Legal notice
Copyright © 2017 Infor. All rights reserved.

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

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

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

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

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

About this workbook ........................................................................................................... 5
Course overview ................................................................................................................ 6
Course description and agenda .......................................................................................... 8

**Lesson 1: Overview of Infor Lawson System Foundation (LSF)** ........................................... 13
  Infor Lawson System Foundation overview .................................................................. 14
  LSF core components ..................................................................................................... 16
  LSF interfaces overview ................................................................................................. 19
  LSF application overview .............................................................................................. 21
  Check your understanding .............................................................................................. 22

**Lesson 2: Overview of Infor Landmark Technology Runtime** ............................................. 23
  Infor Landmark Technology Runtime overview ............................................................ 24
  Infor Landmark core components .................................................................................. 25
  Infor Landmark interfaces overview .............................................................................. 27
  Infor Landmark data area and application overview ..................................................... 29
  Check your understanding .............................................................................................. 30

**Lesson 3: Overview of Infor Security** ................................................................................. 31
  Infor Security overview ................................................................................................ 32
  Infor Security Services overview .................................................................................. 33
  Infor Lawson System Foundation Security overview ................................................... 36
  Infor Landmark Technology Security overview ........................................................... 42
  Authentication protocols ............................................................................................... 45
  Authorization .................................................................................................................. 51
  Single Sign-on services .................................................................................................. 52
  Check your understanding .............................................................................................. 57

**Lesson 4: Infor Security Services and user administration** .................................................. 58
  LSF user overview ........................................................................................................ 59
  Infor Landmark user overview ...................................................................................... 61
  Provisioning a user in ISS .............................................................................................. 63
  Disable users in ISS ....................................................................................................... 74
  Provisioning actors with secdsm utility ......................................................................... 75
  Provision users with loadusers ...................................................................................... 81
  Check your understanding .............................................................................................. 84

**Lesson 5: Defining access and roles for users** .................................................................... 86
  LSF roles and security classes ...................................................................................... 87
  Infor Landmark-delivered security classes ...................................................................... 88
  Check your understanding .............................................................................................. 91

**Lesson 6: Federation and synchronization** ....................................................................... 92
  Stand-alone vs. federated systems ................................................................................. 93
  Federation procedure overview ...................................................................................... 95
  Federation prerequisites .................................................................................................. 96
  Synchronization ............................................................................................................. 97
  Assigning roles .............................................................................................................. 104
  Troubleshooting synching errors ................................................................................... 105
  Check your understanding .............................................................................................. 110

**Lesson 7: Administering user access to Infor Ming.le Enterprise and Infor Lawson for Infor Ming.le** ............................................................................................................. 111
  Infor Ming.le access ....................................................................................................... 112
  Infor Federation Services (IFS) ...................................................................................... 115
  Infor Ming.le plug-ins ..................................................................................................... 119
  Infor Lawson for Infor Ming.le access ........................................................................... 121
  Infor Lawson for Infor Ming.le roles ............................................................................. 124
  Clear the IOS cache ....................................................................................................... 127
Managing access to bookmarks ............................................................. 130
Check your understanding .................................................................. 133

Lesson 8: Administering user access to Infor Lawson Add-ins for Microsoft Office .............................................. 134
User attributes .................................................................................... 135
Administering users for Infor Lawson Add-ins ...................................... 138
Administering users for Infor Spreadsheet Designer ............................. 141
Check your understanding .................................................................. 143

Lesson 9: User proxies ........................................................................ 144
User proxies ....................................................................................... 145
Check your understanding .................................................................. 148

Lesson 10: Administering user access to Infor Smart Office .................. 149
Infor Smart Office ................................................................................ 150
Check your understanding .................................................................. 154

Lesson 11: Administering user access to LSF mobile applications .......... 155
LSF mobile applications overview ...................................................... 156
Infor System Console .......................................................................... 157
Infor System Console installation overview ......................................... 158
User setup for Infor System Console .................................................. 159
Infor Lawson Mobile Requisitions ...................................................... 161
User setup for Infor Lawson Mobile Requisitions ............................... 162
Check your understanding .................................................................. 165

Lesson 12: Administering user access to Infor Landmark Technology mobile applications ....................................... 166
Infor Landmark mobile applications overview ...................................... 167
Infor Landmark Administrator .............................................................. 168
Configure Infor Landmark Administrator on a mobile device .............. 171
Infor Notifications .............................................................................. 173
Check your understanding .................................................................. 175

Lesson 13: User monitoring and reporting ........................................... 176
User monitoring .................................................................................. 177
Check your understanding .................................................................. 181

Lesson 14: Administering user access to Infor Lawson extension applications ......................................................... 182
Mobile Supply Chain Management ...................................................... 183
Infor Lawson Business Intelligence (LBI) .............................................. 188
Check your understanding .................................................................. 192

Course summary ................................................................................ 193
Course review ..................................................................................... 194

Appendices ......................................................................................... 195
Appendix A: Creating a user in Lawson Security Administrator .............. 196
Appendix B: Disabling and enabling a user in ISA ................................. 198
Appendix C: LifeCycle Manager Client 2.0 .......................................... 200
About this workbook

Welcome to this Infor Education course! We hope you will find this learning experience enjoyable and instructive. This Training Workbook is designed to support the following forms of learning:

- Classroom instructor-led training
- Virtual instructor-led training
- Self-directed learning

This Training Workbook is not intended for use as a product user guide.

Self-directed learning (SDL)

If this course is eligible for self-directed learning, demos and exercises throughout this Training Workbook will be hyperlinked to Demonstration/Let Me Try simulations that allow you to view and practice the execution of the demo or exercise in a simulated training environment.

Activity data

You will be asked to complete some practice exercises during this course. Step-by-step instructions are provided in this guide to assist you with completing the exercises. Where necessary, data columns are included for your reference.

Your instructor will provide more information on systems used in class, including server addresses, login IDs, and passwords.

Symbols used in this workbook

- Hands-on exercise ("Exercise")
- For your reference
- Question
- Instructor demonstration ("Demo")
- Your notes
- Answer
- Can be used for either "Scenario" or "Discussion"
- Note
- Task simulation
Course overview

Reference materials
Infor Landmark Runtime Technology and Infor Lawson System Foundation reference materials are available from the following locations:

- Infor Landmark Runtime Technology Help menu
- Infor Lawson System Foundation Help menu
- Infor Xtreme®

Course duration
24 hours

Learning objectives
Upon completion of this course, you will be able to:

- Recognize the architecture components of Infor® Lawson® System Foundation® 10 (LSF) and Infor Landmark Technology Runtime® 10.
- List the components of the Distributed Security Package.
- Explain the differences between authentication protocol, federation, and Primary Authentication Service (PAS).
- Identify the tools available to administer users in version 10 of both LSF and Infor Landmark.
- Describe how the Infor Security Administration® (ISA) tool provides user provisioning, synchronizing, and federation services in environments where Infor Lawson System Foundation and Infor Landmark Technology Runtime are installed and federated.
- Identify utilities used to mass-load users into LSF and Infor Landmark.
- Clarify how roles are used to provide access to Infor applications.
- Define the process for modifying Infor-delivered roles in Landmark to grant or remove user access.
- Describe the difference between a federated and a stand-alone environment and its impact to user administration.
- Explain why you would use ISA to maintain user data between environments where LSF and Infor Landmark are federated.
- Describe the process for synchronizing an environment.
- Describe how to administer access to Infor Ming.le™, Infor Lawson for Infor Ming.le, Infor Landmark Rich Client®, and Infor Smart Office.
- Define the purpose of user attributes in administering user access.
- Describe how to administer user access to Infor Lawson Add-ins for Microsoft® Office®.
- Describe the purpose and setup of user proxies.
- Describe how to set up a user for access to Infor Lawson and Infor Landmark mobile applications.
- Explain how to enable user monitoring and reporting.
- Describe how to administer users of Infor Lawson Mobile Supply Chain Management® and Infor Lawson Business Intelligence®.

Audience
- Technical Consultant
- Support
- System Administrator

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission
System requirements

- EDU: LMRK_LSF 10 Admin Training Environment
Course description and agenda

This course provides the Infor Lawson administrator the knowledge to provision different types of resources and/or users in the Infor Lawson System Foundation and Infor Landmark Technology Runtime environments using the Infor Security Administrator tool.

The course focuses on managing user access in a federated environment through role assignment, role definition by adding or removing Infor-delivered security classes, and provisioning access to Infor applications such as Infor Rich Client, Infor Smart Office, Infor Ming.le, Infor Lawson for Infor Ming.le, Infor Lawson Add-ins, Infor Lawson Mobile applications, Infor Lawson Mobile Supply Chain Management (MSCM), and Infor Lawson Business Intelligence (LBI).

Prerequisite knowledge

To optimize your learning experience, Infor recommends that you have the following knowledge prior to attending this course:

- Familiarity with corporate user profile environments – such as a Lightweight Directory Access Protocol (LDAP) and Active Directory
- Familiarity with Infor-delivered security classes and security rules for both Infor Landmark Technology Runtime and Infor Lawson System Foundation
- Knowledge of system administration and technical foundations for Infor Lawson System Foundation and/or Infor Landmark Technology Runtime

<table>
<thead>
<tr>
<th>Lesson</th>
<th>Lesson title</th>
<th>Learning objectives</th>
<th>Day</th>
</tr>
</thead>
<tbody>
<tr>
<td>Course overview</td>
<td></td>
<td>• Review course expectations.</td>
<td>1</td>
</tr>
</tbody>
</table>
| 1 | Overview of Infor Lawson System Foundation (LSF) | • Recognize the architecture components of Infor® Lawson® System Foundation® 10 (LSF).
• Identify user interfaces in LSF. | 1 |
| 2 | Overview of Infor Landmark Technology Runtime | • Recognize the architecture components of Infor Landmark Technology Runtime® 10.
• Identify user interfaces in Infor Landmark. | 1 |
| 3 | Overview of Infor Security | • Identify where Infor Security Services (ISS) is installed.
• List the components of the Distributed Security Package (DSP).
• Describe Microsoft® Active Directory® Federation Services (AD FS), Lawson Security as Security Token Service (LS as STS) and Kerberos as authentication protocols.
• Define the primary authentication service designation.
• Explain the differences between Single Sign-on (SSO) service and Distributed Single Sign-on (DSSO). | 1 |
<p>| 4 | Infor Security Services and user administration | • Describe how the Infor Security Administration® (ISA) tool provides user provisioning, synchronizing, and federation services in environments where Infor Lawson System | 1/2 |</p>
<table>
<thead>
<tr>
<th>Lesson</th>
<th>Lesson title</th>
<th>Learning objectives</th>
<th>Day</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Foundation and Infor Landmark Technology Runtime are installed and federated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identify the tools available to administer users in version 10 of both LSF and Infor Landmark.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identify the available functions of the secadm command.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe the various types of users in both the LSF and Infor Landmark environments.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Explain why you would use the ISA to maintain user data between environments where LSF and Infor Landmark are federated.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Identify the available functions of the loadusers command.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Defining access and roles for users</td>
<td>• Define the process for modifying roles for LSF in ISA.</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe the difference between a security class and a role.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Define the process for customizing Infor Landmark-delivered security classes using the Configuration Console.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Describe how to modify a role by adding or removing a security class.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Explain how actors and users are assigned roles using ISS.</td>
<td></td>
</tr>
<tr>
<td>Lesson</td>
<td>Lesson title</td>
<td>Learning objectives</td>
<td>Day</td>
</tr>
<tr>
<td>--------</td>
<td>--------------</td>
<td>---------------------</td>
<td>-----</td>
</tr>
</tbody>
</table>
| 6      | Federation and synchronization | - Describe the difference between a federated and a stand-alone environment and its impact to user administration.  
- Explain the differences between authentication protocol, federation, and primary authentication service.  
- Describe the function of Federation Services in ISS.  
- Identify which user data is synchronized between LSF and Landmark.  
- Describe how to execute ISS synchronization to resolve potential user data inconsistencies.  
- Explain how to access the `security_provisioning` log and its use for troubleshooting synchronization conflicts. | 2 |
| 7      | Administering user access to Infor Ming.le Enterprise and Infor Lawson for Infor Ming.le | - Describe how to grant access to Infor Ming.le™ Enterprise.  
- Explain the process of adding a user to Infor Federation Services (IFS).  
- Explain how to create and assign an Infor Lawson for Infor Ming.le role to customize the Infor Lawson for Infor Ming.le display.  
- List the steps to assign bookmarks controlled by groups.  
- Identify the types of user accounts used in setting up Infor Ming.le. | 2 |
| 8      | Administering user access to Infor Lawson Add-ins for Microsoft Office | - Define the purpose of user attributes.  
- Describe how to grant access to Infor Lawson for Infor Ming.le with user attributes.  
- Describe how to administer user access to Infor Lawson Add-ins for Microsoft Office.  
- Identify the purpose of creating custom user attributes in Schema Editor.  
- Describe how to administer access to Infor Spreadsheet Designer. | 3 |
| 9      | User proxies | - Describe the purpose and setup of user proxies. | 3 |
| 10     | Administering user access to Infor Smart Office | - Explain how to administer access to Infor Smart Office. | 3 |
| 11     | Administering user access to LSF mobile applications | - Describe how to set up a user for access to Infor Lawson mobile applications.  
- Define the function of the Infor System Console. | 3 |
| 12     | Administering user access to Infor Landmark Technology mobile applications | - Describe how to set up a user for access to Infor Landmark Technology Runtime mobile applications. | 3 |

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
<table>
<thead>
<tr>
<th>Lesson</th>
<th>Lesson title</th>
<th>Learning objectives</th>
<th>Day</th>
</tr>
</thead>
</table>
| 13     | User monitoring and reporting | • Describe the benefits of user monitoring.  
• Explain how to use the ISS administrative tool to view user monitoring, history, and usage. | 3 |
| 14     | Administering user access to Infor Lawson extension applications | • Describe user administration tasks in Infor Lawson Mobile Supply Chain Management (MSCM).  
• Describe user administration tasks in Infor Lawson Business Intelligence (LBI). | 3 |

**Course summary**

• Debrief course.

**Appendices**

There are appendices at the end of this Training Workbook that you may find useful. They contain information that is not part of the instructional content of this course, but provide additional related reference information.

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Appendix title</th>
<th>Content description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix A</td>
<td>Creating a user in Lawson Security Administrator</td>
<td>How to create a user in Lawson Security Administrator</td>
</tr>
<tr>
<td>Appendix B</td>
<td>Disabling and enabling a user in ISA</td>
<td>How to disable and enable a user in Infor Security Administrator</td>
</tr>
<tr>
<td>Appendix C</td>
<td>LifeCycle Manager Client 2.0</td>
<td>Explore administrator setup for Infor Smart Office</td>
</tr>
</tbody>
</table>
Lesson 1: Overview of Infor Lawson System Foundation (LSF)

Estimated time
30 minutes

Learning objectives
After completing this lesson, you will be able to:

- Recognize the architecture components of Infor® Lawson® System Foundation® 10 (LSF).
- Identify user interfaces in LSF.

Topics
- Infor Lawson System Foundation overview
- LSF core components
- LSF interfaces overview
- LSF application overview
- Check your understanding
Infor Lawson System Foundation overview

Infor Lawson System Foundation (LSF) is a platform that enables developing and running of Infor Lawson Enterprise Applications. A Lawson application is a set of related programs and data files that performs a group of related business tasks. A product line is a set of integrated Lawson application and data.

In LSF, the application product line is the container for all licensed Infor Lawson application suites. It contains a complete repository of application metadata, including screen descriptions, tables, forms, fields, and rules files required to run an Infor Lawson application as well as the actual data that is updated through the applications.

LSF acts as a buffer between Infor Lawson applications and the many services and programs that must run behind the scenes to provide that support. LSF also serves as a buffer to third-party products by providing an environment through which applications interface with third-party products.

Lawson Environment

A major component of Lawson technology, the Lawson Environment provides functionality that supports Infor Lawson applications. It interfaces the Infor Lawson applications and relational databases, and provides administrative, database development, and program development utilities. The Lawson Interface Desktop (often referred to as LID or the Desktop Client) is a desktop client user interface that provides system administrator access to the Lawson Environment.

Within the Lawson Environment, you define product lines (including data areas and data IDs) and you indicate the data storage for these. In addition, you set up job queues, printers, users, and security through the Lawson Environment.

Each Lawson Environment requires system product lines which contain data that the environment requires. In LSF, the system product lines are GEN and LOGAN and they reside in a customer’s relational database management system (RDBMS).

The following diagram shows a simplified view of a single Environment with an application product line (Product Line), a system product line (GEN), and a database.

![Diagram of Application product line in the context of a Lawson Environment](image-url)
Multiple Lawson Environments

An organization can have multiple product lines on the same Lawson Environment – for example, one for quality assurance (QA) and one for development.

Multiple product lines on the same Lawson Environment

However, an organization can also choose to have more than one Environment running on the same LSF server, for instance, a different one for the production product line.

For the scenario in the diagram below, an organization had set up their on-site software developers who write code with a product line on an Environment separate from the production Environment to lessen the risk that their development work will impact the production product line.

Multiple Lawson Environments on the same LSF server run independently of each other and do not interact.

Multiple product lines on separate Lawson Environments on the same server
LSF core components

The diagram below shows the core components of Infor Lawson System Foundation.

The following table describes the core components of Infor LSF depicted above in alphabetical order.

<table>
<thead>
<tr>
<th>Core components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fourth-generation program language (4GL) / RPG</td>
<td>4GL / RPG is a typical Lawson business application written in either 4GL programming language (Unix® or Microsoft Windows), or the RPG language (IBM i™). On IBM i Lawson applications are typically written in 4GL and then translated to RPG.</td>
</tr>
</tbody>
</table>
| Authentication                                        | Authentication is the mechanism by which a user presents credentials for accessing a system, such as Infor LSF. There are three authentication methods available that are supported by Infor Lawson 10.x:  
  - Active Directory Federation Services (ADFS)  
  - Lawson Security as Security Token Service (LS as STS)  
  - Kerberos protocol                                                                                                                                               |
<p>| Browser (Infor Lawson for Infor Ming.le execution)    | A web-browser is the only desktop product required for end users to run Infor Lawson for Infor Ming.le.                                         |
| Client                                                | A client is any subsystem that connects via Hypertext Transfer Protocol (HTTP) to the Lawson server as a client.                                |</p>
<table>
<thead>
<tr>
<th>Core components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>Data is the Lawson service that facilitates read-only client requests for application data contained within Lawson.</td>
</tr>
<tr>
<td>Data Access (DA)</td>
<td>The DA servlet is the main communication component between Infor Process Server and other Infor LSF components.</td>
</tr>
<tr>
<td>Drill</td>
<td>Drill is the Lawson service that facilitates read-only client Drill Around requests.</td>
</tr>
<tr>
<td>Distributed Security Package (DSP)</td>
<td>DSP is the package that allows for communication between Infor LSF and the SharePoint server which handles Kerberos authentication and ADFS.</td>
</tr>
<tr>
<td>HTTP server</td>
<td>The HTTP server, sometimes called a web server, is the server where Infor Lawson for Infor Ming.le is installed and communicates via HTTP.</td>
</tr>
<tr>
<td>Internet Object Services (IOS)</td>
<td>IOS is a subsystem of the Lawson Core Technology that provides services to all of Lawson, in particular, web-based systems, such as Infor Lawson for Infor Ming.le. It is deployed in the servlet container.</td>
</tr>
<tr>
<td>IOS servlets</td>
<td>IOS servlets are individual programs that perform the tasks that make up IOS as a whole.</td>
</tr>
<tr>
<td>Lawson Database Server (LADB)</td>
<td>LADB is the interface between the customer RDBMS system and Lawson database drivers. Lawson provides a driver for each supported RDBMS. LADB routes requests for data to the appropriate driver.</td>
</tr>
<tr>
<td>Lawson Runtime System (LA-RTS)</td>
<td>LA-RTS is the COBOL and RPG (IBM i) runtime collectively.</td>
</tr>
<tr>
<td>Lawson Security Server (LASE)</td>
<td>LASE is the main processing engine for authorization requests to Lawson Security.</td>
</tr>
<tr>
<td>Lawson Application Server (LATM)</td>
<td>LATM provides services to ensure that Lawson transactions move through the system with the best performance and least expenditure of system resources possible.</td>
</tr>
<tr>
<td>Lawson server</td>
<td>The Lawson server is the server where the majority of Infor LSF components are installed.</td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol (LDAP Server and LDAP)</td>
<td>LDAP Server and LDAP is where Lawson stores global user data in a third-party, industry standard LDAP directory.</td>
</tr>
<tr>
<td>Infor Security Services (ISS)</td>
<td>Infor Security Services (ISS) is the suite of security tools. ISA is the desktop tool for performing most tasks related to configuring users and federating systems; for example, federating Infor LSF and Infor Landmark Technology.</td>
</tr>
<tr>
<td>Infor Security Administrator (ISA)</td>
<td>ISA is the desktop tool for performing most tasks related to configuring users and federating systems; for example, federating Infor LSF and Infor Landmark Technology.</td>
</tr>
<tr>
<td>Lawson Security Administrator (LSA)</td>
<td>LSA is a desktop tool for performing all tasks related to writing security policies (authorization). Most user administration tasks can also be performed using this tool.</td>
</tr>
<tr>
<td>Core components</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Infor Landmark runtime</td>
<td>Landmark Runtime is the foundation technology that supports Landmark applications, including IPA.</td>
</tr>
<tr>
<td>Infor Process Automation (IPA)</td>
<td>Infor Process Automation is Infor's Business Process Management (BPM) product that is an Infor Landmark application which is fully compatible with the Infor Lawson System Foundation system.</td>
</tr>
<tr>
<td>Infor Lawson server components</td>
<td>Infor Lawson server components are software components installed on the Lawson server that forward application requests to IPA.</td>
</tr>
<tr>
<td>Infor Smart Office</td>
<td>Infor Smart Office is a Windows-based user interface that can be used instead of or in addition to Infor Lawson for Infor Ming.le.</td>
</tr>
<tr>
<td>Multi-Database System (MDBS)</td>
<td>MDBS is an umbrella term for the Lawson components that support interaction between Lawson and the customer application data and Lawson metadata that is stored in an RDBMS. This includes a database driver for each supported RDBMS and a system of Application Program Interface (API) for interfacing with other Lawson layers. The goal of the MDBS is to provide services to ensure that Lawson Core Technology and applications can remain unaware of vendor-specific differences in RDBMS features and behavior.</td>
</tr>
<tr>
<td>Relational Database Management System (RDBMS)</td>
<td>RDBMS is where Lawson stores customer application data and Lawson metadata in a third-party, Structured Query Language- (SQL) based database system.</td>
</tr>
<tr>
<td>Resource Management Administrator (RMA)</td>
<td>RMA is a desktop tool for performing most tasks related to configuring users and their roles.</td>
</tr>
</tbody>
</table>
| Router                                  | The Router servlet manages the work of the main IOS services:  
  - Data  
  - Drill  
  - Transaction                                                                                                     |
| Single Sign-on (SSO) servlet            | The SSO servlet verifies that a user session is valid.                                                                                       |
| SharePoint server                       | The SharePoint server is where users are authenticated if the installation uses the Kerberos protocol for authentication.              |
| Transaction                             | Transaction is a Lawson service that facilitates requests for application transactions (create, update, delete) between clients and the rest of Lawson. |
LSF interfaces overview

User interfaces

Infor Lawson for Infor Ming.le is the main user interface to LSF. It is the method by which application end users, mobile users, administrators and other users access Lawson.

The main thing for user administrators to know about Infor Lawson for Infor Ming.le user setup is that even though users are not added to the system, some user setup is performed in order to prepare Infor Lawson for Infor Ming.le for user access. This is done through the creation of roles, which contain a set of attributes that specifies access for users who have been assigned the role. For example, user administrators can determine the number of records retrieved in a data query, which printer to use for Lawson reports, which product lines to access and many other things.

As delivered, Infor Lawson for Infor Ming.le gives full access to all options to all users.

The Infor Smart Office refers to the Windows-based interface that can be used instead of or in addition to Infor Lawson for Infor Ming.le.

Administrator interfaces

The table below introduces the various LSF administrator interfaces.

<table>
<thead>
<tr>
<th>Administrator interface</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infor Security Services (ISS)</td>
<td>Infor Security Services (ISS) is the suite of security tools.</td>
</tr>
<tr>
<td>Infor Security Administrator (ISA)</td>
<td>ISA is the desktop tool for performing most tasks related to</td>
</tr>
<tr>
<td></td>
<td>configuring users and federating systems; for example,</td>
</tr>
<tr>
<td></td>
<td>federating Infor LSF and Infor Landmark Technology.</td>
</tr>
</tbody>
</table>

LSF user interfaces
<table>
<thead>
<tr>
<th>Administrator interface</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lawson Interface Desktop (LID)</td>
<td>Used to access the Lawson Core Technology environment services and utilities, access runtime information or logs, and control settings</td>
</tr>
</tbody>
</table>
| Infor Lawson Security Administrator (LSA) and Resource Management Administrator (Resource Management, or RM) | Used to add roles, groups, structures, and Infor Lawson Security configuration for Infor Lawson Lightweight Directory Access Protocol (LDAP)  
  - User information can be viewed |
| Lawson Schema Editor | Used to modify the LSF Infor Lawson LDAP  
  - Requires ldifgen and ldifde/ldapmodify to complete modification |
| Infor Lawson System Mobile Monitor (App) | Used to provide administrative accessibility for the LSF server through smartphone or tablet devices  
  - Supports Android and Apple iOS systems |
| Infor System Console | Used to monitor and administer an Infor Lawson system via the Web |
| Infor Lawson for Infor Ming.le (Administrator access) | Used to access Lawson applications online and batch job parameter forms  
  Administrators can use the Lawson for Infor Ming.le Administration bookmarks in the Lawson for Infor Ming.le.  
  - Bookmarks are links to forms for managing Lawson for Infor Ming.le users and user options |
LSF application overview

As mentioned in the previous topic, a product line is a set of integrated Lawson applications and data. Examples of Infor Lawson applications include General Ledger, Human Resources, and Accounts Payable. An application is uniquely identified by a two-character system code, such as GL for General Ledger and HR for Human Resources. Each system code has data files or tables associated with it.

The data area is a defined storage place within a Lawson product line. A product line can have one or more data areas. Multiple data areas allow you to separate access to different sets of data within the product line.

The following diagram depicts an example client configuration from an LSF application perspective with the end-user and administrator interfaces identified.

![Example Infor Lawson System Foundation application configuration](image-url)
Check your understanding

Which of the following are components of the Infor Lawson System Foundation? Select all that apply.

a) IOS servlet  
   b) Lawson Environment  
   c) LASE  

True or false? A Lawson Environment can have multiple product lines.

a) True  
   b) False  

 _____ is used to access Lawson applications online and batch job parameter forms.

a) Lawson Interface Desktop (LID)  
   b) Infor Lawson for Infor Ming.le  
   c) Infor Smart Office  

In Lawson for Infor Ming.le, a user administrator would manage user access to such things as product line or printers through the assignment of ______________.

a) Roles  
   b) Identities  
   c) Authentication  

In LSF, the application ______ is the container for all licensed Infor Lawson application suite.

a) Database  
   b) Root directory  
   c) Product line
Lesson 2: Overview of Infor Landmark Technology Runtime

Estimated time
1 hour

Learning objectives
After completing this lesson, you will be able to:

- Recognize the architecture components of Infor Landmark Technology Runtime® 10.x.
- Identify user interfaces in Infor Landmark.

Topics
- Infor Landmark Technology Runtime overview
- Infor Landmark core components
- Infor Landmark interfaces overview
- Infor Landmark data area and application overview
- Check your understanding
Infor Landmark Technology Runtime overview

Infor® Landmark Technology Runtime™ (abbreviated as Infor Landmark) is a platform that enables development and running of Service Oriented Architecture (SOA) applications on platforms supporting J2EE architecture application servers.

The Infor Landmark Technology Runtime platform includes both a program model and a runtime (production) system:

- **Program model**
  - Built on the specifications of Landmark Pattern Language (LPL) and managed through a tightly controlled application source code repository
- **Production system (also called Infor Landmark Technology Runtime)**
  - Includes an application server, fully featured relational database implementation, system administration, and configuration utilities

Infor Landmark Technology Runtime provides the runtime environment needed to run Infor Landmark applications. The installation delivers the following components:

- Infor Landmark Technology Runtime
- Infor Process Server
- Infor Landmark Rich Client user interface
Infor Landmark core components

The Infor Landmark platform always includes the Landmark server, Landmark database, and a user interface. It can also include connections to a web server and a corporate Lightweight Directory Access Protocol (LDAP).

