



Infor LN UI Administration Guide

Copyright © 2016 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.

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

Release: Infor LN 10.5

Publication Date: September 8, 2016

Document code: uilnuiag (U9790)

Contents

About this guide.....	7
Contacting Infor.....	7
Chapter 1: Prerequisites.....	9
Compatibility information.....	9
Software requirements.....	9
Supported browser clients.....	10
Hardware requirements and recommendations.....	11
Chapter 2: Overview.....	13
Access.....	13
Overview of administration menus.....	14
Reading instructions.....	16
Chapter 3: Creating an environment for LN connection (Single Sign On).....	17
Chapter 4: Configuring the Tomcat web server.....	19
Security.....	19
Configuring Tomcat HTTPS connector.....	19
Installing or renewing a CA-signed HTTPS certificate.....	20
Configuring a PKCS#12 HTTPS keystore.....	21
Chapter 5: Configuring IFS (Platform Xi version).....	23
Binding LN UI to IFS.....	23
Obtaining a powershell script.....	24
Creating a relying party trust.....	24
Testing SSO.....	24
Chapter 6: Creating a Logical ID mapping.....	25
Chapter 7: Integrating Infor Ming.le - LN application (Platform Xi version).....	27
Configuring the LN application.....	27
Configuring the Documentation utility app.....	28
Configuring the LN Navigator utility app.....	29
Configuring the LN file attachments context app (ODM).....	29
Chapter 8: Installing online help packages.....	31

Chapter 9: Workbenches.....	33
Chapter 10: LN Client Service.....	35
Configuring the LN Client Service.....	35
Enabling the AD FS artifact resolution service.....	35
Importing the AD FS HTTPS certificate.....	35
Enabling or disabling the LN Client Service.....	36
Testing the LN Client Service.....	36
Chapter 11: Configuring stand-alone-mode.....	37
Configuring LN UI for Integrated Windows Authentication.....	37
Configuring LN UI for Backend Authentication.....	38
Creating an environment for LN connection (LN Server Authentication).....	38
Configuring in-context applications.....	38
Starting LN UI with a bookmarked session.....	39
Starting LN UI with a DEM process.....	40
Chapter 12: Exchange Synchronizer.....	41
Prerequisites.....	41
Administration of Exchange Synchronizer.....	41
Configuring Microsoft Exchange.....	42
Prerequisites.....	42
Impersonation.....	42
Enabling the impersonation (Exchange Server 2010 and higher).....	43
Configuring the Exchange Synchronizer in LN.....	43
Configuring LN UI.....	44
Troubleshooting.....	44
Chapter 13: Clickjacking prevention.....	49
Enabling the clickjacking prevention.....	49
Disabling the clickjacking prevention.....	50
Detailed information.....	50
Chapter 14: Other web servers.....	51
Deployment on JBoss.....	51
Configuring the HTTPS port using the JBoss Management console.....	51
Finalizing the configuration of the HTTPS port.....	52
Deployment on WebSphere AS v8.5.5.....	53
Deploying LN UI for the first time.....	54
Deploying LN UI in an existing environment.....	54
Deployment on WebLogic 12c v12.1.x.....	55

Prerequisites.....	55
Preparing the deployment.....	55
Deploying LN UI.....	57
Chapter 15: Configuring IFS (version 11).....	59
Chapter 16: Integrating Infor Ming.le (version 11) and LN.....	61
Configuring the Infor Ming.le-LN Plug-in.....	61
Configuring the Documentation context application.....	62
Adjusting Infor Ming.le's browser compatibility mode.....	63
Configuring LN application and user properties in Infor Federation Services.....	63
Infor Ming.le and ODM.....	64
Chapter 17: Advanced topics.....	67
Post-installation instructions after an upgrade from Web UI.....	67
Troubleshooting.....	68
Appendix A: Configuring SSO in LN.....	69
Overview.....	69
SSO related procedures.....	70
Configuring SSO in LN (Windows).....	70
Update session SSO Parameters (ttams0100m000).....	70
Update session User Data (ttaad2500m000).....	71
Create/update permissions file.....	71
Restart ES Logic Service.....	72
Configuring SSO in LN (non Windows).....	73
Update session SSO Parameters (ttams0100m000).....	73
Update session User Data (ttaad2500m000).....	74
Create/update permissions file.....	74
Activate changes.....	75
Advanced topics.....	76
Non-Windows: Using a generic system user.....	76
Non-Windows: Case-insensitive permission check of SSO user.....	76
Non-Windows: Permission check when System Login and SSO User are different.....	77
Windows: Dedicated SSO permission check.....	77
Non-Windows: Dedicated SSO permission check.....	78

About this guide

Infor LN UI is the HTML5 compliant browser-based user interface for Infor LN. LN UI consists of these components:

- A Web application that facilitates access to LN applications. This is the main component of LN UI.
- A Web application dedicated to the administration of the LN UI deployment.

This document describes the LN UI Administration Webapp.

Intended audience

This document is intended for administrators responsible for the installation and configuration of LN UI.

Contacting Infor

If you have questions about Infor products, go to the Infor Xtreme Support portal.

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

If you have comments about Infor documentation, contact documentation@infor.com.

Compatibility information

For detailed information on the compatibility of LN UI with LN Tools and application versions, see Infor Xtreme KB 1460896 or 1834377.

Software requirements

This table shows the server requirements for successful installation and operation of LN UI:

Product	Supported Version
Operating System	Microsoft Windows Server 2008 R2 Standard or Enterprise 64 bit
	Microsoft Windows Server 2012 R2 Standard and higher
	Linux
	See note 1.
Java Runtime Environment	Java 8
	See note 2. The Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files are also required. Download the files from http://www.oracle.com/technetwork/java/javase/downloads/index.html . For installation instructions, see the README.txt file. After installation, restart the Tomcat web server if it is already running.
Web Server	Tomcat 7.0.x
	Tomcat 8.0.x
	JBoss EAP 6.2.x in combination with Java SE 7
	JBoss EAP 6.3.x in combination with Java SE 7 or 8
	WebSphere AS v8.5.5
	See note 3.

Product	Supported Version
	For installation instructions, see "Deployment on WebSphere AS v8.5.5" on page 53.
	WebLogic 12c 12.1.x
	See note 3.
	For installation instructions, see "Deployment on WebLogic 12c v12.1.x" on page 55.

Note:

- 1 Single Sign On using Integrated Windows Authentication is only supported for Windows-based UI servers.
- 2 This version of LN UI is also compatible with Java 7.
- 3 You can install LN UI on an IBM WebSphere or Oracle WebLogic application server. In that case, Single Sign On using Infor Federation Services must be configured through a command line tool that is bundled with the Enterprise Server Installer.

Supported browser clients

This table shows the browsers that are supported by LN UI:

Client	Supported browsers
Windows clients	Microsoft Internet Explorer 11 in Desktop style
	Microsoft Internet Explorer 11 in Metro style, but with limitations
	Microsoft Edge
	Chrome - latest version
	Firefox - latest version
Mac OS clients	Safari browser - latest version
	Chrome - latest version

Note:

- LN UI does not support Silverlight-based Workbench sessions when using Chrome or the Safari browser.
- Users who are running several homepages with multiple LN UI sessions may run into memory issues when using the 32 bit version of the Internet Explorer browser. We recommend to use the 64 bit version instead.

Hardware requirements and recommendations

For the minimal client requirements for LN UI, see "Client requirements" in the *Infor LN UI 11.x Sizing Guide*. To access this guide, navigate to <https://salesportal.infor.com/pages/default.aspx> and select **Operations > Sizing**.

Access

After installation and configuration, LN UI can be accessed through various URLs. The URLs are described below. The hostname, the fully qualified domain name, and the HTTPS port number of the URLs are just an example and must be adjusted according to the specific installation.

For all URLs, it is assumed that secure HTTP communication (HTTPS) with the browser is used.



Caution: LN UI may also be used with standard (unsecured) HTTP communications. If HTTP is used, the business data and user credentials, such as passwords, are exchanged unsecured with the browser. It is the customer's responsibility to ensure the desired level of information security.

URL to access LN UI from the Infor Ming.le-LN Plug-in

The Infor Ming.le-LN Plug-in must be configured with the following URL to access LN UI. LN UI must be configured with Single Sign On using Infor Federation Services or Integrated Windows Authentication.

In addition, if LN UI is configured to use LN server authentication, you may use this URL to start LN UI using a valid LN username and password.

`https://server1.initrode.com:8443/webui/servlet/fslogin`

You may use this URL to create an extended URL, allowing the LN UI to start in a specific session and record.

For details, see "Starting LN UI with a bookmarked session" on page 39.

URLs to access the LN UI in stand-alone mode

The stand-alone mode of LN UI offers a landing page with favorites, bookmarks, and a list of recently used sessions. These URLs are available:

- This URL shows the LN environments available in stand-alone mode:
`https://server1.initrode.com:8443/webui/servlet/environments`
- This URL shows the user profiles available in stand-alone mode for the default LN environment:
`https://server1.initrode.com:8443/webui/servlet/profiles`

- This URL shows the LN UI landing page for the default LN environment and user profile:
`https://server1.initrode.com:8443/webui/servlet/standalone`

URLs to access the LN UI user settings Webapp

This URL provides direct access to the LN UI user settings Webapp:

`https://server1.initrode.com:8443/webui/servlet/settings`

Users can also open this Webapp by selecting **Options > Settings** in the top-level menu in LN UI.

