Infor XA Configuration Guide for Infor OS using System i Workspace AnyWhere

XA 9.2 and 10.x
Infor OS On-premises 2022-xx

Publication Information

Release: Infor XA Configuration Guide for Infor OS using System i Workspace AnyWhere

Publication date: April 28, 2023

Contents

About this guide

This document describes the integration of XA with Infor OS On-premises using System i Workspace AnyWhere, referred to as SiWA in the rest of this guide. This guide explains the integration requirements, configuration tasks, and troubleshooting information.

Intended audience

This guide is intended for the system administrator or professional service consultant who configures the integration between SiWA and Infor OS.

Required knowledge

To integrate XA and Infor OS, you must understand the concepts behind System Manager, SiWA, and Infor OS.

Related documents

You can find the documents in the product documentation section of the Infor Support Portal, as described in "Contacting Infor" on page 8.

These guides are also needed if the initial installation is not already completed:

- Infor System Manager Quick Installation Guide for Infor XA
- Infor XA Setup Guide for Secure Net-Link
- Infor Operating Service Installation Guide
- Infor Si System Manager Installation Guide
- System i Workspace AnyWhere Installation and Administration Guide
- KB 1365947 – Need Authorization codes
- KB 1136739 – System Manager and Work Management PTFs
- KB 1963350 – System i Workspace AnyWhere

Contacting Infor

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

The latest documentation is available from docs.infor.com or from the Infor Support Portal. To access documentation on docs.infor.com, look under **ERP & Finance > XA**. We recommend that you check this portal periodically for updated documentation.

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

Chapter 1 Introduction

Infor OS is a comprehensive platform for social collaboration, business process improvement, and contextual analytics. You get the most innovative social collaboration technologies translated into a business environment, fully integrated across your business processes.

System i Workspace AnyWhere (SiWA) is the user interface for Infor XA.

The user interface includes these components:

- Most XA IDF objects that are available in IDF Net-Link.
- XA IDF Level 1 tasks that were previously only available through green screen and Host Presentation Server in Power-Link.
- SiWA, an intermediate layer. This layer is required because the NetLink user interface is not displayed as tabbed content directly within the frame of Infor OS.
- Within SiWA, both Net-Link and IDF L1 user interfaces are rendered as tabbed content.

This guide describes the process to configure the components required to run XA within the Infor OS common user interface.

These are the recommended sequence of steps to complete the installation and configuration:

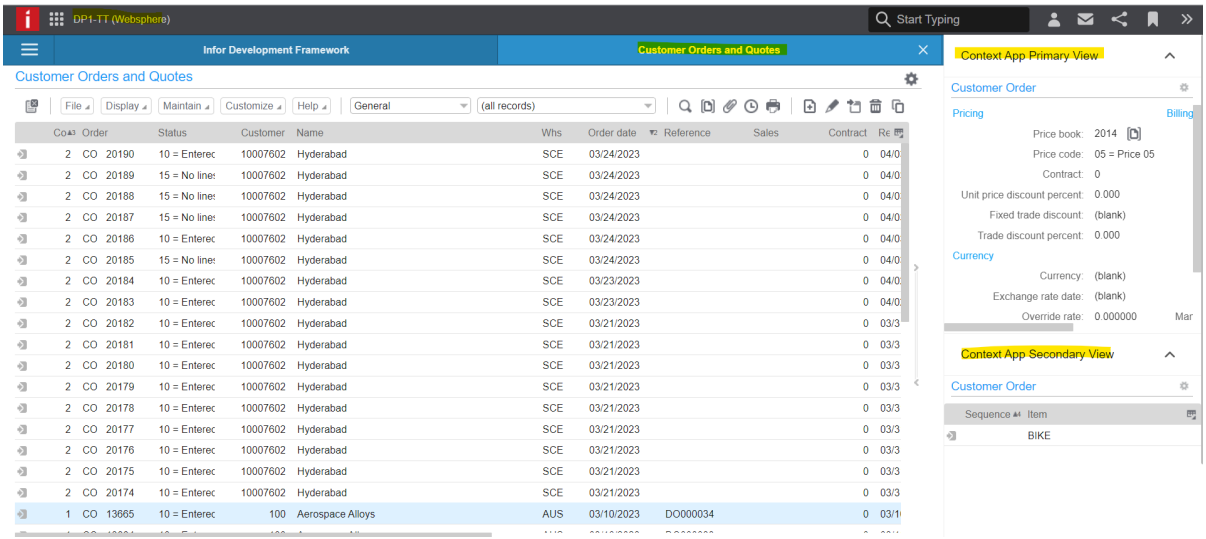
1 Infor XA server and client with Net-Link

