Web server, ensure you install the files in the JRE that belongs to Web UI. To check which JRE belongs to Web UI:

   a. Start the Web UI Administration Console.
   b. Select **Infor Web UI Administration > Diagnostics** to open the Diagnostics page.
   c. Check the Java system property 'java.home'.
4. Restart the webserver to use the new policy files.

If you do not install the policy files, the configuration process to generate the keystore file will fail.

Step 4: Create Login Configuration for Integrated Windows Authentication

1. Start the Web UI Administration Console
2. Select Infor Web UI Administration > Login Configuration to open the Login Configuration Page
3. If secure communication is needed, verify the HTTPS Port Number value. This value will be used for secure communication between the user's browser and the Web UI. If needed, adapt the value and select Submit.
4. Select the Support Multiple Domain SSO checkbox when using Integrated Windows Authentication to authenticate users from multiple domains. Click Submit.
5. Select Integrated Windows Authentication as the Single Sign On type and select Configure SSO.
6. Use the credentials of the pre-authorization account (see Prerequisites) for 'domain account' and 'domain account password' and supply the other required details and select OK
7. Only if secure communication is needed, use the following steps to configure secure communications (HTTPS) between the user's browser and the Web UI:
   - Select Configure HTTPS and enter Organizational Unit, Organisation, Locality (or City), State (or Province) and Country Name of your organisation; select OK to create a new certificate
   - Close and reopen the Login Configuration page.
   - Select Generate Certificate Request and use Copy to Clipboard to submit a request for a signed certificate toward a trusted party (Certificate Authority)
   - Use Import CA Reply and/or Import Trusted Certificate to process the response from the Certificate Authority

Step 5: Generate/Update Keystores.

1. Start the Web UI Administration Console.
2. Select **Infor LN > Infor LN Environments** to open the Manage Infor LN Environments page.
3. Select an environment that uses the BaanLogin SSL Protocol and click **Generate/Update Keystores** to display the corresponding dialog box.
4. Specify the required information. For details, see the online help of the **Generate/Update Keystores** dialog box.
5. Click **OK** in the **Generate/Update Keystores** dialog box.

   This question is displayed: `Are you sure? Existing keystores will be modified.`
6. Click **Yes** in the question window. A dialog showing the progress is displayed.

   During this process, the keystore file and the `ssl.properties` are updated on the LN server.
7. When the process is finished, click **Close** in the **Progress** dialog box.

Important!

- If a step fails, view the generated error message and try to solve the error.

Step 6: Restart Tomcat.

This activates the generated keystores and the changed configuration for IWA.

Step 7: Restart Baan Login Daemon

You must restart the Baan Login Daemon on the LN back-end. Otherwise the BaanLogin daemon will not pick up the new certificates that were generated in the "Generate/Update Keystores" step in this procedure. See the procedure to stop or start the daemon mentioned earlier.

Step 8: Test HTTPS connection

This step is applicable only when secure communications are used between the user's browser and Web UI.

When you have a trusted HTTPS connection, you can verify if the HTTPS connection to the Web UI server is trusted by your browser.

Complete these steps:

1. Open this URL: `https://[hostname].[domain]:[HTTPS port number]`

   A login page must be displayed.
2. Verify that the padlock displayed in the browser's address bar indicates a trusted site.

Step 9: Test SSL connection between Web UI and LN

To test if the SSL connection between the Web UI server and the LN server is configured correctly:

1. Start the Web UI Administration Console.
2. Select Infor LN > Diagnostics.
3. On the **Diagnostics** page, click on the LN Environment which has just been enabled for IWA. A dialog box will be displayed.
   - In the Username field, specify a valid SSO username (Infor Security User: pre-Windows 2000 login name or User Principal Name) and click **Test connection**.
   - When the configuration is correct, a screen with a the message "Connection successfully established" displays.

Step 10: Test Integrated Windows Authentication for Web UI

To verify that IWA for Web UI is correctly configured, open this URL: `https://[hostname].[domain]:[HTTPS port number]/webui/servlet/fslogin`.

Otherwise, use the URL: `http://[hostname].[domain]:[HTTP port number]/[webui-root]/servlet/fslogin`

A Login page will be shown.

You can now proceed as usual, creating a new user profile for this Web UI environment.

Step 11: Optionally, perform additional steps for a setup with Workspace

For a setup with Workspace, you must complete the procedure described in the LN (Manufacturing) to Workspace Integration chapter.

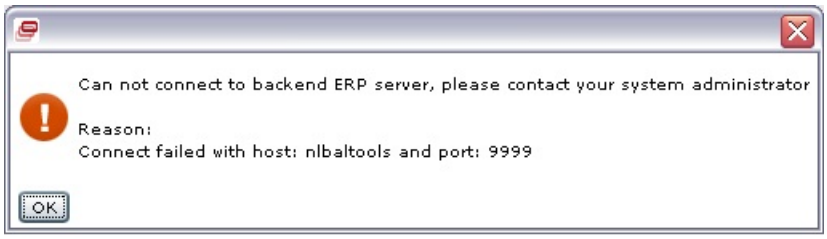
Appendix A
Trouble Shooting

A

Trouble Shooting Single Sign On

Error: Connect failed with host

During login this message is displayed:



In the diagnostics test this information is displayed:

```
A connection to the environment could not be established. An exception occurred during
the connection attempt:Connect failed with host: nlbaltools and port: 9999

Host error. Possible causes:
1) Wrong hostname
2) Wrong port number
3) No listener ('rexec' or 'BaanLogin') running on host

com.ssaglobal.erp.server.connection.BaanConnectionException: Connect failed with host:
nlbaltools and port: 9999
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:204)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
```

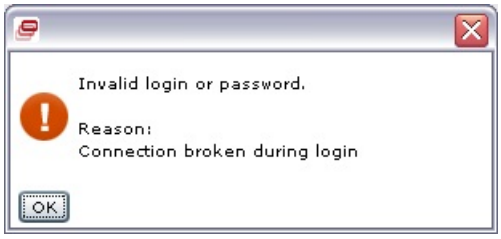
```
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connect failed with host:
nlbaltools and port: 9999
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
```