This diagram provides a high-level look at the structure of Infor Landmark’s architecture:

![Diagram of Infor Landmark architecture]

The following table describes the core components of Infor Landmark.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infor Landmark Technology Runtime</td>
<td>This is the runtime environment needed to run Infor Landmark applications.</td>
</tr>
<tr>
<td>Grid</td>
<td>The Infor ION Grid is an application server that you install separately from Infor Landmark Technology Runtime and within which several Infor Landmark components run.</td>
</tr>
<tr>
<td>Host</td>
<td>A host is a server machine that is participating in a grid. The host may be a physical or a virtual machine.</td>
</tr>
<tr>
<td>Grid agent</td>
<td>The grid agent is a service-like application that the grid uses to start all nodes that are configured to run on the host. Each host, for each grid for which it is a member, needs a grid agent.</td>
</tr>
<tr>
<td>Node</td>
<td>A node is a Java Virtual Machine (JVM) that is registered as part of a grid where grid applications are running. The Infor ION Grid for Infor Landmark typically has several nodes running different Infor Landmark component applications. All nodes run on the grid host.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Router</td>
<td>A router acts as a well-defined entry point that client applications can connect to. A router is configured to listen for client requests on a given network interface and port number. Normally, the selected port number is made accessible through firewalls, when applicable, because it must be reachable from clients. The default name for the grid router for Infor Landmark is &quot;Landmark - YourLandmarkEnvName.&quot;</td>
</tr>
<tr>
<td>Note: An administrative router is a special router used for administrative purposes.</td>
<td></td>
</tr>
<tr>
<td>Multi-database system (MDBS)</td>
<td>MDBS refers to the interface to customer data which is stored in a third-party relational database system (RDBMS).</td>
</tr>
<tr>
<td>User interface</td>
<td>The user interface is Infor Landmark Rich Client.</td>
</tr>
</tbody>
</table>
Infor Landmark interfaces overview

User interface

The *Infor Rich Client* is the integrated desktop “canvas” provided with your Infor Landmark applications. When you enter your user name and password to log in to Infor Rich Client, you are also logging in to your Landmark application.

There are two modes to the Infor Rich Client:

- **User mode**: This mode allows you to access to data and applications on the Landmark server.
- **Administrative mode**: This mode allows you can also access table data and the application forms in addition to everything accessible in the User mode.

Access to features in Infor Rich Client is managed through a user’s security privileges. Therefore, some features and functionality may be hidden to a user depending on the roles they are assigned.

The *My Personalization* console gives users access to menu options and tabs that allow for personalization of their Infor Rich Client canvas. Users can personalize by combining lists or menus in order to create a customized page that they frequently use, or users can create a customized menu to more efficiently navigate from form to form. The *My Personalizations* is the location on Infor Rich Client where objects users have personalized and objects that are available to personalize are stored.

The options available for personalization vary depending on a user’s role and security privileges.
Administrator interface

The Configuration Console is a tool within the Infor Rich Client which enables administrator to make changes that affect Infor Landmark users. They include changes to:

- Application
- Security
- Web services

Configuration changes made through the Configuration Console apply to all users. This is in contrast to the changes made through the My Personalizations console, which apply only to the user making the change unless that user has the privilege to make the change global and chooses to do so.

The table below lists additional administrator interfaces for Infor Landmark:

<table>
<thead>
<tr>
<th>Administrator interface</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infor Security Services (ISS) browser-based</td>
<td>• Used for federation, synchronization, user maintenance, and user monitoring for LSF and Infor Landmark</td>
</tr>
<tr>
<td>Landmark Command Window (LCW)</td>
<td>• Resides on the Infor Landmark server • Used to maintain the Infor Landmark Environment and Grid • Common administrator command line utilities include: Security Administration (secadm) utility, database utilities, and the Infor Landmark build and deploy processes</td>
</tr>
<tr>
<td>Infor Landmark Grid Manager browser-based</td>
<td>• Resides on the Infor Landmark server • Used to maintain and support the Infor Landmark Grid, configuration and running JVMs</td>
</tr>
<tr>
<td>Infor Landmark Security</td>
<td>• Resides in Infor Landmark Rich Client • Used to access applications for administering security and users, including a Create User Wizard • Can perform many of the functions available through secadm command line tool</td>
</tr>
<tr>
<td>Infor Landmark Administrator (Application)</td>
<td>• Resides on the Infor Landmark server • Used to provide administrative accessibility for Infor Landmark server through smartphone or tablet devices • Supports only Apple iOS systems currently</td>
</tr>
<tr>
<td>Async framework</td>
<td>• The Async framework provides background execution processing for an Infor Landmark system, including the processing of set actions and instance actions. • The Async framework uses queues. In addition to queues that are devoted to e-mail and Infor Lawson transaction processing, an Infor Landmark system has a default queue for background processing.</td>
</tr>
<tr>
<td>Infor Process Automation (IPA)</td>
<td>• IPA is the umbrella term for Infor Lawson’s Business Process Management (BPM) product. It includes Infor Process Server and Infor Process Designer. • The Process Server Administrator refers to the server side components of the IPA product. These components include configuration, administration, and troubleshooting tools. They are delivered with Infor Landmark Technology and accessed using Infor Landmark Technology, Infor Rich Client, Infor Smart Office, or the web user interface.</td>
</tr>
<tr>
<td>Infor Process Designer (IPD)</td>
<td>• Infor Process Designer is the desktop tool for creating the actual processes. All process developers must have this tool. Access to this tool is not needed for users who need to take actions on processes that are in production.</td>
</tr>
</tbody>
</table>
Infor Landmark data area and application overview

Landmark employs a multi-tiered architecture, exposing applications enterprise-wide. Multi-tiered means that the presentation layer is separated from the application tier, including the application server. Enterprise-wide means the application can be exposed over the internet as well as the intranet.

The Infor Landmark Technology is designed to connect with the Infor Lawson System Foundation, so that Landmark applications are not isolated from other Lawson applications, and data integrity is carefully maintained.

In Infor Landmark, data areas are comparable to product lines in LSF. Each data area in Infor Landmark Technology Runtime may only contain a single application suite.

In the diagram below, the LSF diagram presented earlier is shown with a comparable diagram for Infor Landmark Technology Runtime.

Example LSF and Infor Landmark server arrangement
Check your understanding

Which of the following does the Inform Landmark Technology Runtime platform include? Select all that apply. ______.

- a) Runtime (production) environment
- b) LDAP model
- c) Program model

Which two modes are part of Infor Rich Client?

- a) User mode
- b) Administrative mode
- c) Development mode

The ______ is a Java Virtual Machine (JVM) that is registered as part of a grid where grid applications are running IOS servlet.

- a) Grid
- b) Agent
- c) Node
Lesson 3: Overview of Infor Security

Estimated time
2 hours

Learning objectives
After completing this lesson, you will be able to:

- Identify where Infor Security Services (ISS) is installed.
- List the components of the Distributed Security Package (DSP).
- Describe Microsoft Active Directory Federation Services (AD FS), Lawson Security as Security Token Service (LS as STS) and Kerberos as authentication protocols.
- Define the primary authentication service designation.
- Explain the differences between Single Sign-on (SSO) service and Distributed Single Sign-on (DSSO).

Topics
- Infor Security overview
- Infor Security Services overview
- Infor Lawson System Foundation Security overview
- Infor Landmark Technology Security overview
- Authentication protocols
- Authorization
- Sign Sign-on (SSO) services
- Check your understanding
Infor Security overview

Infor Security is a highly flexible rules and roles-based system for securing your Infor Lawson system. It is intended to ensure that the appropriate staff have access to the information and system resources that they need to perform their jobs but only the information and resources they need.

Infor Security Services (ISS) is a component of Infor’s security solution. ISS provides user provisioning, synchronizing, and federation services in environments where Infor Lawson System Foundation and Landmark Technology Runtime are installed and federated. ISS and is installed on the LSF server.
Infor Security Services overview

**Infor Security Services Configuration Guide**

Infor Security Administration (ISA) is the web browser-accessible administrative interface of ISS and is used for managing actors and users and for configuring the security system for LSF and Infor Landmark.

**Infor Security Administration tool**

ISA is used to:

- Add and maintain actor/user records, including all attributes related to users
- Federate multiple systems
- Synchronize federated systems

Infor Lawson uses the term *federate* to refer to two systems (for example, LSF and Infor Landmark) sharing user information so that both systems can participate in single sign-on. One system serves as the primary authentication service.

*Synchronization* means identifying and facilitating resolutions of any conflicts that exist between the systems being federated. A synchronization process must be run to federated systems. ISS is the tool that lets you perform this synchronization.

More details about how synchronization works and how to perform a federation is covered in a later lesson.
The following diagram illustrates the high-level architecture of ISS:

ISS architecture model
Demo: Access Infor Security Services
Your instructor will demonstrate how to access Infor Security Services (ISS).

Exercise 3.1: Access Infor Security Services
In this exercise, you will access Infor Security Services (ISS).

Exercise 3.1 steps
2. Type lawson@gdeinfor2.com in the User name field. Note: To prepare any field in the system for text entry, first click in the text field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The ISA tool administrator home page opens.
5. Click through the various menus: Resources, Configuration, SSO, Monitoring and Federation and review options.
In LSF, security is managed using Infor Lawson Security, an object-oriented, security model for building out application-level security that allows administrators to create rules, build roles, and assign roles to users.

LSF Security consists of the following components:

- Infor Security Services (if used, with a federated system)
  - Infor Lawson repository for globally interesting data
  - Contains user records and other information needed by many Infor Lawson components, which does not change frequently
  - The data is stored in an LDAP server
- Infor Lawson Security desktop clients
  - Authentication, authorization, and session management

**LSF Security creation process overview**

1. Create profile
2. Create security classes
3. Create security rules
4. Create role
5. Assign security classes to role
6. Assign role to user/resource

*Infor Lawson Security process*
This course, *Lawson: Administering Users* will focus exclusively on step 6 of the process to allow you to become an Infor Lawson user administrator. This course was designed with the assumption that the Infor Lawson Security administrator has already completed steps 1-5 of the process using the Lawson Security Administrator and Resource Management tools.

Steps 1-5 are addressed in the course *Lawson: Administering Security*. Infor assumes that someone in your organization (possibly you) has taken or will take this course to become an Infor Lawson Security administrator.

**LSF Security policy and access**

The diagram below is another perspective of how tasks managed by the user administrator and the security administrator intersect around provisioning access to securable objects in an organization.

The user administrator focuses on the left side of the diagram – creating users in the system and connecting them to roles. The remainder of the diagram depicts aspects of security managed by a security administrator.

The table below includes LSF Security terms and their descriptions.
<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>A role is a set of access rights that allow a user access to the system. Roles are task-based meaning that they are intended to describe a job that a user performs, rather than describing the user, for example, Accounts Payable (AP) Clerk.</td>
</tr>
<tr>
<td>Group</td>
<td>A group is a set of items that you want to view as a unit, such as user groups, bookmark groups, distribution groups, etc.</td>
</tr>
<tr>
<td>Structure</td>
<td>A structure is a hierarchical view of the Infor Lawson users in an organization, similar to an organization chart that is used to write specialized security rules.</td>
</tr>
<tr>
<td>User attributes</td>
<td>User attributes refers to the descriptive property of a user, such as email address, group affiliation, role assignment, etc.</td>
</tr>
<tr>
<td>Security class</td>
<td>Privileges required to complete a task, are designated by security class, for example, Journal Entry Processing, Employee Maintenance, or Vendor Maintenance.</td>
</tr>
<tr>
<td>Rule</td>
<td>A rule grants access to a securable object, for example, Grant access to HR11.</td>
</tr>
<tr>
<td>Securable object</td>
<td>Objects that can be secured, such as product lines, system codes, programs, forms, fields, tabs, etc. are known as securable objects.</td>
</tr>
</tbody>
</table>

The diagram below parallels the previous diagram and provides a functional example of the concepts it introduced. Again, the user administrator focuses on the left side of the diagram.
LSF Security policy example

Infor Security Service

User administrator

Roles

- Role 1 Employee
- Role 2 HR Administrator
- Role 3 Garnishment Administrator
- Role 2 Asset Management Processor

Your co-worker

Resource Management

- Role 1 Employee
- Role 2 HR Administrator
- Role 3 Garnishment Administrator
- Role 2 Asset Management Processor

Lawson Security

- Security class/task Self service center employee
  - Rules - Employee table
- Security class/task Employee maintenance
  - Rules - HR11.1 form
- Security class/task Time card processing
  - Rules - PR26.1 form
- Security class/task Asset maintenance
  - Rules - AM20 form

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
LDAP

The items described in the previous diagrams are contained in the Infor Lawson LDAP data repository. The LDAP:

- Stores and centralizes static information.
- Is tuned to handle high volumes of requests.

![LDAP data repository](image)

Distributed Security Package

The Distributed Security Package (DSP) is available both as a LifeCycle Manager Installation package and as a Java installer package.

The Distributed Security Package (DSP) delivers the following components of the Infor Lawson Security solution:

**Distributed Single Sign-on (DSSO)**

- The DSSO component enables single sign-on between applications on remote servers and Infor Lawson System Foundation.

**Infor Security Services (ISS)**

- ISS provides user provisioning, synchronizing, and federation services in environments where Infor Lawson System Foundation and Infor Landmark Technology Runtime are installed and federated.

![Distributed Security Package and deployment](image)
Infor Security Services requires the installation of `scwebadminapp.war` and `scwebmonitorapp.war` within the IBM WebSphere® Application Server to support the web administrative tool.
Infor Landmark Technology Security overview

Infor Landmark Security provides features for authentication and authorization. **Authentication** refers to control over which users can log in and how they can log in. **Authorization** refers to control over each user's access after he or she has logged in.

Much like Infor Lawson Security, Infor Landmark Security allows you to build roles and rules and assign multiple roles to users.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role</td>
<td>A role is a set of access rights that allow a user access to the system. Roles are task-based meaning that they are intended to describe a job that a user performs, rather than describing the user.</td>
</tr>
<tr>
<td>User attributes</td>
<td>User attributes are a descriptive property of a user, such as name or email address.</td>
</tr>
<tr>
<td>Rules</td>
<td>Rules are contained in security classes. They determine how the application information modeler wants to allow user access to a securable object.</td>
</tr>
<tr>
<td>Security class</td>
<td>Security classes contain the rules needed to provide the access a user needs to perform a task.</td>
</tr>
</tbody>
</table>

**Infor Landmark Security creation process overview**

1. Create roles
2. Create additional security classes (_ST) if needed
3. Assign security classes to role
4. Assign role to actors

**Infor Landmark Security policy and access**

After the security administrator creates roles and security classes, the user administrator can assign security classes to roles, and then assign roles to actors within the system.
This course, *Lawson: Administering Users* will focus exclusively on steps 3-4 of the process to allow you to become an Infor Lawson user administrator. This course was designed with the assumption that the Infor Landmark Security administrator has already completed steps 1-2 of the process.

Steps 1-4 are addressed in the course *Lawson: Administering Landmark Security*. Infor assumes that someone in your organization (possibly you) has taken or will take this course to become an Infor Landmark Security administrator.

**Security class**

Infor Lawson delivers a set of security classes with the Infor Landmark Environment and with each Infor Landmark application. The delivered security classes are designed to reflect common authorization needs for an application. They have names ending in "_ST" to indicate that they belong to the "standard template" set of security classes.

Security classes can provide security for numerous securable objects, including:

- Business classes (BusinessClass), business tasks (BusinessTask), executables (Executable), and web applications (WebApp)
- Data views, including a business object and its fields, and related business objects and their fields
- Fields, including compound, derived, display, and key fields
- Drills and audit logs

**Configuration Console**

The *Configuration Console* is a tool within the Infor Rich Client which enables administrators to make changes to various Landmark applications and service as well as to configure security policies and rules for an organization.
Configuration changes to security made by a security administrator in the Configuration Console are global, meaning they affect all Landmark users.

**Accessing the Configuration Console for security**

The following table shows the two paths to access the Configuration Console after logging in to the Infor Rich Client:

<table>
<thead>
<tr>
<th>If…</th>
<th>Then select…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Your roles have only the SecurityConfigAccess_ST class but do not have the other configuration access security classes.</td>
<td>Start &gt; Security Configuration</td>
</tr>
<tr>
<td>Your roles have the SecurityConfigAccess_ST class and additional access to other configuration security classes. <strong>Note:</strong> This is how the Lawson user is set up in the training environment.</td>
<td>Start &gt; Configure &gt; Security</td>
</tr>
</tbody>
</table>

The Configuration Console is also known as the Configure Security page. You can access this page from any data area.
Authentication protocols

LSF and Infor Landmark version 10.x can be configured to authenticate users using the following authentication protocols:

- Microsoft Active Directory Federation Services (AD FS)
- Infor Lawson Security as Security Token Service (LS as STS)
- Kerberos

Deciding if LS as STS, Kerberos, or Microsoft AD FS is the best authentication protocol for an organization will depend on several factors:

- If a customer is on a prior release of LSF and using ldapbind to tie the LSF LDAP to the corporate LDAP then LS as STS is likely the best decision based on experience.
- If a customer is using Kerberos for other applications within the organization then Kerberos is likely the best choice.
- If a customer is using Microsoft AD FS for other applications within the organization then Microsoft AD FS is likely the best choice.

<table>
<thead>
<tr>
<th>Features</th>
<th>Kerberos</th>
<th>AD FS</th>
<th>LS as STS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global standards</td>
<td>Yes</td>
<td>Yes</td>
<td>Infor Lawson standard</td>
</tr>
<tr>
<td>Single sign-on with Infor products</td>
<td>Yes</td>
<td>Yes</td>
<td>Only with Infor Lawson applications</td>
</tr>
<tr>
<td>Requires Microsoft knowledge</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Active Directory bound</td>
<td>Yes</td>
<td>Yes</td>
<td>Optional</td>
</tr>
<tr>
<td>Remote access to Infor Lawson products</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Mobile applications accessible</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Seamless SSO</td>
<td>Yes</td>
<td>Yes</td>
<td>Only for Infor Lawson products</td>
</tr>
<tr>
<td>Login prompt</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Shared computers/kiosks available</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Session timeout</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

If an organization uses Infor Ming.le Enterprise then Kerberos or Microsoft ADFS is required. You cannot use LS as STS with the Infor Ming.le Enterprise application.

Authentication services

One of the systems must become the primary authentication service. Deciding if LSF or Infor Landmark Technology Runtime should be the primary authentication service depends on several factors:

- Select the mission critical system as it would closely support 24/7 accessibility.
• Select the busiest system with the most end users. Depending on the applications used by an organization this could be LSF or Infor Landmark Technology Runtime and may change based on application deployment.

The primary authentication service is not fixed and can be changed if required based on new organizational needs. Primary authentication is set in the Infor Security Services (ISS) application. Before editing the primary authentication service, contact Infor Xtreme Support or Infor Consulting Services to understand the impact to your server.

**Infor Lawson Security as Security Token Service (LS as STS) authentication**

In the LS as STS method, Infor Lawson Security authenticates users. The system is federated (both Infor Lawson System Foundation and Infor Landmark Technology Runtime are used), one system provides the authentication service for both systems.

**Federated system with LSF as the primary authentication service (PAS)**
LS as STS sign-in via a browser

![Diagram of LS as STS sign-in via a browser]

**Browser-based sign-on: LS as STS**

**Configuration for LS as STS**
- LSF and Infor Landmark must be using the same “assertion protocol,” HTTP or HTTPS.
- The DSP, which contains security and Distributed Single Sign-on (DSSO), must be configured within both systems.

<table>
<thead>
<tr>
<th>Required system users</th>
<th>Access needs</th>
</tr>
</thead>
<tbody>
<tr>
<td>User who runs application pools (e.g., LocalSystem, spfarm)</td>
<td>The Microsoft SharePoint® application pools user must also be a user on the Infor Lawson primary authentication system.</td>
</tr>
<tr>
<td>spinstall</td>
<td>The default Microsoft SharePoint user for performing the Microsoft SharePoint installation must have an identity on the primary service of the Infor Lawson system.</td>
</tr>
<tr>
<td>spservices</td>
<td>The default Microsoft SharePoint user for running Microsoft SharePoint services performs initial setup and smoke testing for applications running on the Infor Ming.le server. The user must have an operating system (OS) identity on the Infor Lawson system.</td>
</tr>
<tr>
<td>lawson</td>
<td>The domain lawson user is used to install and smoke test most Infor Lawson products. The user needs to exist on the OS, in the domain, and in Microsoft SharePoint.</td>
</tr>
<tr>
<td>SQL Server service account</td>
<td>This domain account is automatically assigned the appropriate permissions as part of the SQL Server installation.</td>
</tr>
</tbody>
</table>
Kerberos authentication

Kerberos is an industry standard authentication protocol that is used by Active Directory/Microsoft Windows®. It is a supported authentication option for Infor Lawson 10. In this method, Active Directory authenticates users. Users must exist in both Infor Lawson and in Infor Active Directory.

**Federated system with LSF as the primary authentication service (PAS)**

![Kerberos authentication protocol](image)

**Kerberos sign-in via a browser**

![Kerberos browser-based sign-on](image)
Configuration for Kerberos
- LSF and Infor Landmark Technology Runtime must be using the same "assertion protocol," HTTP or HTTPS.
- The DSP, which contains security and Distributed Single Sign-on (DSSO) must be configured within both systems.

<table>
<thead>
<tr>
<th>Required system user</th>
<th>Access needs</th>
</tr>
</thead>
<tbody>
<tr>
<td>spinstall</td>
<td>This is the default Microsoft SharePoint user for performing the Microsoft SharePoint installation. The user must have an identity on the primary service of the Infor Lawson system.</td>
</tr>
<tr>
<td>spservices</td>
<td>This is the default Microsoft SharePoint user for running Microsoft SharePoint services. This user performs initial setup and smoke testing for applications running on the Infor Ming.le server. The user must have an OS identity on the Infor Lawson system.</td>
</tr>
<tr>
<td>lawson</td>
<td>The domain lawson user is used to install and smoke test most Infor Lawson products. The user needs to exist on the OS, in the domain, and in Microsoft SharePoint.</td>
</tr>
<tr>
<td>wasServer</td>
<td>This is the Active Directory ID for the user who runs IBM WebSphere® Application Server. Infor recommends that you use wasServer, where Server is the name of the machine where your IBM WebSphere Application Server instance is installed. wasServer Example: If your IBM WebSphere instance is installed on a machine named LSF10, this user is wasLSF10. Note: This name cannot be the same as the IBM WebSphere Administrator ID. This user must also be set up in LSF as a privileged user.</td>
</tr>
<tr>
<td>wasadmin</td>
<td>This is the Active Directory ID for the IBM WebSphere console administrator. When using Kerberos authentication, your IBM WebSphere administration console will always be secured and you will need the wasadmin user name and password to sign in.</td>
</tr>
<tr>
<td>SQL Server service account</td>
<td>This domain account is automatically assigned the appropriate permissions as part of the SQL Server installation.</td>
</tr>
</tbody>
</table>

ADFS and Infor software
Microsoft ADFS works with ISS and other Infor software for user management and user federation. There are multiple configurations for accessing ADFS possible, depending on content location.

The diagram below shows an example configuration of ADFS with Infor components:
Example configuration of ADFS with Infor components
Authorization

Authorization asks the question, “What rights do you have?” The authorization process determines what a particular user can see, use, or do within different areas of the system.

The purpose of authorization is to control who has access to particular objects in the system. Permissions are not typically assigned to individual users because it would take too much time to set up and manage permissions on an individual basis. Instead, permissions are assigned to roles, and roles are linked to users.

Roles, and permissions within a role, can be tailored around tasks. For example, in your company you might grant permission for John to view invoices, for Marta to view and create invoices, and Sam to view, create, and approve invoices that were created by anyone except himself.

A user may be linked to multiple roles, and is authorized to act in the system as each role permits. Additionally, a role may have attributes and rules that apply under certain circumstances.
Single Sign-on services

Single Sign-on is a feature of Infor Security that lets a user log in one time to the Infor Lawson system and be authenticated as a valid user as he or she moves through the system.

Services that perform authentication can be designated as the primary service for a system or, if using multiple Single Sign-on (SSO) domains, can be designated as the primary service for a domain. The installation of Infor Landmark includes the Single Sign-on service (SSOPV2) as a primary service.

If an organization’s services are set up to refer to the Single Sign-on service, then SSOPV2 provides a consistent authentication interface to the user, no matter what Infor Lawson application or service the user is attempting to access.

The following Infor Lawson Security concepts are important when discussing SSO.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service</td>
<td>Service is a set of attributes that define how a user is identified in the sign-on engine for Infor Lawson components.</td>
</tr>
<tr>
<td></td>
<td>• LSF Resource: SSOP: User/password</td>
</tr>
<tr>
<td></td>
<td>• Landmark Actor: SSOPV2: User/password</td>
</tr>
<tr>
<td></td>
<td>• LSF ENV: Domain User login/password</td>
</tr>
<tr>
<td>Identity</td>
<td>An identity is a user entity on a particular Infor Lawson service; it is a user’s electronic passport to the service or agent. All users who need access to an Infor Lawson component defined by a particular service or agent must have an identity on the service.</td>
</tr>
<tr>
<td>Agent</td>
<td>An agent is a type of identity that does not require credentials; it is a special kind of service used only with Infor Lawson self-service applications. For example: LSF PROD_EMPLOYEE: Company/Employee</td>
</tr>
</tbody>
</table>

**Examples**

SSOP (LSF) or SSOPV2 (Infor Landmark) Service

- Resource/Actor identity:
  - User: jsmith
  - Password: summer2013 (Idapbind can eliminate password requirement)

PROD_EMPLOYEE Service

- Resource Agent
  - Company: 1234
  - Employee: 9876

At a minimum, all Infor Lawson System Foundation installations must have the following services:

- OS / Environment service
  - Users who need command line access or who run batch jobs must have identities on this service.
- SSOP service and SSOPV2
  - All Infor Lawson users must have a unique identity on these services. Either SSOP or SSOPV2 is selected as the primary authentication service.

52 Lesson 3: Overview of Infor Security
For customers who are federated, use ISS to administer users assigning SSOP identity for LSF and SSOPV2 identity for Infor Landmark Technology Runtime. If ldapbind is executed for LSF SSOP then ldapbind is required for Infor Landmark SSOPV2 to allow for primary authentication service switching.

**Single sign-on options**

While single sign-on is for the most part behind-the-scenes processing, initial setup for each user is required. Part of the user setup involves creating identities for the user on the services and agents the user needs.

Single sign-on provides the Infor Lawson system the ability to perform session timeout. When a session is inactive (no user interaction) for a programmed number of minutes, the session terminates.

**Single Sign-on (SSO) Service**

Single Sign-on (SSO) Service is a servlet-driven system that resides in the servlet container layer of the Environment.

Information about a user’s session is stored in a session ID, an object with a unique identifier that is created when a new session is launched.

**Microsoft Active Directory Federation Services (ADFS)**

For organizations that use the Active Directory™ service, SSO functionality is enabled through Windows-integrated authentication within the organization’s security walls. ADFS extends this functionality, utilizing single sign-on to authenticate users to numerous, inter-connected Web applications over the life of a single online session providing a streamlined user experience.

**Distributed Single Sign-on (DSSO)**

Distributed Single Sign-on (DSSO) performs authentication for DSSO-enabled Infor Lawson applications against a single, central repository of users in cases where the Infor Lawson Environment and Enterprise applications run within a different server than the application that needs to access them. DSSO makes it easier to administer user accounts, with the added advantage of guaranteeing that Infor Lawson application passwords are always in sync. DSSO links to the primary SSO service, residing on the server with the Infor Lawson Environment, which then authenticates to the LDAP repository where user data is stored.

DSSO is only required on application servers that do not run the Infor Lawson Environment. For example, if you run Infor Lawson Business Intelligence (LBI) under the same IBM WebSphere application server instance as the Infor Lawson Environment and applications, you do not install DSSO. Instead, in the LBI configuration, you specify SSOP as the service name. The Distributed Security Package used to install the DSSO delivered for the product in LSF 10 will automatically configure Bouncy Castle encryption settings.

DSSO can be used with these Infor Lawson applications:

- Infor Ming.le (on Microsoft Windows) or Infor Smart Office (on Microsoft Windows)
- Infor Lawson Business Intelligence suite (on Microsoft Windows)
- Infor Mobile Supply Chain Management applications (on Microsoft Windows or UNIX)
- Infor Lawson Budgeting and Planning (on Microsoft Windows)
- Infor Enterprise Search (on Microsoft Windows)
- Infor Workforce Management

In each of these cases, the Infor Lawson Environment may be on a different platform than the DSSO-enabled application.
Demo: View services for LSF using the command line
Your instructor will demonstrate how to view services for LSF using the command line.

Exercise 3.2: View services for LSF using the command line
In this exercise, you will view services for LSF using the command line.

