Infor LN UI Administration Guide

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

Publication information

Release: Infor LN UI 11.2.0

Publication Date: June 15, 2015

Document number: U9790F US

Contents

About this guide

Infor LN UI is the HTML5 compliant browser-based user interface for Infor LN 10.3 and higher. 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.

Organization

This table shows the sections of the guide:

Section	Description
Prerequisites	Summarizes the prerequisites for operating and using LN UI.
Overview	Provides an overview of the administration capabilities.
Post-installation instructions	Describes the steps you must take after installation.
Online Help	Describes the online help functionality.
Troubleshooting	Describes how to do troubleshooting .
Common tasks	Describes common administration tasks.
Configuring SSO in LN	Provides information on the user identity in LN and user access to LN in order to enable SSO in LN.
"Integrating Infor Ming.leTM and LN" on page 45	Describes the Infor Ming.le configuration steps that are required to integrate Infor Ming.le and LN UI using the Infor Ming.le-LN Plug-in.
Deployment on WebSphere Express v8.5	Describes how to deploy LN UI on IBM WebSphere Express v8.5.

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.

Prerequisites

1

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. Support for Single Sign On is limited to Infor Federation Services.
Java Runtime Environment	Oracle Java SE 7 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	Apache Tomcat 7.0.x
	JBoss EAP 6.2.x
	WebSphere 8.5. For installation instructions, see "Deployment on WebSphere Express v8.5" on page 49.

Supported Browser Clients

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

Client	Supported browsers
Windows clients	Microsoft Internet Explorer 10, Microsoft Internet Explorer 11 in Desktop style
	Microsoft Internet Explorer 10, Microsoft Internet Explorer 11 in Metro style, but with limitations
	Chrome - latest version
Mac OS clients	Safari browser - 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

The minimal client requirements for LN UI are identical to the hardware recommendations for Infor Ming.le clients. For details, see the *Infor Ming.le Installation and Configuration Guide for Active Directory Federation Services* or *Infor Ming.le Installation and Configuration Guide for Active Directory*.

Overview

2

Access

After installation and configuration, LN UI can be accessed through various URLs.

URLs to access LN UI using authentication at the LN server

These URLs provide user access to LN UI using authentication at the LN server:

- `https://[hostname]:[HTTPS port]/webui/servlet/login`
- `https://[hostname].[domain name]:[HTTPS port]/webui/servlet/login`
- `http://[hostname]:[HTTP port]/webui/servlet/login`
- `http://[hostname].[domain name]:[HTTP port]/webui/servlet/login`

To gain access, the user must specify a valid LN username and password.

URLs to access LN UI using Single Sign On

These URLs provide user access to LN UI using Single Sign On, optionally using secure communications (HTTPS) from the browser:

- `http://[hostname].[domain name]:[HTTP port]/webui/servlet/fslogin`
- `https://[hostname].[domain name]:[HTTPS port]/webui/servlet/fslogin`

Depending on the configuration, user authentication is performed with Infor Federation Services or Integrated Windows Authentication.

The Infor Ming.le-LN Plug-in is configured to use one of these URLs.

URLs to access the LN UI user settings Webapp

These URLs provide direct access to the LN UI user settings Webapp:

- `http://[hostname].[domain name]:[HTTP port]/webui/servlet/settings`
- `https://[hostname].[domain name]:[HTTPS port]/webui/servlet/settings`

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

These URLs are 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:

- `https://[hostname]:[HTTPS port]/webui/servlet/admin`
- `https://[hostname].[domain name]:[HTTPS port]/webui/servlet/admin`
- `http://[hostname]:[HTTP port]/webui/servlet/admin`
- `http://[hostname].[domain name]:[HTTP port]/webui/servlet/admin`

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 to change this initial password.