Possible reasons:

- Wrong hostname
- Wrong port number
- No listener ('rexec' or 'BaanLogin') running on host

Error: Connection broken during login

During login this message is displayed:



Blogind does not support SSL

In the diagnostics test this information is displayed:

```
A connection to the environment could not be established.An exception occurred during the
connection attempt:Connection broken during login
Communication error.
The connection was terminated unexpectedly
com.ssaglobal.erp.server.connection.BaanConnectionException: Connection broken during
login
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:204)
```

```
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection
(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connection broken during
login
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
Caused by: javax.net.ssl.SSLHandshakeException: Remote host closed connection during
handshake
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.readRecord(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 ... 29 more
Caused by: java.io.EOFException: SSL peer shut down incorrectly
 at com.sun.net.ssl.internal.ssl.InputRecord.read(Unknown Source)
 ... 33 more
```

Possible Reasons:

- Old version of BaanLogin daemon
- Blogind not started with –ssl option.

Web UI Truststore issues

In the diagnostics test this information is displayed:

```
A connection to the environment could not be established.An exception occurred during
the connection attempt: Connection broken during login
Communication error.
```

```
The connection was terminated unexpectedly
com.ssaglobal.erp.server.connection.BaanConnectionException: Connection broken during
login
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:204)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection
(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connection broken during
login
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
Caused by: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException:
 PKIX path building failed: sun.security.provider.certpath.SunCertPathBuilderException:
unable to find valid certification path to requested target
 at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.fatal(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.fatalSE(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.fatalSE(Unknown Source)
 at com.sun.net.ssl.internal.ssl.ClientHandshaker.serverCertificate(Unknown Source)
 at com.sun.net.ssl.internal.ssl.ClientHandshaker.processMessage(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.processLoop(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.process_record(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.readRecord(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 ... 29 more
Caused by: sun.security.validator.ValidatorException: PKIX path building failed:
sun.security.provider.certpath.SunCertPathBuilderException: unable to find valid
certification path to requested target
```

```
 at sun.security.validator.PKIXValidator.doBuild(Unknown Source)
 at sun.security.validator.PKIXValidator.engineValidate(Unknown Source)
 at sun.security.validator.Validator.validate(Unknown Source)
 at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.validate(Unknown Source)
 at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.checkServerTrusted(Unknown Source)
 at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.checkServerTrusted(Unknown Source)
 ... 37 more
Caused by: sun.security.provider.certpath.SunCertPathBuilderException: unable to find
valid certification path to requested target
 at sun.security.provider.certpath.SunCertPathBuilder.engineBuild(Unknown Source)
 at java.security.cert.CertPathBuilder.build(Unknown Source)
 ... 43 more
```

Possible Reasons:

- No truststore defined for the java virtual machine running the Web UI server application.
- Wrong password specified for the specified truststore.
- Server certificate not found in the Web UI truststore.

Wrong Web UI Truststore password

In the diagnostics test this information is displayed:

```
Communication error.
The connection was terminated unexpectedly
com.ssaglobal.erp.server.connection.BaanConnectionException: Connection broken during
login
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:204)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection
(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
```

```
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connection broken during
login
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
Caused by: java.net.SocketException: java.security.NoSuchAlgorithmException:
Error constructing implementation (algorithm: Default, provider: SunJSSE, class:
com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl)
 at javax.net.ssl.DefaultSSLSocketFactory.throwException(Unknown Source)
 at javax.net.ssl.DefaultSSLSocketFactory.createSocket(Unknown Source)
 ... 29 more
Caused by: java.security.NoSuchAlgorithmException: Error constructing implementation
(algorithm: Default, provider: SunJSSE, class:
com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl)
 at java.security.Provider$Service.newInstance(Unknown Source)
 at sun.security.jca.GetInstance.getInstance(Unknown Source)
 at sun.security.jca.GetInstance.getInstance(Unknown Source)
 at javax.net.ssl.SSLContext.getInstance(Unknown Source)
 at javax.net.ssl.SSLContext.getDefault(Unknown Source)
 at javax.net.ssl.SSLSocketFactory.getDefault(Unknown Source)
 ... 29 more
Caused by: java.io.IOException: Keystore was tampered with, or password was incorrect
 at sun.security.provider.JavaKeyStore.engineLoad(Unknown Source)
 at sun.security.provider.JavaKeyStore$JKS.engineLoad(Unknown Source)
 at java.security.KeyStore.load(Unknown Source)
 at com.sun.net.ssl.internal.ssl.TrustManagerFactoryImpl.getCacertsKeyStore
(Unknown Source)
 at com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl.getDefaultTrustManager
(Unknown Source)
 at com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl.(Unknown Source)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance(Unknown Source)
 at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(Unknown Source)
 at java.lang.reflect.Constructor.newInstance(Unknown Source)
 at java.lang.Class.newInstance0(Unknown Source)
 at java.lang.Class.newInstance(Unknown Source)
 ... 35 more
Caused by: java.security.UnrecoverableKeyException: Password verification failed
 ... 47 more
```

Possible Reasons:

- Wrong password specified for the specified Web UI truststore.

