Infor LN UI Administration Guide (Cloud and On-premises)

Publication Information

Release: Infor LN UI 2022.08
Publication Date: June 22, 2022
Document code: lnui_2022.08_lnuiag__en-us

Contents

About this guide

This document describes the Infor LN UI Administration Webapp.

Intended audience

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

Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

The latest documentation is available from docs.infor.com or from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

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

Chapter 1: Prerequisites

This section describes the prerequisites for successful installation and operation of Infor LN UI.

Compatibility information

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

Server requirements

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

Product	Supported Version
Operating System	Microsoft Windows Server 2016, 2019, 2022
	SUSE Linux Enterprise Server (SLES) 12, 15 See note 1.
	Red Hat Enterprise Linux (RHEL) 7, 8 See note 1.
Java Runtime Environment	Java 8 SE or Java 8 SE compatible See note 2.

Product	Supported Version
Web Server	Minimum supported servlet specification: 3.0
	Apache Tomcat 8.5.x
	Apache Tomcat 9.0.x
	JBoss EAP 6.3.x
	IBM WebSphere Application Server v8.5.5.x and IBM WebSphere Application Server Network Deployment v8.5.5.x See note 3. For installation instructions, see Deployment on WebSphere AS v8.5.5 on page 53.
	Oracle WebLogic Server 14.1.1.x See note 3. For installation instructions, see Deployment on Oracle WebLogic Server on page 55.

Note:

1. Single Sign On using Integrated Windows Authentication is only supported for Windows-based UI servers.
2. LN UI is tested and certified with Amazon Corretto 8.
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.

Client requirements

LN UI is supported only for use on desktop client computers.

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**. See also "Screen resolution" in the *Infor Ming.le User Guide*.

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

Client	Supported browsers
Windows clients	Google Chrome - latest version
	Microsoft Edge (Chromium-based) - latest version
	Mozilla Firefox - latest version
Mac OS clients	Safari browser - latest version
	Google Chrome - latest version

Note: LN UI does not support Silverlight-based Workbench sessions when using Chrome or the Safari browser.

Chapter 2: Overview

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.

Security

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

For detailed information about HTTP Strict Transport Security (HSTS), see Infor Support Portal KB 1893718.

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.

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.

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 33.

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.
IFS Attribute/Provisioning Service	Determine how LN UI supports the communication for centralized user management between LN and Infor Federation Services (IFS).
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.
Clickjacking Prevention	Enable or disable the defense to 'clickjacking' security attacks.

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.

Option	Description
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.
Exchange Synchronizer	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 Parameters	Specify whether online help of LN application and Tools sessions is served from https://docs.infor.com/ or from archives that are uploaded to the LN UI server.
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
- An Apache Tomcat web server
- Use of an HTTPS connector
- Infor Operating Service with claims-based authentication
- LN UI used as an Infor Ming.le integrated application

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 (Infor OS 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 SSO (Infor Operating Service)
  - 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 Apache Tomcat, read the appropriate section from the Other web servers chapter instead of the Configuring the Tomcat web server chapter.

Chapter 3: 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 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 64.

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**.

Chapter 4: Configuring the Tomcat web server

Use this task to configure the web server to use secure communications.

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 the Java Runtime Environment
- 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.

Note: The following steps ensure that an HTTPS Keystore is configured with only a self-signed certificate. When completed, you must replace this self-signed certificate with a CA-signed certificate.

See Installing or renewing a CA-signed HTTPS certificate on page 18.

1. Start the LN UI Administration Webapp.
2. Select **Infor LN UI Administration > HTTPS Keystore**.
3. If required, click **Edit** to change the **Subject Details** fields. Specify the desired values for fields such as **Organizational Unit** and **Organization**, which will be used for the self-signed certificate.

4. Click **Save and Close** 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 **Generate CSR** 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 **Import CA Reply** 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 **Import Trusted Certificate** 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 **Import CA Reply** 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. Establish the basic HTTPS configuration using a self-signed keystore. To do this, complete the steps under *Configuring Tomcat HTTPS connector*.
2. Ensure that the PKCS#12 keystore file has a `.pfx` or `.p12` extension.
3. 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. Locate the `Connector` XML element with `SSLEnabled="true"`.
   b. Replace the value of `certificateKeystoreFile` by the full path of the PKCS#12 keystore file.
   c. Replace the value of `certificateKeystorePassword` by the password of the PKCS#12 keystore file.
   d. Save the file and exit the text editor.
4. Restart the Tomcat web server to apply the changes.
5. 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.
6. Use the padlock of the browser's address bar to inspect the certificate information and verify that the expected CA-signed certificate is displayed.