Exercise 3.2 steps

Part 1: Export Infor Lawson services

1. Double-click the RDP Shortcuts folder on the Infor Landmark server’s training desktop. The folder opens with the list of servers.
2. Select the LSF10.rdp server link. The LSF training desktop opens.
3. Double-click the Command Prompt icon on the LSF training desktop’s task bar. The Administrator: Command Prompt window opens.
4. Type e: in the Command Prompt line.
5. Press Enter.
6. Type cd lsf10 in the Command Prompt line.
7. Press Enter. This changes the directory to LSF10.
8. Type enter.cmd in the Command Prompt line. This command brings in the environment variables to the command line session.
10. Type ssoconfig –c in the Command Prompt line.
11. Press Enter.
12. Type Global08 in the Command Prompt line for the password.
13. Press Enter. The list of services displays.
14. Type 5 (Manage Lawson Services) in the Command Prompt line.
15. Press Enter. The Manage Lawson Services options display.
16. Type 6 (Export service and identity info) in the command line.
17. Press Enter.
18. Type 1 (Yes) when prompted if you want to export all services at the command line.
19. Press Enter.
20. Type none when prompted if you want to export the identities at the command line.
22. Type servicesexport.xml when prompted to enter a file name to save export as at the command line.
23. Press Enter.
24. Type 13 (Exit) at the command line.
25. Press Enter.

Part 2: View Infor Lawson services report
2. Select Apps (E:) > LSF10. The LSF10 window opens.
3. Select the servicesexport.xml file.
4. Right-click the servicesexport.xml file. The options menu displays.
5. Select Edit with Notepad++.
6. The E:\LSF10\servicesexport.xml file opens in Notepad++.
7. Review the report.
8. Right-click the Windows Start.
9. Select Shut down or sign out > Disconnect to return to the Infor Landmark training desktop.
Demo: Explore SSO services for Infor Landmark and LSF
Your instructor will demonstrate how to view the properties and policies associated with SSOP and SSOPV2 services.

Exercise 3.3: Explore SSO services for Landmark and LSF
In this exercise, you will view the properties and policies associated with SSOP and SSOPV2 services.

Exercise 3.3 steps
2. Type lawson@gdeinfor2.com in the Login Name field.
3. Type Tr@in123 in the Password field.
4. Click Login. The Infor Rich Client canvas opens.
5. Select the GEN data area from the Data area menu located on the upper left of the canvas.
7. Click Search (magnifying glass).
8. Type SSOP* in the Service field.
9. Press Enter. The list of services opens.
10. Verify that the SSOPV2 service is a reference to SSOP.
11. Verify that the SSOP service is not a reference service. It has no reference because it is the primary authentication service.
13. Click the Security Policies tab. Notice that there is no lockout policy because the service uses ADFS.
14. Click the Service Properties tab. The Service Properties page opens. Notice the Fully Qualified Distinguished Name (FQDN) of the service.
15. Click the SSO Domain Service tab. The SSO Domain Service page opens.
16. Click the HTTP Endpoints tab. The HTTP Endpoints page opens.
17. Click X to close the Services: SSOPV2 page. Note: To close forms in Infor Rich client, click the X in the upper-right corner of the form or click the X on the thumbnail of the form in the top-left corner of the canvas.
18. Repeat steps 12-17 for SSOP.
19. Click X to close all open pages.

Lesson 3: Overview of Infor Security
Check your understanding

In which server is ISS installed?

a) LSF  
   b) Infor Landmark  
   c) WebSphere

_____ is an object-oriented model that allows you to build roles and rules and assign multiple roles to users?

a) Grid agent  
   b) Infor Security Services  
   c) Infor Lawson Security

Which of the following authentication protocols would be appropriate if an organization uses Infor Ming.le Enterprise? Select all that apply.

a) Kerberos  
   a) Microsoft ADFS  
   b) LS as STS
Lesson 4: Infor Security Services and user administration

Estimated time
4 hours

Learning objectives
After completing this lesson, you will be able to:

- Describe how the Infor Security Administration® (ISA) tool provides user provisioning, synchronizing, and federation services in environments where Infor Lawson System Foundation and Infor Landmark Technology Runtime are installed and federated.
- Identify the tools available to administer users in version 10 of both LSF and Infor Landmark.
- Identify the available functions of the secadm command.
- Describe the various types of users in both the LSF and Infor Landmark environments.
- Explain why you would use the ISA to maintain user data between environments where LSF and Infor Landmark are federated.
- Identify the available functions of the loadusers command.

Topics
- LSF user overview
- Infor Landmark user overview
- Provisioning a user in ISS
- Disable users in ISS
- Provisioning actors with secadm utility
- Provisioning users with loadusers
- Check your understanding
LSF user overview

An LSF user is an entity set up on your Infor Lawson system that allows a person or system process to be authenticated to LSF applications and services. The user is made up of a people resource plus a single sign-on identity (and any other identities the user needs) plus Infor Lawson metadata.

A people resource is any person in your company for whom you maintain an entry in the Resource Management directory. The resource does not have to be an LSF user.

Resource Management

Resource Management is Infor Security's repository for globally interesting data. Globally interesting data is typically user records, groups, roles, identities and other information that is needed by many Infor Lawson components and which does not change frequently. The data is stored in the LDAP directory.

Resource Management Administrator

The Resource Management Administrator is the tool to add resources and to perform some specialized actions like mass-assigning attributes.

- A resource is a person or thing that is being maintained in Resource Management.
- Attributes are descriptive properties of resources. This can be a name or a Yes/No flag or whatever information is applicable to the resource. When adding or modifying a resource, a list of attributes that can be applied to the resource displays.
  - Most attributes are optional, but a few are required:
    - Each resource must have an ID attribute (called RM ID) and must be unique through the entire Resource Management system.
    - The user’s name: First Name, Last Name, Name

To create a fully defined LSF user, the following components must be linked together:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resource Management ID (RM ID)</td>
<td>RM ID is the term for the unique identifier that each user must have. All users must have an RM ID. The RM ID is typically the identifier that is associated with the SSOP identity and with which a user logs in to Lawson for Infor Ming.le (although it does not have to be). The Security and Resource Management Administrators sometimes use the term RD ID; RM ID and RD ID are interchangeable terms. The screen for adding a new user to Resource Management has an attribute called ID. This attribute contains the RM ID.</td>
</tr>
<tr>
<td>Roles</td>
<td>In the Resource Management system, a role is a set of access rights that a user has to the system. You create roles based on the jobs that users perform at your site. You assign security classes(containers of rules) to roles and then assign roles to users. This is a much more efficient way to assign access rights to users, particularly in systems with many users.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Identities</td>
<td>In Infor Security, an identity is a &quot;passport&quot; to an Infor Lawson component. Users might have multiple identities for components that require authentication. For example, a user might have one identity for accessing the database, and another for self-service applications. The single sign-on component makes it unnecessary for users to sign in again. For administrators, part of setting up a user means creating identities for the user on the services he or she will need.</td>
</tr>
<tr>
<td>Groups (if used)</td>
<td>A group is a set of resources in an organization that can be viewed as a unit.</td>
</tr>
</tbody>
</table>

After an administrator defines a user, they provide them with access to services and applications by linking them to roles. The user’s access rights are then determined by the rules within the security classes that make up each role.

---

**Infor Lawson Security Administrator (LSA)**

*Infor Lawson Security Administrator* (referred to as Lawson Security Administrator or LSA) is the main user interface for Infor Lawson Security. It is the tool for writing rules, creating security classes, administering security profiles, maintaining users, performing system configuration, and running system reports. It is used for performing a large number of user maintenance operations. LSA is only installed on the PCs of users who will be the security administrators for your organization.

Infor Lawson Security Administrator is not recommended to provision LSF users if a system is federated. If a system is federated, Infor Security Services is the recommended tool for user provisioning.

**Lawson Interface Desktop (LID)**

You must define Lawson Resource Management information for each Lawson Interface Desktop user and you must set up an identity that links the user’s Resource Management information to an operating system user. This identity is for the server where your Lawson Environment and applications are.

You must use Lawson Security to set up the profiles, roles, security classes, and security rules that apply to Environment securable objects.

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
Infor Landmark user overview

An Infor Landmark user is an entity set up on your Infor Lawson system that allows a person or system process to be authenticated to Infor Landmark applications and services.

An Infor Landmark user is distinct from an operating system (OS) user or a user account set up on the machine where the Infor Lawson system runs. An Infor Landmark user is also distinct from an Infor Lawson user previously set up for an LSF Environment.

To create a fully defined Landmark user (actor), the user administrator would link together three components: an actor record, an identity, and a service. An actor can have multiple identities if they are set up to access multiple services. For example, actors may have one identity for the operating system (Environment service) and another identity for the Single Sign-On service as shown in the diagram below:

The following table contains important Infor Landmark user administration terminology:

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Actor</td>
<td>An actor represents a user who can act upon a Landmark service. Actors can authenticate to a service if they have a set of credentials, called an identity, for that service. Actor data is stored in the GEN product line, and all data areas share the same actor data.</td>
</tr>
<tr>
<td>Identities</td>
<td>An identity is a set of credentials that uniquely identifies a subject for a particular Landmark service. For example, a user name and a password may be sufficient to identify a subject for a service. An actor (or agent, in the case of data area specific applications) must have an identity for the service in order to access that service. An actor can have multiple identities, for example, one for the operating system and one for the Single Sign-On service.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Actor Agent</td>
<td>An agent is a unique subject within a specified application domain. Agent data is stored in the data area the agent is associated with; each data area has its own agent data. For example, a Requester is an agent in the Infor Lawson Buyer application. An Employee is an agent in the Human Resources application. An actor could be a Requester when accessing the Infor Lawson Buyer application and an Employee when accessing the Human Resources system.</td>
</tr>
<tr>
<td>Actor Context</td>
<td>Actor context values are user attributes that can be used for authorization and application defaulting purposes. Administrators designate key fields as a context property and then assign context values for the context property for individual users. The context value is used to filter what a user can see or access. For example, Infor Talent Management requires all users to be associated with a particular HR Organization, e.g., 7000. Actors assigned the HR Organization = 7000 Actor Context will only see data associated with their assigned HR Organization.</td>
</tr>
</tbody>
</table>

After an administrator defines a user, they provide them with access to services and applications by linking them to roles. The user’s access rights are then determined by the rules within the security classes.

![Infor Landmark Technology user example](image)

Identities are associated with authenticating the actor, and roles are associated with authorizing the actor.

This chart provides a comparison between key user administration terms used in LSF and Infor Landmark.

<table>
<thead>
<tr>
<th>LSF</th>
<th>Infor Landmark</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity</td>
<td>Agent</td>
</tr>
<tr>
<td>(The three Infor Landmark terms which together parallel the function of an Identity in LSF.)</td>
<td>Actor Context</td>
</tr>
<tr>
<td>User</td>
<td>Identity</td>
</tr>
<tr>
<td></td>
<td>Actor</td>
</tr>
</tbody>
</table>

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
Provisioning a user in ISS

Infor Security Services Configuration Guide

ISS user provisioning procedures summary

1. Enter shared information, which represents a super-set of information that links all user data in a federated system.

2. Enter Infor Landmark specific attributes which represent fields directly tied to an actor affecting the Infor Landmark security system and processing for the actor.

3. Enter LSF specific attributes, which represent the fields directly tied to a resource affecting the LSF system and processing for the user.

4. Enter identities, which represent the user credentials and agents for Infor Landmark and LSF.

5. If online user, enter data to have basic access rights to the Lawson Environment.

Demo: Add a new user in Active Directory
Your instructor will demonstrate how to add a new user in Active Directory.
Exercise 4.1: Add a new user in Active Directory

In this exercise, you will add a new user in Active Directory.

Exercise 4.1 steps

Part 1: Add a new user

1. Double-click the RDP Shortcuts folder on the Infor Landmark server’s training desktop. The folder opens listing the RDP shortcuts available.
2. Select the GDEDC-2011.rdp server link. The Domain Controller training desktop opens.
4. Right-click Users on the left side of the Active Directory Users and Computers window.
6. Type Taylor in the First name field.
7. Type Wang in the Last name field.
8. Type user08 in the User logon name field.
9. Click Next.
10. Type Tr@in123 in the Password field.
11. Type Tr@in123 in the Confirm Password field.
12. Clear the User must change password at next logon check box.
13. Select the Password never expires check box.
14. Click Next.
15. Click Finish. The user Taylor Wang now appears in the list of users displayed on the right panel.

Part 2: Modify user profile by adding an email account

1. Double-click the Taylor Wang user record from the list of users in the right panel. The Taylor Wang properties window opens.
2. Click the General tab.
3. Type user08@edu.com in the Email field.

Part 3: Add group membership

Note: You will add three objects in this tab. Separate each object with a semicolon. After each object is typed, click Check Names to verify the object exists in the system.

64 Lesson 4: Infor Security Services and user administration
1. Click the Member Of tab.
2. Click Add.
3. Type Administrators in the Enter the object names to select field.
4. Click Check Names. The system searches for the Administrators group and, if found, the word is underlined. If not found, check the spelling to ensure it is spelled correctly.
5. Type lawdev.
6. Click Check Names.
7. Type lawusers.
8. Click Check Names.
9. Click OK. Notice the list of memberships now displays for the user.
10. Click Apply.
11. Click OK.
12. Click X to close the Active Directory Users and Computers window.
13. Select Start > Log off > Disconnect to return to the Infor Landmark training server.

Demo: Create a new Human Capital Management (HCM) user using Infor Security Administrator

Your instructor will demonstrate how to create a new HCM user using ISA.

Exercise 4.2: Create a new Human Capital Management (HCM) user using Infor Security Administrator

In this exercise, you will create a new HCM user using ISA. You will be logged in as the lawson administrator to add the user.

Exercise 4.2 steps

Part 1: Enter user data in Basic tab
1. Double-click the lsf10 server link icon in the RDP Shortcuts folder. The LSF10 training desktop opens.
2. Double-click the Infor Security Admin icon in the LSF10 training desktop. The ISA login screen opens.
3. Type lawson@gdeinfor2.com in the User name field.
4. Type Tr@in123 in the Password field.
5. Click **Sign In**. The **ISA** tool administrator home page opens.


7. Type **user08** in the **Actor ID** field.

8. Select the search icon in the **Role** field. The **Roles** list window opens.

9. Select the **Admin_ST** from the **Roles** list panel.

10. Click the **right-facing arrow** to move the role to the **User Roles** list panel.

11. Repeat steps 9 and 10 to add the following roles:

   - BenefitAdministrator_ST
   - CompensationAnalyst_ST
   - DataAreaAdmin_ST
   - Employee_ST
   - Manager_ST
   - ProcessServerAllAccess_ST

12. Click **OK** to close the **Roles** window.

13. Type **Taylor** in the **Given Name** field.

14. Type **Wang** in the **Family Name** field.

15. Type **user08@edu.com** in the **Email Address** field.

16. Type **en** in the **ISO Language** field.

17. Click **Next**.

**Part 2: Enter data in Landmark tab**

1. Type the following data in the field specified:

<table>
<thead>
<tr>
<th>Field</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Municipality</td>
<td>St Paul</td>
</tr>
<tr>
<td>State Province</td>
<td>MN</td>
</tr>
<tr>
<td>Country</td>
<td>US</td>
</tr>
<tr>
<td>Address Line 1</td>
<td>409 St. Peter Street</td>
</tr>
<tr>
<td>Postal Code</td>
<td>55102</td>
</tr>
</tbody>
</table>

2. Click **Next**.

**Part 3: Enter data in LSF tab**

1. Type the following data in the field specified:

<table>
<thead>
<tr>
<th>Field</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Taylor Wang</td>
</tr>
<tr>
<td>Product Line</td>
<td>Apps10</td>
</tr>
</tbody>
</table>
2. Click **Next**.
3. Click the **Save** icon. The following message displays: “User has been added successfully. Do you want to go to Identity configuration page?”
4. Click **Yes**. The **Manage Identity** page opens.

### Part 4: Enter user identity services

1. Select the **SSOP** service in the **LSS – LSF10.GDEINFOR2.COM** section.
2. Type the following data in the field specified for the **SSOP** service: **Note**: You may have to scroll up to see the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO Locale</td>
<td><strong>en</strong></td>
</tr>
<tr>
<td>User</td>
<td><a href="mailto:user08@gdeinfor2.com">user08@gdeinfor2.com</a></td>
</tr>
<tr>
<td>Password</td>
<td>Tr@in123</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Tr@in123</td>
</tr>
</tbody>
</table>

3. Click **Save**. The message “Add Identity completed successfully” displays.
4. Click **OK**.
5. Select the **LSF10** service in the **LSS – LSF10.GDEINFOR2.COM** section.
6. Type the following data in the field specified for the **LSF10** service:

<table>
<thead>
<tr>
<th>Field</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain User</td>
<td>gdeinfor2\user08</td>
</tr>
<tr>
<td>Password</td>
<td>Tr@in123</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Tr@in123</td>
</tr>
</tbody>
</table>

7. Click **Save**.
8. Click **OK**.
9. Select the **LSS** service in the **LSS – LSF10.GDEINFOR2.COM** section.
10. Type the following data in the field specified for the **LSS** service:

<table>
<thead>
<tr>
<th>Field</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>gdeinfor2\user08</td>
</tr>
<tr>
<td>Password</td>
<td>Tr@in123</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Tr@in123</td>
</tr>
</tbody>
</table>
11. Click **Save**.
12. Click **OK**. **Note:** Notice the three identifies added now have key icons next to their names on the list.
13. Select the **apps10_EMPLOYEE** service.
14. Type the following data in the field specified for the **apps10_EMPLOYEE** service:

<table>
<thead>
<tr>
<th>Field</th>
<th>Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Company</td>
<td>7000</td>
</tr>
<tr>
<td>Employee</td>
<td>1107</td>
</tr>
</tbody>
</table>

15. Click **Save**.
16. Click **OK**.
17. Click **Sign Out** (right-facing arrow in upper right of screen).
18. Click **X** to close the **Infor Security Administrator** session.

### Part 5: Check Taylor Wang’s access to Infor Ming.le application

1. Double-click the **Infor Lawson for Infor Ming.le™** icon on the LSF10 server’s training desktop. The **Infor Lawson for Infor Ming.le** session opens.
2. Type **user08@gdeinfor2.com** in the **User name** field.
3. Type **Tr@in123** in the **Password** field.
4. Click **Sign In**. The error message “**Infor Lawson cannot load because the Profile service return an error: Error occurred while accessing data**” displays. This is because user08 does not have the LSF10 environment added to his profile.
5. Click **X** to close the **Infor Ming.le** tab and session.

### Part 6: Check Taylor Wang’s access to Infor Landmark’s Infor Rich Client application

1. Double-click the **Infor Rich Client HCM** icon on the LSF10 server’s training desktop. The **Infor Rich Client** login window opens.
2. Type **user08@gdeinfor2.com** in the **User Name** field.
3. Type **Tr@in123** in the **Password** field.
4. Click **Login**. The **Taylor Wang** canvas opens. **Note:** Taylor Wang is able to access the Infor Rich Client application because he has the appropriate access to the HCM data area based on the roles he was assigned in ISA.

Notice the applications displayed on the Infor Rich Client HCM canvas include the Manager, Position Budget Manager, and Benefits which are directly related to the roles assigned to Taylor Wang in ISA.
5. Click the **Benefits** icon on the canvas. The **Benefits Manager** window opens.
6. Select **Reports > By Resources**. The **By Resources** list opens.
7. Click **X** to close the **By Resources** list.
8. Click **X** to close the **Benefits Manager** window.
9. Click the **Employee** icon on the canvas.
10. Select **My Profile**. The error message “**Cannot open Profile. Create action is not available**” displays. The My Profile page is not accessible to Taylor Wang because he does not have an Agent attached to his actor record.
11. Click OK to close the error window.
12. Click X to close Infor Rich Client.

Part 7: Check Taylor Wang’s access to Infor Smart Office to access Infor Lawson applications

1. Double-click the Infor Smart Office icon on the LSF10 server’s training desktop. The Infor Smart Office login window opens.
2. Type user08@gdeinfor2.com in the User Name field.
3. Type Tr@in123 in the Password field.
4. Click the blue arrow. Note: The Infor Smart Office home page opens with the error “Unable to establish communications with Lawson application server…” Taylor Wang does not have the necessary role or service to access the Infor Smart Office application to access Infor Lawson Enterprise applications.
5. Click X to close the error window.
6. Click X to close the Infor Smart Office application.

Demo: Assign the Employee Agent to a user
Your instructor will demonstrate how to assign the Employee Agent to a user.

Exercise 4.3: Assign the Employee Agent to a user
In this exercise, you will assign the Employee Agent to Taylor Wang so he can access his My Profile page in Infor Rich Client.

Exercise 4.3 steps

Part 1: Log in as an administrator and assign the Employee Agent to the Taylor Wang actor record

2. Type lawson@gdeinfor2.com in the User Name field.
3. Type Tr@in123 in the Password field.
4. Click Login. The lawson Infor Rich Client canvas opens.
5. Select Start > Data > person > Business Classes > Agent. The Agent list opens.
6. Click Search (magnifying glass) icon.
7. Type Employee in the Agent Type column.
8. Type 7000, 1107 in the Name column.
9. Press Enter. The Agent list displays the result.
10. Select the Employee / 7000, 1107 record.
11. Select Actions > Link to Actor. The Agent window opens.
12. Click the right-facing arrow in the Actor field. The Actor List opens.
13. Type user08 in the Actor ID field.
14. Press Enter. The user08 record displays.
15. Double-click the user08 record.
16. Click OK. Note: The message “Link to Actor Completed” appears in the bottom-left corner of the canvas The Employee Agent is now linked to the Taylor Wang’s Actor record.
17. Select Start > Logoff.
18. Click Yes to the “Did you intend to close Infor Rich Client” message. You will log back in to Infor Rich Client as Taylor Wang in Part 2 of the exercise to re-check his access to the My Profile page.

Part 2: Log in as Taylor Wang to access the My Profile page
2. Type user08@gdeinfor2.com in the Login Name field.
3. Type Tr@in123 in the Password field.
4. Click Login. The Taylor Wang canvas opens.
5. Select Employee > My Profile. The Taylor Wang Profile now opens because his existing employee profile in Talent Management is now tied to his Actor record and is viewable to him.
6. Click X to close all open windows.
7. Click X to close Infor Rich Client.

Demo: Provision access to Infor Lawson applications
Your instructor will demonstrate how to provision access to Infor Lawson applications.

Exercise 4.4: Provision access to Infor Lawson applications
In this exercise, you will provision access to Infor Lawson applications in ISA.
Exercise 4.4 steps

Part 1: Log in as an administrator to ISA to provision Infor Lawson application access to Taylor Wang

1. Double-click the Infor Security Admin icon on the LSF10 server’s training desktop. The ISA login screen opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The ISA tool administrator home page opens.
5. Select the People check box in the Select resource types field (upper right of screen).
6. Type user08 in the Search field.
7. Press Enter. The user08 record displays.
10. Select APPS10: APPS10 in the Data Area/ID field.
11. Click Save.
12. Click Yes to save changes. The message “Environment information for the user user08 was saved successfully” window displays.
13. Click OK.
14. Click X to close the tab and end the browser session for the ISA application.

Part 2: Check Taylor Wang’s access to Infor Lawson applications in Infor Lawson for Infor Ming.le

1. Double-click the Infor Lawson for Infor Ming.le icon in the LSF training desktop. The Infor Lawson for Infor Ming.le server login window opens.
2. Type user08@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Lawson for Infor Ming.le home page opens.
5. Type HR11.1 in the Search field (upper right of page). The Employee application opens. Taylor Wang now has access to Infor Lawson Enterprise applications.
6. Click X to close the browser session for Infor Lawson for Infor Ming.le.

Part 3: Check Taylor Wang’s access to Infor Smart Office to access Infor Lawson applications

1. Double-click the Infor Smart Office icon in the LSF training desktop. The Infor Smart Office login window opens.
2. Type user08@gdeinfor2.com in the User Name field.
3. Type Tr@in123 in the Password field.
4. Click the blue arrow. The Infor Smart Office home page opens displaying the Navigator widget.
5. Select Infor Lawson > Lawson Applications > Benefits Administration > Setup in the Navigator.
7. Click X to close all open windows.
8. Click X to close Infor Smart Office.
9. Click Yes to confirm closing Infor Smart Office.
10. Select Shut down or sign out > Disconnect to return to the Infor Landmark training desktop.

**Actor Context**

Actor context values are user attributes that can be used for authorization and application defaulting purposes. The administrator designates a key field as a context property and then assigns context values for this context property for individual users.

Actor context values are used in both application data and security processing, such as by affecting which data an actor (user) may view.

**Demo: Assign an Actor Context for a user**

Your instructor will demonstrate how to assign an Actor Context value for a user.

**Exercise 4.5: Assign an Actor Context for a user**

In this exercise, you will assign an Actor Context value for Taylor Wang.

**Exercise 4.5 steps**

2. Type lawson@gdeinfor2.com in the User Name field.
3. Type Tr@in123 in the Password field.
4. Click Login. The lawson Infor Rich Client canvas opens.
7. Click the right-facing arrow in the Actor field. The Actor List opens.
8. Type user08 in the Actor ID field.
10. Select the user08 record.
11. Click Select. The Actor Context window opens.
12. Click the right-facing arrow in the Unique ID field.
13. Select the **HROrganization Key** field.
14. Type **7000** in the **Value** field.
15. Click **Save**.
16. Click **X** to close the **Actor Context** field.
17. Click the **Search** icon to open the filter fields.
18. Type **user08** in the **Actor Name** field in the **Context List** page.
19. Press **Enter**. Notice the user08 ActorContext record returns results.
20. Click **X** to close the **Context List** field.
21. Click **X** to close **Infor Rich Client**.
Disable users in ISS

*Resources and Security Administration Guide*

If a user should no longer be permitted to access LSF or Infor Landmark – for example, the user is no longer employed with your organization – the user’s profile should be disabled. Disabling a user prevents the user from logging in but does not delete the user from the system. The user can be enabled again in the future if needed.

A user may be deleted from the system; however, this should only be done after all records involving the user have been archived. Once the user is deleted from the system, any records of his or her interaction with the system such as creating, modifying, or viewing specific data pieces, will be lost unless the data has been archived.
Provisioning actors with secadm utility

*Infor Landmark Utilities Reference Guide*

The Security Administration utility (secadm) is a powerful tool that allows an administrator to configure a wide range of settings for the system, user authentication, or authorization. It is accessed via the Infor Landmark Command Prompt.

The secadm utility can be used in three ways from the Command Prompt.

- **Single command** - A fully qualified command with all parameters identified
- **Menu** prompt - Using –m to launch menu driven option for parameters
- **Script** execution - Using –f to submit a formatted file in Batch mode

**Note:** The secadm utility maybe password protected. If so, the –p parameter must contain the current password for the command to be executed.

**Secadm single command**

The following are typical uses for single command:

- User maintenance (Infor Landmark Rich Client recommended)
- User security listings
- Security maintenance (Infor Landmark Rich Client recommended)

**Note:** Additional instruction on the use of secadm may be accessed by taking the course *Infor: Administering Landmark Technology Runtime.*

**Demo: Execute the secadm security list**

Your instructor will demonstrate how to execute the secadm security list.

**Exercise 4.6: Execute the secadm security list**

In this exercise, you will execute the secadm security list for the user *user08* to view its context, agent, roles and assigned security classes.

**Exercise 4.6 steps**

1. Double-click the *Command Window for LMRK10* on the Infor Landmark server's training desktop. The *Command Prompt* window opens.
2. Type `secadm -p Global08 security list user user08` in the **Command Prompt** line.

3. Press Enter. The security policy for user08 displays.

How to read the input:

```
Security Policy for Actor:user08:
  dataArea: APPS10
  actorContext not found.
  agents not found.
  role: ProcessServerAllAccess_ST
    secClass: BasicProductLineAccess_ST
    secClass: ProcessServerAllAccess_ST
    secClass: ProductLineAccess_ST
    secClass: ScheduledActionsAccess_ST

  dataArea: GEN
  actorContext not found.
  agents not found.
  role: ProcessServerAllAccess_ST
    secClass: BasicProductLineAccess_ST
    secClass: ProcessServerAllAccess_ST
    secClass: ProductLineAccess_ST
    secClass: ScheduledActionsAccess_ST

  dataArea: HCM
  actorContext: 
    Key Field: HROrganization
      Value: J000
    agents:
      businessClassName: Employee
      Value: J000, J007
  role: Employee_ST
    secClass: HRMEmployee_ST
    secClass: AuthoringUserAccess_ST
    secClass: BNEmployee_ST
    secClass: HREmployeeST
    secClass: BasicProductLineAccess_ST
    secClass: CompanyPlnEmp_ST
    secClass: CombinedUser_ST
```

**Secadm security policy list output**

The access (roles) the actor has in the APPS10 data area

The access (roles) the actor has in the GEN data area

The context values the actor has in the HCM data area

The actor agent the actor is tied to in the HCM data area

The access (roles) the actor has in the HCM data area

**Secadm commands to create user records**

Users may be created in secadm individually or in batches.