Cannot open Web UI Truststore file

In the diagnostics test this information is displayed:

```
A connection to the environment could not be established. An exception occurred during
the connection attempt:Connection broken during login
Communication error.
The connection was terminated unexpectedly
com.ssaglobal.erp.server.connection.BaanConnectionException: Connection broken during
login
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:204)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
```

```
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection
(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connection broken during
login
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
Caused by: javax.net.ssl.SSLException: java.lang.RuntimeException: Unexpected error:
java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must be
non-empty
 at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.fatal(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.fatal(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.handleException(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 ... 29 more
Caused by: java.lang.RuntimeException: Unexpected error:
java.security.InvalidAlgorithmParameterException: the trustAnchors parameter must be
non-empty
 at sun.security.validator.PKIXValidator.(Unknown Source)
 at sun.security.validator.Validator.getInstance(Unknown Source)
 at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.getValidator(Unknown Source)
 at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.checkServerTrusted(Unknown Source)
 at com.sun.net.ssl.internal.ssl.X509TrustManagerImpl.checkServerTrusted(Unknown Source)
 at com.sun.net.ssl.internal.ssl.ClientHandshaker.serverCertificate(Unknown Source)
 at com.sun.net.ssl.internal.ssl.ClientHandshaker.processMessage(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.processLoop(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.process_record(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.readRecord(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)
 ... 31 more
Caused by: java.security.InvalidAlgorithmParameterException: the trustAnchors parameter
```

```
must be non-empty
 at java.security.cert.PKIXParameters.setTrustAnchors(Unknown Source)
 at java.security.cert.PKIXParameters.(Unknown Source)
 at java.security.cert.PKIXBuilderParameters.(Unknown Source)
 ... 42 more
```

Possible Reasons:

- Configured Web UI truststore file could not be opened.

Web UI Keystore issues

In the diagnostics test this information is displayed:

```
A connection to the environment could not be established. An exception occurred during
the connection attempt: Connection broken during login
Communication error.
The connection was terminated unexpectedly
com.ssaglobal.erp.server.connection.BaanConnectionException: Connection broken during
login
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:219)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection(Unknown
Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connection broken during
login
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
```

```
Caused by: java.net.SocketException: Software caused connection abort: recv failed
 at java.net.SocketInputStream.socketRead0(Native Method)
 at java.net.SocketInputStream.read(Unknown Source)
 at com.sun.net.ssl.internal.ssl.InputRecord.readFully(Unknown Source)
 at com.sun.net.ssl.internal.ssl.InputRecord.read(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.readRecord(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.waitForClose(Unknown Source)
 at com.sun.net.ssl.internal.ssl.HandshakeOutStream.flush(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.sendChangeCipherSpec(Unknown Source)
 at com.sun.net.ssl.internal.ssl.ClientHandshaker.sendChangeCipherAndFinish(Unknown
Source)
 at com.sun.net.ssl.internal.ssl.ClientHandshaker.serverHelloDone(Unknown Source)
 at com.sun.net.ssl.internal.ssl.ClientHandshaker.processMessage(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.processLoop(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Handshaker.process_record(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.readRecord(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 ... 29 more
```

Possible Reasons:

- No Web UI keystore file defined (missing or wrong javax.net.ssl.keyStore property).
- Web UI keystore file does not contain a key-pair (only certificates)
- Web UI key-pair not in truststore on the LN host.

Web UI Keystore format issue

In the diagnostics test this information is displayed:

```
A connection to the environment could not be established. An exception occurred during
the connection attempt: Connection broken during login
Communication error.
The connection was terminated unexpectedly
com.ssaglobal.erp.server.connection.BaanConnectionException: Connection broken during
login
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:219)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
```

```
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection
(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connection broken during
login
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
Caused by: java.net.SocketException: java.security.NoSuchAlgorithmException: Error
constructing implementation (algorithm: Default, provider: SunJSSE, class:
com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl)
 at javax.net.ssl.DefaultSSLSocketFactory.throwException(Unknown Source)
 at javax.net.ssl.DefaultSSLSocketFactory.createSocket(Unknown Source)
 ... 29 more
Caused by: java.security.NoSuchAlgorithmException: Error constructing implementation
(algorithm: Default, provider: SunJSSE, class:
com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl)
 at java.security.Provider$Service.newInstance(Unknown Source)
 at sun.security.jca.GetInstance.getInstance(Unknown Source)
 at sun.security.jca.GetInstance.getInstance(Unknown Source)
 at javax.net.ssl.SSLContext.getInstance(Unknown Source)
 at javax.net.ssl.SSLContext.getDefault(Unknown Source)
 at javax.net.ssl.SSLSocketFactory.getDefault(Unknown Source)
 ... 29 more
Caused by: java.io.IOException: Invalid keystore format
 at sun.security.provider.JavaKeyStore.engineLoad(Unknown Source)
 at sun.security.provider.JavaKeyStore$JKS.engineLoad(Unknown Source)
 at java.security.KeyStore.load(Unknown Source)
 at com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl.getDefaultKeyManager
(Unknown Source)
 at com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl.(Unknown Source)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance(Unknown Source)
 at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(Unknown Source)
 at java.lang.reflect.Constructor.newInstance(Unknown Source)
 at java.lang.Class.newInstance0(Unknown Source)
 at java.lang.Class.newInstance(Unknown Source)
 ... 35 more
```

Possible Reasons:

- Format of Web UI keystore file not correct (e.g. missing or wrong keystoreType property).