Chapter 5: Configuring SSO (Infor Operating Service)

Use this task to configure LN UI for Single Sign On (SSO) using Infor STS (Security Token Service) from Infor OS.

This task has these prerequisites:

- During Infor OS installation, Infor STS is selected on the **SAML Configuration** page.
- The post-installation steps of Infor OS with Infor STS are completed. See “Post-installation of Infor OS with Infor STS” in the *Infor Operating Service Installation Guide*.
- The InforPlatformBackend site is bound to an HTTP port. See "Enabling HTTP support for IFS Services" in the *Infor Operating Service Installation Guide*.

Infor STS facilitates and provides standards-based SSO services to users of Infor business applications such as LN. Infor STS provides capabilities for the federation with a third-party Identity Provider that supports SAML or direct LDAP authentication.

Binding LN UI to STS

Note: The instructions for binding LN UI to STS 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 STS:

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 STS (IFS)`**.
4. Ensure that the **Application URL** field has the proper value. Click **Set to Default** to generate a value which is usually sufficient. 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 the **Infor STS (IFS)** tab and specify this information:

   Configuration Web Service
   Specify the Infor OS configuration web service URL. You can derive this URL from the **InternalUrl** field that is mentioned in Infor OS Manager under **Services** for **Service Name: Configuration Service**. This URL must be in this format:
   `https://<Infor OS hostname>:<port>/IFSServices/ConfigurationService.svc`

6 Click **STS (IFS) Configuration - Generate** to register LN UI in STS and create the required LN UI configuration.

Take note of the reported Relying Party Identifier.

7 Save the changes and restart the web server.

Creating the Service Provider connection

To create a Service Provider (SP) connection related to LN UI in Infor STS , use the Infor OS Manager.

1 Log in to Infor OS Manager.
2 Select **Applications** and navigate to the row with the expected relying party identifier.
3 Click the download icon. Then, click **Create SP Connection** and confirm when prompted.

When completed, Infor OS Manager indicates that the SP connection was created successfully.

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.

Troubleshooting

Error calling web service: Could not get IDP metadata XML from IFS server

When you use the LN UI Administration Webapp to generate the IFS configuration, this error message is displayed:

```
Error calling web service: Could not get IDP metadata XML from IFS server
```

Cause:

The AD/FS metadata service is disabled.

Solution:

On the AD/FS server, select **Administrative Tools > AD FS Management** and navigate to **AD FS > Service > Endpoints**. Ensure that the metadata endpoint with this URL path is enabled:

```
/FederationMetadata/2007/06/FederationMetadata.xml
```

Chapter 6: Creating a Logical ID mapping

Use this task 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.

Chapter 7: Integrating Infor Ming.le - LN application (Infor OS version)

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
LN - B61U13stnd	10.4.1.1
LN - B61U14stnd	10.4.2
LN - 10.4.2.1	10.4.2.1

Infor Ming.le application name	LN application version
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 that are 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**.

Note: The **Message Name** field is case-sensitive. Ensure that only the B and C in **`inforBusinessContext`** are uppercase. All other characters must be lowercase.

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.

Chapter 8: Installing online help packages

Use this task 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.

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.

Chapter 9: Workbenches

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*.

Chapter 10: LN Client Service

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

If LN UI is installed on premises, client applications employ basic authentication with user name and password to connect to the LN Client Service. Alternatively, if LN UI is installed in the cloud or if the Infor OS ION API gateway is installed, client applications use OAuth 2.0 to authenticate with the ION API gateway. At the ION API gateway, an available API must be configured for access to the LN Client Service. See the *Infor ION API Administration Guide*.

Configuring the LN Client Service

Importing the WS-Trust HTTPS certificate

This step is only applicable if these conditions are met:

1. On the **Login Configuration** page in the LN UI Administration Webapp, the **`Infor STS (IFS)`** authentication type is selected.
2. The LN Client Service is configured for the **`Basic Authentication`** authentication type.
3. Client applications create the connection through a **`BaanLogin SSL`** environment.

Communication between LN UI and the WS-Trust endpoint is based on HTTPS. Therefore, the LN UI trust store must contain the WS-Trust HTTPS root certificate.