URL for mobile service access to LN

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

```
https://[hostname].[domain name]:[HTTPS port]/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.
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.

Option	Description
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.

Infor LN menu

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

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.
Mobile Service	Turn the Mobile Service on or off.

Infor LN Help menu

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

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:

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

Post-installation instructions

3

The Infor Enterprise Server Installer creates the LN UI deployment as a fresh installation, or as an upgrade from Web UI. The following sections describe the administration steps that you must perform after the installation.

Prerequisite

For both supported post-installation scenarios, LN must have been configured to allow Single Sign On access from LN UI. For details, see "Configuring SSO in LN" on page 35. If required, for details on how to first create an environment with backend authentication, see "Creating an environment for LN connection (Backend Authentication)" on page 20.

Post-installation instructions after a fresh installation

Use the LN UI Administration Webapp to create the required configuration items. To allow LN UI access to an LN system through Infor Ming.le, you must complete at least these steps:

1. Create environment for LN connection (Single Sign On). See "Creating an environment for LN connection (Single Sign On)" on page 19.
2. Configure (secure) login and authentication. See "Configuring login and authentication (HTTP)" on page 20 or "Tomcat: Configuring secure login and authentication (HTTPS)" on page 21.
3. Create Logical ID Mapping. See "Creating a Logical ID mapping" on page 24.

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

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 one of the following URLs, depending on the configuration of secure communications using HTTPS:

- `http://[hostname].[domain]:[HTTP port]/webui/servlet/fslogin?LogicalId=<Logical ID>`
- `https://[hostname].[domain]:[HTTPS port]/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.

Online Help

4

You can configure LN UI to show online help of the Enterprise Server Tools and LN application sessions. LN UI also contains online help for the LN UI Administration Webapp and the user settings Webapp. These help packages are available:

- ln: Infor LN application session help
- es: Infor Enterprise Server Tools session help
- lnuisettings: LN UI user settings help
- lnuiadmin: LN UI Administration Webapp help

The help content of the 'lnuisettings' and 'lnuiadmin' packages is always available as part of the LN UI deployment.

The help content in DHTML format of the 'ln' and 'es' packages can be installed using the LN UI Administration Webapp. See "Installing online help packages" on page 24.

You can define language and version fallbacks for the various installed 'ln' and 'es' packages. See the online help of the options in the **Infor LN Help** menu in the LN UI Administration Webapp.

Troubleshooting

5

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 inspection.

Common tasks

6

This section describes common LN UI Administration tasks. For detailed information, see the online help of the respective menu items.

This section assumes that LN UI was installed successfully and that the LN UI Administration Webapp is accessible by browsing to a URL similar to:

```
http://[hostname].[domain name]:[HTTP port]/webui/servlet/admin
```

When prompted, specify **Administrator** as the user name. The default password is **webui**, however this may have been changed during installation. We strongly recommend that you change the default password.

Creating an environment for LN connection (Single Sign On)

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 7.
- 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.

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**.

Creating an environment for LN connection (Backend Authentication)

Use this task to configure an environment that allows to connect to LN using backend authentication.

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** or **rexec** 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:

   ```
   http://[hostname].[domain]:[HTTP port]/webui/servlet/login
   ```

   The user should be prompted for the LN username and password, after which LN UI should start.

Configuring login and authentication (HTTP)

Use this task to integrate LN UI with the user authentication provider. The browser client and LN UI will communicate using HTTP.

Complete these steps:

1. Start the LN UI Administration Webapp and select **Infor LN UI Administration > Login Configuration**.
2. Select **Integrated Windows Authentication** or **Infor Federation Services** as the desired authentication type.
3. 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.
4. Save the changes and restart the Tomcat web server.
5. To verify that the configuration was completed successfully, browse to a URL similar to:

   ```
   http://[hostname].[domain]:[HTTP port]/webui/servlet/fslogin
   ```

   LN UI should start.

Tomcat: Configuring secure login and authentication (HTTPS)

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

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. Do not restart the web server now.
8. Again select **Infor LN UI Administration > Login Configuration**.
9. Select **Integrated Windows Authentication** or **Infor Federation Services** as the desired authentication type.
10. 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.
11. Save the changes and restart the web server.
12. To verify that the configuration was completed successfully, browse to a URL similar to:

    ```
    https://[hostname].[domain]:[HTTPS port]/webui/servlet/fslogin
    ```

    LN UI should start.
13. 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 23.

JBoss: Configuring secure login and authentication (HTTPS)

When 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 will communicate using HTTPS.

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 Select **Profile > 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 Navigate to **Profile > Web > Servlet/HTTP** and select 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**.

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 **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://[hostname].[domain]:[HTTPS port]/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 23.

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 DER encoded Base-64 format.

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.

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 uploaded files must be in DER encoded Base-64 format.

6 Restart the Tomcat web server.

7 To verify that the configuration was completed successfully, browse to a URL with this format:

```
https://[hostname].[domain]:[HTTPS port]/webui/servlet/fslogin
```

LN UI 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.

Creating a Logical ID mapping

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. Save the changes.

3 To verify that the configuration was completed successfully, browse to a URL similar to one of the URLs below. Replace [Logical ID] with the value of the configured Logical ID.

   ```
   http://[hostname].[domain]:[HTTP port]/webui/servlet/fslogin?LogicalId=
   [Logical ID]
   ```

   ```
   https://[hostname].[domain]:[HTTPS port]/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 Plug-in.