This URL is useful if, for some reason, a user cannot start the LN UI with the current default user settings.

URLs to access the LN UI Administration Webapp

These URLs provide access to the LN UI Administration Webapp:

- `http://server1.initrode.com:8080/webui/servlet/admin`
- `https://server1.initrode.com:8443/webui/servlet/admin`

HTTP access is required after first installation, if LN UI has not been configured to use HTTPS. In all other cases, we recommend that you use secure (HTTPS) communications.

When prompted, specify **Administrator** as the user name. Use the password as set with the installer. If LN UI is installed manually for the first time, the password is **webui**. We strongly recommend that you change this initial password.

URL for LN Client Service access to LN

This URL provides access to LN for clients using the LN Client Service:

`https://server1.initrode.com:8443/webui`

Overview of administration menus

The various capabilities of the LN UI Administration Webapp are organized in different menus which are described below. For each menu item, online help with detailed instructions is available.

Infor LN UI Administration menu

This table shows the options in the **Infor LN UI Administration** menu:

Option	Description
Change Admin Password	Change the password of the LN UI Administration Webapp.
Login Configuration	Change the authentication type and other settings that control the access to the LN UI application.

Option	Description
HTTPS Keystore	Generate a keystore containing a public / private key pair and an SSL certificate. This keystore is used for secure communications in the browser client.
HTTPS Configuration	Create or change the web server settings for secure communications in the browser client.
User Profile Permissions	Enable or disable the capability to change the user profile for all users, or for selected users.
User Profile Management	Delete user profiles for selected users.
Logging	Change the settings of server side logging.
Diagnostics	View various properties concerning the web server, the Java Runtime Engine it uses, and the LN UI build information.
Active Users	Show a list of active LN UI users.
Import Web UI Configuration	Import Web UI configuration settings, if LN UI was installed as an upgrade from Web UI.
Clickjacking Prevention	Enable or disable the defense to 'clickjacking' security attacks.
IFS Attribute/Provisioning Service	Determine how LN UI supports the communication for centralized user management between LN and Infor Federation Services (IFS).

Infor LN menu

This table shows the options in the **Infor LN** menu:

Option	Description
LN Environments	Manage the details of the connection with the LN system.
Logical ID Mapping	Manage the mapping from a Logical ID to an LN environment.
BaanLogin SSL Keystore	Show an overview of the contents of the BaanLogin SSL keystore. This keystore is used for secure communications between the UI server and the Enterprise Server.
SSL Truststore	Manage the SSL certificates required by the LN UI to communicate with HTTPS hosts.
Workbench Deployer	Manage the configuration of the Workbench Web Server.
Synchronizer Manager	Manage the Synchronizer for CRM Contacts and Calendar events.
LN Client Service	Turn the LN Client Service on or off.

Infor LN Help menu

This table shows the options in the **Infor LN Help** menu:

Option	Description
Help Content	Upload and manage online help content.
Help Language Fallbacks	Manage language fallbacks for online help.
Help Version Fallbacks	Manage version fallbacks for online help.

Options menu

This table shows the options in the **Options** menu:

Option	Description
Activate trace mode	Start the client side log.
About	Show essential deployment information.

Reading instructions

The chapter ordering of this manual assumes a default LN UI deployment with these characteristics:

- A new LN UI installation
- Access to one LN server through Single Sign On
- A Tomcat web server
- Use of an HTTPS connector
- Authentication based on Single Sign On using Infor Federation Services Xi version
- LN UI used with Infor Ming.le Xi version 12 or higher

If your LN deployment deviates from this default deployment, use the following guidelines to determine the reading order:

- If you do not need to use LN UI with Infor Ming.le, skip these chapters:
 - Creating a Logical ID mapping
 - Integrating Infor Ming.le - LN application (Platform Xi version)
 - Integrating Infor Ming.le (version 11) and LN
- If you also do not need Single Sign On, skip these chapters:
 - Creating an environment for LN connection (Single Sign On)
 - Configuring IFS (Platform Xi version)
 - Configuring IFS (version 11)
- If you also do not need HTTPS, skip the Configuring the Tomcat web server chapter.
- If you have another web server than Tomcat, read the appropriate section from the Other web servers chapter instead of the Configuring the Tomcat web server chapter.

Creating an environment for LN connection (Single Sign On)

3

Use this task to configure an environment that allows to connect to the LN system for Single Sign On usage.

Note:

- This step requires that the Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files are installed on the LN UI server. See "Software requirements" on page 9.
- This step requires an LN user to generate the BaanLogin SSL keystores. The LN user must have modify and write access to the `BSE` folder of the ES Logic Service and its `security` subfolder. The BaanLogin SSL keystores are not related to the HTTPS keystore that is discussed in the next chapter.
- This step requires that the LN system is prepared for SSO. See "Configuring SSO in LN" on page 69.

Complete these steps:

- 1 Start the LN UI Administration Webapp and select **Infor LN > LN Environments**.
- 2 Click **New** to create an environment for the desired LN system.
- 3 On the **General** tab, specify the required details and select **BaanLogin SSL** as the desired protocol.
- 4 On the **BaanLogin SSL** tab, specify the required username, password, and BSE folder path of the ES Login Service (BaanLogin daemon path). Save the changes.
- 5 Click **Generate/Update** to generate the BaanLogin SSL keystores.
- 6 On the LN system, restart the ES Logic Service. Restarting the web server is not required.
- 7 To verify that the configuration was completed successfully, open the **Test** tab and specify a valid domain username. Then click **Test**.

Security

A keystore is required for secure HTTP communication (HTTPS) with the browser.

Note: This keystore is unrelated to the BaanLogin SSL keystores that are discussed in the previous chapter.

If LN UI is installed on the Tomcat web server, you can use the LN UI Administration Webapp to create and update this keystore. These are the supported public/private key pair characteristics:

- Signature algorithm: SHA256withRSA
- Key algorithm and length: RSA, 2048 bits

If the keystore must meet different demands, you can use, for example, these utility programs to manually create or update the keystore:

- Keytool, bundled with Oracle Java SE
- Portecle from <http://portecle.sourceforge.net/>

Note: If the keystore is created or updated using external programs, the LN UI Administration Webapp maybe cannot show the keystore's contents, or support keystore operations!

Configuring Tomcat HTTPS connector

Complete the following steps to configure the web server's usage of the HTTPS port. As an example, 8443 is assumed as the designated HTTPS port value.

- 1 Start the LN UI Administration Webapp.
- 2 Select **Infor LN UI Administration > HTTPS Keystore**.
- 3 Specify the desired values for fields such as **Organizational Unit** and **Organization**, which will be used for the self-signed certificate.
- 4 Click **Keystore - Generate/Update** to create the HTTPS keystore with a self-signed certificate.
- 5 Select **Infor LN UI Administration > Login Configuration**. In the **HTTPS Port** field, specify the designated value, for example **8443**. Save the changes. Do not restart the web server now.
- 6 Select **Infor LN UI Administration > HTTPS Configuration**.

- 7 Click **HTTPS Connector - Generate/Update** to update the Tomcat configuration with the selected HTTPS port value and the HTTPS keystore. Restart the web server now.
- 8 To verify that HTTPS configuration was completed successfully, browse to a URL similar to `https://server1.initrode.com:8443/webui/servlet/admin`
- 9 Use the padlock of the browser's address bar to inspect the certificate information and verify that a self-signed certificate is displayed.

Installing or renewing a CA-signed HTTPS certificate

Use this task to replace the self-signed certificate of the HTTPS keystore with a CA-signed certificate, or to update the existing CA-signed certificate.

- 1 Start the LN UI Administration Webapp and select **Infor LN UI Administration > HTTPS Keystore**.
- 2 Click **Certificate Signing Request - Generate & Download** to create and download a file with the Certificate Signing Request (CSR). The request is encoded in Base-64 according to the PKCS#10 standard; you can view it in a text editor, for example to transfer it to a clipboard.
- 3 Use the CSR contents to obtain a certificate from a Certificate Authority.
- 4 If the CA-signed certificate is supplied as a CA Reply with the complete certificate chain, click **CA Reply - Upload & Import** to upload and import the CA Reply file. If the import is successful, the HTTPS keystore is updated with the CA-signed certificate. The file with the CA Reply must be in Base-64 encoded PKCS #7 format (.p7b).
- 5 If the root certificate, any intermediate certificate, and the CA signed end certificate are supplied separately, click **CA Trusted Certificate - Upload & Import** to upload and import the root certificate. Repeat this step for each intermediate certificate. The uploaded certificate file(s) must be in Base-64 encoded X.509 format (.cer).
Finally, click **CA Reply - Upload & Import** to upload and import the end certificate. If the import is successful, the HTTPS keystore is updated with the certificate. The file with the CA Reply must be in Base-64 encoded X.509 format (.cer).
- 6 Restart the Tomcat web server.
- 7 To verify that the configuration was completed successfully, browse to a URL with this format:
`https://server1.initrode.com:8443/webui/servlet/admin`
LN UI Administration Webapp starts.
- 8 Use the padlock of the browser's address bar to inspect the certificate information and verify that the CA-signed certificate is displayed.

Configuring a PKCS#12 HTTPS keystore

Depending on customer requirements, it may be required to configure LN UI with an existing keystore in PKCS#12 format for HTTPS communications. This type of keystore file typically has a `.pfx` or `.p12` extension.

To use an existing PKCS#12 keystore:

- 1 Ensure that the PKCS#12 keystore file has a `.pfx` or `.p12` extension.
- 2 Locate the `conf/server.xml` file in the installation directory of the Tomcat web server and open it in a text editor.