**Individual secadm commands**

The table below explains the purpose of the secadm commands and how they are built.

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create actor</td>
<td>secadm actor add actor [-firstname &lt;firstname&gt;] [-lastname &lt;lastname&gt;]</td>
</tr>
<tr>
<td></td>
<td>For example: <code>secadm actor add user01 [- -firstname Marcia] [- -lastname Hudson]</code></td>
</tr>
<tr>
<td>Purpose</td>
<td>Command</td>
</tr>
<tr>
<td>---------</td>
<td>---------</td>
</tr>
</tbody>
</table>
| Create actor identity | `secadm identity add <servicename> <identityname> [--password <password>] [-- domainuser domain\user]`  
**For example:** `secadm identity add SSOP user01@gdeinfor2.com --password Tr@in123` |
| Provide actor context record for the actor | `secadm actor context add <actorname> <data area> <KeyField> <Value>`  
**For example:** `secadm actor context add user01 HCM HROrganization 7000` |
| Link actor to an agent in the application | `secadm actor link add <actorname> <data area> <agent type> <KeyField> <key value>`  
**For example:** `secadm actor link add user01 HCM Employee HROrganization 7000` |
| Assign a role to an actor | `Secadm role assign <actor> <role>`  
**For example:** `secadm role assign user01 APIAManager_ST; Employee_ST` |

**Batch secadm commands**

Using batch `secadm` is one of two ways to bulk load users into the system.

- If you have an Infor Landmark standalone application, you may use secadm to bulk load users.
- If you have an Infor Lawson System Foundation standalone system, you may use loadusers to bulk load users.
- If you have a federated system, you may use either utility but synchronization may be required to place both systems into sync.

Multiple `secadm` commands can be aggregated into a file and executed. For example:

- `secadm --f <filename>`
- `secadm provision os` (Loads Infor Landmark Actor based on OS)
- `secadm load classic` (Loads Infor Landmark Actor based on Infor Lawson users)

**Demo: Create a Finance user using the secadm command**

Your instructor will demonstrate how create a Finance user using the secadm command.
Exercise 4.7: Create a Finance user using the secadm command
In this exercise, you will create a Finance user using the secadm command.

Exercise 4.7 steps

Part 1: Create actor
2. Type secadm –p Gloabal08 actor add user01 --firstname Marcia --lastname Hudson in the Command Prompt line.
3. Press Enter. The message “Actor user01 created. DONE.” displays.

Part 2: Add actor identity
1. Type secadm –p Gloabal08 identity add SSOP user01@gdeinfor2.com --password Tr@in123 in the Command Prompt line.
2. Press Enter. The message “Identity user01@gdeinfor2.com for service SSOP created. DONE.” displays.

Part 3: Assign actor identity
1. Type secadm –p Gloabal08 actor assign user01 SSOP user01@gdeinfor2.com in the Command Prompt line.
2. Press Enter. The message “Identity user01@gdeinfor2.com in service SSOP linked to actor use01. DONE.” displays.

Part 4: Assign roles to actor
1. Type secadm –p Gloabal08 role assign user01 APIAManager_ST in the Command Prompt line.
2. Press Enter. The message “Assign role APIAManager_ST to actor use01. DONE.” displays.
3. Type secadm –p Gloabal08 role assign user01 ProcessServerAllAccess_ST in the Command Prompt line.
4. Press Enter. The message “Assign role ProcessServerAllAccess_ST to actor use01. DONE.” displays.
5. Type secadm –p Gloabal08 role assign user01 Employee_ST in the Command Prompt line.
6. Press Enter. The message “Assign role Employee_ST to actor use01. DONE.” displays.

Part 5: Add actor context
1. Type secadm –p Gloabal08 actor context add user01 HCM HROrganization 7000 in the Command Prompt line.
2. Press Enter. The message “Attribute HROrganization and value set to 7000 added to actor user01. DONE.” displays.

Part 6: Link actor to agent
1. Type secadm –p Gloabal08 actor link add user01 HCM Employee 7000 1112 in the Command Prompt line.
2. Press Enter. The message “Agent is not linked to any actor. DONE.” displays. **Note:** This is the correct message to display.

**Part 7: Check Marcia Hudson’s access in Infor Rich Client.**

1. Double-click the **Infor Rich Client HCM** icon on the Infor Landmark server’s training desktop. The **Infor Rich Client** login window opens.
2. Type `user01@gdeinfor2.com` in the **Login Name** field.
3. Type `Tr@in123` in the **Password** field.
4. Click **Login.** The **Marcia Hudson** canvas opens.
5. Select **Start > Applications > Employee.** **Note:** Click the Start button in the upper right of the screen.
6. Click and drag the **Employee** application to the Infor Rich Client canvas.
7. Select **Employee > My Profile.** The **Marcia Hudson Profile** now opens because her existing employee profile in Talent Management is now tied to her Actor record and is viewable to her.
8. Click X to close all open windows.
9. Click X to close **Infor Rich Client.**

The individual secadm commands can also be aggregated and saved to a .txt file for input into the system. The aggregated commands would look like this:

```
secadm --p Global08 actor add user01 --firstname Marcia --lastname Hudson
identity add SSOP user01@gdeinfor2.com --password Tr@in123
actor assign user01 SSOP user01@gdeinfor2.com
role assign user01 APIAManager_ST, ProcessServerAllAccess_ST
actor context add user01 HCM HROrganization 7000
actor link add user01 HCM Employee 7000 1112
```
Provision users with loadusers

Infor Lawson Resources and Security Administration Guide

The loadusers utility

The loadusers utility is an LSF command-line method for:

- Creating a default user
- Mass-loading user data into the Infor Lawson system using an XML file that you create at your site as input

Example command: `loadusers -f file_name -p product_line -d defaultDomain [-a]`

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>file_name</td>
<td>The name of the XML input file</td>
</tr>
<tr>
<td>product_line</td>
<td>The product line that will be used if a product line is not specified for a user in the XML input file</td>
</tr>
<tr>
<td>defaultDomain</td>
<td>This is the user’s Windows domain. This is required when running loadusers on a Windows machine.</td>
</tr>
<tr>
<td>[-a]</td>
<td>The [-a] option appends roles assigned using the loadusers command to the existing list of roles the user has rather than overwriting them.</td>
</tr>
</tbody>
</table>

Loaduser options

```
C:\backup>loadusers
WARNING: Undefined MessageProducer: SecurityConnectionLogger
usage: Load Users
       LoadUsers [options]

options:
   -f xmlFileName  XML file that contains data
   -p defaultProductLine default product line if not set in xml file
   -d defaultDomain  default windows domain, only required for windows
   -u deleteusers  delete roles, groups and users
   -g username     username that was used in the privileged ID
   -a appendroles  append roles to users (default overwrite)
   -t tenantID     select tenant to load users into
   -?               print usage
```

Loaduser option
Mass-loading user attributes

Loadusers may be run at any time to populate the Infor Lawson LDAP with user data. Typically, this is done to initially populate the system. Any attributes that can be associated with a user can be populated, including any unique attributes that you created for your site.

Two example scenarios for which loadusers might typically be used are:

- Adding users and attributes for Self-Service center users: Self-Service center users often have the same or similar access needs on the Infor Lawson system. They also typically make use of the default user.
- Adding users and attributes for users who have unique OS system IDs and who need unique identities on the Infor Lawson Environment service

The loadusers utility is complex and it is easy to make mistakes while using it, especially when creating the XML input file. Depending on your situation, particularly on the number of Infor Lawson users at your site, adding users manually through the Infor Lawson Security Administrator or Infor Security Services may be preferable to using the loadusers utility. The loadusers utility should only be run by administrators who are experienced in creating and troubleshooting XML.

If the loadusers utility is used in a federated system, resynchronization may be required as users will only be loaded to LSF.

The XML input file for loadusers

The loadusers utility takes an XML file as input, which must be created and populated, such as the example shown in this image.

```
<xml version="1.0" encoding="ISO-8859-1"?>
<XML>
    <ROLEDATA>
        <ROLE ID="Employee" Description="Employee" />
        <ROLE ID="Manager" Description="Employee" ParentRole="Employee" />
    </ROLEDATA>
    <GROUPDATA>
        <GROUP ID="EmpGroup" Description="Employee Group" />
        <GROUP ID="MgrGroup" Description="Management Group" />
    </GROUPDATA>
    <USERDATA ProductLine="LAWAPP" SSOFPASSWORD="AbCd1234"
        USER ID="JohnD" RMD="" Name="John Doe"
        FirstName="John" LastName="Doe"
        CheckLS=YES" Roles="Advisor,Manager"
    GROUP="EmpGroup">
    USERDATA>

    <IDENTITIES>
        <IDENTITY ID="johnD" SERVICE="LAWAPP_EMPLOYEE"
            COMPANY="4321" EMPLOYEE="1111" />
        <IDENTITY ID="johnD" SERVICE="LAWAPP_REQUESTER"
            REQUESTER="1111" />
        <IDENTITY ID="janeD" SERVICE="LAWAPP_EMPLOYEE"
            COMPANY="4321" EMPLOYEE="2222" />
    </IDENTITIES>
</XML>
```

Example XML input file - all users use only Self-Service centers
User administration through ISS is recommended in LSF10. This tool keeps the LDAP resources of LSF and the GEN actors of Infor Landmark Technology Runtime in sync.
Check your understanding

In which of the following systems should user administration tasks be completed in a federated system to avoid the need for resynchronization?

a) Lawson Security Administrator  
b) Infor Security Services  
c) Configuration Console  

A _______ is an entity set up on your Infor Lawson system that allows a person or system process to be authenticated to LSF applications and services.

a) Landmark actor  
b) People resource  
c) LSF user  

Which three components would an administrator link to create a fully defined Landmark user (actor)?

a) Identity  
b) Actor record  
c) Service  
d) System password  

The ____________ is the tool to add resources and to perform some specialized actions like mass-assigning attributes.

a) Infor Security Administrator  
b) Infor Rich Client  
c) Resource Management Administrator  

The loadusers utility is an LSF command line used for which of the following? Select all that apply.

a) Creating a default user  
b) Changing the Lawson Environment for a product line  
c) Mass-loading user data into the Infor Lawson system  

In which scenario would an administrator choose to use the [-a] option when using the loadusers utility?

a) To archive a user’s assigned roles  
b) To append a role to a user’s assigned roles  
c) To amend the roles assigned for a user  

Which option should be selected by an administrator when an employee leaves the company?

a) Delete the user record to purge the system  
b) Disable the user and archive the records  
c) Leave the user as active to make the records accessible to the user  

Which of the following are typical uses of the secadm single command? Select all that apply.

a) User maintenance  
b) User security listings  
c) Security maintenance  

d) _________ are typically user records, groups, roles, identities and other information that is needed by many Infor Lawson components and which does not change frequently.

a) Single-sign on credentials  
b) User attributes  
c) Globally interesting data
Where is the globally interesting data stored?

a) Lawson Environment
b) LDAP
c) Infor Landmark Grid
Lesson 5: Defining access and roles for users

Estimated time
2 hours

Learning objectives
After completing this lesson, you will be able to:

- Define the process for modifying roles for LSF in ISA.
- Describe the difference between a security class and a role.
- Define the process for customizing Infor Landmark-delivered security classes using the Configuration Console.
- Describe how to modify a role by adding or removing a security class.
- Explain how actors and users are assigned roles using ISS.

Topics
- LSF roles and security classes
- Infor Landmark-delivered security classes
- Check your understanding
LSF roles and security classes

Roles
In the LSF Resource Management system, a role is a set of access rights that a user has to the system. Administrators create roles based on the jobs that users perform and then assign a role to a user. This is a much more efficient way to assign access rights to users, particularly in systems with many users. Users can, and typically do, have multiple roles.

Inheritance
The concept of inheritance in role creation refers to inheriting security rights of an existing role plus provisioning additional access. For example, let’s say an administrator creates an AP Clerk role with basic security rights. When the administrator then creates an AP Manager role, they would specify AP Clerk as the role it inherits from. The AP Manager role will then automatically have all the rights that the AP Clerk role does. The administrator would simply modify AP Manager to provision the additional access rights.

Lawson role examples
Infor Lawson ships some commonly used roles as examples. Most customers will make use of at least some of these roles after editing them to meet their needs. Most customers will also create new roles to meet unique needs at their sites. Some examples of the roles for which examples are created are:

- Accounts payable clerk
- Accounts payable manager
- Benefits clerk
- Benefits manager

Security class
A security class is a container for security rules. It enables an administrator to create a set of rules that determine the security access needed for a task. After administrators define security classes and the rules they contain, they assign security classes to roles. The result is that rules within security classes govern the security for users with those roles.

Rules
A rule is an instruction for Lawson Security to use to determine the access privileges for users who attempt to use a securable object. Security administrators define rules within security classes. If security classes are constructed appropriately, each security class will contain the rules needed to determine the access for a user to perform a task.

Types of rules:
- Unconditional access
- Unconditional access for one or more actions (e.g. Add, Change, Delete, and Inquire)
- Total denial of access
- Condition access
Infor Landmark-delivered security classes

Security classes
Infor Lawson delivers a set of security classes with the Infor Landmark Technology Runtime environment and with each Infor Landmark application. These delivered security classes have names ending in "_ST" to indicate that they belong to the "standard template" set of security classes.

Infor recommends that you not modify delivered security classes. If the classes do not suit your business needs, we recommend that you copy the delivered security class and configure the copy. Customized security classes can be assigned to roles, and then actors can be assigned to the roles so that they have the appropriate access to your Infor Landmark system. Customized security classes can be created in the Configuration Console if desired.

The Configuration Console
The Configuration Console offers two modes of modification, depending on an end user’s security role: personalizations and configurations.

- **Personalizations**
  Personalizations are changes end users can make to enhance their own experience. These are accessed by clicking Start > My Personalizations. Permission to make personalizations requires the security role of PersonalizationAccess_ST plus another complementary role such as HRGeneralist_ST. Note that the ability to personalize a form, page, or menu may be restricted by some companies or restricted to certain users.

- **Configurations**
  Configurations are global changes an administrator can make to alter a delivered application to fit a business need. These are accessed by clicking Start > Configure > Application. Any application component that can be personalized can also be configured.

A personalization will trump a global configuration; that is, when users personalize their experience, those personalizations will be the default for the individual employee’s view, not the configuration made by another user and set to default.

Configurations may be applied to all users and include customizations of:

- Application layouts
  - Menus
  - Lists
  - Pages
- Form layouts
- Business classes
- Action overrides
- Buttons
- Security roles and security classes
- Mime types
- Web services
- Cache management
Configuration Console security access

A user or administrator must have one of the security roles below to access the Configuration Console and perform configuration tasks.

- ConfigurationAccess_ST
- DataMenuAccess_ST
- SecurityConfigAccess_ST
- ConfigAdminAccess_ST
- GlobalUIConfigAccess_ST

After you open the Configuration Console, you can take action based upon the security classes assigned to your roles as shown in the following table:

<table>
<thead>
<tr>
<th>If you want to grant permission for this task…</th>
<th>Then assign these security classes…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify security classes</td>
<td>SecurityConfigAccess_ST and ConfigAdminAccess_ST</td>
</tr>
<tr>
<td>Work with actors, identity, and roles</td>
<td>SecurityConfigAccess_ST and UserAdminAllAccess_ST</td>
</tr>
<tr>
<td>Note: If a user has the UserAdminAllAccess_ST security class but not the SecurityConfigAccess_ST security class, that user can work with actors, identities, and roles outside of the Configuration Console.</td>
<td></td>
</tr>
<tr>
<td>Application configuration (menus, pages, lists, and forms)</td>
<td>GlobalUIConfigAccess_ST or its equivalent</td>
</tr>
<tr>
<td>Create or modify MIME types and web services</td>
<td>GlobalUIConfigAccess_ST plus create and change action access for the appropriate module and business class. In the case of mime types, a user needs access to the la module and the MimeType business class. In the case of web services, a user needs access to the wsbuilder module and the WebService business class.</td>
</tr>
</tbody>
</table>

Demo: Customize a Landmark-delivered role by adding a security class

Your instructor will demonstrate how to copy a Landmark-delivered role and add a security class to create a custom role using Configuration Console.
Exercise 5.1: Customize a Landmark-delivered role by adding a security class

In this exercise, you will copy a Landmark-delivered role and add a security class to create a custom role using Configuration Console.

Exercise 5.1 steps

Part 1: Create a new role by copying an existing role

2. Type lawson@gdeinfor2.com in the Login Name field.
3. Type Tr@in123 in the Password field.
4. Click Login. The Infor Rich Client canvas opens.
6. Click Roles. The Roles list displays.
7. Click the Search (magnifying glass) icon.
8. Type “personalization” in the Role Name search field.
9. Press Enter. The list of roles with the word ‘personalization’ displays.
10. Select the PersonalizationAccess_ST role from the role list.
11. Select Actions > Copy. The Role window opens. Note: Click the Actions button just at the top of the role search box.
12. Type PersonalizationAccessCustom in the New Role field.
13. Click OK.

Part 2: Add a security class to the newly created role

1. Click the Role Name search field.
2. Press Enter to refresh the search results.
4. Click the Security Classes Assigned to Role tab.
5. Select Actions > Create. Note: Click the Actions button above the Data area. The Role Security Class page opens.
6. Type GEN in the Data Area field.
7. Type GlobalUIConfigAccess_ST in the Security Class field. Note: You may also search for the Data Area and Security Class values.
8. Select Save.
9. Click X to close the Role Security Class page.
11. Click X to close the Role page.
12. Click X to close Infor Rich Client.
Check your understanding

In the LSF system, a _____ is an instruction for Lawson Security to use to determine the access privileges for users who attempt to use a securable object.

   a) Role  
   b) Security class  
   c) Rule

In LSF, an _____ is a container for security rules that allow administrators to create a set of rules that determine the security access needed for a task.

   a) Role  
   b) Actor  
   c) Security class

In LSF, security classes are assigned to __________ that govern the security for users.

   a) Roles  
   b) Actors  
   c) Rules

You can identify security classes in the Infor Landmark Environment because they are appended with the following:

   a) _MD  
   b) _ST  
   c) _LMRK

Which of the following roles would an administrator need to have to make changes to security classes using Configuration Console?

   a) GlobalUIConfigAccess_ST and ConfigAdminAccess_ST  
   b) SecurityConfigAccess_ST and ConfigAdminAccess_ST  
   c) SecurityConfigAccess_ST and UserAdminAllAccess_ST

Which of the following actions are recommended if the security classes delivered by Infor Landmark do not suit your business needs?

   a) Delete the security classes and start over.  
   b) Copy the delivered security class and configure to customize.  
   c) You cannot modify or delete any Infor Landmark security class.
Lesson 6: Federation and synchronization

Estimated time
1 hour

Learning objectives
After completing this lesson, you will be able to:

- Describe the difference between a federated and a stand-alone environment and its impact to user administration.
- Explain the differences between authentication protocol, federation, and primary authentication service.
- Describe the function of Federation Services in ISS.
- Identify which user data is synchronized between LSF and Landmark.
- Describe how to execute ISS synchronization to resolve potential user data inconsistencies.
- Explain how to access the security_provisioning log and its use for troubleshooting synchronization conflicts.

Topics
- Stand-alone vs. federated systems
- Federation procedure overview
- Federation prerequisites
- Synchronization
- Assigning roles
- Troubleshooting synching errors
- Check your understanding
Stand-alone vs. federated systems

Infor Security Services Configuration Guide

Federating

Federating a system means associating two Infor Lawson systems; for example, Infor Lawson System Foundation and Infor Landmark Technology Runtime, so that users (actors or people resources), roles (which include security classes), and groups can be “seen” by either system. Federated systems can have a single source of authentication and administration.

The following diagrams illustrate the problem that federating solves.

Before federation, users/actors who use content on both Infor Lawson platforms must log in to each separately.
After the federation procedure is performed, users/actors can log in to either system (LSF or Infor Landmark) and use applications to which they have been granted access.

After a system has been federated, you should always use Infor Security Services (ISS) to add or update users. This will prevent you from having to run the federation procedure multiple times.
Federation procedure overview

Federation is executed through ISS, following three basic steps:

- Federate a new system (LSF the local system or “TO” and Infor Landmark Technology Runtime the remote system or “FROM”).
- Perform synchronization.
- Configure the primary authentication service.

Federation example

This diagram illustrates federation between LSF and Infor Landmark Technology Runtime.

Federation with LSF and Infor Landmark Technology Runtime
Federation prerequisites

Infor Security Services Configuration Guide

If you are working in a federated system, federation prerequisites have been or will be completed by your installer. Before systems (for example, Infor Lawson System Foundation and Infor Landmark Technology Runtime) are federated, the following prerequisite procedures must be completed:

Infor Lawson System Foundation:
- Perform a complete backup of your LDAP user repository.
- Back up all security-related Infor Lawson configuration files in LAWDIR\system.
- Verify the Infor Lawson LDAP schema has been updated if coming from version 9.x.
- Verify the Readme file for Infor Lawson Security has been examined and all requirements for patching or updating to LSF or DSP have been completed.

Infor Landmark Technology Runtime:
- Perform a complete backup of GEN data area.
- Back up all security-related Infor Lawson configuration files in LASYSDIR:
  - lsservice.properties
  - ssokeystore
  - authen.dat
  - ssotruststore

Both systems:
- Complete all authentication-related configurations. Both pre-federated systems must use the same authentication protocol (LS as STS, Kerberos or Microsoft ADFS). If LS as STS then both systems need to either be bound or the password natively authenticated.
- Test user authentication on each system before federating. To test authentication, log in to LSF Infor Lawson for Infor Ming.le or Infor Landmark Rich Client. This process will cause the SSOServlet to run proving that authentication is working prior to federating.

After federation, an administrator is required to keep the data in sync. If a change to primary authentication service or removal of federated systems is required then contact Infor Xtreme Support or Infor Consulting Services to understand the impact on your system before using ISS to execute.
Synchronization

Synchronization means determining if conflicts exist between the systems being federated. Conflicts occur when one of the systems has the same record (for example, the same security role name exists on both systems). Federated systems, LSF and Infor Landmark Technology Runtime, have been synchronized initially. However, if ISS is not used as the primary tool for updating users then resynchronization may be required. If conflicts exist, the administrator is given options to resolve those conflicts.

Synchronization occurs for the following areas:

- Roles
- Actors
- Services
- Domains
- Endpoints
- Endpoint groups
- Identities

An important job of the federation wizard is synchronizing systems that make up the federation. The wizard assists in the process of resolving identified conflicts. Conflicts occur when one of the systems has the same record (for example, the same security role name exists on both systems).

The wizard groups conflicts by type of data. The sub-sections that follow describe the choices are available in the wizard to resolve conflicts found between the “Local” system being federated TO and the “Remote” system being federated FROM.

Infor Lawson System Foundation is always the “Local” or “To” system due to ISS being installed on that server. Infor Landmark Technology Runtime is always the “Remote” or “From” system.

Roles conflicts

A role conflict means that the synchronization process has found that the system it is currently attempting to federate has at least one role name in common with the system to which it is being federated. The wizard presents the following choices:

<table>
<thead>
<tr>
<th>Federation choices</th>
<th>Default behavior</th>
<th>Risks/implications</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore all conflicts</td>
<td>Applied to all conflicts</td>
<td>The default behavior results in the roles being merged so that they contain all security classes for the role on each system. All users from both systems are assigned the role. Take this action if you know that the role provides access to classes that users on both systems should have. This action could have potential security risks. For example, if you have a role on System A called &quot;AppAdmin&quot; that gives access to all programs and data in the AP system. On System A, this role is assigned to the AP department managers. On System B, you also have a role called &quot;AppAdmin&quot; that gives access to all programs and data in the Infor Talent Management system that is assigned to HR managers. If you select &quot;Ignore all conflicts&quot; in this case, the AP managers are able to see confidential HR information and HR managers have access to Enterprise vendor payment tools.</td>
</tr>
</tbody>
</table>

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
<table>
<thead>
<tr>
<th>Federation choices</th>
<th>Default behavior</th>
<th>Risks/implications</th>
</tr>
</thead>
</table>
| Rename the role on the “local” machine (the machine that you are federating to) OR Rename the role on the “remote” machine (the machine that you are federating) | Using the AppAdmin role as an example, and assuming that System A is the local machine, if you select Rename the role on the local machine (new name = APAppAdmin), the remote system retains the role AppAdmin role (full access to Infor Talent Management) and System A users are removed from the role. The role APAppAdmin also exists on the federated system and only the System A users of the “old” AppAdmin role are attached to APAppAdmin. | Do not include spaces in role names; use an underscore as a separator if needed.  

![Diagram showing before and after federation](image)

Before federation:

- **System A** (Local; System that is being federated TO)
  - AppAdmin Role: access to all vendor payment programs and data

- **System B** (Remote; System that is being federated)
  - AppAdmin Role: access to all HR programs and data

After federation:

- **System A+B, federated**
  - Renamed role: APAppAdmin Role: access to all vendor payment programs and data
  - AppAdmin Role: access to all HR programs and data

Role conflicts example
**Actor conflicts**

Actor conflicts occur when the unique ID of an actor (user) is found on both systems but some attributes that must be the same, for example: LastName and FirstName are not the same. This could happen for a number of reasons, including a misspelling of LastName on one system, using a nickname for FirstName on one system, or incorrectly assigning a unique ID.

When the synchronization process identifies actor conflicts, they are displayed in a list. The wizard presents the following choices:

- **Handle all conflicts in the same way**
  For this response, you select Update Local Actor or Update Remote Actor. With this choice you are indicating that when a conflict exists, the selected machine (Local or Remote) contains the correct information. Match differences on the other system to this system’s information.

- **Handle each conflict individually**
  For this option, you select a conflict from the list and, when a dialog box showing the attributes that are in conflict appears, make changes as needed to the attributes.

**Service, domain, endpoints, and endpoint group conflicts**

Service conflicts arise when both systems have a service with the same name. These conflicts are handled the same as roles.

**Identity conflicts**

An identity conflict arises when the same identity is found in both systems. These conflicts are handled the same as actors, for example the SSOP identity and the SSOPV2 identity password do not match.
Resolve conflict icons

An example of the kinds of icons that the synchronization process displays when it encounters a conflict differs depending on the type of resource and type of conflict. In general, the icons to the left of the blue vertical bar are for displaying conflicts. The icon to the right is for taking action.

![Conflict icons diagram]

**Demo: Explore ISS Federation Services**

Your instructor will demonstrate how to explore ISS Federation Services.

---

**Exercise 6.1: Explore ISS Federation Services**

In this exercise, you will explore ISS Federation Services.

**Exercise 6.1 steps**

1. Double-click the **RDP Shortcuts** folder on the Infor Landmark server’s training desktop. The folder opens with the list of servers.
2. Select the **LSF10.rdp** server link. The **LSF** training desktop opens.
3. Double-click the Infor Security Admin icon on the LSF server’s training desktop. The ISA login screen opens.

4. Type lawson@gdeinfor2.com in the User name field.

5. Type Tr@in123 in the Password field.


Note the following:
- The LSF10 (server name ending in LSF) is the primary system and federated to the remote system Infor Landmark (server name ending in Landmark).
- The ISS (server name ending in LSS) is showing a connection (called the Hub) between the two systems.
- The areas of roles, actors, services, domains, endpoints, endpoint groups, and identities are all marked green.
- The Sync column allows the ability to resynchronize the remote system (Infor Landmark) to LSF.

7. Click – to minimize ISA.

Demo: Locate and delete the security_provisioning.log

Your instructor will demonstrate how to locate and delete the security_provisioning.log.

-------------------------------------------------------------------------------------------------------------------

Exercise 6.2: Locate and delete the security_provisioning.log

In this exercise, you will locate and delete the security_provisioning.log.

Exercise 6.2 steps

1. Select Start > This PC > Apps (E:) > LSF10 > law > system. The System folder opens.
2. Right-click the security_provisioning.log file.
3. Select **Delete**. You should remove this log file before the synchronization to limit the records to only this federation synchronization run.

4. Click **X** to close the **System** folder.

**Demo: Sync the environment**

Your instructor will demonstrate how to sync the environment.

**Exercise 6.3: Sync the environment**

In this exercise, you will sync the environment. Before synching the environment, you will first check to see if the custom role you had created *PersonalizationAccessCustom* appears in the role list in ISA as well as check whether Marcia Hudson, user01, appears in Lawson Security Administrator.

**Exercise 6.3 steps**

**Part 1: Check for the custom role in ISA**

1. Click the **ISA** icon from the task bar to maximize the application.
2. Select the **Role** check box in the **Select resource type** field (upper right of screen).
3. Type **Personalization** in the **Search** field.
4. Press **Enter**. Notice that there is no resulting record for the search. The custom role only exists in Infor Landmark and not in LSF. A sync is required to align the data in both environments.