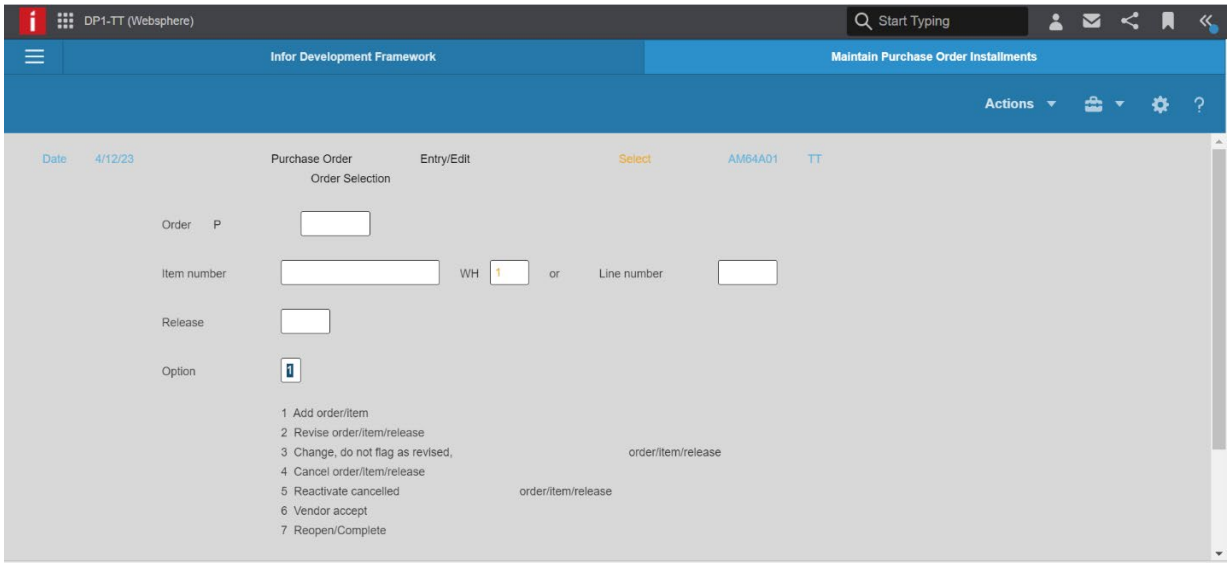
2 Infor System i System Manager

3 Infor System i Workspace AnyWhere

4 Infor Operating Service (OS)

These examples show the System i Workspace AnyWhere in Infor OS:


DP1-TT (Websphere)
Start Typing
Infor Development Framework
Customer Orders and Quotes
Customer Orders and Quotes
File
Display
Maintain
Customize
Help
General
(all records)
Co
Order
Status
Customer
Name
Whs
Order date
Reference
Sales
Contract
Re
2 CO 20190 10 = Enterec 10007602 Hyderabad SCE 03/24/2023 0 04/0
2 CO 20189 15 = No line 10007602 Hyderabad SCE 03/24/2023 0 04/0
2 CO 20188 15 = No line 10007602 Hyderabad SCE 03/24/2023 0 04/0
2 CO 20187 15 = No line 10007602 Hyderabad SCE 03/24/2023 0 04/0
2 CO 20186 10 = Enterec 10007602 Hyderabad SCE 03/24/2023 0 04/0
2 CO 20185 15 = No line 10007602 Hyderabad SCE 03/24/2023 0 04/0
2 CO 20184 10 = Enterec 10007602 Hyderabad SCE 03/23/2023 0 04/0
2 CO 20183 10 = Enterec 10007602 Hyderabad SCE 03/23/2023 0 04/0
2 CO 20182 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
2 CO 20181 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
2 CO 20180 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
2 CO 20179 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
2 CO 20178 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
2 CO 20177 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
2 CO 20176 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
2 CO 20175 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
2 CO 20174 10 = Enterec 10007602 Hyderabad SCE 03/21/2023 0 03/3
1 CO 13665 10 = Enterec 100 Aerospace Alloys AUS 03/10/2023 DO000034 0 03/1
Context App Primary View
Customer Order
Pricing
Billing
Price book: 2014
Price code: 05 = Price 05
Contract: 0
Unit price discount percent: 0.000
Fixed trade discount: (blank)
Trade discount percent: 0.000
Currency
Currency: (blank)
Exchange rate date: (blank)
Override rate: 0.000000 Mar
Context App Secondary View
Customer Order
Sequence
Item
BIKE


DP1-TT (Websphere)
Start Typing
Infor Development Framework
Maintain Purchase Order Installments
Actions
Date 4/12/23
Purchase Order Entry/Edit
Order Selection
Select
AM64A01
TT
Order P
Item number
WH 1
or
Line number
Release
Option 1
1 Add order/item
2 Revise order/item/release
3 Change, do not flag as revised, order/item/release
4 Cancel order/item/release
5 Reactivate cancelled order/item/release
6 Vendor accept
7 Reopen/Complete

Chapter 2 Requirements

This chapter describes the requirements for configuring Infor XA with Infor OS using SiW Anywhere.

Infor XA Server and client with Net-Link requirements

Install System Manager on each IBMi which runs XA environments. This is a pre-requisite for SiW Anywhere. Review this list to determine what you need:

- Infor Development Framework for Infor XA 06.03 (IDF R9) and any additional IDF licensed applications like IDF Power-Link with Integrator and Net-Link.
- Infor XA IDF 9.2.2 client software build must be 02.09.02.02.30 or later.
- Infor XA IDF 9.2.2 server PTFs is PCM SH16055 (XA 9.2.2 with PTF level 025000).
- Infor XA IDF 10.0 client software build must be 03.10.00.01.03 or later
- Infor XA IDF 10.0 server PTFs is PCM SH16231 (XA 10.0 with PTF level 00100).
- IBMi standard software set option 5770SS1: Option 8 – AFP Compatibility Fonts (required for TIFF image support).
- IBMi standard software set option 5770TS1 on V7R2/R3/4 i5/OS, must have both the base option and Option 1 installed (required for PDF support).

Additional software required for System i System Manager:

- The required OS/400 level for Infor System Manager 3.0.4 must be at least V7R3.
- Infor System Manager v3 plus latest PTF (143 minimum)

These PTFs are required to correctly generate self-signed certificates within the IBM HTTP Server as additional software for System i Workspace with IBMi deployment:

- OS400 V7R2 - R720 PSY SI67104 UP18/09/12 P 8249
- OS400 V7R3 - R730 PSY SI67280 UP18/05/04 I 1000
- IBM J9 VM 1.8.0 64-bit JVM (5770-JV1 option 17)

  Note: This JVM version must be installed and enabled over all application servers installed within the WebSphere profile that you intend to use with System i Workspace.
- IBM HTTP Server (latest updates required)

- WebSphere Application Server Base v9.0.0.11 (or higher)
- WebSphere Application Server Plugins v9.0.0.11 (or higher)

Note: You need to ensure that a default profile and server is created. The initial name of this profile is "default" and the server name is "server1."

Infor System i System Manager requirements

Review these requirements before installation and configuration.