Complete these steps:

- a Create/update the HTTPS connector (identified by `SSLEnabled="true"`) corresponding to the PKCS#12 keystore.
- b Ensure that the values of the `keystoreFile` and `keystorePass` attributes are correct.
- c Ensure that `keystoreType="pkcs12"` is present.
- d Save the file and close the text editor.

For detailed instructions, see http://tomcat.apache.org/tomcat-8.0-doc/config/http.html#SSL_Support.

- 3 Restart the Tomcat web server to apply the changes.
- 4 To verify that the configuration was completed successfully, browse to a URL with this format:
`https://server1.initrode.com:8443/webui/servlet/admin`
LN UI Administration Webapp starts.
- 5 Use the padlock of the browser's address bar to inspect the certificate information and verify that the expected CA-signed certificate is displayed.

Use this task to configure LN UI, IFS, and AD FS to allow Single Sign On for LN UI using Infor Federation Services. This task has these prerequisites:

- An IFS Xi version is up and running.
- IFS is configured for SAMLToken authentication.
- The XiPlatformBackend is bound to an http port. See "Enabling HTTP support for IFS Services" in the *Infor Xi Platform Installation Guide*.

Binding LN UI to IFS

Note: The instructions for binding LN UI to IFS are not applicable if LN UI is installed on an IBM WebSphere or Oracle WebLogic application server. Instead, you must use a command line tool that is bundled with the Enterprise Server Installer. For further information, unzip the `lnuiconfig.zip` file that is present in the installation directory and consult the `README` file.

To bind LN UI to IFS:

- 1 Start the LN UI Administration Webapp and select **Infor LN UI Administration > Login Configuration**.
- 2 Validate that the LN UI web server **HTTPS Port** value is filled.
- 3 In the **Authentication Type** field, select **Infor Federation Services**.
- 4 Open the **Infor Federation Services** tab and specify this information:

Configuration Web Service

Specify the IFS configuration web service URL. This URL must be in this format:

`http://<ifs_hostname>:<port>/IFSServices/ConfigurationService.svc`

Application URL

Usually you can leave this field at its default value. Only if your LN UI web server is behind a load balancer, you must specify the public URL of the LN UI application.

- 5 Click **IFS Configuration - Generate/Update** to register LN UI in IFS and create the required LN UI configuration.
- 6 Save the changes and restart the web server.

Obtaining a powershell script

To obtain a powershell script related to LN UI from IFS, complete these steps on the Xi Platform server:

- 1 Open Xi Platform Manager and sign-in.
- 2 Select **Applications**.
- 3 Click the download icon and specify the download path for the LN UI application. Save this file in a location where it can be moved to your AD FS server.

Creating a relying party trust

To create a relying party trust in AD FS for LN UI, complete these steps on the AD FS Server:

- 1 Open the Windows PowerShell as an administrator.
- 2 Run the `Set-ExecutionPolicy Unrestricted` command and confirm the execution policy change by pressing **Y**. Press **Enter**.
- 3 Run the PowerShell script that was previously downloaded for LN UI.
- 4 Open AD FS manager.
- 5 Select **ADFS > Trust Relationships > Relying Party Trusts**.
- 6 Select the relying party trust related to LN UI. For example, `Infor_LN_UI_<hostname><port>`
...
- 7 Right-click and select **Properties**.
- 8 Click the **Advanced** tab.
- 9 Change **Secure hash algorithm** to **SHA-1** and click **OK**.

Testing SSO

To verify that the IFS configuration was completed successfully, browse to a URL similar to:

`https://server1.initrode.com:8443/webui/servlet/fslogin`

LN UI should start.

Creating a Logical ID mapping

6

To create a Logical ID mapping:

- 1 Start the LN UI Administration Webapp and select **Infor LN > Logical ID Mapping**.
- 2 Click **New** to create a mapping from the Logical ID to the desired LN environment.
The logical ID must have a format such as `lid://infor.ln.<environment>`, where `<environment>` is a free-to-choose name.

Save the changes.

- 3 To verify that the configuration was completed successfully, browse to a URL similar to the URL below. Replace `<Logical ID>` with the value of the configured Logical ID.

`https://server1.initrode.com:8443/webui/servlet/fslogin?LogicalId=<Logical ID>`

LN UI should start using the LN environment designated by the Logical ID. To verify the name of the selected LN environment, select **Options > About**.

Make a note of the Logical ID, so you can use it later when you configure the Infor Ming.le-LN application.

Integrating Infor Ming.le - LN application (Platform Xi version)

7

This task describes the Infor Ming.le configuration steps to integrate Infor Ming.le and LN UI. Before you perform the described procedures, ensure that all tasks up to and including the Creating a Logical ID mapping task have been performed.

The configured LN UI HTTPS port number *<HTTPS port>* and the Logical ID *<Logical ID>* are required below.

Configuring the LN application

- 1 Open the Infor Ming.le portal and log on. You must have at least these Infor Ming.le security roles:
 - MingleAdministrator
 - UserAdmin
 - IFSApplicationAdmin
- 2 Open the Infor Ming.le Admin Settings page.
- 3 Click **Add Application** and specify this information:

Application Type

Specify **Infor Application**.

Application Name

Specify **LN -B61U.....** This table shows how Infor Ming.le application names relate to LN application versions.

Infor Ming.le application name	LN application version
LN - B61U9stnd	10.3
LN - B61U10stnd	10.4
LN - B61U11stnd	10.4.0.1
LN - B61U12stnd	10.4.1

Infor Ming.le application name	LN application version
LN - B61U13std	10.4.1.1
LN - B61U14std	10.4.2
LN - 10.4.2.1	10.4.2.1
LN - 10.5	10.5

Display Name

Specify the name that must be displayed on the App Switcher panel.

Application Icon

Click the button to choose your icon.

Logical ID

Specify the logical id that is previously configured in LN UI.

Use HTTPS

Select this check box.

Host Name

Specify the fully qualified domain name of the LN UI web server.

Port

Specify the HTTPS port number as configured in LN UI.

Context

Leave this field to its default value, **webui**, unless you have installed LN UI on a different context.

Default Tenant

Specify **infor**.

4 Click **Save.**

You can verify the default application security roles by opening the **Permissions** tab on the Application Details page. Here you can add or remove security roles. A user must have one of the listed security roles to get access to this LN application in Infor Ming.le.

Configuring the Documentation utility app

The Documentation utility application can be used to open the top page of the LN application help.

To enable this app for LN in Infor Ming.le:

- 1 Open the Infor Ming.le Admin Settings page.
- 2 Double-click the LN application.
- 3 Click the **Manage Context / Utility Apps** tab.
- 4 Select the Documentation utility application.

Configuring the LN Navigator utility app

The LN Navigator utility app shows a tree representation of the available LN sessions. From this utility app the user can start the available sessions.

To enable this app for LN in Infor Ming.le:

- 1 Open the Infor Ming.le Admin Settings page.
- 2 Double-click the LN application.
- 3 Click the **Manage Context / Utility Apps** tab.
- 4 Select the LN Navigator utility application.

Configuring the LN file attachments context app (ODM)

The LN file attachments context app allows access to files and documents attached to specific records in LN. This app collaborates with the ODM functionality on the LN system. Therefore it requires that the ODM functionality on the LN system is enabled and configured.

To enable this app for LN in Infor Ming.le:

- 1 Open the Infor Ming.le Admin Settings page.
- 2 Click the **Manage Context / Utility Apps** tab.
- 3 Click **Add Context/Utility App** and specify this information

Type

Specify **Context App**.

Name

Specify **LN File Attachments**.

Description

Specify **LN File Attachments stored in ODM**.

URL

Specify a URL in this format: `https:<lnuihostname>:<port>/webui/servlet/odm`

Note: The URL must correspond with the host name and port specified in the Configuring the LN application section.

Application Help URL

Leave blank.

- 4 On the **Permissions** tab, click **Add New Users and/or IFS Security Roles**.
In the **Security Role** field, specify **LN-User**. Then click **Done**.
- 5 On the **Context Message** tab, click **Add Message**.
In the **Message Name** field, specify **inforBusinessContext**. Then click **Done**.
- 6 On the **Applications** tab, click **Add/Remove Applications**.

Select the LN application/version to which the file attachments context app must be added. Then click **Done**.

- 7 Click the **Enabled** option for the added LN application.

Installing online help packages

8

To install an online help package:

- 1 Obtain the .zip file of the 'In' or 'es' help package and save it to disk.
The file must contain help in DHTML format.
- 2 Start the LN UI Administration Webapp and select **Infor LN Help > Help Content**.
- 3 Click **New**. Browse to the help package file and confirm the selected file.
- 4 Click **OK** to start the installation of the help package file.

To define version fallback rules in the LN UI Administration Webapp, select **Infor LN Help > Help Version Fallbacks**. See the online help page related to this session for a detailed description of how to define version fallback rules.

To find out for which packages you must define fallback rules, log on to LN and start the Packages by Package Combination (ttaad1121m000) session.

To define language fallback rules in the LN UI Administration Webapp, select **Infor LN Help > Help Language Fallbacks**. See the online help page related to this session for a detailed description of how to define language fallback rules.

You can use LN UI to deploy and run HTML5 based Workbenches. For a detailed description of the configuration and administration tasks, see the *Infor LN HTML5 Workbench Administration Guide*.

LN UI provides an LN Client Service, allowing mobile clients and on premise printing to access LN.