**Part 2: Check for user01 in the Infor Lawson environment using Lawson Security Administrator**

1. Double-click the **Lawson Security Administrator** icon on the training desktop. The **Lawson Security Administrator** application opens.
2. Select **https://lsf10.gdeinfor2.com** in the **Server URL** field.
3. Click **Connect**. The **Lawson Security Administrator** login window opens.
4. Type **lawson@gdeinfor2.com** in the **User name** field.
5. Type **Tr@in123** in the **Password** field.
6. Click **Sign in**.
7. Click the **User Management** tab.
8. Select **User Maintenance**. The **People** form opens.
9. Click the Advanced tab.
10. Select ID in the Define Criteria section.
11. Type user01.
12. Click Add.
13. Click Find Now. Notice that the user doesn’t exist in the LSF environment. A sync is required to align the data in both environments.
14. Click – to minimize the Lawson Security Administrator application.

Part 3: Sync the environment using the ISA tool
1. Click the ISA icon from the task bar to maximize the application.
3. Click the sync icon (double circular arrows). The Federation Window opens.
4. Click Yes to confirm the sync.
5. Click the Ignore (minus sign) icon for Role conflicts. Note: All roles are in conflict because they already existed.
6. Click the Ignore icon for Services conflicts. Note: All services are in conflict because they already existed.
7. Click the Ignore icon for Domain conflicts. Note: All domains are in conflict because they already existed.
8. Click the Ignore icon for Endpoint conflicts. Note: All endpoint are in conflict because they already existed.
9. Click the Ignore icon for Endpoint Group conflicts. Note: All endpoint are in conflict because they already existed.
10. Click OK on the Federation Manager message box.
11. Click X to close the ISA tab and browser session.

Part 4: Recheck user01 in Lawson Security Administrator
1. Click the Lawson Security Administrator application from the task bar to maximize.
2. Click the User Maintenance tab. The People form opens.
3. Click the Advanced tab.
4. Select ID in the Define Criteria section.
5. Type user01.
6. Click Add.
7. Click Find Now. Notice that the user now exists in the LSF environment.
8. Click X to close out of LSA.
Assigning roles

A role is a set of access rights that allow a user access to the system. After creating roles and security classes, you can assign security classes to roles, and then assign roles to actors within the system.

**Demo: Assign the custom role to the Finance user**

Your instructor will demonstrate how to assign the custom role to the Finance user.

**Exercise 6.4: Assign the custom role to the Finance user**

In this exercise, you will modify a user’s record using ISA post federation to assign the custom role you had created in exercise 5.2. In addition, you will update the user record by adding an email account.

**Exercise 6.4 steps**

**Part 1: Enter user data in Basic tab**

1. Double-click the **Infor Security Admin** icon on the LSF10 server’s training desktop. The **ISA** login screen opens.
2. Type *lawson@gdeinfor2.com* in the **User name** field.
3. Type *Tr@in123* in the **Password** field.
4. Click **Sign In**. The **ISA** tool administrator home page opens.
5. Select the **People** check box in the **Select resource type** field (upper right of screen).
6. Type *user01* in the **Search** field.
7. Press **Enter**. The **People** list displays the **user01** record.
8. Click the **Edit resource** (pencil icon). The **user01** record opens.
9. Click the **Basic** tab.
10. Click the search icon in the **Role** field. The **Roles** list window opens.
11. Select the **PersonalizationAccessCustom** role from the **Roles** list panel.
12. Click the **right-facing arrow** to move the role to the **User Roles** list panel.
13. Click **OK**.
14. Type *user11@edu.com* in the **Email** field.
15. Click **Save**. The confirmation message window opens.
16. Click **OK** to close the message window. The custom role is now assigned to **Marcia Hudson**, user01.
17. Click **X** to close the ISA tab and browser session.
Troubleshooting synching errors

You should execute all user provisioning in the Infor Security Administrator tool in a federated environment. If Lawson Security Administrator, loadusers, ssoconfig, RM Update node, actor management, secadm, or Landmark node is used to administer or provision users then potentially user data across federated systems may no longer be synchronized.

To validate that data is synchronized, use the Infor Security Administrator tool to resynchronize and resolve any conflicts or issues.

Demo: Create a new Procurement user in a federated environment

Your instructor will demonstrate how to create a new Procurement user in a federated environment.

Exercise 6.5: Create a new Procurement user in a federated environment.

In this exercise, you will create a new Procurement user in a federated environment using the Lawson Security Administrator tool. This procedure is supported, however it is not recommended once an environment is federated.

Exercise 6.5 steps

Part 1: Enter user data in Basic tab

1. Double-click the Lawson Security Admin icon on the LSf10 server’s training desktop. The Lawson Security Administrator server window opens.
3. Click Connect. The Lawson Security Administrator login window opens.
4. Type lawson@gdeinfor2.com in the User name field.
5. Type Tr@in123 in the Password field.
6. Click Sign In. The Lawson Security window opens.
9. Type en in the ISOLocale field.
10. Type APPS10 in the Product Line field.
11. Type Matthew in the First Name field.
12. Type user02 in the ID field.
13. Type Lincoln in the Last Name field.
14. Type user02@edu in the Email field. Note: This is the incorrect syntax you will be correcting for this exercise.
15. Click Next. The Identity Information window opens.

Part 2: Add identities
2. Type gdeinfor2\user02 in the Domain_User field.
3. Type Tr@in123 in the Password field.
4. Type Tr@in123 in the Password Confirm field.
5. Select LSS. The LSS form opens.
6. Type Tr@in123 in the Password field.
7. Type Tr@in123 in the Password Confirm field.
8. Type gdeinfor2\user02 in the User field.
9. Select SSOP. The SSOP form opens.
10. Type Tr@in123 in the Password field.
11. Type Tr@in123 in the Password Confirm field.
12. Type user02@gdeinfor2.com in the User field.
13. Select APPS10_EMPLOYEE. The APPS10_Employee form opens.
14. Type 7000 in the Company field.
15. Type 1119 in the Employee field.

Part 3: Add Lawson Environment
1. Click the arrow in the Data Area/ID field. A list of data areas displays.
2. Select APPS10.
3. Click Finish.
4. Click – to minimize the Lawson Security Administrator.

Part 4: Delete security_provisioning.log
1. Select Start > This PC > Apps (E:) > LSF10 > law > system. The System folder opens.
2. Right-click the security_provisioning.log file.
3. Select Delete. You should remove this log file before the synchronization to limit the records to only this federation synchronization run.
4. Click X to close the System folder.

Part 5: Re-run the sync
1. Double-click the Infor Security Admin icon on the LSF10 server’s training desktop. The ISA login screen opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The ISA tool administrator home page opens.
6. Click the sync icon (double circular arrows). The Federation Window opens.
7. Click Yes to confirm the sync.
8. Click the Ignore (minus sign) icon for Role conflicts. Note: All roles are in conflict because they already existed.
9. Review Actor conflict. Note: During the actor synchronization, The Federation Manager window opens with an error (see below) regarding the incorrect email syntax.

![Federation Manager Window]

10. Click OK. The environment is now out of sync as indicated by the yellow status bar.
11. Click – to minimize the ISA application.

Part 6: Troubleshoot error logs

1. Select Start > This PC > Apps (E:) > LSF10 > law > system. The System folder opens.
4. Type user02@edu in the Find what field.
5. Click Find Next. Note: Look for the user02 email syntax error.
6. Click X to close Notepad.
7. Delete the security_provisioning.log file.
8. Click X to close the System folder.

Demo: Update a user record using LSA
Your instructor will demonstrate how to update a user record using LSA.
Lesson 6: Federation and synchronization

Exercise 6.6: Update a user record using LSA

In this exercise, you will update a user record using LSA.

Exercise 6.6 steps

Part 1: Update Matthew Lincoln’s email

1. Click the Lawson Security Admin icon on the task bar. The Lawson Security Administrator window opens.
2. Click the User Management tab.
4. Type Lincoln, Matthew in the Name field.
5. Click Find Now. The result brings back all employees with the name Matthew Lincoln.
6. Right-click the Matthew Lincoln record in the fourth row. The Edit User menu displays.
7. Select Manage RM Information. The Change RM Object page opens.
8. Scroll down to the Email field.
9. Type user02@edu.com in the Email field.
11. Click Yes to save the changes.
12. Click X to close the Lawson Security Administrator.

Part 2: Clear the locked process

1. Double-click the Command Prompt window on the LSF server. The Command Prompt window opens.
2. Type E: in the prompt line. The directory changes from C: to E:.
3. Press Enter.
4. Type cd lsf10 in the prompt line. The directory changes to LSF10.
5. Press Enter.
6. Type enter.cmd in the prompt line.
7. Press Enter.
8. Type enter in the prompt line.
10. Type `ssoconfig -c` in the prompt line.
11. Press Enter.
12. Type `Global08` in the Please Enter the password for Lawson Security utilities prompt.
13. Press Enter. The list of processes displays.
14. Type `12` (Manage locked processes). The list of locked processes displays.
15. Type the `<number>` for the locked process.
16. Press Enter.
17. Type `27` to exit.
18. Click X to close the LSF Command Prompt window.

Part 3: Re-run the sync
1. Click the Infor Security Admin icon on the task bar to maximize. The ISA login screen opens.
3. Click the sync icon (double circular arrows). The Federation Window opens.
4. Click Yes to confirm the sync.
5. Click the Ignore (minus sign) icon for Role conflicts. Note: All roles are in conflict because they already existed.
6. Click the Ignore icon for Service conflicts. Note: All services are in conflict because they already existed.
7. Click the Ignore icon for Domain conflict (if any). Note: All domains are in conflict because they already existed.
8. Click the Ignore icon for Endpoint conflicts. Note: All endpoint are in conflict because they already existed.
9. Click the Ignore icon for Endpoint Group conflicts. Note: All endpoint are in conflict because they already existed.
10. Click the Ignore icon for Identity conflicts (if any). Note: All identities are in conflict because they already existed.
11. Click OK to confirm sync executed successfully.
12. Click X to close the ISA tab and browser session.
13. Select Windows Start > Shut down or sign out > Disconnect to return to the Infor Landmark training server.
Check your understanding

Which of the following best describes the purpose of federation?

- a) Associating two Infor Lawson systems so that users, roles and groups can be "seen" by either system
- b) Resolving conflicts between two systems
- c) Assigning security classes to roles

What is the purpose of synchronization?

- a) To remove old user records from database
- b) To determine if conflicts exist between the systems being federated
- c) To identify role assignments in an environment

In what system should user administration tasks be completed in a federated system to avoid the need for resynchronization?

- a) ISS
- b) Infor Rich Client
- c) Lawson Security Administrator

Which of the following user data is synchronized? Select all that apply.

- a) Roles
- b) Identities
- c) Domain
- d) Actors
- e) Services

True or false? In a federated system, the user must log in to both LSF and Infor Landmark applications to be able to access shared data.

- a) True
- b) False

Which of the following best explains the impact of federating a system? Select all that apply.

- a) Users can log in to either system seamlessly and use the applications for which they have been granted access
- b) A single source of authentication and administration is utilized
- c) Infor Security Services (ISS) should be used to add or update users to avoid having data become out of sync

Which of the following explains why the Infor Lawson System Foundation is always the "Local" or "To" system?

- a) ISS being installed on the LSF server
- b) ISS being installed on the Landmark server
- c) There is no Landmark server to be the remote system
Lesson 7: Administering user access to Infor Ming.le Enterprise and Infor Lawson for Infor Ming.le

Estimated time
2 hours

Learning objectives
After completing this lesson, you will be able to:

- Describe how to grant access to Infor Ming.le™ Enterprise.
- Explain the process of adding a user to Infor Federation Services (IFS).
- Explain how to create and assign an Infor Lawson for Infor Ming.le role to customize the Infor Lawson for Infor Ming.le display.
- List the steps to assign bookmarks controlled by groups.
- Identify the types of user accounts used in setting up Infor Ming.le.

Topics
- Infor Ming.le access
- Infor Federation Services (IFS)
- Infor Ming.le plug-ins
- Infor Lawson for Infor Ming.le access
- Infor Lawson for Infor Ming.le roles
- Clear the IOS cache
- Managing access to bookmarks
- Check your understanding
Infor Ming.le access

Infor Ming.le (formerly Infor Workspace) is a web application framework that provides a common user interface for integrated Infor Enterprise Resource Planning (ERP) applications. Infor Ming.le resides within the Microsoft SharePoint framework. All of the integrated Infor applications in Infor Ming.le use Microsoft SharePoint functionality, navigational elements, and connectivity to social media outlets, providing access for Infor partners and customers.

The Infor Ming.le interface includes a header with menu options and icons that activate the display of Infor ERP applications in the area below the header. To the right of the application area is a collapsible panel, which hosts a series of Infor Ming.le contextual applications.

Infor Ming.le provides drill-back capability among Infor applications so that users can navigate from one application to another to track transactions, the transfer of data, and report updates. Additionally, Infor Ming.le, along with HTML and JavaScript technologies, provides an infrastructure for sharing content among Infor ERP applications and Infor Ming.le contextual applications.

There are two version of Infor Ming.le:

- Infor Ming.le Foundation
  - Default browser-based user interface for Infor Lawson applications
  - No charge
  - No Infor social collaboration
  - Infor ION is not required

- Infor Ming.le Enterprise
  - Chargeable
  - Includes all Infor Ming.le Foundation feature functionality
  - Infor social collaboration
  - ION is required and is chargeable

Infor Ming.le supported browsers

Infor Ming.le has been tested in the following browsers:

- Microsoft® Internet Explorer*
- Mozilla Firefox™
- Safari™ 6 (Basic testing of functionality)
- Chrome™

Please see the Infor Lawson Compatibility matrix published in Infor Xtreme’s Knowledge Base for specific versions that were tested and more details.

*On Microsoft Internet Explorer browsers that access Infor Ming.le, the “display of mixed content” setting must be enabled.

To enable the display of mixed content on Microsoft Internet Explorer:

- Launch **Internet Explorer**.
- Select **Tools > Internet Options**.

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
Click the Security tab. Select the zone where the Infor Ming.le server and other Infor applications are running. Most likely this is the local intranet.

Click Custom level and on the Security Settings dialog box, locate the Display mixed content options under Miscellaneous.

Select Enable.

Click OK to save your settings and close the dialog box.

Note: If you continue to receive security warnings about content that was not delivered securely, you may need to repeat this configuration for the Internet and Trusted sites zones.

### Required system users

There are several accounts required for Infor Ming.le installation and configuration.

In a Microsoft SharePoint farm installation, Microsoft recommends separate accounts for each of these tasks:

- Administrative tasks such as installation
- Running the Microsoft SharePoint Farm application pools and the Infor Ming.le configuration wizard
- Running the Microsoft SharePoint services and Infor Ming.le web application in Microsoft SharePoint
- Running the Microsoft SQL Server services

These are domain accounts that you create in Active Directory. See the appropriate Microsoft documentation for creating domain accounts.

These are the required accounts and their privilege requirements. Although the names provided are only suggestions, Infor strongly recommends that you use similar names to facilitate communications with Infor Xtreme Support:

<table>
<thead>
<tr>
<th>Account</th>
<th>Suggested name</th>
<th>Purpose</th>
<th>Requirements</th>
</tr>
</thead>
</table>
| Setup User Account | SPIinstall    | This account is used to do all administrative tasks including but not limited to: | - Domain account  
                      |                 | - Run SharePoint installation  
                      |                 | - Must be assigned an SQL Server logon with the dbcreator and securityadmin security roles  
                      |                 | - Run SharePoint Products Configuration wizard  
                      |                 | - Member of the Administrators group on the SharePoint and SQL Servers  
                      |                 | - Configure server farm and management from SharePoint Central Administration  
                      |                 | - As part of the SharePoint products and technologies configuration wizard, will automatically be made a farm administrator in SharePoint Central Administration  
                      |                 | - Run IFS Security Administration  
                      |                 | - Run social integration tool  
                      |                 | - Log on to the server form Remote Desktop  

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
<table>
<thead>
<tr>
<th>Account</th>
<th>Suggested name</th>
<th>Purpose</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Farm Account</td>
<td>SPFarm</td>
<td>Used to:</td>
<td>• Domain account</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Act as the application pool identity for the SharePoint Central Administration website.</td>
<td>• Automatically assigned the appropriate permissions by the SharePoint Products and Technologies Configuration wizard</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run Microsoft SharePoint Foundation Workflow Timer Service jobs under the context of this user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Run Infor Ming.le feature activation.</td>
<td></td>
</tr>
<tr>
<td>SharePoint Services Account</td>
<td>SPServices</td>
<td>Use this account to run the Infor Ming.le web application.</td>
<td>• Domain account</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Automatically assigned the appropriate permissions when the Infor Ming.le web application is created in SharePoint Central Administration</td>
</tr>
<tr>
<td>SQL Server Service Account</td>
<td>SQLService</td>
<td>Use this account to run the SQL Server related services.</td>
<td>• Domain account</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Automatically assigned the appropriate permissions as part of the SQL Server installation</td>
</tr>
</tbody>
</table>

**Authentication requirement of Microsoft SharePoint for Infor Ming.le Foundation/Enterprise**

For users to access the Infor site they must first be configured with grant rights to the site in Microsoft SharePoint. Infor Ming.le expects that upon sign-in, the user belongs to a pre-determined security group in the Active Directory used by the domain. For access to the Infor Ming.le site, all users must have their domain account associated with the “Infor” security group in the Active Directory.
Infor Federation Services (IFS)

IFS provides central authentication and authorization for multiple applications. The currently supported Security Token Service (STS) is Microsoft AD FS.

Microsoft AD FS can use multiple sources to create a set of claims for a user. The primary source is Active Directory (AD), which is used to verify the user’s identity and to provide their basic claims such as a user’s first name, last name, and email address. When a user accesses an application, the application relies on the STS to verify the user credentials and provide sufficient information about the user.

Infor applications require additional information such as security roles and accounting entities. This information is not available in AD. Therefore, this data is read from an SQL Server database. The IFS application maintains the data in this SQL Server database.

The Infor Ming.le application uses claims to limit the set of applications a user sees in their navigation. Within an application, the security role can be used to grant access to the functionality related to that role.
Demo: Add a user in Infor Federation Services to gain access to Infor Ming.le
Your instructor will demonstrate how to add a user in Infor Federation Services to gain access to Infor Ming.le.

Exercise 7.1: Add a user in Infor Federation Services to gain access to Infor Ming.le
In this exercise, you will add a user in Infor Federation Services to gain access to Infor Ming.le. You will log in as an administrator to execute this exercise.

Exercise 7.1 steps

Part 1: Log in as Taylor Wang (user08) to check access to Infor Ming.le
1. Double-click the Infor Ming.le icon on the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type user08@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The “Access Denied” page displays. Note: Taylor Wang (user08) has not been added to IFS, therefore, has no access to the Infor Ming.le application.
5. Click X to close the Infor Ming.le tab and browser session.

Part 2: Log in as administrator to add Taylor Wang to IFS
1. Double-click the RDP Shortcuts folder on the Infor Landmark training desktop. The RDP Shortcuts folder opens.
3. Click the Internet Explorer icon in the task bar. A browser session opens.
4. Click the Infor Federation Services tab in the Favorites bar. The IFS login page opens.
5. Type lawson@gdeinfor2.com in the User name field.
6. Type Tr@in123 in the Password field.
7. Click Sign In. The Infor Federation Services application opens.
8. Select Manage > Users. The list of users displays.
10. Type user08 in the AD name field.
11. Click Load. The user08 AD record displays.

12. Select the Taylor Wang record check box.

13. Click Apply.

14. Click OK.

15. Click Refresh.

16. Click Sync. The User Synchronization window opens.

17. Click Sync Now.

18. Click Refresh. Note: Once Refresh is clicked, the Synchronization Status changes from Idle to Running. Note: You may have to repeat steps 17-18 a few times for the status to change.

19. Click X to close the User Synchronization window.

20. Type user08 in the User Filter field to check if user08 appears in IFS.

21. Click Filter. Note: If the user08 record displays, the user has now been added to IFS.

22. Click X to close the tab and the IFS browser session.

23. Select Start > Logoff > Disconnect to disconnect from the Domain Controller server. The Infor Landmark training desktop opens.

24. Click X to close the RDP Shortcuts folder.
Part 3: Log in as Taylor Wang (user08) to re-check access to Infor Ming.le

1. Double-click the Infor Ming.le icon on the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type user08@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. Note: Taylor Wang (user08) has now been added to IFS, therefore, has access to the Infor Ming.le application.
5. Click the Globe icon (Infor Lawson) to access the Infor Lawson Enterprise applications. Note: Recall Taylor Wang was provisioned the Infor Lawson Enterprise application access in an earlier exercise.
6. Click X to close the Infor Ming.le tab and browser session.
Infor Ming.le plug-ins

Infor Ming.le is packaged with a set of product-specific plug-ins that lay the groundwork for Infor products to run within Infor Ming.le. The plug-ins are installed on the Infor Ming.le server and provide essential configuration information to Infor Ming.le. Before a plug-in for any Infor Lawson application can be installed, the DSSO for Infor Ming.le must be installed from the DSP.

Demo: Map a role for Infor Ming.le plug-in access – HCM
Your instructor will demonstrate how to map a role for Infor Ming.le plug-in access – HCM.

Exercise 7.2: Map a role for Infor Ming.le plug-in access – HCM
In this exercise, you will map a role for Infor Ming.le plug-in access – HCM and assign it to Taylor Want (user08).

Exercise 7.2 steps

Part 1: Create HCM Plug-in role in IFS

1. Double-click the RDP Shortcuts folder on the Infor Landmark training desktop. The RDP Shortcuts folder opens.
3. Click the Internet Explorer icon in the task bar. A browser session opens.
4. Click the Infor Federation Services tab in the Favorites bar. The IFS login page opens.
5. Type lawson@gdeinfor2.com in the User name field.
6. Type Tr@in123 in the Password field.
7. Click Sign In. The Infor Federation Services application opens.
8. Select Manage > Master Data. The Master Data window opens.
10. Click New.
11. Type HCMPluginRole in the Node name field.
13. Type user08 in the User Filter field.
14. Click Filter.
15. Select user08@gdeinfor2.com.
16. Click Apply.
17. Click OK.
18. Click X to close the tab and the IFS browser session.
19. Select Start > Logoff > Disconnect to disconnect from the Domain Controller server. The Infor Landmark training desktop opens.
20. Click X to close the RDP Shortcuts folder.

Part 2: Log in to Ming.le and add HCMPluginRole to a SharePoint group
1. Double-click the Infor Ming.le icon in the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type administrator@gdeinfor2.com in the User name field.
3. Type Global08 in the Password field.
4. Click Sign In. The Administrator Home page for the Infor Ming.le application opens.
5. Click the Talent Management plug-in icon.
6. Select Site Actions > Site Settings > Users and Permissions > Site Permissions. The list of site permissions displays.
7. Select the Infor Ming.le Owners group. The list of owners displays.
10. Type HCMPluginRole in the Find field.
11. Click Search. The list of security roles displays.
12. Select Security Group. The HCMPluginRole displays on the right panel.
13. Click Add.
14. Click OK. The Grant Permissions window reopens.
15. Click OK.
16. Select administrator@gdeinfor2.com > Sign Out in the Open Menu (upper right).
17. Click X to close the Infor Ming.le browser.

Part 3: Check Taylor Wang’s access to HCM plugin
1. Double-click the Infor Ming.le icon in the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type user08@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Infor Ming.le application opens.
5. Select the Talent Management (HCM) plug-in icon. Note: You may need to click the drop-down menu to find the Talent Management icon.
Infor Lawson for Infor Ming.le access

Infor Lawson for Infor Ming.le End-Users

End users log in to and interact with Infor Lawson for Infor Ming.le via browsers on their client machines. They navigate via bookmarks they or their administrators have set up or by performing searches.

A Lawson for Infor Ming.le home page contains the data (links to forms, a company intranet page, or other information as defined locally) that a user sees initially. When the user navigates off the home page, the new data appears in the Lawson for Infor Ming.le content window.

A user would require base access to the Infor Ming.le. Infor Ming.le does not include application access. Access to Infor Ming.le should be granted in a manner to address the users for an organization. Infor Ming.le options include:

- Selecting all Authenticated Users
- Selecting an Active Directory group or Active Directory user (Kerberos)
- Selecting an RM role or Resource/user (LS as STS)
- A user added to Infor Federation Services (IFS).

Regardless of the access granting approach, the type of access each user requires influences the procedure required to grant access.

Online only users

Users who run form-based transactions with Infor Lawson applications but who do not perform batch processing have the access requirements described below. Typically, you will create a role with minimum access rights and assign it to each user.

- The user must have an identity on the SSOP service.
- The user must have some basic access rights in the Infor Lawson Environment.
- The user must be assigned at least one role in Infor Lawson Security that will grant access to the data and applications the user needs to perform his or her job.
- The user must have access to some programs and files in the LOGAN product line to allow the user to work with bookmarks and subscriptions. (This access could be assigned through the role you create for all users.)

LOGAN access requirements for users

Infor Lawson delivers a role, Bookmark, which can be assigned to end-users to give them required access. If you prefer to create your own role, users must have access to the following LOGAN data source and to the following programs and forms:

- LOBMARK (Bookmarks)
- LO15.1 (User Subscription)
- LOUSRBKOPT (User Subscriptions)

Batch job users

In addition to the access requirements for online only users, batch job users require the following:

- The user must have a unique OS ID that will be linked to the Infor Lawson RMID.
- The user must have access to additional data and programs in the Infor Lawson Environment. One way to assign these rights is through the Infor Lawson-delivered role BATCH. This can be assigned when the user is added to the system. (BATCH delivers a minimum set of access requirements for batch users. Users at your site might need additional rights.)
- The user must be a member of an Environment user group.
Batch job user Environment access requirements

The batch job user must have access to the following Environment objects. Typically, you will create a security class for batch users and give them the access rights they need.

- On the GEN profile in Infor Lawson Security, the user must have access to the QUEUEDJOB object. (Create a rule for Files, UN system code, QUEUEDJOB.)
- On the ENV profile in Infor Lawson Security, the user must have access to Batch Job Scheduling and the job executables you want the user to have access to. (Create a rule for Executables, Batch Job Scheduling, and then the specific executables.)
- Also on the ENV profile, the user must have access to a job queue.

Batch job users must be members of Environment user groups.

- Each user who runs batch jobs must be a member of an Environment user group.
- Environment user groups are special groups that are assigned through the Environment command line tool, usergrpdef. You cannot create these groups or assign users to them through either the Infor Lawson Security Administrator or the Resource Management Administrator. Further, because the user must have an RMID before they can be assigned to an Environment user group, adding a user to a group must be performed after the user is added to the system.
- The instructions in this training workbook for adding a user include basic steps for adding a user to an Environment user group. Additional details are in Lawson Administration: Jobs and Reports.

Demo: Compare access between lawson administrator role and Taylor Wang’s role for Infor Lawson for Infor Ming.le

Your instructor will compare access between lawson administrator role and Taylor Wang’s role for Infor Lawson for Infor Ming.le.

Exercise 7.3: Compare access between lawson administrator role and Taylor Wang’s role for Infor Lawson for Infor Ming.le

In this exercise, you will compare access between lawson administrator role and Taylor Wang’s role for Infor Lawson for Infor Ming.le.

Exercise 7.3 steps

Part 1: Log in as lawson administrator to Infor Ming.le

1. Double-click the Infor Ming.le icon on the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click **Sign In**. The **Infor Ming.le** application opens.

5. Click the **Globe** icon (Infor Lawson) to access the Infor Lawson Enterprise applications.

   Notice the list that appears in the Common Tasks list. Because you are logged in as the *lawson* administrator, this list will differ from Taylor Wang’s access as you will see in Part 2 of the exercise.

6. Select **lawson@gdeinfor2 > Sign Out** in the **Open Menu** (upper right).

7. Click **X** to close the tab and the **Infor Ming.le** browser session.

**Part 2: Log in as Taylor Wang (user08)**

1. Double-click the **Infor Ming.le** icon on the Infor Landmark training desktop. The **Infor Ming.le** login page opens.

2. Type **user08@gdeinfor2.com** in the **User name** field.

3. Type **Tr@in123** in the **Password** field.

4. Click **Sign In**. The **Infor Ming.le** application opens.

5. Click the **Globe** icon (Infor Lawson) to access the Infor Lawson Enterprise applications. Notice the much shortened Common Tasks list as compared to the **lawson** user.

6. Click **X** to close the tab and the **Infor Ming.le** browser session.
In Infor Lawson for Infor Ming.le, a role is a set of attributes that specifies accesses for users who have been assigned the role.

**Infor Lawson for Infor Ming.le roles**

The Resource Management attribute, PortalRole, determines the role and, therefore, the access rights, of a user. There are several ways to assign a role to a user. You can use any of the methods described here individually or in combination.