Software Requirements

The required OS/400 level for Infor **System Manager 3.0.4** must be at least V7R3.

Note: If you are using iASPs (Independent Auxiliary Storage Pools) on your IBMi machine, you must contact an Infor Consultant to discuss how to proceed with your System i Workspace installation.

Security requirements for IBMi accounts

These user accounts must be created if not already present on your IBMi server. If the accounts already exist, then ensure that their security configuration matches these specifications.

User	Requirement
Security Officer User with sufficient authorities to install System i System Manager (the install must default to **QSECOFR**)	This user must have a profile with ***ALLOBJ** and ***SECADM** special authorities to be able to install System i Workspace.

Infor System i Workspace AnyWhere Requirements

SiW AnyWhere can be installed with Windows or IBMi deployments. One SiW AnyWhere server can support multiple XA machines or environments, or you can use multiple SiW servers.

Note: After you complete the SiW AnyWhere installation, update the installation with latest Feature Pack version. FP10 is the minimum required version for this implementation.

Hardware requirements

See “Hardware requirements and recommendations” section from “Chapter 2 Preparing for the installation” in *System i Workspace AnyWhere Installation & Administration Guide*.

Software requirements

See “Software requirements” section from “Chapter 2 Preparing for the installation” in *System i Workspace AnyWhere Installation & Administration Guide*

Security and account requirements

This section covers the IBMi and SSL/TLS encryption requirements.

IBMi accounts required

These user accounts must be created if not already present on your IBMi server. If the accounts already exist, ensure that their security configuration complies with these specifications.

User	Requirement
Security Officer User with Sufficient authorities to install System i Workspace. The installation will default to QSECOFR.	This user must have a profile with*ALLOBJ and SECADM* special authorities to be able to install System i Workspace.
Database User to access System Manager, WFi files depending on the version of System Manager you selected. The installation will default to JDBC_AMV3. If an account does not exist, the installer will create an account and configure the account per the requirements.	This user must have a Group Profile of AULUSER, Supplemental Groups of AULSECOFR, AULEXTOWN, AULAMDBUSR and (PWDEXPITV) set to *NOMAX. It is also recommended that this user is set to *SIGNOFF for security reasons. This user should also have a library list set up either by defining the job description or using an initial program, which should include the System Manager libraries as part of their initial library list. **Note:** If you are using iASPs (Independent Auxiliary Storage Pools) on your IBMi machine, you should contact an Infor Consultant to discuss how to proceed with your System i Workspace installation.

User	Requirement
	This Database User must have enough authority to read the Spool, Message and Job queues of all IBMi users that have access to the My Spool Files, My Jobs and My Messages widgets, along with authority to carry out certain actions on their behalf such as delete a Spool File. This authority will not be enabled by the installer and must be applied manually.

SSL/TLS encryption

System i Workspace uses SSL/TLS encryption for all communication over HTTP between the Client and Server. You can select one of these options from the System i Workspace installer:

- **Self-Signed Certificate**, which is created automatically by the installer.
- **Certificate Authority**, if performing a Microsoft Windows deployment, use one that has been purchased or generated such as Comodo, Symantec or from one of the many other providers.

If you are using a certificate from a Certificate Authority, you need these items during the installation of System i Workspace:

- A Keystore file that contains your purchased SSL Certificate and a **full** Certificate Authority Chain
- The password to this Keystore file
- The Alias Name for this Certificate within the Keystore file

See “Secure Sockets Layer (SSL)” section from “Chapter 14 Security**”** in *System i Workspace AnyWhere Installation & Administration Guide* for additional details regarding how to obtain these items before you begin installation of Infor SiWA.

IBMi deployment

Ensure the appropriate PTF for your IBMi Operating System, documented in the Software Requirements section, is applied.

See IBMi deployment section of the Prerequisite installations chapter for more information on configuring SSL before installing Infor SiWA

Infor Operating Service requirements

This section describes the server requirements for Infor Operating Service (Infor OS).