To import the WS-Trust HTTPS root certificate into the LN UI trust store:

1. Start the LN UI Administration Webapp.
2. Obtain the WS-Trust URL from the **Infor STS (IFS)** tab on the **Login Configuration** page.
3. Open a new browser tab and navigate to the relevant address:
   - If the WS-Trust URL starts with "`https://server:port/adfs/services`", then navigate to `https://server:port/adfs/ls`.
   - If the WS-Trust URL starts with "`https://server:port/inforsts/wstrust`", then navigate to `https://server:port/inforsts`.

   Replace *server* and *port* by the actual server name and port number.

4 Open the browser's dialog box that shows the certificates. For example, use the padlock of the address bar.
5 Navigate the certification path. Select the root certificate and view its details.
6 Click **Copy to File** or a similar button to export the details of the root certificate. In the export dialog box, select the Base-64 encoded X.509 (.CER) export file format .
7 Select **Infor LN > SSL Trust store**.
8 Click **Import Certificate** and import the certificate from the file that was exported in step 6.

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.

Chapter 11: Configuring stand-alone-mode

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

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

- Single Sign On through Infor Federation Services

  To use this authentication mechanism, ensure that you have performed all tasks up to and including Configuring SSO (Infor Operating Service) on page 20.

  You can now continue with the steps that are described in Configuring in-context applications on page 32.
- Single Sign On through 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 16
  - Configuring LN UI for Integrated Windows Authentication on page 31
  - Configuring in-context applications on page 32
- Backend Authentication

  To use this authentication mechanism, perform the tasks described in these sections:
  - Configuring LN UI for Backend Authentication on page 32
  - Creating an environment for LN connection (LN Server Authentication) on page 32

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 Auhentication:

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:

- 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 Enterprise Modeler authorizations, defined on the LN server, for this user are disregarded.

If the extended URL starts with `https://<server>:<port>/webui/servlet/fslogin`, then LN UI is displayed in a minimal browser frame. If the extended URL starts with `https://<server>:<port>/webui/servlet/standalone`, then the browser frame includes a shell with a sign-out button and a sidebar for in-context apps. Replace *<server>* and *<port>* as appropriate.

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	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, these attributes are required to select a specific record:
	• 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. The value of the session index corresponds to one of the views that can be selected from one of these menus in the bookmarked session:
	  • The **Search** button's menu
	  • The **Views > Sort by** menu
	  Which of these menus is available depends on LN Tools parameter settings.
	• startupwhere - Query information about the record to be displayed. The attribute value must be properly percent-encoded according to RFC3986.

startupSession	Similar to startupform, but the landing page and navigation menu are displayed.

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&startup
form=ttaad2500m000&startupwhere=(ttaad200.user=%27jdoe%27)
```

Starting LN UI with an Enterprise Modeler process

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

The user that opens this URL must be an Enterprise Modeler user and must be authorized to access this specific Enterprise Modeler process.

The URL must always start with `https://<server>:<port>/webui/servlet/fslogin`. Replace `<server>` and `<port>` as appropriate.

This table shows the attributes that you can use as parameters to start a specific Enterprise Modeler 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" Enterprise Modeler role and must be authorized for the "DCO007" Enterprise Modeler process.

Chapter 12: Exchange Synchronizer

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

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

Prerequisites

Exchange Synchronizer supports these versions of on-premises Microsoft Exchange Server:

- Microsoft Exchange 2007 with SP1 or a later SP
- Microsoft Exchange 2010
- Microsoft Exchange 2013
- Microsoft Exchange 2016
- Microsoft Exchange 2019

Exchange Synchronizer supports cloud-based Exchange Online.

Exchange Server must be enabled for Exchange Web Services using basic authentication.

Exchange Online must be enabled for Exchange Web Services using OAuth 2.0 authentication.

When using Exchange Online, push synchronization can only be supported if the LN UI endpoint URL is exposed to the internet. Push synchronization requires Exchange Online to access the notification service of Exchange Synchronizer across the internet.

Caution: If the LN UI endpoint URL is exposed to the internet, it is the customer's responsibility to ensure the desired level of application security. As a minimum, secure communications using HTTPS should be used. Additionally, a perimeter network or DMZ with, for example, reverse proxy may be used.

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 > Exchange Synchronizer**.

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.

Configuration for on-premises Exchange Server

This section describes how to configure on-premises Exchange Server.

Basic authentication

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

- To enable Basic Authentication on Exchange Server 2007 and 2010:
  a Run this Exchange command:

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

  There is no GUI equivalent to set the Authentication.
  b To confirm that Basic Authentication is enabled on the Exchange web services, run this command:

  ```
  Get-WebServicesVirtualDirectory |FL
  ```

  c Verify that the BasicAuthentication parameter has the value 'True'.
  See http://technet.microsoft.com/en-us/library/aa997233(EXCHG.80).aspx.
- To enable Basic Authentication on Exchange Server 2013 and later:
  a Open the Exchange admin center and select **servers > virtual directories**.
  b Edit the **EWS (Default Web Site)** entry and ensure that Basic authentication is selected.
  c Save the changes.

Impersonation

Impersonation must be allowed and configured on the Exchange Server.

See these sections:

- Enabling the impersonation - Exchange Server 2010 and later on page 37
- "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 later

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

For Exchange Server 2010 and later, see https://technet.microsoft.com/nl-nl/library/dd297943(v=exchg.141).aspx for the description of permissions.

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

1. For example, to enable impersonation with user 'syncuser' for allOpen the Exchange Management Shell.
2. Run this command:

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

Configuration for cloud-enabled Exchange Online

This section describes the configuration steps to use Synchronizer with Exchange Online

App registration

To enable OAuth 2.0 authentication, Synchronizer must be registered as a Microsoft Azure app for the tenant.

To complete the app registration:

1. Use the browser to navigate to the Microsoft Azure portal at https://portal.azure.com/.
2. Select **App registrations** and click **+ New registration**.
3. Specify this information:

   Name
   Specify a suitable user-facing display name, such as **`LN Synchronizer`**.

Supported account type
Select **`Accounts in this organizational directory only`**.

4 Under **Certificates & secrets**, create a client secret and copy the value for later use.

5 Under **API permissions**, add this application permission for the Exchange API: **`full_access_as_app`**

6 Under **API permissions**, ensure that the **`full_access_as_app`** permission is granted for the tenant. This requires admin consent.

After finishing these steps, navigate to the app's overview page and take note of **Directory (tenant) ID** and **Application (client) ID**. These items, and the client secret that was obtained under step 4, are required when you configure Exchange Synchronizer in LN.

Configuring the HTTPS certificate in LN

This section is only applicable if these settings are used in the **MS Exchange Synchronization Settings (ttaad2140m000)** session:

- The **Enable push synchronization** check box is selected.
- The URL in the **LN UI Server URL** field starts with **`https://`**.

When sending messages to the Exchange Synchronizer during push synchronization, the LN server must have access to the HTTPS certificate of LN UI. Therefore, you must configure this certificate in LN. To perform this configuration, you must be familiar with the "HTTPS" chapter in the *Infor Enterprise Server - Administration Guide*.

1 Obtain the HTTPS certificate of the LN UI web server:
   a Use the browser to navigate to the LN UI endpoint using HTTPS, such as `https://<lnui-server>.<domain>.com:8443/webui/servlet/admin`.
   b Use the browser's dialog box to view the certification path. For example, if you use Chrome, select **More Tools > Developer Tools**. Click the **Security** tab and click **View certificate**.
   c View the details of the root certificate.
   d Click **Copy to File** and export the root certificate to a file. Use the **`DER encoded binary X.509 (.CER)`** export file format.
   e Convert the `.CER` file to a file in `PEM` format. For details, see "How to convert a number of formats to PEM format" in the "HTTPS" chapter in the *Infor Enterprise Server - Administration Guide*.

2 Place the server certificate in `PEM` format in the `$BSE/security/certs/server` folder on the LN server.

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 affected. In LN you can have multisite 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 Optionally, enable contact synchronization. To do so, select the **Synchronize Contacts** check box in the **COM Parameters (tccom0000s000)** session. If this check box is selected, you must also specify ISO codes in the **Countries (tcmcs0510m000)** and **Languages (tcmcs0146m000)** sessions.

4 Optionally, enable calendar synchronization. To do so, select the **Synchronize Activities** check box in the **COM Parameters (tccom0000s000)** session.

5 Start the **MS Exchange Synchronization Settings (ttaad2140m000)** session and define a configuration.
   - If Exchange Server is used, select **`Basic Authentication`** and specify the impersonation user in the **User**, **Password**, and **Domain** fields. In the **User** field, you must specify the SAM account name.

     Ensure that the **MS Exchange URL** field has a value similar to `https://<server>.<domain>:<port>/EWS/Exchange.asmx`.
   - If Exchange Online is used, select OAuth 2.0 and specify this information:

     MS Exchange URL
     Specify https://outlook.office365.com/ews/exchange.asmx.

     Authentication URL
     Specify https://login.microsoftonline.com.

     Azure Tenant
     Use **directory (tenant) ID** from the Azure app registration.

     Client ID
     Use **application (client) ID** from the Azure app registration

     Client Secret
     Use client secret from the Azure app registration.

   - We recommend that you specify a value of 15 minutes or higher in the **Pull Interval** fields for contact synchronization and calendar synchronization.

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, these conditions must be met 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 this condition is met: 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 uses HTTPS for secure access to Exchange Server or Exchange Online. If Exchange Server is used, you must configure LN UI with the SSL certificate of the Client Access Server.

Synchronization may be enabled for several hundreds of users. In that case, you must configure the Java Runtime Environment (JRE) that is used by the Tomcat web server with sufficient memory.

Configuring LN UI with the SSL certificate of the Client Access Server

Skip this step if Exchange Online is used.

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.

Configuring memory usage

To configure the maximum memory pool size for the JRE, when the Tomcat web server is used:

1. Locate the Tomcat monitor application on the file system of the web server.

   For example, the application may be stored in this directory: `C:\Infor\ESE\apache-tomcat-8.0.21\bin`. See https://tomcat.apache.org/tomcat-8.0-doc/windows-service-howto.html.
2. Run the Tomcat monitor application as an administrator.
3. Click the **Java** tab and specify this information:

   Maximum memory pool
   Specify a value in MB. For example, 6144 for 700 users or more.
4. Confirm the changes and exit the Tomcat monitor application.
5. Restart the Tomcat service.

Troubleshooting the Exchange Synchronizer

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 this synchronizer log file: `lnui-synchronizer-<date>.log`. To find the location of this file, start the LN UI Administration Webapp and select **Infor LN UI Administration > Logging**.

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.
- Incorrect credentials of MS Exchange impersonation account.

Solution:

1. In Active Directory, verify the configuration of the impersonation user.
2. 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.
3. If any changes were made, restart the Synchronizer.

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 email 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 email address configured for each activated Exchange Synchronizer user corresponds with the MS Exchange email address. The email 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 email address in the attendee's employee data does not correspond with the email address that is configured for the Exchange Synchronizer user.

Solution: for any employee for which appointments may require 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 email address in this session corresponds with the Exchange Synchronizer user's email address in the **MS Exchange Synchronization Users (ttaad2141m000)** session.

   The email 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 email address of Exchange Synchronizer user(s)

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

The server sent HTTP status code 401: Unauthorized

This error message is displayed:

```
com.sun.xml.ws.client.ClientTransportException: The server sent HTTP status code 401: Unauthorized
```

Cause: The on-premises Exchange server is not enabled for basic authentication.

Solution: Enable basic authentication.

See Basic authentication on page 36.

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.SSLHandsha
keException: sun.security.validator.ValidatorException: PKIX path building failed: sun.securi
ty.provider.certpath.SunCertPathBuilderException: unable to find valid certification path to re
quested target
```

Cause: incorrect 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 with the SSL certificate of the Client Access Server on page 40.

Contact or calendar events are not synchronized

Cause:

1. Users have not been activated for synchronization.
2. Calendar category mismatch between Synchronizer and MS Exchange.

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 email 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.

LN UI and synchronizer become unresponsive

Synchronizer initialization appears correct but LN UI and synchronizer become unresponsive after some time. This error message may be recorded in one of the log files of the web server:

```
java.lang.OutOfMemoryError: GC overhead limit exceeded
```

Cause: the Java Runtime Environment that is used by the web server has an insufficient size of the memory pool.

Solution: increase the maximum memory pool size.

See Configuring memory usage on page 40.

Calendar events are synchronized at pull interval but the push mechanism is not working

Cause: The HTTPS certificate of the LN UI server is not configured on the LN server.

Solution: Ensure that the HTTPS certificate is configured in LN.

See Configuring the HTTPS certificate in LN on page 38.