Configuring the LN Client Service

If LN UI is configured for Single Sign On using Federation Services, the LN Client Service relies on the AD FS artifact resolution service for authentication.

Enabling the AD FS artifact resolution service

By default the AD FS artifact resolution service is not enabled. To enable this AD FS service, complete these steps on the server where AD FS is installed:

- 1 Open AD FS manager.
- 2 In the AD FS Panel Tree, select **AD FS > Service > Endpoints**.
- 3 If the `/adfs/services/artifactresolution` endpoint is disabled, enable the endpoint and restart the AD FS service.

Importing the AD FS HTTPS certificate

Communication between LN UI and AD FS is based on HTTPS. Therefore the LN UI trust store must contain the AD FS HTTPS certificate or its related root certificate.

To import the AD FS HTTPS certificate into the LN UI trust store:

- 1 Get the AD FS certificate by opening this page in the Internet Explorer (IE) browser:
`https://<ad fs host>/adfs/ls`
- 2 Export the certificate through IE by clicking on the “padlock”. Save as a Base-64 encoded X.509 certificate file.

- 3 Start the LN UI Administration Webapp.
- 4 Select **Infor LN > SSL Trust store**.
- 5 Click **Import Certificate** and import the certificate that was exported in step 2.

Enabling or disabling the LN Client Service

To enable or disable the LN Client Service:

- 1 Start the LN UI Administration Webapp.
- 2 Select **Infor LN > LN Client Service** and click the **Configuration** tab.
The LN Client Service URL is displayed.
- 3 Select or clear the **Enable Service** check box, as desired.
- 4 Save the changes.

Testing the LN Client Service

To test the LN Client Service connection:

- 1 Start the LN UI Administration Webapp.
- 2 Select **Infor LN > LN Client Service** and click the **Test** tab.
- 3 In the **Environment Name** field, select the environment that mobile clients will use to access the LN Client Service.
- 4 If the selected environment has the BaanLogin SSL protocol, specify the credentials of a Windows domain user in the **Username** and **Password** fields.
- 5 If the selected environment has the BaanLogin or rexec protocol, specify the credentials of an LN user in the **Username** and **Password** fields.
- 6 Click **Test** to create a test connection.

In some situations it is desired to run LN UI, or a single LN UI session, outside Infor Ming.le.

If you want to run LN UI outside Infor Ming.le, you can use one of these authentication mechanisms:

- **Single Sign On using Infor Federation Services**
To use this authentication mechanism, ensure that you have performed all tasks up to and including "Configuring IFS (Platform Xi version)" on page 23.
You can now continue with the steps described in "Configuring in-context applications" on page 38.
- **Single Sign On using Integrated Windows Authentication**
To use this authentication mechanism, perform the tasks described in these sections:
 - "Creating an environment for LN connection (Single Sign On)" on page 17
 - "Configuring LN UI for Integrated Windows Authentication" on page 37
 - "Configuring in-context applications" on page 38
- **Backend Authentication**
To use this authentication mechanism, perform the tasks described in these sections:
 - "Configuring LN UI for Backend Authentication" on page 38
 - "Creating an environment for LN connection (LN Server Authentication)" on page 38

Configuring LN UI for Integrated Windows Authentication

Integrated Windows Authentication is only available if LN UI is deployed on a Windows server platform.

To configure LN UI for Integrated Windows Authentication:

- 1 Start the LN UI Administration Webapp and select **Infor LN UI Administration > Login Configuration**.
- 2 In the **Authentication Type** field, select **Integrated Windows Authentication**.
- 3 Click **Save**.

- 4 To verify that you can open LN UI, browse to this URL: `https://server1.initrode.com:8443/webui/servlet/standalone`.

Configuring LN UI for Backend Authentication

To configure LN UI for Backend Authentication:

- 1 Start the LN UI Administration Webapp and select **Infor LN UI Administration > Login Configuration**.
- 2 In the **Authentication Type** field, select **Backend**.
- 3 Click **Save**.

Creating an environment for LN connection (LN Server Authentication)

Use this task to configure an environment that allows to connect to LN through username/password authentication at the LN server. This task assumes that LN UI has been configured for the **Backend** authentication type.

Complete these steps:

- 1 Start the LN UI Administration Webapp and select **Infor LN > LN Environments**.
- 2 Click **New** to create an environment for the desired LN system.
- 3 On the **General** tab, specify the required details and select **BaanLogin** as the desired protocol. Save the changes.
- 4 To verify that the configuration was completed successfully, open the **Test** tab and specify a valid LN username and password. Then click **Test**.
- 5 To verify that LN UI is available for the designated server, browse to a URL similar to:
`https://server1.initrode.com:8443/webui/servlet/standalone`
The user should be prompted for the LN username and password, after which LN UI should start.

Configuring in-context applications

LN UI in stand-alone mode supports these in-context applications:

- LN Navigator
- Attached Files context application (ODM)

To enable or disable these context applications for LN UI in stand-alone mode:

- 1 Start the LN UI Administration Webapp and select **Infor LN > LN Environments**.
- 2 Select the environment that you want to change and open the details for this environment.
- 3 On the **General** tab, under **Stand-alone Mode**, select or clear the check box for the appropriate in-context application.
- 4 Click **Save**.
- 5 To verify the new setting, browse to a URL similar to `https://server1.initrode.com:8443/webui/servlet/standalone`.

Starting LN UI with a bookmarked session

If the URL to start LN UI is extended with specific parameters, LN UI can start in a predetermined session. In the URL, you can include query information about the record to be displayed. The supported parameters are described below.

Note: If LN UI is started using an extended URL, a new instance of LN UI is created in the browser and a new bshell is started on the LN server. Only AMS authorizations are applied. The DEM authorizations, defined on the LN server, for this user are disregarded.

This table shows the attributes that you can use as parameters in an extended URL that starts LN UI:

Name	Description
startupArgument	The name of the LN environment for which LN UI must be launched. If this attribute is not passed, the default environment for this user is used.
profileName	The name of the user profile. If this attribute is missing, the default user profile for the selected environment is used.
startupform	<p>The session code of the session that will be started automatically upon LN UI start. Frame and navigation options are suppressed. If the session code pertains to a multi-occurrence session, you can use these attributes to select a specific record:</p> <ul style="list-style-type: none">• startupcompany - The company number for the started session. If this attribute is missing, the default company is used.• startupindex - The session index for the started session. If this attribute is missing, the default session index is used.• startupwhere - Query information about the record to be displayed. The attribute value must be properly percent-encoded according to RFC3986.

This example shows an extended URL that starts LN UI in the User Data session for a specific user:

```
https://server1.initrode.com:8443/webui/servlet/fslogin?startupArgument=lnprod&startupform=ttaad2500m000&startupwhere=(ttaad200.user='jdoe')
```

Starting LN UI with a DEM process

The URL through which LN UI is started is extended with specific parameters to start the DEM Process Viewer for a specific DEM process model.

The user that opens this URL must be a DEM user and must be authorized to access this specific DEM process.

This table shows the attributes that you can use as parameters to start a specific DEM process:

Name	Description
startupArgument	The name of the LN environment for which LN UI must be launched. If this attribute is not passed, the default environment for this user is used.
profileName	The name of the user profile. If this attribute is missing, the default user profile for the selected environment is used.
demPath	The path of IDs of the process model that must be displayed in the Process Viewer. This is a mandatory attribute for starting a Process Viewer. These IDs may only contain alphanumeric characters and underscores. IDs are separated with a semicolon. The path starts with the role ID and is followed by the process ID. If a sub process must be started, it is also followed by the sub process ID.

This example shows a complete URL to start a Process Viewer:

```
https://server1.initrode.com:8443/webui/servlet/fslogin?startupArgument=lnprod&demPath=EUPU10;DCO007
```

In this example, the user must have the "EUPU10" DEM role and must be authorized for the "DCO007" DEM process.

This chapter describes how to configure and administer the Exchange Synchronizer.

The Exchange Synchronizer synchronizes contacts and calendar events between Microsoft Exchange and LN CRM.

Prerequisites

One of these Microsoft Exchange versions must be installed on the Exchange server:

- Microsoft Exchange 2007 with SP1 or a higher SP
- Microsoft Exchange 2010
- Microsoft Exchange 2013

Administration of Exchange Synchronizer

The Exchange Synchronizer runs on the web server of LN UI.

To start or stop the Exchange Synchronizer, start the LN UI Administration Webapp and select **Infor LN > Synchronizer Manager**.

Before you can start the Exchange Synchronizer for the first time, you must specify various configuration settings for Microsoft Exchange, LN, and LN UI. See the following subsections.

Configuring Microsoft Exchange

Prerequisites

Basic authentication must be allowed for the Exchange webservice, only on https. In a default Microsoft Exchange Server configuration, basic authentication is allowed.

To enable Basic Authentication on the Exchange Web Services, run the following Exchange command; there is no GUI equivalent to set the Authentication:

```
Set-WebServicesVirtualDirectory -Identity * BasicAuthentication $True
```

To confirm that Basic Authentication is enabled on the Exchange Web Services, run this command:

```
Get-WebServicesVirtualDirectory |FL
```

Verify that the BasicAuthentication parameter has the value 'True'.

See [http://technet.microsoft.com/en-us/library/aa997233\(EXCHG.80\).aspx](http://technet.microsoft.com/en-us/library/aa997233(EXCHG.80).aspx).