Note: Infor OS 2020-06 is the minimum version required for successful integration.

See the latest *Infor Operating Service Installation Guide* for a better understanding of requirements and installation of Infor OS on premises.

Chapter 3 Installation

This chapter provides information on System Manager, SiWA, and Infor Operating Service installations.

Installing System Manager

For the complete set of instructions required to install System Manager, see *Infor System Manager Quick Installation Guide for Infor XA* on docs.infor.com under version 9.1.

For additional information, see *Infor Si System Manager Installation Guide.*

Installing System i Workspace AnyWhere

This section describes the process of SiWA installation for both Microsoft Windows and IBMi deployments.

Microsoft Windows deployment

For installation and configuration of SiWA to run on Tomcat Web Server, see *Infor System i Workspace AnyWhere Installation and Administration Guide* and follow all the steps related to *Microsoft Windows deployment*.

Note: If you want to install and run multiple instances of SiWA in a single Windows server using unique ports for each individual installation, see the required additional settings mentioned in “Multiple SiWAW WebSphere installations on a single IBMi server.”

IBMi deployment

For installation and configuration of SiWA to run on WebSphere Application Server, see *Infor System i Workspace AnyWhere Installation and Administration Guide* and follow all the steps related to IBMi deployment.

Refer to these sections for any issues or missing steps observed during this deployment process:

- Chapter 3 Pre-requisite installations -> IBM i deployment -> *Creating a local Certificate of Authority* section in the *Infor System i Workspace AnyWhere Installation and Administration Guide* can include the **Select Applications** page. Select all applications on this page that have your XA IBMi server in the **Assigned Certificate** column.

- In Chapter 3 Pre-requisite installations -> IBM i deployment -> *Creating an IBM HTTP Server instance* section in the *Infor System i Workspace AnyWhere Installation and Administration Guide*, verify that the default WebSphere profile is displayed in the application list. If not, see the *Creating an additional default WebSphere Profile* section in this chapter to create the **default** profile in WebSphere.
- After selecting the **default** WebSphere profile, if a message of **Indicate which installed application should be mapped to the selected Web Server** displays, select the **Default Applications only** value.

- After successful installation of SiWA on WebSphere, if you receive an **Internal Server Error** when you try to launch the SiWA for the first time, refer to Appendix C in this guide.

Integration data sheet

During the installation and the configuration tasks, you are prompted for information in this table. Prior to installation, print this table and fill in the applicable information.

Data	Your value
System Name System i server on which Infor XA is installed Identify one server as the default	
User ID System i log-on User ID for an account on the machine on which ERP XA is installed. For the Account, the supplemental group authority must be AULSECOFR	

Data	Your value
Password Password for the System i user ID	
Net-Link URL	
IDF environment code	

You can gather some of the information, such as server names and log-ons, before you begin the installation. You can fill in the remaining data as you proceed through the installation so that you have the required data when prompted.

Installing Infor Operating Service

We recommend that you use XA with System i Workspace and Infor OS installed.

You can use XA with System i Workspace but without Infor OS. During installation, you can omit the Infor OS installation and configuration steps, but you must complete these steps:

- Install System Manager.
- Install System i Workspace.
- Export the metadata.

You can then access System i Workspace directly using a standalone URL as described in the *System i Workspace AnyWhere Installation & Administration Guide*.

You must verify the System i Workspace function even if you plan to use Infor OS.

For the complete set of instructions required to install Infor OS, see the *Infor Operating Service Installation Guide*.

Chapter 4 Post installation

This chapter provides the post-installation information for SiWA.

System i Workspace AnyWhere

Refer to the *System i Workspace AnyWhere Installation & Administration Guide* for detailed information about the tasks in this section.