Web UI keystore password

In the diagnostics test this information is displayed:

```
A connection to the environment could not be established.
An exception occurred during the connection attempt:
Connection broken during login
Communication error.
```

```
The connection was terminated unexpectedly
com.ssaglobal.erp.server.connection.BaanConnectionException: Connection broken during
login
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:219)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection
(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connection broken during
login
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
Caused by: java.net.SocketException: java.security.NoSuchAlgorithmException: Error
constructing implementation (algorithm: Default, provider: SunJSSE, class:
com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl)
 at javax.net.ssl.DefaultSSLSocketFactory.throwException(Unknown Source)
 at javax.net.ssl.DefaultSSLSocketFactory.createSocket(Unknown Source)
 ... 29 more
Caused by: java.security.NoSuchAlgorithmException: Error constructing implementation
(algorithm: Default, provider: SunJSSE, class:
com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl)
 at java.security.Provider$Service.newInstance(Unknown Source)
 at sun.security.jca.GetInstance.getInstance(Unknown Source)
 at sun.security.jca.GetInstance.getInstance(Unknown Source)
 at javax.net.ssl.SSLContext.getInstance(Unknown Source)
 at javax.net.ssl.SSLContext.getDefault(Unknown Source)
 at javax.net.ssl.SSLSocketFactory.getDefault(Unknown Source)
 ... 29 more
Caused by: java.security.UnrecoverableKeyException: Get Key failed: / by zero
 at com.sun.net.ssl.internal.pkcs12.PKCS12KeyStore.engineGetKey(Unknown Source)
 at java.security.KeyStore.getKey(Unknown Source)
```

```
 at com.sun.net.ssl.internal.ssl.SunX509KeyManagerImpl.(Unknown Source)
 at com.sun.net.ssl.internal.ssl.KeyManagerFactoryImpl$SunX509.engineInit(Unknown Source)
 at javax.net.ssl.KeyManagerFactory.init(Unknown Source)
 at com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl.getDefaultKeyManager
(Unknown Source)
 at com.sun.net.ssl.internal.ssl.DefaultSSLContextImpl.(Unknown Source)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method)
 at sun.reflect.NativeConstructorAccessorImpl.newInstance(Unknown Source)
 at sun.reflect.DelegatingConstructorAccessorImpl.newInstance(Unknown Source)
 at java.lang.reflect.Constructor.newInstance(Unknown Source)
 at java.lang.Class.newInstance0(Unknown Source)
 at java.lang.Class.newInstance(Unknown Source)
 ... 35 more
Caused by: java.lang.ArithmeticException: / by zero
 at com.sun.crypto.provider.PKCS12PBECipherCore.a(DashoA13*..)
 at com.sun.crypto.provider.PKCS12PBECipherCore.a(DashoA13*..)
 at com.sun.crypto.provider.PKCS12PBECipherCore.a(DashoA13*..)
 at com.sun.crypto.provider.PKCS12PBECipherCore.a(DashoA13*..)
 at com.sun.crypto.provider.PKCS12PBECipherCore$PBEWithSHA1AndDESede.engineInit
(DashoA13*..)
 at javax.crypto.Cipher.a(DashoA13*..)
 at javax.crypto.Cipher.a(DashoA13*..)
 at javax.crypto.Cipher.init(DashoA13*..)
 at javax.crypto.Cipher.init(DashoA13*..)
 ... 48 more
```

Possible Reasons:

- Password for opening the Web UI keystore file not defined or not correct (property javax.net.ssl.keyStorePassword).

Web UI wrong keypair type

In the diagnostics test this information is displayed:

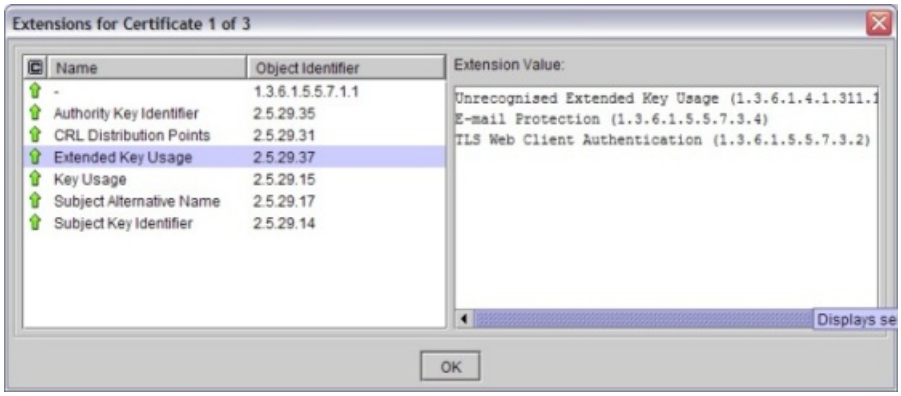
```
A connection to the environment could not be established. An exception occurred during
the connection attempt: Connection broken during login
Communication error.
The connection was terminated unexpectedly
com.ssaglobal.erp.server.connection.BaanConnectionException: Connection broken during
login
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:213)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
```

```
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection
(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Connection broken during
login
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
Caused by: javax.net.ssl.SSLHandshakeException: Received fatal alert:
unsupported_certificate
 at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Unknown Source)
 at com.sun.net.ssl.internal.ssl.Alerts.getSSLException(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.recvAlert(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.readRecord(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.performInitialHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 at com.sun.net.ssl.internal.ssl.SSLSocketImpl.startHandshake(Unknown Source)
 ... 29 more
```

Possible Reasons:

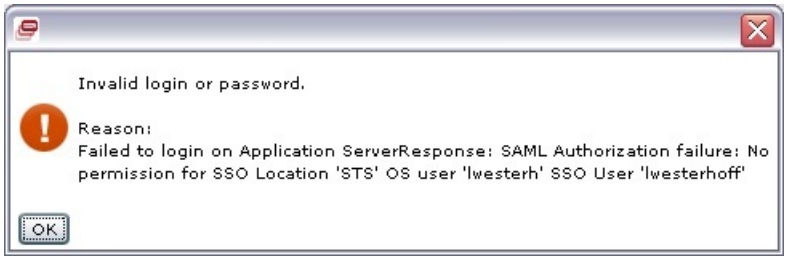
- Key-pair in Web UI keystore file is a WebServer key-pair and not a client key-pair.

A suitable client key-pair must have an Extended Key Usage property with value: “TLS Web Client Authentication”.