To verify the configuration of the LN server:

1. Log on to LN.
2. Select **Options > Debug bshell**. The **Run time debugging of bshell (ttstpbshdebug)** session starts.
3. On the **Bshell Debug Levels** tab, select the **Debug cURL** check box.
4. On the **General Options** tab, select the **Add Time stamps** check box. Then, on the toolbar, click **Start Trace**. Do not close the **Run time debugging of bshell (ttstpbshdebug)** session.
5. Start the **Activities (tccom6100m000)** session. Create or change an appointment and save the changes. Ensure that the appointment's **Synchronize** check box is selected.
6. Return to the **Run time debugging of bshell (ttstpbshdebug)** session. On the toolbar, click **Stop Trace** and **Download File**.
7. Download the file and inspect the text content. See the examples:

   Example of bad or missing HTTPS certificate configuration on the LN server:

```
C:0000044:2018-06-21[14:00:12.473]:::(00024):cURL *   Trying 1.2.3.4...
C:0000045:2018-06-21[14:00:12.473]:::(00024):cURL * TCP_NODELAY set
C:0000046:2018-06-21[14:00:12.474]:::(00024):cURL * Connected to server.domain.com (1.2.3.4)
port 8443 (#3)
C:0000047:2018-06-21[14:00:12.474]:::(00024):cURL * ALPN, offering http/1.1
C:0000048:2018-06-21[14:00:12.474]:::(00024):cURL * successfully set certificate verify locations:
C:0000049:2018-06-21[14:00:12.474]:::(00024):cURL *   CAfile: none
C:0000050:2018-06-21[14:00:12.474]:::(00024):cURL *   CApath:
/prod/toolsdev/Latest/bse/security/certs/server
C:0000051:2018-06-21[14:00:12.474]:::(00024):cURL * TLSv1.2 (OUT), TLS handshake, Client hello
 (1):
C:0000052:2018-06-21[14:00:12.476]:::(00024):cURL * TLSv1.2 (IN), TLS handshake, Server hello
(2):
C:0000053:2018-06-21[14:00:12.476]:::(00024):cURL * TLSv1.2 (IN), TLS handshake, Certificate
(11):
C:0000054:2018-06-21[14:00:12.477]:::(00024):cURL * TLSv1.2 (OUT), TLS alert, Server hello (2):
C:0000055:2018-06-21[14:00:12.477]:::(00024):cURL * SSL certificate problem: self signed
certificate
C:0000056:2018-06-21[14:00:12.477]:::(00024):cURL * Closing connection 3
```

   Example of successful HTTPS certificate configuration on the LN server:

```
C:0000058:2018-06-21[14:05:26.861]:::(00027):cURL *   Trying 1.2.3.4...
C:0000059:2018-06-21[14:05:26.861]:::(00027):cURL * TCP_NODELAY set
C:0000060:2018-06-21[14:05:26.861]:::(00027):cURL * Connected to server.domain.com (1.2.3.4)
port 8443 (#4)
C:0000061:2018-06-21[14:05:26.861]:::(00027):cURL * ALPN, offering http/1.1
C:0000062:2018-06-21[14:05:26.861]:::(00027):cURL * successfully set certificate verify locations:
C:0000063:2018-06-21[14:05:26.861]:::(00027):cURL *   CAfile: none
C:0000064:2018-06-21[14:05:26.861]:::(00027):cURL *   CApath:
/prod/toolsdev/Latest/bse/security/certs/server
C:0000065:2018-06-21[14:05:26.862]:::(00027):cURL * TLSv1.2 (OUT), TLS handshake, Client hello
```

```
 (1):
C:0000066:2018-06-21[14:05:26.865]:::(00027):cURL * TLSv1.2 (IN), TLS handshake, Server hello
(2):
C:0000067:2018-06-21[14:05:26.865]:::(00027):cURL * TLSv1.2 (IN), TLS handshake, Certificate
(11):
C:0000068:2018-06-21[14:05:26.866]:::(00027):cURL * TLSv1.2 (IN), TLS handshake, Server key
exchange (12):
C:0000069:2018-06-21[14:05:26.866]:::(00027):cURL * TLSv1.2 (IN), TLS handshake, Server finished
 (14):
C:0000070:2018-06-21[14:05:26.867]:::(00027):cURL * TLSv1.2 (OUT), TLS handshake, Client key
exchange (16):
C:0000071:2018-06-21[14:05:26.867]:::(00027):cURL * TLSv1.2 (OUT), TLS change cipher, Client
hello (1):
C:0000072:2018-06-21[14:05:26.867]:::(00027):cURL * TLSv1.2 (OUT), TLS handshake, Finished (20):
C:0000073:2018-06-21[14:05:26.869]:::(00027):cURL * TLSv1.2 (IN), TLS handshake, Finished (20):
C:0000074:2018-06-21[14:05:26.869]:::(00027):cURL * SSL connection using TLSv1.2 /
ECDHE-RSA-AES128-GCM-SHA256
C:0000075:2018-06-21[14:05:26.869]:::(00027):cURL * ALPN, server did not agree to a protocol
C:0000076:2018-06-21[14:05:26.869]:::(00027):cURL * Server certificate:
C:0000077:2018-06-21[14:05:26.869]:::(00027):cURL *  subject: C=C; ST=ST; L=L; O=O; OU=OU;
CN=server.domain.com
C:0000078:2018-06-21[14:05:26.869]:::(00027):cURL *  start date: May 18 12:47:22 2018 GMT
C:0000079:2018-06-21[14:05:26.869]:::(00027):cURL *  expire date: May 17 12:47:22 2020 GMT
C:0000080:2018-06-21[14:05:26.869]:::(00027):cURL *  subjectAltName: host "server.domain.com"
matched cert's "server.domain.com"
C:0000081:2018-06-21[14:05:26.869]:::(00027):cURL *  issuer: DC=DC; CN=YourCA
C:0000082:2018-06-21[14:05:26.869]:::(00027):cURL *  SSL certificate verify ok.
```