- Assign a custom role, that is, a role that has been created at your site, to an individual user.
- Assign a custom default role to all or most users.
- Retain the Lawson-delivered default role (default.xml) for all or most users.

An Infor Lawson for Infor Ming.le role is assigned to every user.

Although a system can have multiple special roles, a user can have only one role for Infor Lawson for Infor Ming.le.

**Infor Lawson for Infor Ming.le user customizations**

Custom roles allow an administrator to customize how the Infor Lawson for Infor Ming.le user interface will look and what options the user will be allowed. Creating Infor Lawson for Infor Ming.le custom roles for different types of users can help control options and reduce issues of navigation for end users.

The user’s experience of Infor Lawson for Infor Ming.le can be controlled through a variety of settings. A summary of key settings is offered in this workbook. Additional information on setup can be found in source documents as well as additional courses focusing on Infor Lawson for Infor Ming.le.

**Prevent users from changing hotkey assignments**

By default, users are allowed to make changes to the Infor Lawson-delivered hotkeys. You can prevent them from doing so by eliminating this option in the user’s role.

**Hide the search box from users**

You may choose to hide the search box from certain users, such as users who only have access to Employee Self Service. This option is changed in the user’s role.

**Change user menu options**

By default, Infor Lawson for Infor Ming.le makes the ability to change user options and content available to all users. This menu lets users customize aspects of Infor Lawson for Infor Ming.le. Administrators can make some changes to these menus and even remove them completely. The following sections provide a high-level overview of the content of these menus.

**Note:** This lesson assumes that you are using Role Manager to configure the specified attributes. Installations that do not use custom roles can configure some of these attributes through the configuration file (portalconfig.xml).
Content

The Content submenu lets users unsubscribe to bookmarks (or re-subscribe to bookmarks they have access to) and change the layout of the workspace. The ability to customize Content is an on/off switch. Administrators can remove the Content option from users but they cannot pick and choose options to allow or deny. Instructions for users who want to make customizations on Content options are described in Help for Users and in the user guide *Getting Started with Infor Lawson for Ming.le*.

User Settings

User Settings is a group of options that lets users customize operation of the following items, many of which control how Infor Lawson applications appear in a user's workspace.

Control access to individual user options

User Options is a set of user-customizable features, most of which are related to operation of applications and data retrieval.

The ability to make changes to all items on the User Options submenu is given to users by default. If an administrator wants to deny the ability to change some user options, they do so from Role Manager.

Administrators can use items in the User Options menu in conjunction with roles. For example, suppose an organization has a group of power users who must be able to fetch large loads of data in their queries, but, for performance reasons, administrators generally prefer to limit fetch sizes. An administrator can create a role for power users (poweruser.xml) that would allow them to change fetch size.

Disabling users’ ability to change options and setting required values

An item is disabled when a check mark appears in the “Disabled?” column for the item. When an item has been disabled, users (of the role from which it has disabled) will see the option on the User Options menu but will not be able to change it.

To restrict all users (of a role) to a particular value for an option, supply the value and also select the "Disabled?” check box.

User options controlled by the Options tab

The following table describes the options for which administrators can deny access or set required values.

Several options that appear on the User Options submenu cannot be disabled, for example: the Navigation Bar on Startup, Open Navigation Menus at Startup, and Display Field Help. Users will always be able to make selections for these items (unless you have removed the User Options submenu altogether).

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Locale</strong></td>
<td>This is the language that Infor Lawson for Ming.le uses. (This option may be disabled if the site is not multi-lingual.)</td>
</tr>
<tr>
<td><strong>Productline</strong></td>
<td>This option is the default product line for the role.</td>
</tr>
<tr>
<td><strong>Value separator</strong></td>
<td>This option determines whether commas, tabs, or semicolons will be used to separate columns for data import.</td>
</tr>
<tr>
<td><strong>Toolbar button display</strong></td>
<td>This option determines whether buttons on applications forms appear as text or icon.</td>
</tr>
<tr>
<td><strong>Default report type</strong></td>
<td>This is the output format of Infor Lawson system reports. Choices are text, PDF and LSR (Infor Lawson Smart Reports).</td>
</tr>
<tr>
<td><strong>Default printer</strong></td>
<td>This is the default printer for the role.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Auto select required fields</strong></td>
<td>This option indicates Infor Lawson applications can be set so that required fields on forms are automatically selected.</td>
</tr>
<tr>
<td><strong>Explorer record count</strong></td>
<td>These options determine the number of records that are displayed per page when a user performs a drill transaction (Explorer Record Count), or selects from a list (Select Record Count). By default, the options are 25, 50, 100, and 200. You set the options that are available for selection.</td>
</tr>
<tr>
<td><strong>Select record count</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Default search option</strong></td>
<td>When this option is selected, Infor Lawson application records will search using the Find or Filter options.</td>
</tr>
<tr>
<td><strong>Use list style presentation</strong></td>
<td>When this option is selected, Infor Lawson application records display in a list format when the user opens a form. This lets users quickly select the record to work with or perform a search.</td>
</tr>
<tr>
<td></td>
<td>When this option is <strong>not</strong> selected, an application form is blank and users must enter a key field to select a record or perform a search.</td>
</tr>
<tr>
<td><strong>List style record count</strong></td>
<td>This option determines the number of records that will be displayed per page when a user selects to display a data query results list. By default the options are 25, 50, 100 and 200.</td>
</tr>
<tr>
<td><strong>Use list view presentation</strong></td>
<td>When this option is selected, Infor Lawson application records are displayed in a list of records. Users can apply search conditions to filter what records must appear on the list. If this List View is enabled, three additional buttons appears on the toolbar: Show Form, Filter, and Clear Filter.</td>
</tr>
<tr>
<td></td>
<td>If List View is disabled, the number of records returned is 500, and the tokens to skip are empty.</td>
</tr>
<tr>
<td><strong>List view record count</strong></td>
<td>This option determines the number of records that will be displayed in the list. The list will display up to the maximum number of records defined by the user or Infor Lawson Administrator in the User Options. By default, the options are 250 and 500.</td>
</tr>
</tbody>
</table>
Clear the IOS cache

When administrators make certain changes to Infor Lawson for Infor Ming.le, for example, creating or changing roles with Role Manager or adding or removing bookmarks, the cache must be updated before the changes will appear in a user’s workspace. This is also true of changes made with other Infor Lawson administrative applications, including updates to the Resource Management repository.

The cache will be cleared automatically whenever the Infor Lawson system is restarted or a particular server is bounced. However, if you need changes to take effect immediately, use the Cache menu to clear the entire cache or just the cache for the affected component.

The table below highlights under which circumstances to clear the cache.

<table>
<thead>
<tr>
<th>If the cache component is</th>
<th>Clear the cache when…</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bookmarks</td>
<td>You create new or delete bookmarks, which are stored in tables in the LOGAN database.</td>
</tr>
<tr>
<td>Programs</td>
<td>You create or update application programs using pgmdef.</td>
</tr>
<tr>
<td>Tokens</td>
<td>Application forms are modified. This could happen, for example, through an MSP delivery.</td>
</tr>
<tr>
<td>Locale</td>
<td>Programs are changed through pgmdef.</td>
</tr>
<tr>
<td>Translations</td>
<td>You update the locale using locdef.</td>
</tr>
<tr>
<td>UI definitions</td>
<td>You have installed an application upgrade. Or You have run pgmdef and have made changes.</td>
</tr>
<tr>
<td>RM cache</td>
<td>A change to an RM entry (people, thing, or organization resource) needs to be visible to all applications immediately. If the cache is not cleared, a change could take up to five minutes before the change is seen by all applications.</td>
</tr>
</tbody>
</table>

Demo: Creating and assigning an Infor Lawson for Infor Ming.le role

Your instructor will demonstrate creating and assigning an Infor Lawson for Infor Ming.le role.

Exercise 7.4: Creating and assigning an Infor Lawson for Infor Ming.le role

In this exercise, you will be creating and assigning an Infor Lawson for Infor Ming.le role. You will customize the role and then assign the role to Matthew Lincoln (user02).
Exercise 7.4 steps

Part 1: Log in as lawson administrator and create a custom role in Infor Lawson for Infor Ming.le

1. Double-click the Infor Ming.le icon on the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Infor Ming.le application opens.
5. Click the Globe icon (Infor Lawson). The Infor Lawson for Infor Ming.le home page opens.
6. Select Common Tasks > Manage Roles. The Role Manager page opens.
7. Click Migrate. The Infor Lawson Message box opens.
8. Click OK to confirm migrating role files to version LSF 10.0.8.
10. Type ClassEss.xml in the Please enter name of new role file field.
11. Click OK. The General tab opens displaying list of General options.
12. Clear the check boxes for the following options to disable them:
   - Allow use of search
   - Allow use of favorites
   - Allow keyboard customizations
13. Click the Menus tab. The list of menus displays.
14. Select Content in the Preferences menu list.
15. Click Delete. The Infor Lawson Message window opens.
16. Click OK to confirm deletion.
17. Select the User Options in the Preferences menu list.
18. Click Delete. The Infor Lawson Message window opens.
19. Click OK to confirm deletion.
20. Click Apply.
21. Click OK.
22. Click Close to close the Role Manager.
23. Select Manage Roles. Notice the classess.xml role is now listed along with the ess.xml role.
24. Select lawson@gdeinfor2 > Sign Out in the Open Menu (upper right).
25. Click X to close the tab and end the browser session.

Part 2: Check Matthew Lincoln’s access to Infor Lawson for Infor Ming.le

1. Double-click the Infor Ming.le icon on the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type user02@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Infor Ming.le application opens.
5. Click the **Globe** icon (Infor Lawson). The **Infor Lawson for Infor Ming.le** home page opens.

6. Click the **Preferences** menu (cogwheel icon). Notice the **Content** is displayed and that the **Search** box is available. Once the classes.xml role is assigned to the user, the changes will take effect on his home page.

7. Select **user02@gdeinfor2 > Sign Out** in the **Open Menu** (upper right).

8. Click X to close the tab and end the browser session.

**Part 3: Assign the custom role to Matthew Lincoln (user02)**

1. Double-click the **Infor Security Admin** icon on the Infor Landmark training desktop. The **ISA** login screen opens.

2. Type **lawson@gdeinfor2.com** in the **User name** field.

3. Type **Tr@in123** in the **Password** field.

4. Click **Sign In**. The **ISA** application opens.

5. Select the **People** check box in the **Select resource types** field (upper right of screen).

6. Type **user02** in the **Search** field.

7. Press **Enter**. The **People** list displays the **user02** record.

8. Click the **Edit resource** (pencil icon). The **user02** record opens.

9. Click the **LSF** tab. The **LSF** form opens.

10. Type **classess.xml** in the **Portal Role** field. **Note:** You will be replacing the default.xml that is there.

11. Click **Update Actor**.

12. Click **OK** to confirm update.

13. Click **Sign Out**.

14. Click X to close the tab and end the ISA browser session.

**Part 4: Recheck Matthew Lincoln’s access in Infor Lawson for Infor Ming.le**

1. Double-click the **Infor Ming.le** icon in the Infor Landmark training desktop. The **Infor Ming.le** login page opens.

2. Type **user02@gdeinfor2.com** in the **User name** field.

3. Type **Tr@in123** in the **Password** field.

4. Click **Sign In**. The **Infor Ming.le** application opens.

5. Click the **Globe** icon (Infor Lawson). The **Infor Lawson for Infor Ming.le** home page opens.

6. Click the **Preferences** menu (cogwheel icon). **Note:** the Content and the Search box are no longer available.

7. Select **user02@gdeinfor2 > Sign Out** in the **Open Menu** (upper right).

8. Click X to close the tab and end the browser session.
Managing access to bookmarks

Access to bookmarks can be allowed or denied. If left globally allowed, any user of Infor Lawson for Infor Ming.le with the Content option can subscribe to any open bookmark.

**Note:** The bookmark access does not give a user authorization to the area connected to the bookmark. Security must still allow the user access for the bookmark to be fully functional. If a bookmark is globally denied then either the user must be explicitly granted access by his or her ID or participate in a group that is allowed to use the denied bookmark. Using the right combinations of Allow and Deny bookmarks on an Infor Lawson for Infor Ming.le role can create unique setups even for those users sharing the same xml PortalRole assignment.

Administrators may choose to lock bookmarks. There are two types of bookmark locks:

- **Layout lock** - prevents users from removing the bookmark from their workspaces
- **Subscription lock** - prevents users from unsubscribing to a bookmark (but they could remove it from their workspaces if there is no layout lock)

### Demo: Add a user to group

Your instructor will demonstrate how to add a user to group.

### Exercise 7.5: Add a user to group

In this exercise, you will assign a bookmark that is allowed through a group. First you will create a group in Infor Lawson Resource Management Administrator (RMA). You will then assign the bookmark to the users belonging to the group.

**Exercise 7.5 steps**

**Part 1: Log in as lawson administrator and create a new group**

1. Double-click the Lawson RM Administrator icon on the Infor Landmark training desktop. The Lawson RM Administrator login page opens.
3. Click Connect. The Lawson RM Administrator login window opens.
4. Type lawson@gdeinfor2.com in the User name field.
5. Type Tr@in123 in the Password field.
6. Click Sign In. The Resource Manager Administrator application opens.
7. Click Exit.
9. Type Employee in the ID field.
10. Type Employee in the Description field.
11. Click outside the Description field to confirm you are done editing the description.

Part 2: Add a user to a group
2. Click OK. The Pick Resource Type window opens.
4. Type “wa” in the Name field.
5. Click Find Now. Two records display for Taylor Wang.
6. Right-click the second record for Taylor Wang (user08).
7. Select Edit. The Change RM Object window opens.
8. Double-click the Group field. You will be creating a query string by adding criteria.
9. Select ID in the second Query field.
10. Select = in the third Query field.
11. Type Employee in the fourth Query field.
12. Click Add Criteria. The criteria is added to the query box.
13. Click Next. The Choose Data Field to Display window displays.
14. Select the Description check box.
15. Click Next. The Assign Values window displays.
16. Select Employee.
17. Click the (>) right-facing arrow. The Employee value is added.
18. Click Finish.
   Note: Adding a user to an existing group can also be done in ISS on the user’s People record > LSF > Groups.
20. Click X to close all RM Administrator windows.

Part 3: Edit access
1. Double-click the Infor Ming.le icon in the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Infor Ming.le application opens.
5. Click the Globe icon (Infor Lawson). The Infor Lawson for Infor Ming.le home page opens.
7. Type Employee in the Search box.
8. Click Find.
10. Click the lock icon to the right of Default Access to lock the Employee Self-Service default access.
11. Select the Add option directly across from Group. The Groups window opens.
12. Select Employee.
13. Click Close.
14. Click Update Cache. The Infor Lawson Message window opens.
15. Click OK.
16. Click Close. Now only those users in the Employee group can access the Employee Self-Service bookmark.
17. Select Common Tasks > Manage Roles.
18. Double-click ClassEss.xml.
19. Click the Locks tab.
20. Select the Employee Self-Service check box for both Subscription Lock and Layout Lock.
21. Click Apply.
22. Click OK.
23. Click Close to return to the Infor Lawson for Infor Ming.le Administration Home page.
25. Click Submit. The IOS Cache Refresh Results window opens.
26. Click Close.
27. Select lawson@gdeinfor2 > Sign Out in the Open Menu.
28. Click X to close the tab and end the Infor Ming.le browser session.

Part 4: Validate changes
1. Double-click the Infor Ming.le icon in the Infor Landmark training desktop. The Infor Ming.le login page opens.
2. Type user08@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Infor Ming.le application opens.
5. Click the Globe icon (Infor Lawson). The Infor Lawson for Infor Ming.le home page opens.
6. Click Manage Subscriptions.
7. Click and drag the Employee Self Service bookmark from the Subscriptions panel to the Layout panel.
8. Click Save.
11. Select user08@gdeinfor2 > Sign Out in the Open Menu.
12. Click X to close the tab and end the Infor Ming.le browser session.
Check your understanding

Infor Ming.le resides within the ______ framework.
   a) Microsoft Outlook  
   b) Microsoft SharePoint  
   c) UNIX

All of the integrated Infor applications in Infor Ming.le use __________ for its navigational elements and connectivity to social media outlets as well as providing access for Infor partners and customers.
   a) Microsoft SharePoint  
   b) Microsoft Outlook  
   c) Google

For access to the Infor Ming.le site, all users must have their ______ associated with the “Infor” security group in the Active Directory.
   a) Passwords  
   b) Identities  
   c) Domain accounts

Which Resource Management attribute determines the role and subsequent access rights of a user?
   a) Employee  
   b) PortalRole  
   c) SharePoint_ST

Which of the following authentication methods is currently supported in IFS?
   a) Kerberos  
   b) LS as STS  
   c) Microsoft AD FS

True or false? Although a system can have multiple special roles, a user can have only one role for Lawson for Infor Ming.le.
   a) True  
   b) False

Which option would an administrator choose to prevent users from unsubscribing to a bookmark?
   a) Layout Lock  
   b) Subscription Lock  
   c) Access Lock

Which Infor Ming.le option would an administrator access to customize user-customizable features related to the operation of applications and data retrieval?
   a) New Page  
   b) Edit Workspace  
   c) User Settings

Which of the following best explains why administrators would create custom roles for different types of users in Infor Lawson for Infor Ming.le?
   a) To help control options and reduce issues of navigation for end users  
   b) To automate the creation of roles when an employee is hired  
   c) To categorize the functionality of Infor applications
Lesson 8: Administering user access to Infor Lawson Add-ins for Microsoft Office

Estimated time
1 hour

Learning objectives
After completing this lesson, you will be able to:

- Define the purpose of user attributes.
- Describe how to grant access to Infor Lawson for Infor Ming.le with user attributes.
- Describe how to administer user access to Infor Lawson Add-ins for Microsoft Office.
- Identify the purpose of creating custom user attributes in Schema Editor.
- Describe how to administer access to Infor Spreadsheet Designer.

Topics
- User attributes
- Administering users for Infor Lawson Add-ins
- Administering users for Infor Spreadsheet Designer
- Check your understanding
User attributes

User attributes are descriptive properties of users (resources or actors). This can be a name, email address, a Yes/No flag, or whatever information is applicable to that user. When you add or modify a user, a list of attributes that can be applied to the user appears. In Infor Security Services, this is done through the user’s People record. User attributes can be set when the user is initially added to the system or at any time thereafter.

Some user attributes are delivered by Infor Lawson. Attributes can also be created or customized.

Infor Lawson Schema Editor

User attributes can be created or customized using the Infor Lawson Schema Editor. The Infor Lawson Schema Editor is a desktop tool for changing the schema (data format) of Infor Lawson objects stored in the Resource Management repository. Infor Lawson Schema Editor is the only Infor Lawson-recommended method for making changes to Infor Lawson schema. Do not use LDAP native tools for this purpose.

Infor Lawson Schema Editor is intended to be used by LDAP administrators who need to add new objects (people or things) or attributes to the system so that security rules can be written against them. You would also use Infor Lawson Schema Editor to make some simple changes to Infor Lawson-delivered attributes, including changing an attribute default value or hiding an attribute that you do not use at your site.

Administrators who use Infor Lawson Schema Editor must be knowledgeable about LDAPs in general and about their LDAP schema. They should also have experience running programs that create LDAP Data Interchange Format (LDIF) files and importing LDIF files. Instruction on the use of Infor Lawson Schema Editor is available in other courses.

With the Infor Lawson Schema Editor you can:

- Add an attribute to the Infor Lawson Schema. You would use these attributes only for writing special rules that are unique to your site.
- Change a default value for an attribute. For example, the PortalRole attribute is shipped with a default value (default.xml) that can be overridden for a single user, for many users, or for all users.
- Hide attributes that you don’t use at your site. You might want to do this if, for example, Infor Lawson delivers attributes that you don’t use. Hiding those attributes would simplify the attributes dialog box when you are adding users.
- Map your existing schema objects to Infor Lawson schema objects. Note: You might have mapped some common schema objects when you installed Infor Lawson but you can also map objects or remove mapping from objects after installation.

Infor Lawson Schema Editor does not allow you to alter or delete objects that were delivered by Infor Lawson.

Infor Lawson Schema Editor process overview

If you determine that you need to make schema changes at your site, you will perform the following general procedures:

- Implement the changes using Infor Lawson Schema Editor.
- If you have added a new attribute, link it to the resource with which you want it to be used.
- Run the Infor Lawson ldifgen utility to create an LDIF file (or files).
- Load the LDIF file into your LDAP server. You perform this step using your LDAP native tools, not Infor Lawson Schema Editor.
Demo: Edit a user's access to Infor Lawson for Infor Ming.le with user attributes

Your instructor will demonstrate how to edit a user’s access to Infor Lawson for Infor Ming.le with user attributes.

Exercise 8.1: Edit a user’s access to Infor Lawson for Infor Ming.le with user attributes

In this exercise, you will edit a user’s access to Infor Lawson for Infor Ming.le with user attributes.

Exercise 8.1 steps

Part 1: Log in to Lawson Security Administrator to edit the Portal Administrator attribute

3. Click Connect. The Lawson Security Administrator login window opens.
4. Type lawson@gdeinfor2.com in the User name field.
5. Type Tr@in123 in the Password field.
6. Click Sign In. The Lawson Security window opens.
8. Type Hudson in the Name field.
9. Click Find Now. Two records for Marcia Hudson display.
10. Select the second record for Marcia Hudson.
12. Click the drop-down menu in the Portal Administrator role row.
13. Select Yes.
15. Click Yes to confirm changes.
16. Click X to close the User Maintenance window.
18. Click OK to confirm changes.
19. Click X to close all open Lawson Security Administrator windows.
20. Click X to close the Lawson Security Administrator tab and the browser session.

Part 2: Log in as Marcia Hudson to Infor Lawson for Infor Ming.le

1. Double-click the Infor Ming.le icon on the Infor Landmark server’s training desktop. The Infor Ming.le login page opens.
2. Type user01@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Infor Ming.le application opens.
5. Click the Globe icon (Infor Lawson). The Infor Lawson for Infor Ming.le home page opens. Notice that Marcia Hudson now has access to more options under Common Tasks.
6. Click X to close the Infor Lawson for Infor Ming.le browser session.
Administering users for Infor Lawson Add-ins

Infor Lawson Add-ins for Microsoft Office

The Infor Lawson Add-ins for Microsoft Office (abbreviated as Infor Lawson Add-ins) product consists of several applications or wizards that integrate the Infor Lawson applications with Microsoft Excel. This tool allows a user to extract data from Infor Lawson into Excel and to load the Excel worksheet data directly into specified Infor Lawson application form fields.

Security requirements

All Infor Lawson Add-ins users must be set up with appropriate security prerequisites before they can use the Infor Lawson Add-ins product. The following prerequisites are required:

- Add a user to the Infor Lawson repository. The user must have identities on the appropriate services or agents.
- Assign the user appropriate Infor Lawson access rights. Granting access to Infor Lawson Add-ins does not grant a user access to query or change specific data in Infor Lawson. This access must be granted via security roles. Granting access to Infor Lawson Add-ins allows the user to query or change data as permitted via his or her security roles via the Infor Lawson Add-ins tool.
- Set the ADDINS attribute to YES to permit a user to access the Infor Lawson Add-ins. If the ADDINS attribute for a user is blank or is set to NO, the user will be denied access to Infor Lawson Add-ins.
  - You can use the Mass Assign feature to update the attribute for a large number of users. Note: This method should only be used if the Infor Lawson Add-ins users have a characteristic in common or if you want to change the attribute setting to YES for all users.
  - You can also set a default value of YES or NO through Schema Editor.
- Install the LawsonQueryToolsRole template and then assign the LawsonQueryToolsRole role in the GEN profile to each Infor Lawson Add-ins user in your organization. This gives users access to the tables necessary to use the Infor Lawson Add-ins.

Demo: Grant access to Infor Lawson Add-ins

Your instructor will grant access to Infor Lawson Add-ins.
Exercise 8.2: Grant access to Infor Lawson Add-ins

In this exercise, you will grant access to Infor Lawson Add-ins.

Exercise 8.2 steps

Part 1: Edit user access

1. Double-click the RDP Shortcuts folder on the Infor Landmark server’s training desktop. The RDP Shortcuts folder opens.
2. Select the LSF10.rdp server link. The LSF training desktop opens.
3. Double-click the Infor Security Admin icon on the LSF server’s training desktop. The ISA login screen opens.
4. Type lawson@gdeinfor2.com in the User name field.
5. Type Tr@in123 in the Password field.
6. Click Sign In. The ISA tool administrator home page opens.
7. Select the People check box in the Select resource type field (upper right of screen).
8. Type user02 in the Search field.
9. Press Enter. The People list displays the user02 record.
10. Click the Edit resource (pencil icon). The Basic tab for user02 opens.
11. Click the Search icon in the Roles field. The Roles list window displays.
12. Select the LawsonQueryToolsRole role.
13. Click the right-facing arrow > to move the role to the User Roles panel.
14. Select the LSSSuperAdmin role.
15. Click the right-facing arrow > to move the role to the User Roles panel.
16. Click OK.
17. Click the LSF tab. The LSF Details form opens.
18. Select Allow in the Addins attribute drop-down menu.
19. Click Update Actor.
20. Click OK.
21. Click Sign Out.
22. Click X to close the ISA browser session.

Part 2: Explore user access

2. Select Add-Ins > Infor Lawson > Lawson Query Wizard.
4. Click Connect.
5. Type user02 in the Username field.
6. Type Tr@in123 in the Password field.
7. Click Sign In.
8. Select the Database Tables radio button.
9. Click Next.
10. Type EMP in the Table Prefix Translation > Prefix field in the lower-left corner.
11. Press Tab. The long form of the table name, Employee (HR), appears next to the prefix.
12. Double-click APPS10. This list of System Codes/Files displays.
13. Double-click HR, Human Resources. The list of HR Files displays.
14. Click Employee under the Human Resources tree. The list of Employee fields displays.
15. Double-click the following items in the Fields column.
   - First-Name
   - Last-Name
   - Zip
16. Click Finish. The spreadsheet is populated with the data from the query. Note: If the data did not appear, double-check the steps in part 1 of the exercise.
17. Select File > Close. Do not save the spreadsheet.
Administering users for Infor Spreadsheet Designer

The Infor Spreadsheet Designer for Microsoft Excel (abbreviated as Infor Spreadsheet Designer) provides a reporting and analysis interface between Infor Landmark-based applications and Microsoft Excel. This tool allows a user to extract data from Infor Landmark into Excel and to load Excel worksheet data directly into specified Infor Landmark application form fields.

Access to data is controlled by the Infor Landmark applications’ role-based security authorization policies and rules. Data may be downloaded and uploaded directly from Microsoft Excel into Infor Landmark applications.

Demo: Set up user access to Infor Spreadsheet Designer

Your instructor will set up user access to Infor Spreadsheet Designer.

Exercise 8.3: Set up user access to Infor Spreadsheet Designer

In this exercise, you will set up user access to Infor Spreadsheet Designer.

Exercise 8.3 steps

Part 1: Log in as lawson administrator and assign role to user08

1. Double-click the Infor Security Admin icon on the LSF server’s training desktop. The ISA login screen opens.
2. Type lawson@gdeinfor2.com in the User name field. Note: To prepare any field in the system for text entry, first click in the text field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The ISA tool administrator home page opens.
5. Select the People check box in the Select resource type field (upper right of screen).
6. Type user08 in the Search field.
7. Press Enter. The People list displays the user08 record.
8. Click the Edit resource (pencil icon). The Basic tab for user08 opens.
9. Click the Search icon in the Roles field. The Roles list displays.
10. Select the LsuserappAccess role.
11. Click the right-facing arrow to move the role to the User Roles panel.
12. Click OK.
13. Click **Update Actor**.
14. Click **OK**.
15. Click **Sign Out**.
16. Click **X** to close the ISA browser session.

**Part 2: Log in as user08 to access HCM data in Infor Spreadsheet Designer**


2. Select **Infor > Insert Query > Business Class**.

3. Type **user08** in the **Username** field.

4. Type **Tr@in123** in the **Password** field.

5. Type **lmrk10.gdeinfor2.com** in the **Server** field.

6. Click **Log On**. The **Insert Business Class Query** window opens.

7. Select **hcm** in the **Select a Data Area** drop-down menu.

8. Select **Job** in the **Business class** drop-down menu.

9. Select the check box next to each of the following fields:
   - HROrganization
   - Job
   - Short Description
   - Description
   - Active
   - Exempt from Overtime

10. Click **Insert**.

11. Click **Refresh**.

12. Click **X** to close Microsoft Excel. Do not save the spreadsheet.
Check your understanding

Where in ISS would an administrator go to add or modify a user's list of attributes?