No permission for SSO

During login this message is displayed:



In the diagnostics test this information is displayed:

```
A connection to the environment could not be established. An exception occurred during the
connection attempt: Failed to login on Application Server
Response: SAML Authorization failure: No permission for SSO Location 'STS' OS user
'lwesterh' SSO User 'lwesterhoff'
Login error. Possible causes:
1) Wrong Username
2) No mapping for Username in sso_permissions.xml file on ERPLN server
3) Username is linked to non existing OS user on ERPLN server
com.ssaglobal.erp.server.connection.BaanConnectionException: Failed to login on Application
Server
Response: SAML Authorization failure: No permission for SSO Location 'STS' OS user
'lwesterh' SSO User 'lwesterhoff'
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:215)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Failed to login on
Application Server
Response: SAML Authorization failure: No permission for SSO Location 'STS' OS user
```

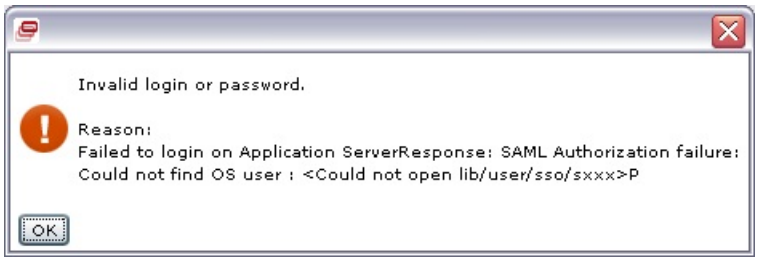
```
'lwesterh' SSO User 'lwesterhoff'
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
```

Possible Reasons:

- No mapping for Username in sso_permissions.xml file on ERPLN server

Could not find OS user

During login this message is displayed:



In the diagnostics test this information is displayed:

```
A connection to the environment could not be established.
An exception occurred during the connection attempt:
Failed to login on Application Server
Response: SAML Authorization failure: Could not find OS user : <Could not open
lib/user/sso/sxxx>
Login error. Possible causes:
1) Wrong Username
2) No mapping for Username in sso_permissions.xml file on ERPLN server
3) Username is linked to non existing OS user on ERPLN server
com.ssaglobal.erp.server.connection.BaanConnectionException: Failed to login on
Application Server
Response: SAML Authorization failure: Could not find OS user: P
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:216)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
```

```
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Failed to login on
Application Server
Response: SAML Authorization failure: Could not find OS user: P
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
```

Possible Reasons:

- SSO Username not defined in LN Userdata session.
- No convert to runtime for Userdata done on the LN server.

Could not impersonate user

During login this message is displayed:

In the diagnostics test this information is displayed:

```
A connection to the environment could not be established. An exception occurred during the
connection attempt:
Failed to login on Application Server
Response: Could not impersonate user
Login error. Possible causes:
1) Wrong Username
2) No mapping for Username in sso_permissions.xml file on ERPLN server
3) Username is linked to non existing OS user on ERPLN server
com.ssaglobal.erp.server.connection.BaanConnectionException: Failed to login on Application
Server
Response: Could not impersonate user
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:133)
 at com.ssaglobal.erp.servlet.DiagnosticBaanEnvironment.showTestConnection
(DiagnosticBaanEnvironment.java:216)
 at com.ssaglobal.erp.servlet.Diagnostic.showTestConnection(Diagnostic.java:219)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoGet(DiagnosticsServlet.java:172)
 at com.ssaglobal.erp.servlet.DiagnosticsServlet.handleDoPost(DiagnosticsServlet.java:102)
```

```
 at com.ssaglobal.webtop.servlet.WebTopServlet.handleRequest(WebTopServlet.java:202)
 at com.ssaglobal.webtop.servlet.WebTopServlet.doPost(WebTopServlet.java:108)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:709)
 at javax.servlet.http.HttpServlet.service(HttpServlet.java:802)
 at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter
(ApplicationFilterChain.java:252)
 at org.apache.catalina.core.ApplicationFilterChain.doFilter
(ApplicationFilterChain.java:173)
 at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:213)
 at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:178)
 at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:126)
 at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:105)
 at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:107)
 at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:148)
 at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:869)
 at org.apache.coyote.http11.Http11BaseProtocol$Http11ConnectionHandler.processConnection
(Http11BaseProtocol.java:664)
 at org.apache.tomcat.util.net.PoolTcpEndpoint.processSocket(PoolTcpEndpoint.java:527)
 at org.apache.tomcat.util.net.LeaderFollowerWorkerThread.runIt
(LeaderFollowerWorkerThread.java:80)
 at org.apache.tomcat.util.threads.ThreadPool$ControlRunnable.run(ThreadPool.java:684)
 at java.lang.Thread.run(Unknown Source)
Caused by: createManagedConnection failed
 at com.infor.erpln.jca.ManagedConnectionFactoryImpl.createManagedConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionManagerImpl.allocateConnection(Unknown Source)
 at com.infor.erpln.jca.ConnectionFactoryImpl.getConnection(Unknown Source)
 at com.ssaglobal.erp.server.connection.JcaConnection.connect(JcaConnection.java:122)
 ... 22 more
Caused by: com.infor.erpln.protocol.BaanConnectionException: Failed to login on Application
Server
Response: Could not impersonate user
 at com.infor.erpln.protocol.DsSessionLayer.baanLoginSSL(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connectSetup(Unknown Source)
 at com.infor.erpln.protocol.DsSessionLayer.connect(Unknown Source)
 ... 26 more
```

Possible Reasons:

- The OS user which is linked to this SSO user cannot be impersonated because it is no valid OS user on the LN system.
- The OS user which is linked to this SSO user cannot be impersonated because it has not home directory on this LN system.

AD FS login failed

When using the AD FS Web UI login (../webtop/servlet/fslogin) this error message dislays:

Error

NLBAVWMARSTS.mar.com

There was a problem accessing the site. Try to browse to the site again.

If the problem persists, contact the administrator of this site and provide the reference number to identify the problem.

Reference number: b6498b2a-8c1f-46e3-a7de-45db162597bc

The event log on the AD FS system contains this entry:

```
The Federation Service encountered an error while processing the SAML authentication request.

Additional Data
Exception details:
Microsoft.IdentityServer.Service.Policy.PolicyServer.Engine.ScopeNotFoundPolicyRequestException: MSIS3020: The relying party trust with identifier 'fedlet_wriphage' could not be located.
  at Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ValidateSignatureRequirements(SamlMessage samlMessage)
  at Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.Issue(IssueRequest issueRequest)
  at Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ProcessRequest(Message requestMessage)
```

Possible Reasons:

- Web UI metadata (Service Provider) not imported into AD FS.