Installing online help packages

To install an online help package:

1 Obtain the .zip file of the 'ln' 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.

Exchange Synchronizer

7

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

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.

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)" on page 27
- "Enabling the impersonation (Exchange Server 2007)" in the *Infor Enterprise Server Web UI - Installation and Configuration Guide (U8715)*

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)

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

See 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.

Workbenches

8

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 (U9858)*.

Mobile service

9

LN UI provides a mobile service, allowing mobile clients to access LN.

Configuring the mobile service

To enable or disable the mobile service:

1. Start the LN UI Administration Webapp.
2. Select **Infor LN > Mobile Service** and click the **Configuration** tab.

   The mobile service URL is displayed.
3. Select or clear the **Enable Mobile Service** check box, as desired.
4. Save the changes.

Testing the mobile service

To test the mobile service connection:

1. Start the LN UI Administration Webapp.
2. Select **Infor LN > Mobile Service** and click the **Test** tab.
3. In the **Environment Name** field, select the environment that mobile clients will use to access the mobile 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.

Advanced topics

10

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

Configuring the PKCS#12 HTTPS keystore type

By default, the LN UI Administration Webapp supports Java's standard keystore format when creating the HTTPS keystore for secure communications in the browser client.

See "Common tasks" on page 19.

Alternatively, if the web server supports it, you can use the PKCS#12 keystore format.

> ⚠ **Caution:** If LN UI is configured for Infor Federation Services (IFS) SSO, Java's standard keystore format (JKS) MUST be used and the PKCS#12 format is not valid for the HTTPS keystore.

Note the following if you use the PKCS#12 keystore format:

- You must manually create the initial contents of the PKCS#12 keystore file.
- The PKCS#12 keystore file must have a `.p12` extension.
- If the Tomcat web server is used, you must manually configure the HTTPS connector (identified by SSLEnabled="true") in the `conf/server.xml` file for the PKCS#12 keystore type.

  For detailed instructions, see http://tomcat.apache.org/tomcat-7.0-doc/config/http.html#SSL_Support
  .

Configuring SSO in LN

A

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

The required 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 needed because the security domain may have identified the end user with an account name that is different than the LN account. In addition, the system account which will later be used to run the bshell must be derived.
- Permission checking is needed because the mapping information is not sufficiently secured.
- Impersonation is about the LN operating system account which will run the bshell binaries on behalf of the end user.

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

End User	The person using LN
Application User	An LN account for an end user
System User	The operating system account which runs the bshell on behalf of the end user

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

SSO Related Procedures

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

Prerequisites

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

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

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

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

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

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 session SSO Parameters (ttams0100m000).

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 (ttams1100s000)

To SSO enable LN users:

1 Select **User Management > General User Data**.

2 Start the User Data (ttaad2500m000) session.

3 Open the User Data details for the Application user which needs SSO access.

4 Specify the SSO User (pre-Windows 2000 login name or User Principal Name) in the **Infor Security User** field.

5 Repeat steps 3 and 4 for other Application Users that need SSO access.

6 Save and Close the User Data (ttams1100s000) session. You will return to the Main User Data (ttaad1100m000) session.

7 On the appropriate menu in the User Data (ttaad2500m000) session, select **Convert Changes To Runtime DD**. The Convert Changes to Runtime DD (ttams2200m000) session appears.

8 Enter the required data in the Convert Changes to Runtime DD (ttams2200m000) session. See the session help for details.

9 Click **Convert** to convert the user data to an encoded s[SSO User] file in the directory: `$BSE/lib/user/sso/`

Create/Update Permissions file

1 Ensure that a directory with the name `security` exists within the BSE directory of the ES Logic Service. You can find the BSE path under **Start > Administrative Tools > Services > ES Logic Services > Properties**.

2 Assume the path to the ES Logic Service executable is: `C:\Infor\ERPLN\commonx64\bin\rexecd.exe`

Then the path of the directory security must be:

`C:\Infor\ERPLN\commonx64\security`

3 Use the Windows Domain and Generic System User as specified in the SSO parameters session, to create file `sso_permissions.xml` as shown in the example (replace ‘domain’ and ‘username’ with the actual values).

4. Save file `sso_permissions.xml` in directory `security`.
5. To avoid unauthorized changes or deletions, ensure that file `sso_permissions.xml` and the containing directories are sufficiently secure.