- a) People record
- b) Domain Controller
- c) Active Directory

The Schema Editor is used to:

- a) Add new objects (people or things) or attributes to the system so that security rules can be written against them
- b) Create new actors in Infor Landmark
- c) Disable users in LSF

Which value should an administrator select for the ADDINS attribute to permit a user to access the Infor Lawson Add-ins?

- a) No
- b) Yes
- c) Null

Access to data in Infor Spreadsheet Designer for users is controlled by:

- a) Infor Landmark applications' role-based security authorization policies and rules
- b) The actor's identity
- c) The user's direct supervisor's access

A user's name, email address, address, and other people records are examples of:

- a) LDAP entries
- b) User attributes
- c) Infor Ming.le credentials
Lesson 9: User proxies

Estimated time
30 minutes

Learning objectives
After completing this lesson, you will be able to:

- Describe the purpose and setup of user proxies.

Topics
- User proxies
- Check your understanding
User proxies

A user proxy is a means to temporarily transfer the access privileges of one user to another user. User proxies can be set up by administrators or by individual users. Administrators can set up proxies for any user and assign them to other users. Individual, non-administrator users can only set up a proxy for themselves and assign it to another user.

Proxies are set up for grantors and grantees.

- **Grantor** - the user whose access privileges are to be assigned to another user
- **Grantee** - the user to whom the grantor’s access privileges are assigned

A proxy can be set up for one or more of the grantor’s roles. Multiple proxies can also be set up for a grantor, such that, one proxy assigns some roles to one grantee and another proxy assigns other roles to another grantee.

A user’s ability to set up user proxies is controlled by the following security classes:

- **ProxyAdminAccess** - Enables a user to set up proxies for any user
- **ProxyGrantorAccess** - Enables users to set up proxies only for themselves
- **ProxyInquireAccess** - Enables users to view any proxies assigned to them

If a proxy is assigned to a user, when the user logs in to Infor Landmark Rich Client and some web applications, the user can switch to the proxy and perform actions based on the security privileges of that proxy.

**Setting up user proxies as an administrator**

A security administrator may set up user proxies for other users. Security administrators with the default security roles can set up proxies for any user and can assign those proxies to any other user. An administrator may set up a proxy through either Infor Landmark Rich Client or secadm.

**Demo: Set up a user proxy as an administrator through Infor Landmark Rich Client**

Your instructor will demonstrate how to set up a user proxy as an administrator through Infor Landmark Rich Client.
Exercise 9.1: Set up a user proxy as an administrator through Infor Landmark Rich Client

In this exercise, you will set up a user proxy as an administrator through Infor Landmark Rich Client.

In this example, you will work with two users – Taylor Wang (user08) and Matthew Lincoln (user02). Matthew will fill in for Taylor while Taylor is on vacation.

You will also establish Matthew as the proxy for Taylor’s process server access. This proxy can be activated as needed whenever Taylor is unavailable.

Exercise 9.1 steps

Part 1: Make a role proxyable

2. Type lawson@gdeinfor2.com in the Login Name field.
3. Type Tr@in123 in the Password field.
4. Click Login. The Infor Rich Client canvas opens.
5. Select the GEN data area from the Data area menu located on the upper left of the canvas. The GEN canvas opens.
7. Click Search (magnifying glass icon).
8. Type user08 in the Actor ID field.
9. Press Enter to execute the query.
10. Double-click user08. Taylor Wang’s Actor record opens.
11. Click the Roles tab. Notice that the ProcessServerAllAccess_ST role is already assigned to the user.
12. Click X to close the Actor record.
13. Click X to close the Actor List.
15. Click Search (magnifying glass icon).
16. Type ProcessServerAllAccess_ST in the Role Name field.
17. Press Enter to execute the query.
19. Select the Proxyable check box to make the role proxyable.
20. Click Save.
21. Click the Role Assigned to Actors tab.
22. Click Search (magnifying glass icon).
23. Type user02 in the Actor field.
24. Press Enter. Note: The user02 record does not appear as a result because Matthew Lincoln is not currently assigned the ProcessServerAllAccess_ST role.

25. Click X to close the Role page.

26. Click X to close the Role List.

27. Click X to close User Management and return to the GEN canvas.

Part 2: Set up proxy

2. Select Actions > Create. The Proxy Details page opens.
3. Type user08 in the Grantor field.
4. Type ProcessServerAllAccess_ST Proxy in the Proxy Name field.
5. Select <today’s date> in the From Date field. Note: Allow the To Date field to remain blank so that the proxy is always available to be activated when needed.
6. Select the Is Enabled check box. Note: In this example, the proxy is being created so that the grantee can activate it when needed.
7. Click Save. The Proxy Information displays.
8. Click the Proxy Roles tab.
10. Type ProcessServerAllAccess_ST role in the Role field.
11. Click Save.
12. Click X to close the Proxy Role window.
13. Click the Proxy Granted to Actors tab.
15. Type user02 in the Granted To field.
16. Click Save.
17. Click X to close Infor Rich Client.
18. Click Yes to confirm closing the application.
Check your understanding

Which of the follow best explains user proxy?

a) A means to temporarily transfer the access privileges of one user to another user
b) A means for users to share passwords
c) A means for a user to lock down their access to an application
Lesson 10: Administering user access to Infor Smart Office

Estimated time
1 hour

Learning objectives
After completing this lesson, you will be able to:

- Explain how to administer access to Infor Smart Office.

Topics
- Infor Smart Office
- Check your understanding
Infor Smart Office provides a user interface to access Infor Lawson Enterprise applications. Its framework is designed to host and enable interaction among multiple Infor applications. Using the canvas, a user can navigate and switch between applications with ease to access personal widgets, event notifications, bookmarks, and process monitors to better manage data.

The Infor Smart Office installation includes the following components:

- **Infor Smart Office server**
  This is where authentication, settings, and configuration data are defined. The server is bundled with the installation point, which hosts the Infor Smart Office client component for download to users' desktop machines.

- **Infor Smart Office client**
  This is installed on end users' desktop machines. End users update Infor Smart Office client from the installation point.

**User authentication**

By default, all users can log in to Infor Smart Office (ISO).

- When accessing the Infor Smart Office server, the Grid authenticates the user with the configured Session Provider before forwarding the request to Infor Smart Office server.
- To restrict access to certain users, an administrator can use the Role Mapping feature in Grid to control which users are included in the ISO Users role. All users that are included in the ISO Users role are allowed access to Infor Smart Office. By default, all authenticated users belong to the ISO Users role.

When using Infor Smart Office, its components will need to authenticate against other applications, such as the Infor Lawson Enterprise applications or Infor LBI. Infor Smart Office only handles one user ID and password. This means that all applications used with Infor Smart Office must authenticate against the same user registry or have some replication of user IDs and passwords between the different user registries.

**Single sign-on**

The Infor Smart Office user will experience single sign-on for all of the applications running in Infor Smart Office. Infor Lawson System Foundation uses Infor Lawson SSO to provide single sign-on capabilities for Infor Lawson Enterprise applications, Infor Process Automation, LBI, and Infor Landmark applications. When LSF is part of the Infor Smart Office configuration, all of these applications authenticate to the LSF LDAP.
Personalizations

For Infor Lawson Enterprise applications in Infor Smart Office, users have several options for customizing their experience. These personalizations are stored on the Infor Lawson System Foundation 10 server in LAWDIR/persistdata/lawson/SmartClient/data/forms/Data Area.

There are three sub-directories:

- /global
- /roles/RoleName
- /users/UserName

An additional role - FormPersonalizationRole - should be assigned if the Infor Smart Office user should be allowed to customize the user interface experience. Users without this role will not be allowed to make personalizations.

Demo: Grant access to allow user interface personalization in Infor Smart Office

Your instructor will demonstrate how to grant access to allow user interface personalization in Infor Smart Office.
Exercise 10.1: Grant access to allow user interface personalization in Infor Smart Office

In this exercise, you will access Infor Security Services and grant the proper access to allow a user to personalize his or her Infor Smart Office interface. You will then access Infor Smart Office and perform a personalization.

Exercise 10.1 steps

Part 1: Assign a role

1. Double-click the Infor Security Admin icon on the LSF10 training desktop. The ISA login screen opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The ISA tool administrator home page opens.
5. Select the People check box in the Select resource type field (upper right of screen).
6. Type user08 in the Search field.
7. Press Enter. The People list displays the user08 record.
8. Click the Edit resource (pencil icon). The user08 Basic tab opens.
9. Click the search icon in the Role field. The Roles list window opens.
10. Select the FormPersonalizationRole role.
11. Click the right-facing arrow > to move the role to the User Roles list panel.
12. Click OK.
13. Click Update Actor.
14. Click OK.
15. Click X to close ISA.

Part 2: Personalize Infor Smart Office

1. Double-click the Infor Smart Office on the LSF server’s training desktop.
2. Type user08@gdeinfor2.com in the User Name field.
3. Type Tr@in123 in the Password field.
4. Press Enter. The Infor Smart Office Canvas opens.
5. Right-click the Infor Smart Office Canvas. A menu option opens.
6. Select Settings > Infor Lawson > Applications. This Application tab displays.
7. Clear the Use list to access application form check box.
8. Click Save.
9. Click Close.
10. Type AP10.1 in the Start (search) field.
13. Clear the check boxes next to both the label and the field for Tax ID.
14. Click Save. Note: The Tax ID field and label are no longer visible.
15. Click X to close the AP10.1 window.
16. Click Log off to exit Infor Smart Office.

Part 3: View hidden fields
1. Double-click the Windows Explorer window.
2. Select E:\LSF10\law\persistdata\lawson\SmartClient\data\forms\APPS10\users\user08\ap10.1.xml. The IE browser window opens. Note: The two fields that were hidden are listed in the Hidden Fields definition.
3. Click X to close the IE browser window.
4. Right-click the Windows Start.
5. Select Shut down or sign out > Disconnect to return to the Infor Landmark training desktop.
Check your understanding

Which of the following actions would an administrator employ to limit access to Infor Smart Office?

a) Use the Role Mapping feature in the Grid
b) Remove the Infor Smart Office application from a user’s system
c) Select the No Access user attribute for a user
Lesson 11: Administering user access to LSF mobile applications

Estimated time
2 hours

Learning objectives
After completing this lesson, you will be able to:

- Describe how to set up a user for access to Infor Lawson mobile applications.
- Define the function of the Infor System Console.

Topics
- LSF mobile applications overview
- Infor System Console
- Infor Lawson System Console installation overview
- User set up for Infor System Console
- Infor Lawson Mobile Requisitions
- User setup for Infor Lawson Mobile Requisitions
- Check your understanding
The following mobile applications are available to function with Infor Lawson System Foundation applications. Mobile applications continue to be developed and enhanced. Please continue to check Infor Xtreme and Infor product communications to learn about mobile applications.

<table>
<thead>
<tr>
<th>Mobile application</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infor System Console®</td>
<td>This application enables administrators to monitor Infor Lawson System Foundation and perform some administrative tasks using a mobile device.</td>
</tr>
<tr>
<td>Infor Lawson Mobile Assets®</td>
<td>This application enables assets teams and other staff to quickly look up assets, perform inventory, and update asset information using a mobile device.</td>
</tr>
<tr>
<td>Infor Lawson Mobile Financials®</td>
<td>This application enables finance and accounting staff to quickly research and get statuses on account balances, invoices, and payments using a mobile device.</td>
</tr>
<tr>
<td>Infor Lawson Mobile Inventory®</td>
<td>This application enables materials, logistics, and other staff to quickly look up and update inventory information from Infor Lawson Procurement using a mobile device.</td>
</tr>
<tr>
<td>Infor Lawson Mobile Employee®</td>
<td>This application enables users to access and take action on their own employee information from the Infor Lawson Human Resources Management suite using a mobile device.</td>
</tr>
<tr>
<td>Infor Lawson Mobile Manager®</td>
<td>This application enables managers to view employee information such as dates of service, work assignments, compensation data, and performance history from the Infor Human Resources Management suite using a mobile device.</td>
</tr>
<tr>
<td>Infor Lawson Mobile Requisitions®</td>
<td>This application enables users to create and review requisitions from Infor Lawson Procurement using a mobile device.</td>
</tr>
<tr>
<td>Infor Lawson Mobile Inbasket</td>
<td>This application enables users to access and take action on electronic workflows and approvals produced by Infor Process Automation via a mobile device.</td>
</tr>
</tbody>
</table>

In this course, two mobile applications – Infor System Console and Infor Lawson Mobile Requisitions – are used as examples of the user setup procedures for Infor Lawson mobile applications. For details on the setup of other mobile applications, refer to that application’s reference guide.
Infor System Console

**Infor Lawson System Mobile Monitor Installation and User Guide**
**Infor Lawson Core Technology Installation Guide**
**Infor Lawson System Foundation Server Setup and Maintenance**
**Infor Lawson Resources and Security Administration Guide**

Infor System Console is a tool for Infor Lawson system administrators. The following features are accessible:

- View Infor Lawson Environment settings
- Start and stop the Infor Lawson Environment
- View the status of the Infor Lawson Environment services
- View diagnostic information, such as CPU, memory, user sessions, and processes
- View job status and restart Needs Recovery jobs
- View compile status and error logs
- View patch information
- View network diagnostics information
- View diagnostics information and run smoke tests for the Infor Lawson Environment
- Used on Android and iPhone devices
- Monitor LSF and perform administrative tasks via mobile device

![Initial screen for the Infor Lawson System Mobile Monitor](image)
Infor System Console installation overview

Infor System Console requires installation and configuration of components on both the Infor Lawson server and on the client (the user’s mobile device).

Server-side installation of Infor System Console

- Verify Java SDK version.
- Install Hyperic Sigar 1.6.4 (required for Mobile App).
- Establish a Web Server for the Mobile Monitor.
- Configure IBM WebSphere with an Application Server for the Mobile Monitor.
- Deploy lsmm.ear and lawsec.ear for the IBM WebSphere Application Server.
- Create lsmm.xml Service and load in ssoconfig.
- Establish SYSADMIN category of required Mobile Monitoring Form IDs.
- Establish lsmm Service with same user and password as SSOP.
- Connect authorized users with the roles S3MobileITAdminRole and S3MobileSysAdminRole (the roles and security classes are established prior to assignment to user).

Client-side installation of Infor Lawson System Console

- Download the Infor Lawson System Console from the application store of the device.
- Create a profile for connection to the server (server name and port).
- Access the Infor Lawson System Console.
User setup for Infor System Console

Users who need to access the Infor Lawson System Foundation environment through the Infor System Console mobile application must meet the following requirements:

- The security roles and security classes for the Infor System Console must be loaded.
- The form IDs for the Infor System Console must be present in the Form ID Definition utility (tokendef). These may be pre-loaded by the installation. If not, you must add them.
- User identities must be added for the lsmm service.
- The users who need access to the Infor System Console must be assigned either the S3MobileSysAdminRole or the S3MobileITAdminRole role.
- The user must download the app to his or her mobile device. Upon first access of the app, the user is prompted to accept the license agreement and then to create the first profile. You can later create additional profiles.

Roles

Two roles exist, which allow access to the Infor Lawson System Console, and in turn allow two levels of access within the mobile app. These roles and their associated security classes are configured by the system administrator following the procedures in the Infor System Console and Infor Lawson System Mobile Monitor Installation and User Guide. If this configuration is completed as outlined in the guide, the following privileges are granted to each role:

- **S3 Mobile System Admin** – This role accesses most app functions, including viewing job statuses, diagnostics, and system logs; it does not allow the user to stop and start the Infor Lawson environment from the mobile app.
- **S3 Mobile IT Admin** – This role allows the user to start and stop the Infor Lawson environment from the mobile app.

Some users may be given one or the other role or both roles, depending on their job function and desired level of mobile access. In the following exercise, you will provision a user who is permitted to view system information but not to stop and start the Infor Lawson environment.

**Demo: Grant user access to Infor System Console**

Your instructor will demonstrate how to grant user access to Infor System Console.

**Exercise 11.1: Grant user access to Infor System Console**

In this exercise, you will grant user access to Infor System Console.
Exercise 11.1 steps

Part 1: Add the S3MobileMonitorSysAdm role to Matthew Lincoln’s record

1. Double-click the Infor Security Admin icon on the LSF server’s training desktop. The ISA login screen opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The ISA tool administrator home page opens.
5. Select the People check box in the Select resource type field (upper right of screen).
6. Type user02 in the Search field.
7. Press Enter. The People list displays the user02 record.
8. Click the Edit resource (pencil icon). The User Provisioning / Basic tab for user02 opens.
9. Select the Roles field. The Roles window opens.
10. Select the S3MobileMonitorSysAdmin from the Roles list panel.
11. Click the right-facing arrow to move the role to the User Roles list panel.
12. Click OK.
13. Click Update Actor.
14. Click OK.
15. Click X to exit out of ISA.

Part 2: Validate access

1. Double-click the Infor Security Console icon on the LSF server’s training desktop. The Infor System Console login screen opens.
2. Type user02@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Infor Security Console tool administrator home page opens. Note: Matthew Lincoln now has access to the tool.
Infor Lawson Mobile Requisitions

Infor Lawson Mobile Requisitions allows you to create requisitions, view status, and receive shipments through an interface to Infor Lawson Procurement applications. This app provides mobile access to requester defaults, creating a new requisition, managing lines on a requisition, receiving shipments against purchase orders, and viewing the status of submitted requisitions.

![Infor Mobile Requisitions]

Infor Mobile Requisitions
User setup for Infor Lawson Mobile Requisitions

To use Infor Lawson Mobile Requisitions, a user must download the Infor Lawson Mobile Requisitions app to his or her device. In addition, an Infor Lawson Security profile must be enabled for Infor Lawson Mobile Requisitions for each mobile user.

Users of Infor Lawson Mobile Requisitions must be assigned to a custom user attribute in order to access the application. It is necessary to create the custom mobile attribute in the Infor Lawson Resource Management (RM) system and assign users to the attribute.

Users must also be assigned a role which allows them to perform the required functions in Infor Lawson Procurement. The custom user profile attribute does not provide access to perform system functions within Infor Lawson Procurement. Rather, it provides access to perform tasks allowed by other roles via a mobile device.

Creating a custom user profile attribute alters your LDAP schema. The person who performs these steps must:
- Be an experienced LDAP administrator
- Have security access to the Infor Lawson Resource Management system
- Have knowledge of and access to the Infor Lawson Schema Editor

In addition, it is important to note that the custom mobile attribute must be added to the LDAP schema used by the Infor Lawson server where Requisition Center (RQC) is installed.

User setup process overview

1. Install Infor Lawson Schema Editor (if not already installed).
2. Add a custom MobileUser attribute to Infor Lawson Resource Management (RM).
3. Link the custom MobileUser attribute to an RM object definition.
4. Assign the custom MobileUser attribute to mobile users.
5. Configure client application settings on the user’s mobile device.

Infor Lawson Mobile Requisition provisioning process

In this course, it is assumed that steps 1-3 are completed by a system administrator who is proficient with the use of the Infor Lawson Schema Editor. More information about steps 1-3 is available in the Infor Lawson Mobile Requisitions Reference Guide and the Infor Lawson Resources and Security Administration Guide.
Demo: Assign the custom MobileUser attribute to an Infor Lawson Mobile Requisitions user

Your instructor will demonstrate how to assign the custom MobileUser attribute to an Infor Lawson Mobile Requisitions user.

Exercise 11.2: Assign the custom MobileUser attribute to an Infor Lawson Mobile Requisitions user

In this exercise, you will assign the custom MobileUser attribute to an Infor Lawson Mobile Requisitions user.

Exercise 11.2 steps

1. Double-click the Lawson Security Admin icon on the LSF10 server’s training desktop. The Lawson Security Administrator server window opens.
3. Click Connect. The Lawson Security Administrator login window opens.
4. Type lawson@gdeinfo2.com in the User name field.
5. Type Tr@in123 in the Password field.
6. Click Sign In. The Lawson Security window opens.
8. Type Lincoln in the Name field.
9. Click Find Now. The list of records with Lincoln displays.
10. Right-click Matthew Lincoln (last row).
11. Select Edit RM Information.
13. Select Requisitions in the Available Attribute Values list.
14. Click the right-facing arrow > to move the attribute to the Assigned Attributes Values panel.
15. Click OK.
17. Select File > Close.
18. Click X to close the Lawson Security Administrator.
Note: To assign a value to the MobileUser attribute for a large number of users using the Resource Management tool, reference the "Mass Assigning Attributes to Users" section in the *Infor Lawson Resources and Security Administration* guide.
Check your understanding

In order to provide user access to the Infor Lawson Mobile Requisitions application, the user administrator would execute which of the following actions? Select all that apply.

a) Assign the custom MobileUser attribute to mobile users
b) Configure client application settings on the user’s mobile device
c) Add a custom MobileUser attribute to Infor Lawson Resource
d) Link the custom MobileUser attribute to an RM object definition

This application enables administrators to monitor Infor Lawson System Foundation and perform some administrative tasks using a mobile device.

a) Infor Lawson Mobile Assets
b) Infor Lawson Mobile Inventory
c) Infor System Console
Lesson 12: Administering user access to Infor Landmark Technology mobile applications

Estimated time

2 hours

Learning objectives

After completing this lesson, you will be able to:

- Describe how to set up a user for access to Infor Landmark Technology Runtime mobile applications.

Topics

- Infor Landmark mobile applications overview
- Infor Landmark Administrator
- Configure Infor Landmark Administrator on a mobile device
- Infor Notifications
- Check your understanding
Infor Landmark mobile applications overview

The following mobile applications are available to function with Infor Landmark Technology Runtime applications. Currently, Infor Landmark mobile applications are available for the Apple iOS® operating system. Mobile applications continue to be developed and enhanced. Please continue to check Infor Xtreme and Infor product communications to learn about mobile applications.

<table>
<thead>
<tr>
<th>Mobile app</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Infor Landmark Administrator®</td>
<td>This app enables administrators to monitor and manage Infor Landmark security, Infor Process Automation, and async queue information from mobile devices.</td>
</tr>
<tr>
<td>Infor Talent Manager®</td>
<td>This app enables managers to view employee information such as dates of service, work assignments, compensation data, and performance history from Infor Talent Management using a mobile device.</td>
</tr>
<tr>
<td>Infor Talent Recruiter®</td>
<td>This app enables recruiters to access interview and candidate information from Infor Talent Management using a mobile device.</td>
</tr>
<tr>
<td>Infor Notifications®</td>
<td>This app enables users to review and approve business process notifications managed by Infor Process Automation (IPA) and/or Infor Process Integration (IPI).</td>
</tr>
</tbody>
</table>

In this course, two mobile applications – Infor Landmark Administrator and Infor Notifications – are used as examples of the user setup procedures for Infor Landmark mobile applications. For details on the setup of other mobile applications, refer to that application's reference guide.
The Infor Landmark Administrator is a mobile application for Apple iPhone®, Apple iPad®, and Apple iPod Touch® devices that provides an administrator with access to key administrative tasks, such as:

- **Security administration** - Manage business application actor, role, and security class associations
- **Async queues** - Monitor and manage async queues, requests, and triggers
- **System log files** - View various system log files
- **Infor Process Automation** - Monitor and manage live and pending work units and configuration details

To install the Infor Landmark Administrator, download it from the application store for your device. Before an administrator can access the Infor Landmark Environment with the Infor Landmark Administrator the account must be assigned a role that includes the MobileAdministrationWebappAccess_ST security class. Upon starting the Infor Landmark Administrator, an administrator will be prompted to provide an account, password, server name, the Infor Landmark port, and the SSL setting (on or off).

The functionality available is the same as through the forms in the Infor Landmark Rich Client except that some minor features may not be included.

The Infor Landmark Administrator is accessible from the Infor Landmark Technology Runtime without additional installation procedures. If an administrator has the Infor Landmark Administrator application installed and the administrator’s account has the appropriate role then with server name and port, access to the app should be achieved.

**Note:** The functions available within the Infor Landmark Administrator application are configurable via General Properties. Refer to the Infor Landmark administration documentation for more information.
Demo: Assign the MobileAdministrationWebappAccess_ST security class to an administrator’s role to grant access to the Infor Landmark Administrator application.

Your instructor will demonstrate how to assign the MobileAdministrationWebappAccess_ST security class to an administrator’s role to grant access to the Infor Landmark Administrator application.

Exercise 12.1: Assign the MobileAdministrationWebappAccess_ST security class to an administrator’s role to grant access to the Infor Landmark Administrator application.

In this exercise, you will assign the MobileAdministrationWebappAccess_ST security class to an administrator’s role to grant access to the Infor Landmark Administrator application.

Exercise 12.1 steps
2. Type lawson@gdeinfor2.com in the Login Name.
3. Type Tr@in123 in the Password field.
4. Click LOGIN.
5. Select GEN in the data area field. The GEN applications display.
7. Click Search (magnifying glass).
8. Type security in the Role Name field.
9. Press Enter. The list of Roles displays.
10. Right-click the SecurityAdministrator_ST role.
11. Select Copy.
12. Type SecurityAdministratorwithMobile in the New Role field.
13. Click OK.
15. Click the Security Classes Assigned to Role tab.
17. Type GEN in the Data Area field.
18. Click the select arrow in the Security Class field. The Role Security Class window opens.
19. Type MobileAdministrationWebappAccess in the field.
20. Press Enter. The list of security class displays.
22. Click Save.
23. Click X to close the Role Security Class window.
24. Click the Security Classes Assigned to Role tab.
25. Review the list of security classes and note that MobileAdministrationWebappAccess_ST has been added.
26. Click X to close the Infor Rich Client.
Configure Infor Landmark Administrator on a mobile device

To use Infor Landmark Administrator, the user first downloads the app to his or her mobile device. If the user attempts to use the app prior to being granted appropriate security authorization, the “This user has no applications available.” error is generated. See image below.

![Infor Landmark Administrator no applications error](image)

After the user is granted appropriate access, as shown in the preceding exercise, the following information is entered into the application to create the user’s profile enabling the user to log in to the application with his or her existing Infor Landmark username and password:

- Profile name
- Server name
- Port number
Lesson 12: Administering user access to Infor Landmark Technology mobile applications

Infor Landmark Administrator New Profile and Login screens

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
Infor Notifications

Infor Process Automation Administration Guide

Infor Notifications is a powerful mobile interface for reviewing and approving your business process notifications managed by Infor Process Automation (IPA) and/or Infor Process Integration (IPI).

Notifications include work flow items and application messages that are proactively sent to users for review and action. Simply select a notification, review core information and other details included for decision making and then take action. For example, approve or reject an approval request and move your defined business process on to the next step.

User administration for Infor Notifications

Access to specific data and notifications is determined by the user’s role or roles in Infor Process Automation and/or Infor Process Integration. The Infor Landmark Technology Runtime framework and Infor Process Automation or Infor Process Integration handles the provisioning of Infor Notifications via the role InbasketUser_ST. If your user is new to IPA or IPI, you may need to assign the role InbasketUser_ST.
Scenario: Grant access to IPA and Infor Notifications

Grant Matthew Lincoln (user02) the ability to access Infor Process Automation and the Infor Notifications feature. Granting access to an application is done through the assignment of roles.

Considerations:

- You will want to log in as the lawson administrator and use the Infor Security Administrator (ISA) tool to update Matthew’s record.
- Do a People search for Matthew Lincoln’s record.
- You will want to assign the ProcessServerAllAccess_ST role to Matthew.
- You will want to assign the InbasketUser_ST role to Matthew.
- Make sure to save and update Matthew’s record.
Check your understanding

Which of the following roles must be set up before a user can access the Infor Landmark mobile applications?

a) A role that includes the MobileAdministrationWebappAccess_ST security class
b) A domain that includes the MobileAdministrationWebappAccess_ST security class
c) An identity that includes the MobileAdministrationWebappAccess_ST security class

A user has been granted access to Infor Notifications. The functions the user is permitted to complete by using the application are determined by _____________________.

a) The roles specific to the access of the Infor Notifications which have been granted to the user
b) The roles the user has as an Infor Process Automation (IPA) and/or Infor Process Integration (IPI) user that are not specific to Infor Notifications
c) The inquire/update permissions on the Infor Notifications user attribute on his or her user profile
Lesson 13: User monitoring and reporting

Estimated time

1 hour

Learning objectives

After completing this lesson, you will be able to:

- Describe the benefits of user monitoring.
- Explain how to use the ISS administrative tool to view user monitoring, history, and usage.

Topics

- User monitoring
- Check your understanding
User monitoring

**Infor Security Services Configuration Guide**

The user monitoring feature of LSF 10 enables customers to verify software licensing compliance by providing customers with the ability to:

- Monitor peak usage.
- Keep track of high-level information about users' interaction with the system (session, connectivity, application modules accessed).
- Create summary reports.
- Export data in CSV format to view and manipulate using the tool of choice.

User monitoring is not enabled by default. User monitoring can be enabled by your system administrator. After user monitoring is enabled in ISS, you must establish a session for users to show up in the monitoring.