Importing sp.xml in AD FS fails

After importing the sp.xml file into AD FS, the EndPoints tab of the relying party is empty.

Possible Reasons:

- The Web UI url in the sp.xml file does not start with https:// but with http://

Single Sign On failed

While opening the AD FS Web UI login URL this error message displays:

Single Sign On failed.

SAML Response status:

urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy

SAML2 response XML:


```
<samlp:Response Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"
Destination="https://nlbanwriphage1.infor.com:8443/webtop/servlet/faassologin" ID="_69f9a5e4-b1c4-42b3-
InResponseTo="s2349c59f06ea86dea45a3fe48bbfe15a9973ee384" IssueInstant="2010-09-21T07:49:37.636Z" Versi
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"><Issuer
xmlns="urn:oasis:names:tc:SAML:2.0:assertion">http://NLBAVWMARSTS.mar.com/adfs/services/trust</Issuer><
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/><ds:SignatureMethod Algorithm="http://www.w3.org/2
sha256"/><ds:Reference URI="#_69f9a5e4-b1c4-42b3-b464-1f77be725a6a"><ds:Transforms><ds:Transform
```


Possible Reasons:

- No claim rules added at the AD FS side.
- First or second claim rule missing or wrong.

See Event log of AD FS on the system where AD FS runs for more details.

No identity passed

While opening the AD FS Web UI login URL the following error message displays:

No Claim attributes in returnd SAML2 response

SAML2 response XML:


```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" ID="_fa5e961e-62b4-4147-8471-f21772f34dd3"
InResponseTo="a24ad8d083e13f21cda46f30f080e92f7243f090e2" Version="2.0" IssueInstant="2010-09-21T11:39:04Z"
Destination="https://nlbanwriphage1.infor.com:8443/webtop/servlet/faassologin"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://NLBAVWMARSTS.mar.com/adfs/services/trust</saml:Issuer><samlp:Status
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">
<samlp:StatusCode  xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
Value="urn:oasis:names:tc:SAML:2.0:status:Success">
```


Or

Missing required Claim attribute: 'http://schemas.infor.com/claims/Identity' in SAML2 response

SAML2 response XML:


```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
ID="_939a6c12-6407-4d45-8564-7d55458ebd56"
InResponseTo="s2a6d17a7e702d8e295d4880ffa077a20e2a7a412b" Version="2.0"
IssueInstant="2010-09-21T11:56:32Z"
Destination="https://nlbanwriphage1.infor.com:8443/webtop/servlet/faassologin"
Consent="urn:oasis:names:tc:SAML:2.0:consent:unspecified"><saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://NLBAVWMARSTS.mar.com/
adfs/services/trust</saml:Issuer><samlp:Status
```


Possible Reasons:

- Third claim rule (http://schemas.infor.com/claims/Identity) missing or wrong formatted.

Trouble shooting Single Sign Out

The Web UI supports a “Sign Off “command (top right button in the framework). Running this command can cause errors.

Logout request not signed

After the sign out command is given from the Web UI, this error page displays:

Error

NLBAVWMARSTS.mar.com

There was a problem accessing the site. Try to browse to the site again.

If the problem persists, contact the administrator of this site and provide the reference number to identify the problem.

Reference number: 955bb810-e00c-4810-bdca-de3e4b88617f

The event viewer on the AD FS server contains the following event:

```
The verification of the SAML message signature failed.

Message issuer: fedlet_wriphage

Exception details:

MSIS1014: SAML LogoutRequest and LogoutResponse messages must be signed when using SAML
HTTP Redirect or HTTP POST binding.
```

Possible reasons:

- idp-extended.xml does not contain: "wantLogoutReqeustSigned" attribute

The event viewer on the AD FS server contains the following event:

```
The Federation Service encountered an error while processing the SAML authentication
request.

Additional Data

Exception details:
Microsoft.IdentityModel.Protocols.XmlSignature.SignatureVerificationFailedException:
MSIS0037: No signature verification
certificate found for issuer 'fedlet_wriphage'.

   at
Microsoft.IdentityServer.Protocols.Saml.Contract.SamlContractUtility.CreateSamlMessage
(MSISSamlBindingMessage message)

   at
Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.Logout(LogoutRequest
logoutRequest)

   at
Microsoft.IdentityServer.Service.SamlProtocol.SamlProtocolService.ProcessRequest(Message
requestMessage)
```

Possible reasons:

- The Signature used by the Web UI for signing the logout request was not added to trusted party in AD FS

The event viewer on the AD FS server contains the following event:

```
SAML request is not signed with expected signature algorithm. SAML request is signed with
 signature algorithm
http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 . Expected signature algorithm is
http://www.w3.org/2000/09/xmldsig#rsa-sha1

User Action:

Verify that signature algorithm for the partner is configured as expected.
```

Possible reasons:

- Secure hash algorithm for relying trust party not set to SHA-1 in AD FS.

Failed to create logout request

After the sign out command is given from the Web UI, this error page displays:

HTTP Status 400 - Error creating LogoutRequest. Error redirecting the LogoutRequest.

type Status report

message Error creating LogoutRequest. Error redirecting the LogoutRequest.

description The request sent by the client was syntactically incorrect (Error creating LogoutRequest. Error redirecting the LogoutRequest.).