Example

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

Restart ES Logic Service

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

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

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

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

   The meaning of these two arguments is:

   - -d for logging additional information. An event will be logged in the Event Viewer to announce the file name to which the additional information will be logged.
   - -ssl <ssl properties file> for specifying a non-default SSL properties file. Prefix the file name with an @-sign to indicate that it must not be interpreted relative to the BSE directory of the ES Logic Service. For example use: `-ssl @local_file` or `-ssl @/etc/absolute_path`.

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

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

SSO parameters		
Field	**Usage**	**Remarks**
Windows Domain	Impersonation: System User domain	

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

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

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

Configuring SSO in LN (non Windows)

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

Update session SSO Parameters (ttams0100m000)

To activate Single Sign On:

1. Log on to LN using the LN UI.
2. Select **LN Tools > Application Configuration > Parameters**.
3. Start session SSO Parameters (ttams0100m000).
4. Select the **SSO Active** check box.
5. Specify this information:
    - In the **Generic System User** field specify a username.
    - Select the **Overrule System User Allowed** check box.
6. Click **Dump** to place the information in the directory:

    ```
    $BSE/lib/sso_config
    ```

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

Update session User Data (ttams1100s000)

To SSO enable LN users:

1 Select **User Management > General User Data**.

2 Start the User Data (ttaad2500m000) session.

3 Open the User Data details for the Application user which needs SSO access.

4 Specify the SSO User (pre-Windows 2000 login name or User Principal Name) in the **Infor Security User** field.

5 Repeat steps 3 and 4 for other Application Users that need SSO access.

6 Save and Close the User Data (ttams1100s000) session. You will return to the Main User Data (ttaad1100m000) session.

7 On the appropriate menu in the User Data (ttaad2500m000) session, click **Convert Changes To Runtime DD**. The Convert Changes to Runtime DD (ttams2200m000) session appears.

8 Specify the required data in the Convert Changes to Runtime DD (ttams2200m000) session. See the session help for details.

9 Click **Convert** to convert the user data to an encoded s[SSO User] file in the directory:

`$BSE/lib/user/sso/`

Create/Update Permissions file

To create/update the permissions file:

1 Ensure that a directory with the name `security` exists within the BSE directory of the BaanLogin daemon (`$BSE/security`).

2 Create the file `sso_permissions.xml` as shown in the example section.

This example `sso_permissions.xml` file assumes that all involved combinations of Application User and SSO User are pairs of identical strings. If the strings within one or more pairs are different, see "Advanced topics" on page 42.

3 Save file `sso_permissions.xml` in directory security.

4 To avoid unauthorized changes or deletions, ensure that file `sso_permissions.xml` and the containing directories are sufficiently secure.

Example

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

Activate Changes

To activate changes:

1. Stop the BaanLogin daemon with this command:

   ```
   blogind6.2 -k
   ```

2. Start the BaanLogin daemon with this command:

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

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

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

   Prefix the file name with 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 will be sent to the file `${BSE}/log/blogin.log`.

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

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

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

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

Advanced topics

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

Non-Windows: Using a generic system user

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

To use a generic system user:

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

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

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

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

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

instead of

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

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

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

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

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

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

Windows: Dedicated SSO permission check

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

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

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

Non-Windows: Dedicated SSO permission check

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

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

Integrating Infor Ming.le^{TM} and LN

B

This appendix 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 these prerequisites are met:

- LN UI has been deployed successfully.
- The applicable post-installation procedures have been performed. See "Post-installation instructions" on page 13.

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 "Installation Instructions: Configuring Infor Workspace" 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 Applicaton Views** list, select **Infor Applicaton 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:

a Select **Manage > Master Data** . The Master Data types are listed.

b Select the "Security Role" Master Data type and click **Details** to display the Security Role details.

c In the left pane, click **New**.

d In the right pane, specify this information:

Node name
Specify **LN**.

Description
Specify a description for the new role.

e In the Users in this Instance pane, click **New** to start the Add Users dialog box.

f 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 (U9663)*.

g Click **Submit**.

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

Complete these steps:

a 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**.

Deployment on WebSphere Express v8.5

C

This procedure describes how to deploy LN UIon IBM WebSphere Express v8.5.

Before you begin the deployment of LN UI, consult the IBM WebSphere v8.5 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 v8.5 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 post-installation instructions. See "Post-installation instructions" on page 13.

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 directily 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. 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.