Impersonation

To use the Exchange Synchronizer, impersonation must be allowed and configured on the Exchange Server. See these sections:

- "Enabling the impersonation (Exchange Server 2010 and higher)" on page 43
- "Enabling the impersonation (Exchange Server 2007)" in the *Infor Enterprise Server Web UI - Installation and Configuration Guide*

This table shows the user account types that are used in the impersonation configuration:

Account type	Description
Impersonation User	A user who can impersonate a given user account. The impersonation user can perform operations with the authorizations of the impersonated account, instead of the impersonation user's own authorizations. The user account of the impersonation user matches the Exchange account specified in the MS Exchange Synchronization Settings (ttaad2140m000) session.
Impersonated user	A user for whom changes must be done, by the Exchange Synchronizer, via the impersonation user. The user accounts of the impersonated users match the e-mail addresses of the users specified in the MS Exchange Synchronization Users (ttaad2141m000) session.

Enabling the impersonation (Exchange Server 2010 and higher)

To assign permissions to accounts, Microsoft Exchange Server 2010 and higher use Role-Based Access Control (RBAC).

See [http://msdn.microsoft.com/en-us/library/exchange/bb204095\(v=exchg.140\).aspx](http://msdn.microsoft.com/en-us/library/exchange/bb204095(v=exchg.140).aspx).

For example, to enable impersonation with user 'syncuser' for all users:

- 1 Open the Exchange Management Shell.
- 2 Run this command:

```
New-ManagementRoleAssignment -Name:exchangeImpersonation - Role:
ApplicationImpersonation -User:syncuser
```

Configuring the Exchange Synchronizer in LN

The Exchange Synchronizer runs on the LN UI web server. Before you can start the Exchange Synchronizer, you must specify configuration settings on the LN server.

To configure the Exchange Synchronizer:

- 1 Log on to the LN server.
- 2 When using the synchronizer, the table sharing of the tables which are synchronized is impacted. In LN you can have multi site setups such as single logistic/multi finance and multi logistic/multi finance. MS Exchange is not aware of these company structures, so you cannot synchronize activities in a specific company. Therefore, you must ensure these tables are shared:
 - Contacts:
 - tccom140 - Contacts
 - tccom190 - Contacts Synchronization Table
 - Activities:
 - tccom600 - Activities
 - tccom605 - Attendees
 - tccom690 - Activity Synchronizations
 - tccom691 - Activity Synchronization Users
 - All tables related to the tables mentioned

See "Table Sharing Modeler" in the Enterprise Server online help.

- 3 Select the **Synchronize Contacts** check box in the COM Parameters (tccom0000s000) session if you want to enable contact synchronization. If this check box is selected, you must also specify ISO codes in the Countries (tcmcs0510m000) and Languages (tcmcs0146m000) sessions.

- 4 Select the **Synchronize Activities** check box in the COM Parameters (tccom0000s000) session if you want to enable calendar synchronization.
- 5 Start the MS Exchange Synchronization Settings (ttaad2140m000) session and define a configuration.
- 6 In the MS Exchange Synchronization Settings (ttaad2140m000) session, click **Users**. The MS Exchange Synchronization Users (ttaad2141m000) session starts. Specify the users that require synchronization of their contacts and calendars.

See the session help.

Note: To synchronize activities for attendees of the **Employee** type, who are specified in the Attendee (tccom6105m000) session, the following must be applicable for the employee:

- The **User** field is specified in the Employees - General (tccom0101m000) session.
- The **E-Mail** field is specified in the Employees - People (bpmdm0101m000) session.
- The **Email Address** in the MS Exchange Synchronization Users (ttaad2141m000) session is equal to the **E-Mail** field in the Employees - People (bpmdm0101m000) session.

Invitations to an activity can only be sent to the attendees' calendars if the activity's **Meeting Organizer**, as specified in the Attendee (tccom6105m000) session, is also defined in the MS Exchange Synchronization Users (ttaad2141m000) session. The reason for this is that MS Exchange generates the invitations for the organizer.

Configuring LN UI

The Exchange Synchronizer requires HTTPS access to the Microsoft Exchange Client Access Server (CAS).

To configure LN UI with the SSL certificate of the Client Access Server:

- 1 Use the browser to navigate to the Microsoft Exchange URL. This URL is similar to `https://<server>.<domain>/EWS/Exchange.asmx` and is also used in the MS Exchange Synchronization Settings (ttaad2140m000) session.
An XML document is displayed in the browser.
- 2 Use the browser's padlock icon to show the certificate details of the connection.
- 3 Copy the certificate information to a file, selecting the Base-64 encoded X.509 format.
- 4 Start the LN UI Administration Webapp and select **Infor LN > SSL Truststore**.
- 5 Click **Import Certificate** and select the file with the certificate information.
The information of the imported certificate is displayed.

Troubleshooting

This section describes common problems, that can occur when you run the Exchange Synchronizer, and their possible causes and solutions.

Error messages are stored in the LN UI log file. To find the location of this file, start the LN UI Administration Webapp and select **Infor LN UI Administration > Logging**.

The SMTP address has no mailbox associated with it

This error message is displayed:

```
com.sun.xml.ws.fault.ServerSOAPFaultException: Client received SOAP
Fault from server: The SMTP address has no mailbox associated with it.
Please see the server log to find more detail regarding exact cause
of the failure.
```

Cause:

- Incorrect credentials of MS Exchange impersonation account
- Incorrect e-mail address of Exchange Synchronizer user(s)

Solution:

- 1 Start the MS Exchange Synchronization Settings (ttaad2140m000) session. Verify that the **User**, **Password**, and **Domain** fields have been configured according to the MS Exchange impersonation user.
- 2 Start the MS Exchange Synchronization Users (ttaad2141m000) session. Verify that the e-mail address configured for each activated Exchange Synchronizer user corresponds with the MS Exchange e-mail address. The e-mail addresses must be identical, including the use of uppercase and lowercase.

An appointment or call can have only one meeting organizer

This error message is displayed:

```
ERROR DllExecutor yyyy-mm-dd hh:mm:ss [pool-x-thread-y] - Error in
adding attendee to attendees by activity. ERROR DllExecutor yyyy-mm-dd
hh:mm:ss [pool-x-thread-y] - An Appointment or Call can have only one
Meeting Organizer.
```

Cause: the e-mail address in the attendee's employee data does not correspond with the e-mail address that is configured for the Exchange Synchronizer user.

Solution: for any employee for which appointments may need to be synchronized, complete these steps:

- 1 Start the Employees – General (tccom0101m000) session.
- 2 View the details for the employee.
- 3 Click **Employee -People Data**. The Employees - People (bpmdm0101m000) session starts.
- 4 Verify that the e-mail address in this session corresponds with the Exchange Synchronizer user's e-mail address in the MS Exchange Synchronization Users (ttaad2141m000) session.
The e-mail addresses must be identical, including the use of uppercase and lowercase.

Exception occurred attempting to run SynchronizerService

This error message is displayed:

```
ERROR SynchronizationLoader yyyy-mm-dd hh:mm:ss [futures-handler] -  
Exception occurred attempting to run SynchronizerService  
com.infor.pim.synchronizer.TechnicalSynchronizationException: java.  
lang.NullPointerException
```

Cause: incorrect e-mail address of Exchange Synchronizer user(s)

Solution: start the MS Exchange Synchronization Users (ttaad2141m000) session. Verify that the e-mail address configured for each activated Exchange Synchronizer user corresponds with the MS Exchange e-mail address. The e-mail addresses must be identical, including the use of uppercase and lowercase.

The account does not have permission to impersonate the requested user.

This error message is displayed:

```
com.sun.xml.ws.fault.ServerSOAPFaultException: Client received SOAP  
Fault from server: The account does not have permission to impersonate  
the requested user. Please see the server log to find more detail  
regarding exact cause of the failure.
```

Cause: the MS Exchange impersonation user does not have sufficient permissions in MS Exchange.

Solution: in MS Exchange, verify the configuration of the impersonation user.

The server sent HTTP status code 404: Not Found

This error message is displayed:

```
com.sun.xml.ws.client.ClientTransportException: The server sent HTTP  
status code 404: Not Found
```

Cause: incorrect MS Exchange URL

Solution: start the MS Exchange Synchronization Settings (ttaad2140m000) session. Check the value of the **MS Exchange URL** field and correct it if required.

Unable to find valid certification path to requested target

This error message is displayed:

```
com.sun.xml.ws.client.ClientTransportException: HTTP transport error:  
javax.net.ssl.SSLHandshakeException: sun.security.validator.Validator  
Exception: PKIX path building failed: sun.security.provider.certpath.
```

```
SunCertPathBuilderException: unable to find valid certification path  
to requested target
```

Cause: wrong or missing SSL certificate for MS Exchange connection

Solution: In the LN UI Administration Webapp, select **Infor LN > SSL Truststore**. Import the public certificate of the MS Exchange server.

For details, see "Configuring LN UI" on page 44.

Contact and/or calendar events are not synchronized

Cause:

- 1 Users have not been activated for synchronization.
- 2 Calendar category mismatch between Synchronizer and MS Exchange.
- 3 The push mechanism of the Exchange Synchronizer uses an incorrect LN UI URL.

Solution:

- 1 Start the MS Exchange Synchronization Users (ttaad2141m000) session. Ensure that one or more users have the **Active** check box selected and that the **Email Address** field contains the user's MS Exchange e-mail address.
- 2 Start the MS Exchange Synchronization Settings (ttaad2140m000) session. Verify that the category specified under **Calendar Synchronization** corresponds with the category that was selected for the meeting in Outlook.
- 3 Start the MS Exchange Synchronization Settings (ttaad2140m000) session. Verify that the **WebUI Server URL** field contains the LN UI HTTP URL. For example, `http://server.domain:8080/webui`.