Chapter 13: LN Multi-Tenant Cloud Exchange Synchronizer

This section describes how to configure and administer the LN Multi-Tenant Cloud Exchange Synchronizer, also known as Cloud Exchange Synchronizer.
Note: This section is only applicable for LN Cloud customers. It describes the configuration and administration of an on-premises installation of LN UI. This LN UI installation is exclusively used to synchronize contact and calendar events between LN CE and Microsoft Exchange Online.

The Cloud Exchange Synchronizer synchronizes contacts and calendar events between Microsoft Exchange Online and LN in the multi-tenant cloud.

Similar to the Exchange Synchronizer used for on-premises LN, the Cloud Exchange Synchronizer is an integral component of LN UI. Cloud Exchange Synchronizer is installed and operated on premises, independently of the multi-tenant LN and its corresponding LN UI for transactional access. Cloud Exchange Synchronizer connects to the multi-tenant LN in the cloud through the Infor OS ION API gateway and OAuth 2.0 authorization.

Note: Cloud Exchange Synchronizer does not support push synchronization of calendar information. Only periodic pull retrieval of contact and calendar information is supported!

Prerequisites

Cloud Exchange Synchronizer is only available if these conditions are met:

- The Enterprise Server Installer was used to create an on-premises installation of LN UI.
- During this installation, the **Install LN UI as LN Multi-Tenant Cloud Exchange Synchronizer** option was selected.

Administration of the Cloud Exchange Synchronizer

The Cloud Exchange Synchronizer runs as part of the LN UI that is installed on premises. To start and stop the Cloud Exchange Synchronizer, start the on-premises LN UI Administration Webapp and select **Infor LN > MT Cloud Exchange Synchronizer**.

Configuring Exchange Online and the Cloud Exchange Synchronizer

Before you can start the Cloud Exchange Synchronizer for the first time, you must specify various configuration settings for Exchange Online, LN, and the Cloud Exchange Synchronizer.

1 Configure Exchange Online.

   See Configuration for cloud-enabled Exchange Online on page 37 and apply the described steps.

2 Configure the Cloud Exchange Synchronizer in LN.

   See Configuring the Exchange Synchronizer in LN on page 38, and apply the described steps.

   Note: When you make changes in the **MS Exchange Synchronization Settings (ttaad2140m000)** session:

   - In the **Pull Interval** fields for contact synchronization and calendar synchronization, specify a value of at least 15 minutes.
   - Clear the **Enable push synchronization** check box.

3 Configure the Cloud Exchange Synchronizer.

   See these sections:

   - Configuring ION API gateway connection and LN properties on page 47
   - Configuring memory usage on page 48

Configuring ION API gateway connection and LN properties

You must configure Cloud Exchange Synchronizer with the credentials that are required to connect to the ION API gateway.