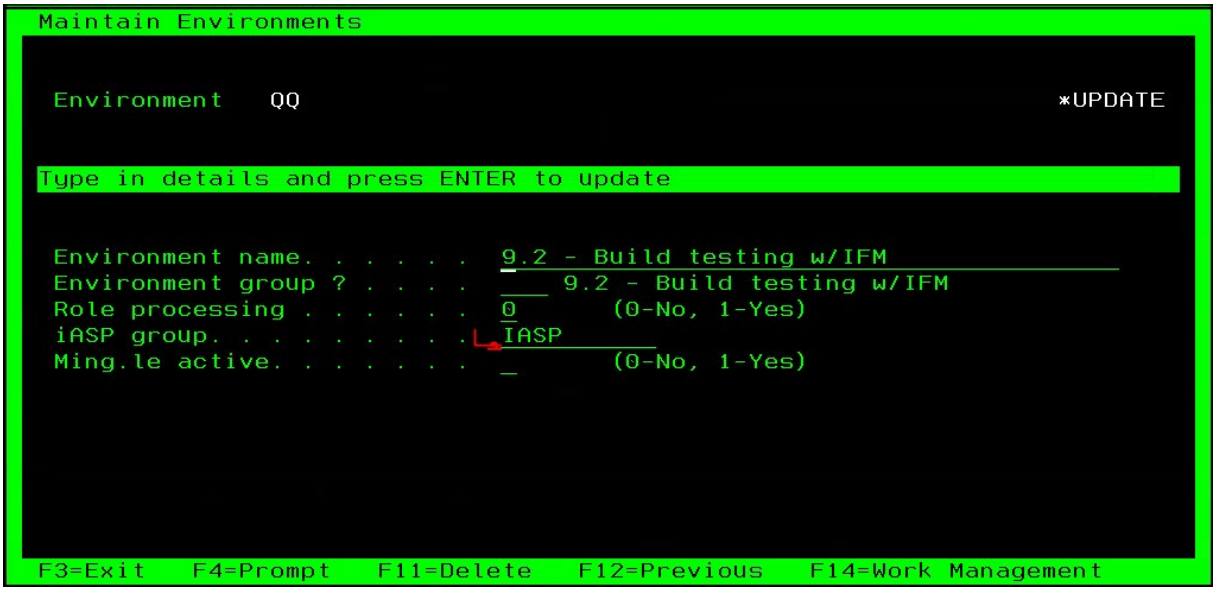
Verifying the installations

After the installation of all the components, you must execute the process described in the "*Verifying the System i Workspace deployment*" section of the *System i Workspace AnyWhere Installation & Administration Guide*.

Setting the iASP

If your XA environment is on an iASP, execute these processes to ensure that the iASP group is set to the correct iASP:

1. Specify **`STRM400`** on the **AS400** screen to start the System Manager.
2. Select **`Application Manager`** and press **Enter**.
3. Select **`Maintain Environments`** and press **Enter**.
4. Press **F4** and select **`Environment`**.
5. Ensure that the iASP group is set to the correct iASP.



Securing Net-Link and Secure Socket Layer configuration

The standard installation process involves secure socket layer (SSL) configuration and accessing Net-Link through a URL to the IBMi. This configuration restricts user access to a secure network.

Microsoft Windows deployment

For SSL configuration, complete the process described in the “Chapter 14 Security” section in the *System i Workspace AnyWhere Installation & Administration Guide*.

To set up a secured Net-Link in the SiWA application, follow the steps in *Infor XA Setup Guide for Secure Net-Link.*

1 Generate war file by referring to the *WAR file generation* section.

2 Deploy the war file on SiWA Tomcat by referring to the *WAR file deployment -> Tomcat (version 7.0 +) s*ection.

3 Configure the Net-Link URL in SiWA Admin.html by referring to *Appendix B Workspace Net-Link URL configuration*.

Client settings

This section explains the client settings that need to be configured on each client PC that accesses the SiWA. See “Chapter 8 Client settings" in the *System i Workspace AnyWhere Installation & Administration Guide*.

System i Workspace profiles

We recommend that you set one SiWA profile for each configured XA environment.