Note: Although LN UI may have been configured for HTTPS usage, this field only supports the HTTP URL.

The configuration of clickjacking prevention provides a defense against certain security attacks. Read this chapter to learn more about clickjacking prevention and how to configure it through the LN UI Administration Webapp.

Limitations

You cannot enable clickjacking prevention if the same LN UI installation is used for stand-alone mode and inside Infor Ming.le. This is because of a technical restriction on the HTTP protocol level where only one expected HTML parent frame can be specified.

Clickjacking prevention does not work if the Safari browser is used. The Safari browser does not provide the required support.

Overview

Clickjacking is an attack that tries to hijack the user's mouse click action. If the attack is successful, the click action is used for a different, often malicious, purpose than intended. Clickjacking is achieved by overlaying the desired LN UI web content with invisible HTML frame content that is controlled by the attacker.

For details, see <https://www.owasp.org/index.php/Clickjacking>.

LN UI's clickjacking prevention ensures that the browser is aware of the expected HTML parent frame through which all normal LN UI access should occur. This way, if an attacker embeds LN UI in a malicious website, the browser denies access to LN UI and prevents the attack.

Enabling the clickjacking prevention

To enable the clickjacking prevention:

- 1 Start the LN UI Administration Webapp.
- 2 Select **Infor LN UI Administration > Clickjacking Prevention**.
- 3 Select the **Enable Clickjacking prevention** check box.
- 4 In the **Trusted Host** field, specify the base URL for LN UI access:

- If LN UI is used through the Infor Ming.le portal, specify the base URL of the Infor Ming.le server.
For example: `https://mingle.mydomain/`
- If LN UI is used in stand-alone mode, specify the base URL of the LN UI server.
For example: `https://lnui.mydomain:8443/webui/`

5 Save the changes. The changes are effective immediately.

Disabling the clickjacking prevention

To disable the clickjacking prevention:

- 1** Start the LN UI Administration Webapp.
- 2** Select **Infor LN UI Administration > Clickjacking Prevention**.
- 3** Clear the **Enable Clickjacking prevention** check box.
- 4** Save the changes. The changes are effective immediately.

Detailed information

If clickjacking is enabled, LN UI adds a number of HTTP response headers. See the following examples.

X-Frame-Options: ALLOW-FROM `https://lnui.mydomain:8443/`

Content-Security-Policy: frame-ancestors `https://lnui.mydomain:8443/`

P3P: CP=Infor doesn't have any p3p policies.

Deployment on JBoss

If LN UI is installed on the JBoss web server, use this task to integrate LN UI with the user authentication provider. The browser client and LN UI communicate using HTTPS.

Configuring the HTTPS port using the JBoss Management console

Complete the following steps to configure the HTTPS port using the JBoss Management console. As an example, 8443 is assumed as the designated HTTPS port value.

- 1 Ensure that the JBoss web server is running.
- 2 Use the browser to start the JBoss Management console. The default address is `http://localhost:9990/console`. Log on using the administrator credentials provided during installation.
- 3 Depending on the JBoss version, complete one of these steps:
 - a With JBoss 6.2, select **Profile > General Configuration > Socket Binding**.
 - b With JBoss 6.3, select **Configuration > General Configuration > Socket Binding**.
- 4 Select **Standard-sockets > View**.
- 5 To add the HTTPS port definition, click **Add**.
Specify this information:
Name
Specify **https**.
Port
Specify **8443**.
Binding Group
Specify **standard-sockets**.
- 6 Click **Save**.
- 7 Depending on the JBoss version, complete one of these steps:
 - a With JBoss 6.2, select **Profile > Web > Servlet/HTTP** and click the **Connectors** tab.

- b With JBoss 6.3, select **Configuration > Subsystems > Web > Servlet/HTTP** and click the **Connectors** tab.
- 8 To add the HTTPS port to the Servlet/HTTP configuration, click **Add**.
 - a Specify this information:
:
Name
Specify **https**.
Socket Binding
Specify **https**.
Protocol
Specify **HTTP/1.1**.
Scheme
Specify **https**.
 - b Select **Enabled**.
- 9 Click **Save**.

You must finalize the configuration of the HTTPS port in the LN UI Administration Webapp.

See "Finalizing the configuration of the HTTPS port" on page 52.

Finalizing the configuration of the HTTPS port

To finalize the configuration of the HTTPS port:

- 1 Start the LN UI Administration Webapp.
- 2 Select **Infor LN UI Administration > HTTPS Keystore**.
- 3 Specify the desired values for fields such as **Organizational Unit** and **Organization**, which will be used for the self-signed certificate.
- 4 Click **Keystore - Generate/Update** to create the HTTPS keystore with a self-signed certificate.
- 5 Select **Infor LN UI Administration > HTTPS Configuration**.
- 6 Click **HTTPS Connector - Generate/Update** to update the JBoss configuration with the HTTPS keystore.
- 7 Select **Infor LN UI Administration > Login Configuration**. In the **HTTPS Port** field, specify the designated value, for example **8443**.
- 8 Select **Backend**, **Integrated Windows Authentication**, or **Infor Federation Services** as the desired authentication type.
- 9 If you selected **Infor Federation Services**, open the **Infor Federation Services** tab and specify the IFS Configuration Web Service URL. Then click **IFS Configuration - Generate/Update** to create the required LN UI configuration.
- 10 Save the changes.
- 11 To verify that the configuration was completed successfully, browse to a URL similar to:

`https://server1.initrode.com:8443/webui/servlet/fslogin`

LN UI should start.

- 12 Use the padlock of the browser's address bar to inspect the certificate information and verify that a self-signed certificate is displayed.

For instructions to replace the self-signed certificate of the HTTPS keystore with a CA-signed certificate, see "Installing or renewing a CA-signed HTTPS certificate" on page 20.

Deployment on WebSphere AS v8.5.5

This procedure describes how to deploy LN UI on IBM WebSphere AS v8.5.5.

Before you begin the deployment of LN UI, consult the IBM WebSphere AS v8.5.5 documentation and ensure that these prerequisites are met:

- An HTTP Server must be up and running, for example IBM HTTP Server or IIS.
- IBM WebSphere AS v8.5.5 must be up and running.
- The HTTP Server must be able to connect to the IBM WebSphere installation (plug-in setup).

You can use the following procedure to perform these actions:

- Deploy LN UI for the first time (first installation).
- Deploy a new LN UI version in an existing environment (LN UI upgrade).

When completing a first installation, proceed with the tasks starting at the Creating an environment for LN connection (Single Sign On) chapter.

LN UI must run on Java 1.7. Therefore you must install the IBM WebSphere SDK Java Technology Edition (Optional) - Version 7.x. To perform this installation, use the IBM Installation Manager application that comes with WebSphere AS.

- 1 To activate the usage of Java 1.7:
 - a Start the IBM WebSphere Administrative Console.
 - b Select **Servers > Server Types > WebSphere application servers > <your server> > Server Infrastructure > Administration > Java SDKs**.
 - c Select the 1.7 version and click **Make Default**.
 - d Click Save directly to the master configuration.
- 2 To ensure that the Java Heap size for the used application server is large enough:
 - a Start the IBM WebSphere Administrative Console.
 - b Select **Servers > Server Types > WebSphere application servers > <your server> > Server Infrastructure > Java and Process Management > Process definition**.
 - c On the Process definition Configuration page, under **Additional Properties**, click Java Virtual Machine.
 - d On the **Java Virtual Machine Configuration** tab, ensure that the values in the **Initial Heap size** and **Maximum Heap size** fields are at least 1024.

If you changed the values, complete the following steps.

- e At the bottom of the page, click **Apply** and **OK**.
- f On the next page, click Save directly to the master configuration.
- g Restart the WebSphere server.

Note: WebSphere does not always provide feedback when it is processing changes. Wait until the restart is finished.

Deploying LN UI for the first time

To deploy LN UI:

- 1 Start the IBM WebSphere Administrative Console.
- 2 Open the **Applications** node.
- 3 Click **New Application**.
- 4 In the next screen, click **New Enterprise Application**.
- 5 In the next screen, browse to the `lnui.war` file.
- 6 Click **Next**.
- 7 In the Preparing for the application installation screen also click **Next** accepting the default settings.
- 8 To accept the default settings for step 1, 2, and 3, click **Next**.
- 9 In step 4, "Map context roots for Web modules", change the **Context Root** to `/webui`.
- 10 To accept the default settings for step 5, click **Next**.
- 11 Click **Finish** in step 6.
- 12 Click Save to save the changes to the master configuration.
- 13 Select **Applications > Application Types > WebSphere enterprise applications**.
- 14 Click lnui.war.
- 15 Under **Modules**, click Manage Modules.
- 16 Click Infor LN UI module.
- 17 Select the **Infor LN UI** module and change the class loader order to **Classes loaded with local class loader first (parent last)**.
- 18 Apply and save the changes to the master configuration.
- 19 Start the web application. Click **Websphere Enterprise Applications**. Select the LN UI web application and click **Start**.