1 Obtain a file with credential information:

   a Log on to Infor Ming.le.
   b On the app menu, select **Infor ION API**. The **Available APIs** page is displayed.
   c Click the hamburger icon and select **Authorized Apps**.
   d Click **Add New Application**.
   e Specify the **Name**.
   f In the **Type** field, select **`Backend Service`**.
   g Specify the **Description**.
   h Specify the desired validity period of the **OAuth 2.0 Access Token**.
   i Ensure **Issue Refresh Token** is enabled.
   j In the **Refresh Token Grant Lifetime** field, specify the desired length of time and specify whether the value is in hours or days. If you specify **`0`**, the token never expires.

      Note: The **Refresh Token Grant Lifetime** value must be greater than or equal to the **OAuth 2.0 Access Token** value.

   k Click **Save**.
   l Click **Download Credentials**. A dialog box is displayed. Ensure to select **Create Service Account**. Leave the **User Name** blank and click **Download**. Keep the `.ionapi` file for later use.

2 Configure Cloud Exchange Synchronizer with the ION API gateway credentials:

   a Start the on-premises LN UI Administration Webapp and select **Infor LN > MT Cloud Exchange Synchronizer**.
   b Click **Upload & Import** behind the **Credentials (*.ionapi file)** field. Import the file with the `.ionapi` extension that was generated in the previous steps.
   c Save the changes.

d To verify the OAuth 2.0 authorization at the ION API gateway, click **Test** behind the **Test authorization** field.

3 Configure Cloud Exchange Synchronizer with LN properties:

a Start the on-premises LN UI Administration Webapp and select **Infor LN > MT Cloud Exchange Synchronizer**.

b Under **LN properties**, change the **Company** to the LN company that supports the retrieval of contact and calendar information.

c Save the changes.

Configuring memory usage

Synchronization may be enabled for several hundreds of users. In that case, you must configure the Java Runtime Environment (JRE) that is used by the on-premises Tomcat web server with sufficient memory.

For instructions, see Configuring memory usage on page 40.

Chapter 14: Clickjacking prevention

The configuration of clickjacking prevention provides a defense against certain security attacks.

Read this section 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.
```

Chapter 15: Other web servers

Read this section if you have another web server than Apache Tomcat.

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 18.

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.

To ensure that the Java Heap size for the used application server is large enough:

1 Start the IBM WebSphere Administrative Console.

2 Select **Servers > Server Types > WebSphere application servers > <your server> > Server Infrastructure > Java and Process Management > Process definition**.

3 On the **Process definition Configuration** page, under **Additional Properties**, click Java Virtual Machine.

4 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.

5 At the bottom of the page, click **Apply** and **OK**.

6 On the next page, click Save directly to the master configuration.

7 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 Oracle WebLogic Server

This procedure describes how to deploy LN UI on Oracle WebLogic Server 14.1.1.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 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 preparation procedure:

Abbreviation	Description
<wlInstDir>	The installation directory of WebLogic
<wlDomain>	The WebLogic domain

To prepare the deployment, modify the server's `config.xml` file:

1 Open the `<wlInstDir>\user_projects\domains\<wlDomain>\config\config.xml` file.
2 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.

Deploying LN UI

To deploy LN UI:

1. Start the WebLogic Administrative Console. The default URL is `http://localhost:7001/console`.
2. Navigate to **Domain Structure > Deployments**.
3. Click **Install**.
4. On the **Locate deployment to install and prepare for deployment** page, set the path to the LN UI Enterprise Archive file (`.ear`).
5. Click **Next**. The LN UI Enterprise Archive is loaded.
6. On the **Choose installation type** page, select the **Install this deployment as an application** option.
7. Click **Next**.
8. 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 11.

Chapter 16: Configuring IFS (version 11)

Use this task to configure LN UI, IFS, and AD FS to allow Single Sign On for LN UI through 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 UIapplication.

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 in the "Configuring Applications" section in the *Infor Federation Services Administration Guide* version 11.0.

Chapter 17: Integrating Infor Ming.le (version 11) and LN

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 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*.

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**.

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.ln`.

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.ln`.

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.ln`**.

Application Logical ID
Specify **`lid://infor.ln.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*

Chapter 18: Advanced topics

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

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:
  a Start the LN UI Administration Webapp.
  b 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.

Appendix A: Configuring SSO in LN

This section provides information on the user identity in LN and user access to LN 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 section 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	
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	
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 **Overrule 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 70.

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>
```

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	
Overrule 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>
```