Currently, the Tenant specified during deployment of SiWA within Infor OS is used is the same as the Workspace profile ID.

Chapter 5 Exporting metadata

You can export metadata from Infor Development Framework (IDF) to SiW. This metadata contains the information for the cards, card files, and the contents in IDF. The metadata is used by SiW to construct the menus and the options.

Enabling host reports

Enabling the export metadata job is required to ensure that AULAMP3 is in the library list for the environment.

1. Specify **STRXA** at the command on the green screen to start your XA environment and select the required environment.
2. Specify **CAS** on the command line.
3. Specify **AMZM70** on the command line.
4. Select **Maintain Library List**.
5. Add **AULAMP3** to the **Library List**.

Requirements

To run exports, sign in with a user ID that has supplemental group authority AULUSER and AULSECOFR.

System Manager and SiW PTFs must be the latest versions.

Exporting metadata from IDF to Workspace

After installations, the users need to export the metadata from IDF to SiW. The IDF metadata is the data that describes the objects in IDF and how these objects are arranged into cards and card files.

This metadata must be converted to SiW metadata that describes the tasks available in SiW and how the tasks are grouped into menus.

The two interfaces use different terminology and different styles to present the application tasks available to a user. This export process maps the IDF metadata to the SiW metadata.

Although the Net-Link interface of IDF is integrated with SiW, you can use Power-Link or release 10 of Net-Link to invoke the export process.

Export public or private metadata

The **Export public metadata to Workspace** host job exports the metadata for public card files, cards, and the related objects. The host job ignores export of metadata for private card files or cards even for the user who runs the job. However, user defined public card files, cards, and objects are included.

If you need to export private card files and cards as well as the public ones, you are not required to run both the public and the private export jobs. The **Export private metadata to Workspace** host job includes the public card files and cards.

You can rerun either export job if card files or cards are added or modified. You must include users when you run the host job again, or authorization to access the menu may not be valid.

The export jobs also export definitions for the environment, applications, library lists, companies, and users.

The **Export public metadata to Workspace** host job is available in these cards:

- Business Objects object on the Integrator card
- User Profiles object on the Integrator card
- User Profiles object on the Environment card

The process and screenshots in this section explain the host jobs from the Business Objects object. The process is similar for the User Profiles object.

The **Export private metadata** host job is only available on the User Profiles object. This host job is very similar to the **Export private metadata to Workspace** host job but allows the selection of the users to be exported.

Exporting metadata

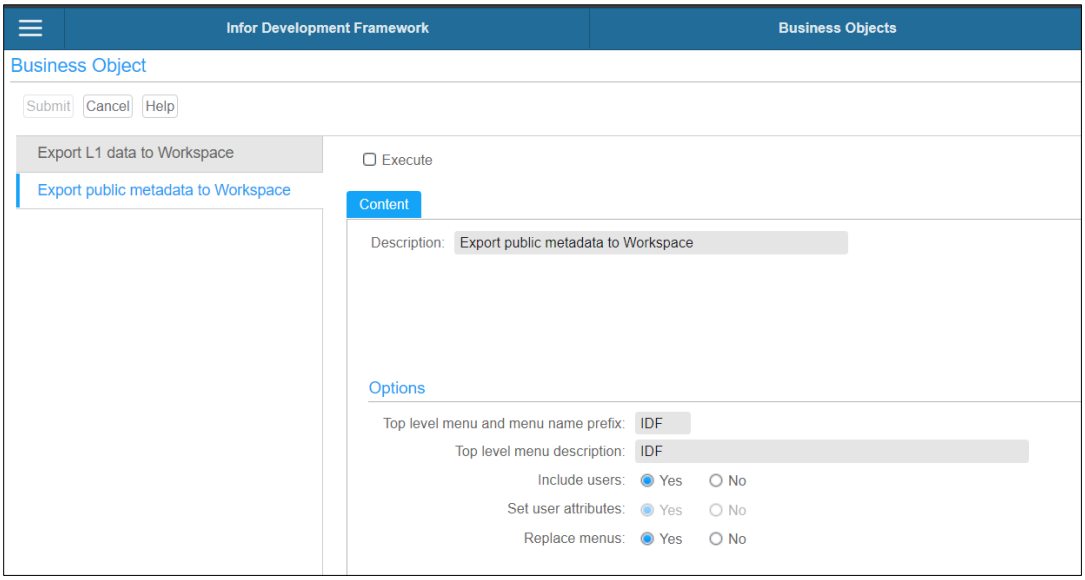
1. Start Net-Link.
2. Navigate to the Business Objects object on the Integrator application card or the User Profiles object on the Integrator or Environment object.
3. Select **File > Host Jobs**.