Apache Tomcat/5.5.30

The file libSAML which can be found in directory: debug on the fedlet configuration directory, contains the following lines:

```
libSAML:10/14/2010 01:29:43:123 PM CEST: Thread[http-8443-Processor25,5,main]

ERROR: mapPk2Cert.JKSKeyProvider:

java.io.FileNotFoundException: C:\Data\webuiconfig\fedlet\conf\keystore.jks (The system
cannot find the file specified)
```

Possible reasons:

- Keystore not configured correctly in the FederationConfig.properties

When the libSAML file contains the following lines:

```
libSAML:10/14/2010 01:39:16:047 PM CEST: Thread[http-8443-Processor25,5,main]

ERROR: mapPk2Cert.JKSKeyProvider:

java.io.IOException: Keystore was tampered with, or password was incorrect

 at sun.security.provider.JavaKeyStore.engineLoad(Unknown Source)
```

Possible reasons:

- The password in the .storepass file in the Fedlet conf directory does not contain a password which matches with the password for the related keystore file.

The file libSAML2 which can also be found in directory: debug on the fedlet configuration directory, contains these lines:

```
ERROR: Incorrect configuration for Signing Certificate.

libSAML2:10/14/2010 01:46:46:996 PM CEST: Thread[http-8443-Processor24,5,main]

ERROR: Exception :

com.sun.identity.saml2.common.SAML2Exception: Error retrieving meta data.

 at
com.sun.identity.saml2.common.SAML2Utils.signQueryString(Unknown Source)

 at
com.sun.identity.saml2.profile.LogoutUtil.doSLOByHttpRedirect(Unknown Source)
```

```
 at
com.sun.identity.saml2.profile.LogoutUtil.doLogout(Unknown Source)
```

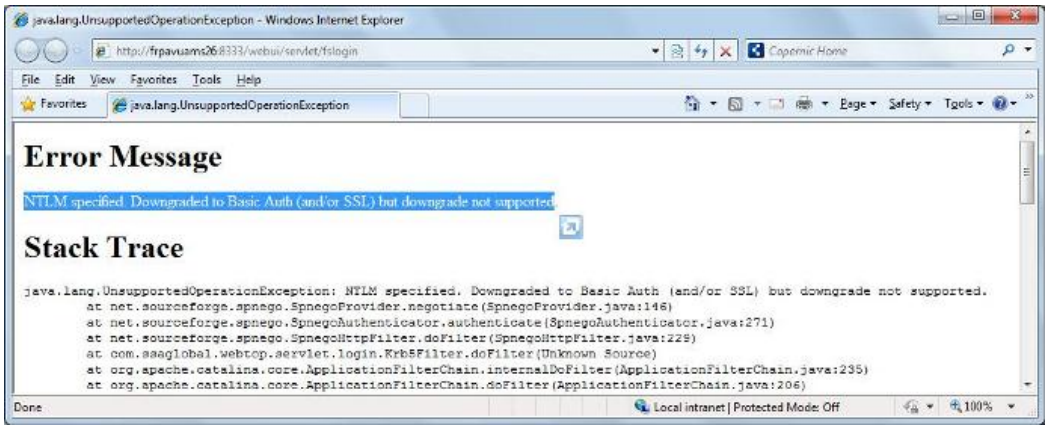
Possible reasons:

- The configuration file: sp-extended.xml does not contain correct value for: signingCertAlias attribute. This must be the alias of the key-pair in the keystore file which is used for signing the logout request.

Error pages

Symptom: Error Page “GSSException: Defective token detected”

This error page can display when accessing the Web UI:

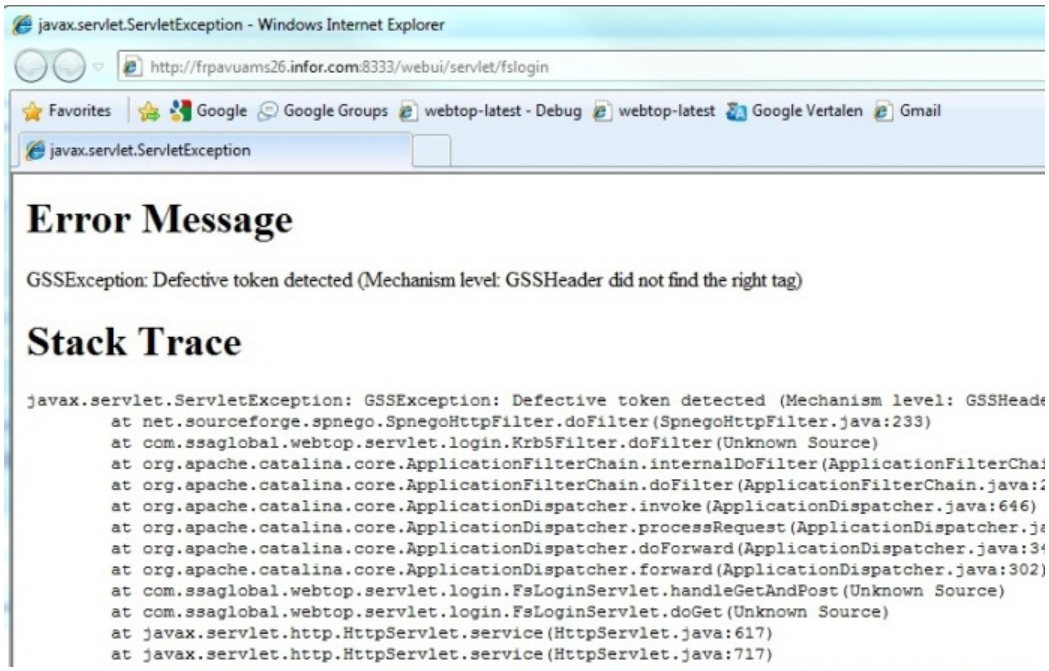


Cause: the domain name is missing from the URL

Solution: to access the Web UI use the URL: `http[s]://[hostname].[domainname]:[port]/webui/servlet/fslogin`

Symptom: Error Page “GSSException: Defective token detected

This error page can display when accessing the Web UI:

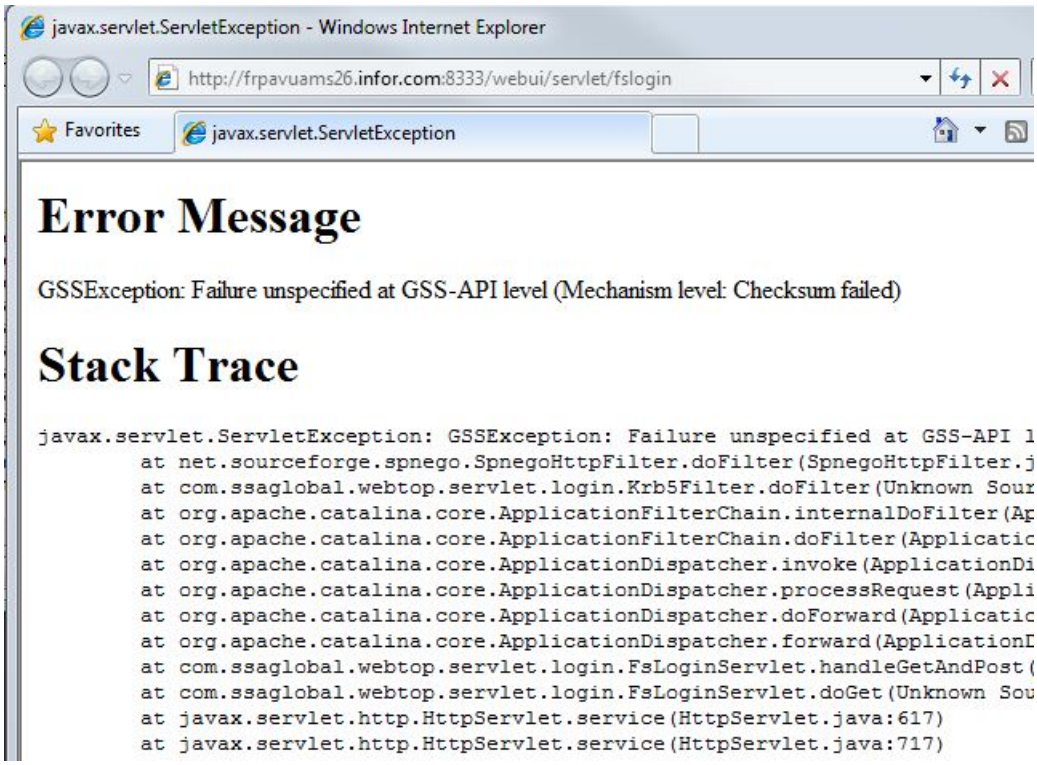


Cause: the pre-authentication account (used for the configuration of Integrated Windows Authentication) is not correct configured in Active Directory

Solution: On the Domain Controller's Active Directory Users and Computers dialog the account option "Use Kerberos DES encryption types for this account" of the pre-authorization account must be cleared.

Symptom: Error Page "GSSException: Failure unspecified (…)"

This error page can display when accessing the Web UI:

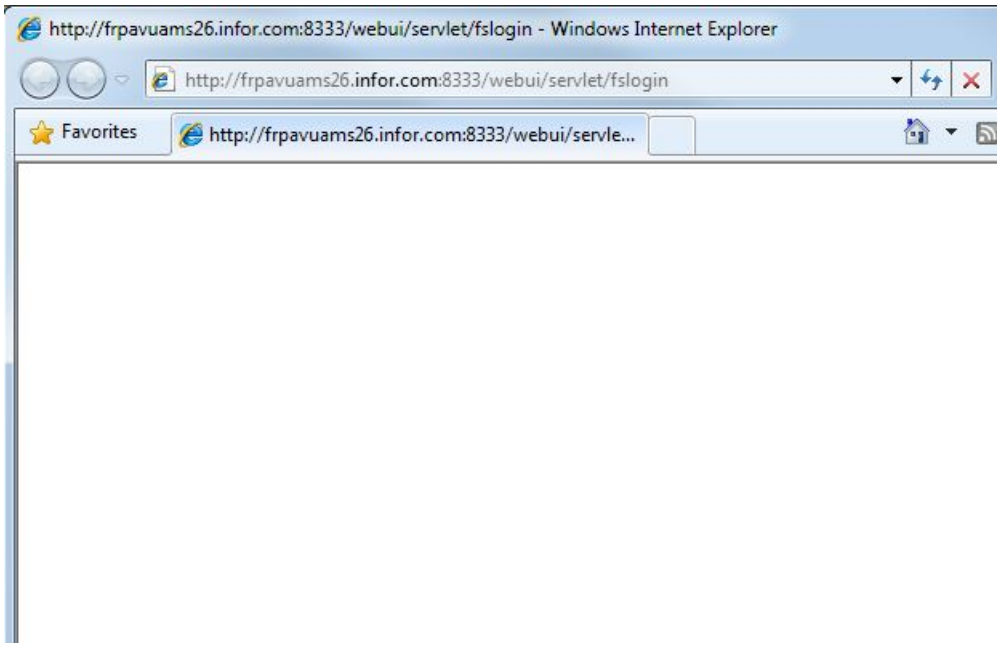


Cause: the Domain Account Password (configured for Integrated Windows Authentication) is incorrect.

Solution: In the Integrated Windows Authentication Configuration, specify the correct password and restart the Web UI server.

Symptom: Blank Page

A blank can display when accessing the Web UI:



Cause: The Web UI is configured for Integrated Windows Authentication but not enabled in the browser.

Solution for Internet Explorer:

- Click menu item Tools -> Internet Options -> Advanced -> Security
- Select the option "Enable Integrated Windows Authentication.

Solution for Mozilla Firefox:

- Specify ‘about:config’, locate Preference Name ‘network.negotiate-auth.trusted-uris’.
- Specify the domain name of the Web UI server.

Index

Advanced, 21
Federation Services
    configuring, 25
IFS, 25
introduction, 9
IWA, 31**,** 32
overview, 13
Single Sign In
    error, 37
    problem, 37
    trouble shooting, 37
Single Sign Out
    error, 56
    problem, 56
    trouble shooting, 56
SSO, 25**,** 32
UNIX, 18
Windows, 14