**Demo: Enable user monitoring**

Your instructor will demonstrate how to enable user monitoring.

**Exercise 13.1: Enable user monitoring**

In this exercise, you will enable user monitoring.

**Exercise 13.1 steps**

1. Double-click the Infor Security Admin icon on the LSF server’s training desktop. The ISA login screen opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The ISA tool administrator home page opens.
5. Click the Monitoring tab.
6. Select the Configuration > Configure Monitoring.
7. Select the Enable Monitoring check box. Note: If this is already checked, checking it again will disable it.
8. Click Submit.
9. Click – to minimize the ISA tool.
Demo: Establish user sessions for review in user monitoring
Your instructor will demonstrate how to establish user sessions for review in user monitoring.

Exercise 13.2: Establish user sessions for review in user monitoring
In this exercise, you will establish user sessions for review in user monitoring.

Exercise 13.2 steps

Part 1: Establish an administrator session in Infor Lawson for Infor Ming.le.
1. Double-click the Infor Lawson for Infor Ming.le application on the LSF10 training server. The Infor Lawson for Infor Ming.le login window opens.
   1. Type lawson@gdeinfor2.com in the User name field.
   2. Type Tr@in123 in the Password field.
   3. Click Sign In. The Infor Lawson for Infor Ming.le home page opens.
   4. Type AP10.1 in the Search field.
   5. Press Enter. The AP10.1 Vendor form opens.
   6. Type 4321 in the Vendor Group field.
   7. Type 1000 in the Vendor field.
   8. Click Inquire. The vendor record for 4321 company displays.
   9. Click – to minimize the Infor Lawson for Infor Ming.le window. Note: Do not close the session.

Part 2: Establish a user session in Infor Smart Office
1. Double-click the Infor Smart Office shortcut icon in the LSF training desktop. The Infor Smart Office login window opens.
   1. Type user08@gdeinfor2.com in the Username field.
   2. Type Tr@in123 in the Password field.
   3. Click the blue arrow. The Infor Smart Office canvas opens.
   4. Type HR11.1 in the Search field (upper right of screen).
   5. Press Enter. The HR11.1 Employee form opens.
   6. Type 4321 in the Company field.
   7. Type 1003 in the Employee field.

178 Lesson 13: User monitoring and reporting
9. Click **Inquire. Charles Holley's** user record displays.
10. Click – to minimize the **HR11.1** form.
11. Click – to minimize the **Infor Smart Office** application. **Note:** Do not close the application.

**Demo: Access active user sessions in ISS**

Your instructor will demonstrate how to access active user sessions in ISS.

________________________________________

________________________________________

________________________________________

________________________________________

**Exercise 13.3: Access active user sessions in ISS**

In this exercise, you will access active user sessions in ISS.

**Exercise 13.3 steps**

**Part 1: Review user active sessions in ISA**

1. Click the **ISA** icon in the task bar to maximize the application. The **ISA** application opens.
2. Select **Monitoring > Sessions > Active Sessions**.
3. Review the session for **lawson**, including:
   - Session ID number: Unique number assigned to a session
   - IP address: Of the computer that is running the session
   - Client Type: Typically, this is the application running in the session.
   - Start Time: The time the session began
   - Last Update: Most recent transaction performed by the user
4. Review the session for **user08**, including:
   - Session ID number: Unique number assigned to a session
   - IP address: Of the computer that is running the session
   - Client Type: Typically, this is the application running in the session.
   - Start Time: The time the session began
   - Last Update: Most recent transaction performed by the user

**Part 2: Review session history**

1. Select **Monitoring > Sessions > Session History**. The **Session History** page opens.
2. Select the **lawson** history session and view the available information. The **lawson** record displays.
3. Select the **user08** history session and view the available information. The **user08** record displays.
Part 3: Review peak usage history
2. Select This Month in the Select date range drop-down menu.
3. View the available information.
4. Select Monitoring > Sessions > Usage Peaks by Module.
5. Select This Month in the Select date range drop-down menu.
6. View the available information.

Part 4: Export user monitoring data in ISS
2. Select Session Summary in the Export Type field.
3. Select the <first day of the month> in the first date range field.
4. Select <today's date> in the second date range field.
5. Click Export.
6. Click the Windows Explorer icon in the task bar. The Windows Explorer window opens.
7. Select E:\ LSF10\law\system.
8. Double-click the session_summary_<date>.zip file. The list of files opens.
10. Click X to close the .csv file and Windows Explorer.
11. Click X to close ISA and end the browser session.
12. Click X to close the Infor Lawson for Infor Ming.le browser and session.
Check your understanding

True or false? User monitoring is enabled by default.
   a) True
   b) False

Which of the following best explains the benefits of user monitoring? Select all that apply.
   a) Monitors peak usage
   b) Keeps track of high-level information about users’ interaction with the system
   c) Creates summary reports for analysis
Lesson 14: Administering user access to Infor Lawson extension applications

Estimated time
1 hour

Learning objectives
After completing this lesson, you will be able to:

- Describe user administration tasks in Infor Lawson Mobile Supply Chain Management (MSCM).
- Describe user administration tasks in Infor Lawson Business Intelligence (LBI).

Topics
- Mobile Supply Chain Management (MSCM)
- Infor Lawson Business Intelligence (LBI)
- Check your understanding
The Infor Lawson Mobile Supply Chain Management (MSCM) suite of products works with the Infor Lawson Procurement application in Infor Lawson System Foundation. It leverages mobile handhelds, automated data collection, and wireless technology to simplify receiving, delivery, and inventory processes. MSCM applications are designed to minimize lost packages and improve service while providing better control and tracking of inventory through mobile receiving, delivery, package tracking, issues, par counting, and cycle counting. The MSCM suite contains the following applications (of which a client may license one, several, or all):

- Mobile Par and Cycle Counting (MPC) - streamlines replenishment, uses wireless handheld devices to manage medical supply inventory
- Receiving and Delivery (RAD) - tracks receipts, verifies deliveries to storage locations
- Point of Use (POU) - streamlines the process of capturing patient charges while managing supply inventory
- Surgical Instrument Management (SIM) - tracks surgical instruments and trays throughout their lifecycle, from procurement, assembly, packaging, sterilization, storage, distribution, to utilization

User Management in MSCM

User Management is a function within the Administration menu of MSCM. It is designed to control which users of the application have access to certain features and functions. For example, one user may be able to do Pull and Return transactions, but not view the productivity reports. Much like Windows security, User Management uses a schema of users, groups and rights to control access privileges. Users can be loaded from Infor Lawson for Infor Ming.le or entered directly into User Management. Each individual uses one user ID and
password to log in to Mobile Supply Chain Management and, if used, the Infor Lawson Point of Use for Nursing and Department Inventory application.

Groups
Groups contain users who perform the same tasks, such as administrators or nurses. Administrators assign tasks to user groups based on the role of the users in that group. When the users log in to the application, only those tasks that are assigned to them appear.

Location management
Location management refers to setting up locations, companies, and sub-locations for use with Infor Lawson Mobile Supply Chain Management, Receiving and Delivery, and Point of Use for Nursing and Department Inventory. Locations are used in tracking the positions of inventory and medical supplies.

Demo: Modify a user profile for MSCM
Your instructor will demonstrate how to modify a user profile for MSCM.

______________________________________________________________________
______________________________________________________________________
______________________________________________________________________
______________________________________________________________________

Exercise 14.1: Modify a user profile for MSCM
In this exercise, you will modify a user profile for MSCM.

Exercise 14.1 steps
Part 1: Create a new group in MSCM
1. Double-click the MSCM icon in the LSF10 server’s training desktop. The MSCM login window opens.
2. Type MSCADMIN@gdeinfor2.com in the Username field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The MSCM application window opens
6. Click the Groups tab. The Add Group page opens.
7. Type Nurses in the Create New Group Name field.
8. Click Continue.
9. Select the check boxes for the following roles from the All Roles list:
   o Point of Use – Modify Patient Location
   o Point of Use – View Patient Location
   o Point of Use – Desktop – Enter Records

Lesson 14: Administering user access to Infor Lawson extension applications

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
Part 2: View or print a group

1. Select Actions > View/Print.
2. Click Continue. The View/Print Group page appears. **Note:** The list may be printed if needed by selecting the Print button. Do not print the list for this exercise.
3. Click Cancel.
4. Leave MSCM open for the next exercise.

**Demo: Add a new MSCM user from the list of Infor Lawson for Infor Ming.le (Portal) users**

Your instructor will demonstrate how to add a new MSCM user from the list of Infor Lawson for Infor Ming.le (Portal) users.

**Exercise 14.2: Add a new MSCM user from the list of Infor Lawson for Infor Ming.le (Portal) users**

In this exercise, you will add a new MSCM user from the list of Infor Lawson for Infor Ming.le (Portal) users

**Exercise 14.2 steps**

Part 1: Add an existing Portal user to the Nurses group

1. Select Administration > User Management.
2. Click the Users tab. The User Information page opens.
4. Type user08 in the Portal User ID field.
5. Click Search. Taylor Wang’s record displays.
6. Select Nurses in the Group drop-down menu.
7. Select the **Create new default assignments** radio button.

8. Select **Location Access**. The **Assign Access to Locations** window opens.

9. Select the **1000-Class Company** in the **System Location** drop-down menu. The list of locations associated with **1000** company displays.

10. Select the **2200-Regional Office** check box.

11. Click **Add (>)**.

12. Click **OK**.

13. Click **Locations**.

14. Select the following in the **RAD** section – **Default Delivery To** row.
   - Company-1000-Class Company
   - Location-2200-Regional Office

15. Click **OK**.

16. Click **Save**.

17. Click **Done**.

**Part 2: Creating a new MSCM user by copying an existing MSCM user assignment**

If the user is already a user of Infor Lawson for Infor Ming.le, you may pull data from this existing user profile to streamline the creation of a MSCM user profile.

1. Click the **Users** tab. The **User Management** page displays.

2. Select **Actions > Add User from Portal**.

3. Type **user01** in the **Portal User ID** field.

4. Click **Search**. **Marcia Hudson’s** record displays.

5. Select **Nurses** from the **Group** drop-down menu.

6. Select the **Copy existing user assignments** radio button.

7. Click **Copy Assignments**.

8. Type **user08** in the **User ID** field.

9. Click **Search**. **Taylor Wang’s** record displays.

10. Select the **user08** radio button.

11. Click **OK**.

12. Click **Save**.

13. Click **Done**.

**Note:** If the user should access MSCM via Infor Lawson for Infor Ming.le, an administrator must also set up the distributed single sign-on for MSCM and create a set of custom bookmarks for MSCM in Infor Lawson for Infor Ming.le. See the *Mobile Supply Chain Management and POU Administration Guide* for these procedures.

**Part 3: Modify an existing user profile’s group membership**

1. Select **Actions > Modify** from the **Users** tab.

2. Type **user08** in the **User ID** field.

3. Click **Search**. **Taylor Wang’s** record displays.

4. Select **Admin** from the **Group** drop-down menu.

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
5. Click **Save**.
6. Click **Done**.
7. Click **X** to close the **MSCM** tab and browser session.

**Part 4: Validate access to MSCM for user01**

1. Double-click the **MSCM** icon in the desktop. The **MSCM** login window opens.
2. Type `user01@gdeinfor2.com` in the **Username** field.
3. Type `Tr@in123` in the **Password** field.
4. Click **Sign In**. The **MSCM** application window opens. Notice the options for Marcia Hudson differ from the MSCMADMIN user.
5. Click **X** to close the **MSCM** tab and browser session.

**Part 5: Inactivate a user**

If the user is no longer a user of MSCM, the user profile should be inactivated, not deleted, so that connections between the user and data they created or modified are still recorded in the system. If an inactive user becomes a user of the system again, the user profile may be reactivated.

1. Double-click the **MSCM** icon in the desktop. The **MSCM** log in window opens.
2. Type `MSCMADMIN@gdeinfor2.com` in the **Username** field.
3. Type `Tr@in123` in the **Password** field.
4. Click **Sign In**. The **MSCM** application window opens
5. Select **Administration > User Management**. The **User Management** page opens.
6. Click the **Users** tab. The **User Management** page displays.
7. Select **Actions > Inactivate/Activate**. The **Search for a user to Activate/Inactivate** page opens.
8. Type `user01` in the **User ID** field.
9. Click **Search**. Marcia Hudson’s record displays.
10. Click **Inactivate this User** next to the user’s current **Status**.
11. Click **Done**.
12. Click **X** to close **MSCM**.

**Part 6: Validate access to MSCM for user01**

1. Double-click the **MSCM** icon in the desktop. The **MSCM** login window opens.
2. Type `user01@gdeinfor2.com` in the **Username** field
3. Type `Tr@in123` in the **Password** field.
4. Click **Sign In**. An “**Access Denied**” error displays because Marcia Hudson no longer has access to MSCM.
5. Click **X** to close the **MSCM** tab and browser session.
6. Select **Shut down or sign out > Disconnect** to return to the Infor Landmark training desktop.
User administration in Infor Lawson Business Intelligence

Infor Lawson Business Intelligence (LBI) is the Infor Lawson solution for operational business intelligence. It is a full-featured suite that is tightly integrated with Infor Lawson business applications and can also pull in non-Infor Lawson data.

Information is delivered to users through automated notifications, bursted reports, role-based dashboards, and other solutions. Users can navigate smoothly from alerts to interactive analysis down to detailed reports and even to transactions all while maintaining the context that is critical to root cause analysis.

The LBI application includes the following components:

- Framework Services
- Reporting Services
- Smart Notification

Note: Your particular installation may not include all of the Infor Lawson Business Intelligence components.

Framework Services

Framework Services is the main component of the Infor Lawson Business Intelligence application, providing a central user interface and access point for all Infor Lawson Business Intelligence application components. After each component is installed, it should be registered with Framework Services and accessed from its user interface.

Framework Services:

- Integrates the LBI application’s components
  - Dashboards combine data from Reporting Services, Smart Notifications, and other sources for quick access by users
- Provides functionality such as rendering and searching
- Provides cross platform communications
- Facilitates a central user interface and data repository
- Facilitates authentication between applications

Users and roles

A user is a person. Roles are associations of users in LBI. Groups are associations of users in the authentication provider that are mapped to roles in LBI.

Users are associated in roles so that multiple access privileges can be assigned to multiple users. Users are assigned to roles during installation but you can modify user/role associations using Manage Users & Roles on the Tools dashboard.

Framework Services has three predefined roles. These are:

- Administrators
- Power Designers (and Designers)
- Users

You can map these roles to other roles or groups in the authentication provider as needed.
For example, a role may be called HRManagement. You assign all users in HR management positions to this role and assign the role type Users to the role HRManagement. Another example might be a role called BusinessAnalysts. You assign all business analysts to this role and assign the role type Power Designer to the role BusinessAnalysts thus enabling business analysts to design dashboards.

**Administrator**

Administrators are defined as a group in the authentication provider and mapped to the administrative role in LBI using the System Settings option on the Tools dashboard.

Administrators are the managers of the LBI system. They can view, create, and edit all dashboards and content, add dashboards to the Framework Services menu bar, and reassign content. Administrators can also use the Tools dashboard to perform tasks such as registering applications and modifying the contents of the sysconfig.xml file using the System Settings tool on the Tools dashboard.

**Power Designer/Designer**

The Power Designer group in LBI is mapped to a group in the authentication provider with the default name PowerDesigners (no space). You can change the role mapping using the System Settings tool on the Tools dashboard.

Power Designers have access rights assigned by an Administrator. They can view, create, and edit all dashboards and content. Power Designers do not have access to the administrative tools in the Tools dashboard.

A subset of Power Designer is the Designer. Designers have editing rights to one or more specified dashboards or content modules. This right is assigned by the Administrators or, more usually, by Power Designers provided they have been granted the right to do so by an Administrator.

**User**

A User can view the dashboards, content modules, and content links and items to which the Administrator or Power Designer has given them viewing access.

### Summary of user roles and dashboard rights

In summary, an administrator can design and view all dashboards and the Tools dashboard, a Power Designer can design and view all dashboards to which they have been given designer access; a Designer can design...
and view one or more dashboards; a User can view one or more dashboards to which they have been given viewing access.

**System administration tools**

LBI system administration tools are described briefly below.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Install Validator</td>
<td>This tool validates the installation. For more information, see the <em>Infor Lawson BI Installation Guide</em>.</td>
</tr>
<tr>
<td>System Settings</td>
<td>This tool opens the System Configuration Assistant which is a window into the configuration file, sysconfig.xml. Here you can configure authentication and repository settings and localize LBI for language and time zone differences. Restart the application server to have the changes take effect.</td>
</tr>
<tr>
<td>Services</td>
<td>This tool opens the Services dashboard where you can modify services attributes</td>
</tr>
<tr>
<td>Synchronize Users and Roles</td>
<td>This tool synchronizes new users and roles or remove expired users.</td>
</tr>
<tr>
<td>Manage Users and Roles</td>
<td>This tool manages the associations between users and roles.</td>
</tr>
</tbody>
</table>

**LBI authentication**

Authentication is a post-installation requirement that determines whether users and their passwords are valid in a given context. Most LBI components do not store passwords. Instead, they use a third-party provider of authentication, called an **authentication provider**. The third-party product that provides lists of roles and users is a **role provider**. There are multiple available authentication providers and role providers. Most installations use Distributed Single Sign-on (DSSO) as the authentication provider. For more information, review the *Framework Services Administration Guide*.

**Demo: Configure user access on Infor LBI**

Your instructor will demonstrate how to configure user access on Infor LBI.
Exercise 14.3: Configure user access on Infor LBI

In this exercise, you will configure user access on Infor LBI.

Exercise 14.3 steps

1. Double-click the Infor Ming.le shortcut icon on the Infor Landmark server’s training desktop. The Infor Ming.le login window opens.
2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The Infor Ming.le home page opens.
5. Select the Infor Lawson BI icon. The Infor Lawson LBI application opens.
6. Click the Lawson Dashboards Menu (gear) icon in the blue header bar in the top-right corner of the screen.
7. Select New Dashboard Tab.
8. Type Training Dashboard in the Dashboard Title field.
9. Click OK. The new dashboard opens.
10. Click the Training Dashboard + icon. The Options menu displays.
12. Click the Sharing tab.
13. Click Edit Viewers. The User & Role Picker window opens.
14. Clear the users check box.
15. Select the role check box.
16. Select the following roles:
   - Administrators
   - LBIAdmin
   - Security
17. Click the right-facing arrow > to move them to the Selected column.
18. Click OK.
19. Click Save.
20. Click X to close the LBI session. The Windows Internet Explorer dialog window opens.
21. Select Leave this page.
Check your understanding

Which of the following functions in MSCM allows an administrator to manage user access?

a) Framework Services  
b) User Management  
c) Point of Use

__________ uses a schema of users, groups and rights to control access privileges in MSCM.

a) User Management  
b) Identities  
c) Single sign-on

__________ is the main component of the Infor Lawson Business Intelligence application.

a) User Management  
b) Framework Services  
c) Administrator Services

Which option describes a typical way in which users are granted access to MSCM?

a) A user is designated as an Administrator, a Power Designer, or a User.  
b) A user is assigned to a group. A group is assigned one or more roles.  
c) A user is assigned one or more security classes. Security classes are joined together into groups for reference.

__________ are the managers of the LBI system and can view, create, and edit all dashboards and content and use the Tools dashboard.

a) Power Designers  
b) Administrators  
c) Users
Course summary

Estimated time
30 minutes

Learning objectives
Now that you have completed this course, you should be able to:

- Recognize the architecture components of Infor® Lawson® System Foundation® 10 (LSF) and Infor Landmark Technology Runtime® 10.
- List the components of the Distributed Security Package.
- Explain the differences between authentication protocol, federation, and Primary Authentication Service (PAS).
- Identify the tools available to administer users in version 10 of both LSF and Infor Landmark.
- Describe how the Infor Security Administration® (ISA) tool provides user provisioning, synchronizing, and federation services in environments where Infor Lawson System Foundation and Infor Landmark Technology Runtime are installed and federated.
- Identify utilities used to mass-load users into LSF and Infor Landmark.
- Clarify how roles are used to provide access to Infor applications.
- Define the process for modifying Infor-delivered roles in both LSF and Landmark to grant or remove user access.
- Describe the difference between a federated and a stand-alone environment and its impact to user administration.
- Explain why you would use ISA to maintain user data between environments where LSF and Infor Landmark are federated.
- Describe the process for synchronizing an environment.
- Describe how to administer access to Infor Ming.le™, Infor Lawson for Infor Ming.le, Infor Landmark Rich Client®, and Infor Smart Office.
- Define the purpose of user attributes in administering user access.
- Describe how to administer user access to Infor Lawson Add-ins for Microsoft Office.
- Describe the purpose and setup of user proxies.
- Describe how to set up a user for access to Infor Lawson and Infor Landmark mobile applications.
- Explain how to enable user monitoring and reporting.
- Describe how to administer users of Infor Lawson Mobile Supply Chain Management® and Infor Lawson Business Intelligence®.

Topics
- Course review
Course review

If a user no longer works for your organization, what action should you take to prevent the user from accessing your Infor Lawson system?

a) Delete the user from the system
b) Change the user’s password and reassign his or her username to a new employee
c) Disable the user in the system

Which of the following are examples of why federation is beneficial to user administration when an installation is running both LSF and Infor Landmark. Select all that apply.

a) Single system (ISS) in which to provision users
b) Users in LSF and Infor Landmark kept synchronized automatically (if ISS is used)
c) Single sign-on for users of LSF and Infor Landmark applications
d) Users, roles, and groups can be “seen” by both systems

Which of the following customizations can an administrator apply to the user experience of Infor Ming.le Foundation? Select all that apply.

a) Add a new application
b) Add a link to a new site
c) Allow the user to logout and log back in as a different user
d) Add a company logo
e) Add an announcement

Which of the listed mobile applications requires the setting of a custom user attribute to allow user access?

a) Infor Lawson System Mobile Monitor
b) Infor Lawson Mobile Requisitions
c) Infor Landmark Administrator
d) Infor Notifications

Name the two utilities used to mass-load users to LSF and Landmark, respectively.

a) Loadusers - LSF
b) Secadm – Infor Landmark

ame) Which feature could you use to determine when your peak usage times occur and how your servers are performing if you are working in a system on which Infor Security Services is installed?

a) Framework Services
b) User monitoring
c) Infor Rich Client
Appendices

Appendix A: Creating a user in Lawson Security Administrator
Appendix B: Disabling and enabling a user in ISA
Appendix C: LifeCycle Manager Client 2.0
Appendix A: Creating a user in Lawson Security Administrator

**Exercise: Provision a user in LSF 10**

In this exercise, you will provision a user in LSF 10 using Lawson Security Administrator.

**Exercise steps**

**Part 1: Create user**

1. Double-click the Lawson Security Admin icon on the LSf10 server's training desktop. The Lawson Security Administrator server window opens.
3. Click Connect. The Lawson Security Administrator login window opens.
4. Type lawson@gdeinfor2.com in the User name field.
5. Type Tr@in123 in the Password field.
6. Click Sign In. The Lawson Security window opens.
7. Select User Management > User Maintenance.
8. Click New User.
9. Click the ISO Locale attribute.
10. Type en in the ISO Locale field.
11. Click the Product Line attribute.
12. Type APPS10 in the Product Line field.
13. Double-click the Role attribute.
14. Select <any role> in the Role field.
15. Click > to move the role to the right.
16. Click Finish.
17. Type Kristie in the First Name field.
18. Type user03 in the ID field.
19. Type Fisher in the Last Name field.
20. Type user03@edu.com in the Email field.
21. Type Kristie Fisher in the Name field.
22. Click Next.

**Part 2: Manage identities**

1. Select User Management > Manage Identities (below User Maintenance).
2. Select LSF10 in the Services list.
3. Double-click the Domain User field.
4. Type `gdeinfor2\user03` in the **Domain_User** field.
5. Press Tab.
6. Type `Tr@in123` in the **Password** field.
7. Type `Tr@in123` in the **Password Confirm** field.
8. Select **SSOP** in the **Services** list.
9. Click Yes to save changes.
10. Double-click the **Password** field.
11. Type `Tr@in123` in the **Password** field.
12. Type `Tr@in123` in the **Password Confirm** field.
13. Type `user03@gdeinfor2.com` in the **User** field.
14. Select **apps10_Employee** in the **Services** list.
15. Click Yes to save changes.
16. Type `4321` in the **Company** field.
17. Press Tab.
18. Type `1126` in the **Employee** field.
19. Click Next.
20. Click Finish.
21. Type `Fisher, Kristie` in the **Name** field.
22. Click Find Now. User records for Kristie Fisher appear in the **Query Results** field.
23. Click the Close (X) icon in both Lawson Security Administrator windows to exit the Lawson Security Administrator.
Appendix B: Disabling and enabling a user in ISA

You must have Infor Landmark 10.1.1.34 or higher to enable a user using ISA. This training image is only at version 10.1.1.33.

Exercise: Disable a user

In this exercise, you will log in as the lawson administrator to disable a user. After you disable the user, you will log out as administrator and sign back in as the user to validate access.

Exercise steps

Part 1: Log in as an administrator to ISA to disable Taylor Wang

2. Type lawson@gdeinfor2.com in the User name field.
3. Type Tr@in123 in the Password field.
4. Click Sign In. The ISA tool administrator home page opens.
5. Select the People check box in the Select resource types field (upper right of screen).
6. Type user08 in the Search field.
7. Press Enter. The People list displays the user08 record.
8. Click the Disable Resource (crossed out circle icon). The Resource Manager window opens.
9. Click Yes to confirm that you want to disable user08.
10. Click OK.
11. Click the Edit resource (pencil icon). The Basic tab opens. Note: The Run As Enabled field now displays NO.
12. Click – to minimize Infor Security Administrator.

Part 2: Log in to Infor Rich Client as user08 to check access

2. Type user08@gdeinfor2.com in the Login Name field.
3. Type Tr@in123 in the Password field.
4. Click Login. The error “Invalid username/password” displays.
5. Click OK.
6. Click Cancel to close Infor Rich Client.

Part 3: Re-enable user08

1. Select the Infor Security Administrator application from the task bar to maximize.

© 2017 Infor Education. All rights reserved. No part of this document may be reproduced or transmitted in any form, without written permission.
2. Click the **Enable Resource** (check mark inside a circle icon).
3. Click **Yes** to confirm you want to enable user08.
4. Click **OK**.
Appendix C: LifeCycle Manager Client 2.0

Administrator users

Administrator users must have access to the Infor Smart Office administrator tools and have read-write permissions to directories on the Infor Smart Office server where configuration and settings files reside. Administrators should also be LifeCycle Manager Administrators.

LifeCycle Manager is a framework that facilitates standardized and uniform installation, maintenance, and management of Infor M3 and Infor Lawson products. This framework enables administration and customization of several servers and products from a centralized location. Lifecycle Manager is used with Infor Smart Office for certain user administration tasks, such as setting up administrator user profiles.

Exercise: Explore administrator setup for Infor Smart Office

In this exercise, you will explore administrator setup for Infor Smart Office.

Exercise steps

Part 1: Add a user to LifeCycle Manager

1. Double-click the RDP Shortcuts folder on the Infor Landmark server’s training desktop. The folder opens with the list of servers.
4. Type LCMAdmin in the User field.
5. Type Lawson123 in the Password field.
6. Click Log On. The LifeCycle Manager application opens.
7. Click the Applications tab.
8. Click the plus sign (+) next to Lawson Grid 10.11.0.
9. Right-click LCM_Grid.
10. Select Lawson Grid 10.11.0 > Configuration Manager. The Configuration Manager window opens.
11. Select User and Role Mappings. The User and Role Mappings window opens.
   Locate the MangoServer/Administrator row. Note: In the green Included Members column inforuser and lawson are currently the only administrators of Infor Smart Office.
12. Click Edit in the Included Members (green) column in the MangoServer/Administrator row. The Role Mappings window opens.
13. Click Add. The Add Role Mappings to MangoServer/Administrator window opens.
14. Type user02 in the Custom field in the Global section.
15. Click Add directly to the right of the Custom field to add user02.
16. Click OK. Notice that user02 is now listed in the Role Mappings window along with lawson and inforuser.
17. Click OK.
18. Click Save in the top-left corner of the User and Role Mappings tab.
19. Click Save to confirm your changes. The new user will display in the green column MangoServer/Administrator row.
20. Click X to close the LifeCycle Manager.

Part 2: Validate changes

1. Double-click the Isf10 server in the RDP Shortcuts folder. The LSF10 server’s training desktop opens.
2. Double-click the Infor Smart Office - Train desktop icon.
3. Type user02@gdeinfor2.com in the User Name field.
4. Type Tr@in123 in the Password field.
5. Press Enter. The Infor Smart Office application opens. Notice the Administration Tools menu is now available in the Navigator pane.
6. Click X to close Infor Smart Office.