Deploying LN UI in an existing environment

To deploy LN UI in an existing environment:

- 1 Copy the contents of the `config` directory from the `<installation-directory>\lnui_war.ear\lnui.war\` directory to a directory that will not be overwritten by the new installation.
- 2 Start the IBM WebSphere Administrative Console.
- 3 Select **Applications > Application Type node > Webshpere Enterprise Applications**.
- 4 Select the **lnui_war** check box and click **Update**.
- 5 On the Preparing for the application update page, select **Replace the entire application**.
- 6 Select **Local file system** and specify the full path to the `lnui.war` file.
- 7 Click **Next**.
- 8 Click **Next**.
- 9 Click **Next** on the Step 1, Step 2, and Step 3 pages.
- 10 Click **Finish** on the Step 4 page.
- 11 Click [Save directly to the master configuration](#).
- 12 Move the saved `config` directory back to its original location; see step 1.

Deployment on WebLogic 12c v12.1.x

This procedure describes how to deploy LN UI on Oracle Weblogic 12c v12.1.x.

You can use the following procedure to deploy or redeploy LN UI. When the installation is complete, you can proceed with the tasks starting at the [Creating an environment for LN connection \(Single Sign On\)](#) chapter.

Prerequisites

Before you start the deployment of LN UI, consult the Oracle WebLogic 12c documentation and ensure that these prerequisites are met:

- WebLogic is installed and a domain is set up.
- The WebLogic Administrative Console is accessible and administrator rights are available.

Preparing the deployment

Before you can deploy LN UI, you must make various preparations.

This table shows the abbreviations that are used in the following procedure:

Abbreviation	Description
<code><wlInstDir></code>	The installation directory of WebLogic

Abbreviation	Description
<wlDomain>	The WebLogic domain
<wlServer>	The server on which LN UI will be installed
<lnuiConfigPath>	The configuration folder for LN UI
<memArgs>	The preferred settings for java heap size See the <i>Infor LN UI 11.x Sizing Guide</i> .

To prepare the deployment:

- 1 Modify the server's `config.xml` file.
 - a Open the `<wlInstDir>\user_projects\domains\<wlDomain>\config\config.xml` file.
 - b At the end of the `<security -configuration>` node , add this line:

```
<enforce-valid-basic-auth-credentials>false</enforce-valid-basic-auth-credentials>
```

This stops WebLogic from forcing on its own security model. LN UI provides this itself, and WebLogic interferes with this.
- 2 Set the configuration directory parameter.
 - a Create a folder where the LN UI configuration should be stored.
For example: `C:\Infor\lnui\config`
This is the `<lnuiConfigPath>`.
 - b If the WebLogic Node Manager is used for starting the WebLogic server:
 - 1 Start the WebLogic Administrative Console that is used to administer the used node.
 - 2 Under **Domain Structure**, open `<wlDomain> > Environment > Servers`.
 - 3 In the **Servers** list on the Summary of Servers page, click the link of the `<wlServer>`.
 - 4 On the Settings for `<wlServer>` page, click the **Configuration > Server Start** tab.
 - 5 In the **Arguments** field, specify this argument:
`-Dln.configuration=<lnuiConfigPath> <memArgs>`
 - c If the WebLogic server is started without using the Node Manager:
 - 1 Create a batch script with the following content:

```
set USER_MEM_ARGS=<memArgs>
set JAVA_OPTIONS=%JAVA_OPTIONS% -Dln.configuration=<lnuiConfigPath>

<wlInstDir>/user-projects/domains/<wlDomain>/bin startWebLogic.cmd
```

- 2 Run this script.

Deploying LN UI

To deploy LN UI:

- 1 Start the WebLogic Administrative Console. The default URL is <http://localhost:7001/console>.
- 2 Under **Helpful Tools**, click Configure Applications.
- 3 Click **Install**.
- 4 On the Locate deployment to install and prepare for deployment page, set the path to the `.ear` file.
- 5 Click **Next**. The `.ear` file is loaded.
- 6 On the Choose targeting style page, select the **Install this deployment as an application** option.
- 7 Click **Next**.
- 8 On the Optional Settings page, under **General**, preferably change the name to **webui**.
- 9 click **Finish**.

LN UI is now deployed.

A Summary of Deployments page is displayed. The summary contains these messages: All changes have been activated. No restarts are necessary and The deployment has been successfully installed.

The name of the new application is displayed in the **Deployments** list.

For details on how to access the LN UI application, see "Access" on page 13.

Use this task to configure LN UI, IFS, and AD FS to allow Single Sign On for LN UI using Infor Federation Services version 11. This task has these prerequisites:

- An IFS version 11 is up and running.
- IFS is configured for SAMLToken authentication (Claims-based authentication).
- The IFS is bound to an http port.

To bind LN UI to IFS:

- 1 Start the LN UI Administration Webapp and select **Infor LN UI Administration > Login Configuration**.
- 2 Validate that the LN UI web server **HTTPS Port** value is filled.
- 3 In the **Authentication Type** field, select **Infor Federation Services**.
- 4 Open the **Infor Federation Services** tab and specify this information:

Configuration Web Service

Specify the IFS configuration web service URL. This URL must be in this format:

`http://<ifs_hostname>:<port>/IFSServices/ConfigurationService.svc`

Application URL

Usually you can leave this field at its default value. Only if your LN UI web server is behind a load balancer, you must specify the public URL of the LN UI application.

- 5 Click **IFS Configuration - Generate/Update** to register LN UI in IFS and create the required LN UI configuration.
- 6 Save the changes and restart the web server.

To create a relying party trust in AD FS for LN UI, complete the steps described in the "Configuring Applications" section in the *Infor Federation Services Administration Guide* version 11.0.

This task describes the Infor Ming.le configuration steps to integrate Infor Ming.le and LN UI using the Infor Ming.le-LN Plug-in.

Before you perform the described procedures, ensure that all tasks up to and including the Creating a Logical ID mapping task have been performed.

The configured HTTPS port number *<HTTPS port>* and the Logical ID *<Logical ID>* are required below.

Configuring the Infor Ming.le-LN Plug-in

During the configuration of Infor Ming.le, you must select and configure each of the required Infor Ming.le features. See the "Post-installation tasks: Running the Infor Ming.le configuration" section in these guides:

- *Infor Ming.le Installation and Configuration Guide for Active Directory*
- *Infor Ming.le Installation and Configuration Guide for Active Directory Federation Services*

Complete these steps during the configuration of Infor Ming.le:

- 1 When selecting the Infor Ming.le features, include the Infor Ming.le-LN Plug-in in the selection.
- 2 When prompted to configure the Infor Ming.le-LN Plug-in, specify these details:

Title

Specify "Infor LN" as the name of the deployed application.

Site

Use the drop-down list to select a path ending with '/ln'.

Logical Id

Specify the Logical ID value as configured in LN UI.

Application Version

Specify the LN version. The default value is B61Ua9stnd.

Host Name

Specify the Fully Qualified Domain Name of the LN UI web server.

Port

Specify the HTTPS port number as configured in LN UI.

Context

Leave this field blank.

Use Https

Select this check box if LN UI is configured to use secure communications (HTTPS) with the browser. Otherwise, clear this check box.

Default Tenant Id

Do not change this field.

Configuring the Documentation context application

The Documentation context application configuration by default assumes that the Infor LN documents, which are part of the LN online help packages, are installed on the Infor Ming.le server. In case of LN UI however, these documents are stored on the LN UI Webserver. Therefore, to change these settings, you must complete these steps:

- 1 Log on to the Infor Ming.le suite with the site collection administrator account.
- 2 Open the Infor Application views - Infor LN version <version> - Documentation.
Complete these steps:
 - a Select **Site Actions > View all site content**.
 - b In the **Lists** section, click **Infor Application Views**.
 - c On the **Infor Application Views** list, select **Infor Application Drillback Views - Infor LN version <version> - Documentation**. Select the **Items** tab above the Infor Ming.le toolbar, and click **Edit Item**.
- 3 Modify URL Template
On the Infor Application Views - Infor LN version <version> - Documentation page, the **URL Template** field by default has these contents:
{SharePointSite}/_layouts/Infor.LN/help/{LanguageCode}/ln/{ProductVersion}/documentation.html
Replace this with:
{Hostname}:{Port}/{Context}/servlet/help/{LanguageCode}/ln/{ProductVersion}/documentation.html
Then click **Save**.

Adjusting Infor Ming.le's browser compatibility mode

When using Internet Explorer (IE), LN UI requires that the most recent IE Compatibility mode ('edge') is used for all users. For details on how to set this property, see the "Adding the Browser Compatibility Mode property" subsection in the *Infor Ming.le Administrator Guide*.

Configuring LN application and user properties in Infor Federation Services

This section is applicable if Infor Federation Services has been chosen as the Single Sign On authentication type.

To allow users to have access to the LN application tab in Infor Ming.le:

1 Sign in to IFS.

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/`

2 Add the "LN" security role and link users to this role.

Complete these steps:

- Select **Manage > Master Data**. The Master Data types are listed.
- Select the "Security Role" Master Data type and click **Details** to display the Security Role details.
- In the left pane, click **New**.
- In the right pane, specify this information:

Node name

Specify **LN**.

Description

Specify a description for the new role.

- In the Users in this Instance pane, click **New** to start the Add Users dialog box.
- Select the users that must use the LN application and click **OK**. The selected users are displayed in the Users in this Instance pane.

Note: Alternatively, you can use the Users page to link users to the "LN" role. To open this page, select **Manage > Users**. On the Users page you can also synchronize and/or upload users from Active Directory to the IFS application. See the *Infor Federation Services Administration Guide*.

- Click **Submit**.

3 Link the "LN" security role to the LN application.

Complete these steps:

- Select **Configure > Applications**.

- b On the Applications list page, select the LN application. The available security roles are displayed in the Security Roles pane.
- c Select the "LN" role and click **Submit**.

Infor Ming.le and ODM

Complete the following steps to show the ODM file attachments in-context application in Infor Ming.le.

The description below is based on SharePoint Foundation 2013 and Infor Ming.le Foundation 11.1.5. With other versions of this software the terms used below might be named slightly different.

1 Create Infor Application View for LN File Attachments.

- a Open Infor Ming.le and log on as Site Collection Administrator.
- b On the Infor Ming.le homepage click the **Settings** gear icon. Then select **Site Contents > Infor Application Views**.
- c Add an item in the Infor Application Views list.
Specify this information:

Title

Specify **Infor LN 10.4 - LN File attachments**.

Logical Id Prefix

Specify **lid://infor.In**.

Application Version

Specify **B61U10stnd**.

View Id

Specify **LN File Attachments**.

URL Template

Specify **{Hostname}:{Port}/{Context}/servlet/odm?LogicalId={LogicalId}&Tenant={Tenant}**.

- d Add an item in the Infor Application Generic Views list.
Specify this information:

Title

Specify **Infor LN 10.4 - LN File attachments**.

Logical Id Prefix

Specify **lid://infor.In**.

Application Version

Specify **B61U10stnd**.

View Id

Specify **LN File Attachments**.

2 Add the LN File Attachments web part to the LN site.

- a Open the Infor Ming.le site and log on as Site Collection Administrator.
- b Navigate to the LN site page.
- c Click the **Context Applications Manager** gear icon.
- d In the left panel, expand the **Infor** category. Select the Generic web part and add it to the list on the right side. The Generic web part is added to your page.
- e Navigate to a web part named "Generic" and select it. Click the down arrow button in the newly added Generic web part and select **Edit Web Part**. The configuration settings panel of the Generic web part is displayed.
- f In the **Custom Settings** section of the configuration settings panel, specify this information:

Application Logical ID Prefix

Specify **lid://infor.In**.

Application Logical ID

Specify **lid://infor.In.1**.

Application View ID

Specify **LN File Attachments**.

Title

Specify **File Attachments**.

Height

Specify **400 pixels**.

- g Click **OK**.

For details about the configuration of ODM, see these guides:

- *Infor LN Data Management Administrator's Guide*
- *Infor LN Data Management User's Guide for ODM Set-up Data Procedure*

This chapter describes manual configuration steps to meet specific customer requirements.

Post-installation instructions after an upgrade from Web UI

Through the Infor Enterprise Server Installer you can install LN UI as an upgrade from Web UI. After the installation, to provide a smooth transition from Web UI to LN UI, you can import these configuration items from Web UI:

- Settings of all LN environments. See note.
- The BaanLogin SSL keystore file, if one or more LN environments are imported with BaanLogin SSL as the selected protocol.
- Logical ID mappings.
- The HTTPS port number.
- The Single Sign On type.
- If Web UI was configured to use Infor Federation Services (IFS):
 - The IFS configuration web service URL
 - Configuration files required to operate IFS
- The Tomcat HTTPS keystore file, if it is contained in the Web UI configuration folder tree.

Note: Baan IV environments are ignored during import; Baan 5 environments are imported but will not be functional.

To perform the import:

- 1 Start the LN UI Administration Webapp and navigate to **Infor LN UI Administration > Import Web UI Configuration**.

The **Import Path** field shows a file folder which should correspond to the Web UI configuration folder.

- 2 Click **Import**.

The import of configuration items from Web UI in the LN UI deployment starts.

- 3 When completed, the **Log** field shows the configuration items that were imported, along with any anomalies. You can view the same information by opening the `import.log` file in the LN UI configuration folder.
- 4 Restart the web server.

You can now start LN UI. To verify this, browse to this URL:

```
https:// server1.initrode.com:8443/webui/servlet/fslogin?LogicalId=<Logical ID>
```

LN UI should start using the LN environment designated by the Logical ID. To verify the name of the selected LN environment, select **Options > About**.

When these steps are completed successfully, proceed with the installation and configuration of Infor Ming.le and the Infor Ming.le-LN Plug-in, if required.

Troubleshooting

To help solve operational problems of LN UI, diagnostic information is available as follows:

- LN UI log messages are captured in a centralized log file. The messages are available at the error, info, and debug level. To look up the name of the log file and control the level of the emitted messages:
 - 1 Start the LN UI Administration Webapp.
 - 2 Select **Infor LN UI Administration > Logging**.
For details, see the online help of the Logging page.
- During the LN UI trace mode, the message flow between LN UI and the server, for a specific user, is logged. If the user selects **Activate trace mode** on the **Options** menu, a new window with logged messages is displayed. The user can download the contents for offline examination.

Configuring SSO in LN



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 LN UI.

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

- LN UI obtains the end user's identity from the identity provider, such as Active Directory Federation Services, 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 LN configuration is the scope of this chapter and facilitates connecting, mapping, (permission) checking, and impersonation.

- Connecting means that the LN UI's request for the secure connection is acknowledged and that the data exchange between LN UI and LN can start.
- Mapping is required because the identity provider 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 required because the mapping information is not sufficiently secured.
- Impersonation is about the 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. In the configuration steps, these terms are used:

End User

The person using LN

Application User

An LN account for an end user

System User

The operating system account that runs the bshell on behalf of the end user

SSO User

The identification of the end user according to the identity provider.

Generic System User

A, non-personal, operating system account that 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* 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*.

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 LN UI.
- 2 Select **LN Tools > Application Configuration > Parameters**.

- 3 Start the SSO Parameters (ttams0100m000) session.
 - 4 Select the **SSO Active** check box.
 - 5 Specify this information:
 - 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 (ttaad2500m000)

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 that requires SSO access.
- 4 Specify the SSO User (pre-Windows 2000 login name or User Principal Name) in the **SSO User** field.
- 5 Repeat steps 3 and 4 for other application users that require SSO access.
- 6 Save the changes and close the details session. You will return to the User Data (ttaad2500m000) main session.
- 7 On the appropriate menu in the User Data (ttaad2500m000) main session, select **Convert Changes To Runtime DD**.
- 8 Specify the required data in the Convert Changes to Runtime DD (ttams2200m000) session. For details, see the session help.
- 9 Click **Convert** to convert the user data to an encoded `s<SSO User>` file in the `$BSE/lib/user/sso/` directory.

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 `security` directory 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 the `sso_permissions.xml` file as shown in the example (replace 'domain' and 'username' with the actual values).
- 4 Save the `sso_permissions.xml` file in the `security` directory.
- 5 To avoid unauthorized changes or deletions, ensure that the `sso_permissions.xml` file 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 'BaanLoginSSL' 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	
Override 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	
SSO 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 LN UI.
- 2 Select **LN Tools > Application Configuration > Parameters**.
- 3 Start the SSO Parameters (ttams0100m000) session.
- 4 Select the **SSO Active** check box.
- 5 Specify this information:
 - In the **Generic System User** field specify a username.
 - Select the **Override System User Allowed** check box.
- 6 Click **Dump** to place the information in the `$BSE/lib/sso_config` directory.

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

Update session User Data (ttaad2500m000)

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 that requires SSO access.
- 4 Specify the SSO User (pre-Windows 2000 login name or User Principal Name) in the **SSO User** field.
- 5 Repeat steps 3 and 4 for other application users that require SSO access.
- 6 Save the changes and close the details session. You will return to the User Data (ttaad2500m000) main session.
- 7 On the appropriate menu in the User Data (ttaad2500m000) main session, select **Convert Changes To Runtime DD**.
- 8 Specify the required data in the Convert Changes to Runtime DD (ttams2200m000) session. For details, see the session help.
- 9 Click **Convert** to convert the user data to an encoded `s<SSO User>` file in the `$BSE/lib/user/sso/` directory.

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 `sso_permissions.xml` file as shown in the example section.
This example `sso_permissions.xml` file assumes that all involved combinations of System Login and SSO User are pairs of identical strings. If the strings within one or more pairs are different, see "Advanced topics" on page 76.
- 3 Save the `sso_permissions.xml` file in the `security` directory.
- 4 To avoid unauthorized changes or deletions, ensure that the `sso_permissions.xml` file 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>
```

```

    </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 `-p <port number>` option specifies the port number used by the daemon. When this option is omitted, the default port number is 7150.

The `-ssl <ssl properties file>` option 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 an `@`-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 is sent to the `${BSE}/log/blogin.log` file.

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

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

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

User data		
Field	Usage	Remarks
User	Mapping: Application User	
SSO 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 the bshell is started using the System Login 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** check box is selected.
- 4 Create the `sso_permissions.xml` file 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 the `sso_permissions.xml` file implementing a case-sensitive permission check; this is desired when all involved System Login / SSO User pairs consist of identical strings. However, if the case is different for one or more application users, the permission check must be case-insensitive. To achieve this in the `sso_permissions.xml` file, specify this information:

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

instead of

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

Non-Windows: Permission check when System Login and SSO User are different

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

For example, if an application user with System Login 'jdoe' is associated to SSO user 'JRDoe', the `sso_permissions.xml` file must have these contents:

```
<?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

The `sso_permissions.xml` file 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 only for application users with SSO User 'jdoe' or '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

The `sso_permissions.xml` file 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 only for application users with SSO User 'jdoe' or '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>
```