   The **Host Job** option is not displayed if System i Manager is not properly installed or the AULAMP3 library is not added to the XA Environment library list.

4 Select the **Export public metadata to Workspace** tab. The tabs are displayed in alphabetical order, but this order is not the best sequence to run them.

5 Select the **Execute** check box.

The **Description** attribute is applicable only for the logs and does not affect the exported data.



6 Specify the name of the top level menu that is created in the **Top level menu and menu name prefix** field.

From the top level menu, you have access to all other exported menus. This name is used as a prefix for all other exported menus to limit the length. The default top level menu is **`IDF`**. We recommend that you use IDF unless IDF clashes with an existing menu. We recommend that you do not run the job multiple times with different top level menu names to avoid creating similar menus in System i Manager. If you need to delete redundant menus, use System i Manager functions.

7 Specify the description of the Top level menu in System i Manager.

8 Select **`Yes`** for the **Include users** field if the users must be included in the Export process. If you do not include users, you must run the Export again and include the users or create the users manually in System i Manager. If the Export job exports new menus or menu options, you must select **`Yes`** or the authority to the menus and options will not be available in Workspace.

9 Specify **`Yes`** in the **Set User Attributes** field if user attributes must be set. For an XA user, selecting **`Yes`** for this attribute is usually appropriate. The exception is when you have non-XA tasks and menus in System i Manager. In this case, you might require an initial menu that references the exported IDF top level menu and the non-XA tasks.

10 Specify **`Yes`** in the **Replace Menus** field if the menus are replaced. Select **`Yes`** to delete the previous version of the menu and export a new version. Selecting **`No`** allows the export to run

more quickly, but if objects are removed from cards in IDF, obsolete options may remain in System i Manager.

Selecting **Yes** is appropriate, except in the case of exporting additional languages.

11 Specify **Yes** for each language only if translated card file, card, and object descriptions must be exported. Otherwise, leave as **No**. A maximum of five languages can be exported in one run. If you need to export more than five languages, you can run the Export again with additional languages. If you run the export host job again to add languages, you must set **Replace menus** option to **No** or the previous translations are lost.

12 Click **Submit**.

The Export public and private metadata to SiW jobs run on the client; therefore, the system is slow to respond when you click **Submit**.

A report is generated with the list of exported files and list of errors, if any. This report is displayed on the system used for the Submit process and not on the host.

Export IDF level 1 tasks

You must run the **Export L1 data to Workspace** host job to use IDF Level 1 tasks in SiW. The **Export L1 data to Workspace** host job exports both Infor supplied, and additional user defined L1 options.

If you do not require L1 tasks in SiW, do not run this export process. The **Export L1 data to Workspace** host job is available in Business Objects on the Integrator application card. The **Export L1 data to Workspace** host job is also available in the User Profiles object on the Integrator or Environment application cards. Having the **Export L1 data to Workspace** host job available from the Environment application card provides access without an Integrator license.

You must run the Export public or private metadata job before executing this job or the **Export L1 data to Workspace** host job will fail.

Note: You must run the Export public or private metadata job again after executing this job.

The **Export L1 data to Workspace** host job generates the tasks and menus required in SiW to run user IDF L1 options.

Exporting IDF tasks

1 Start Power-Link.

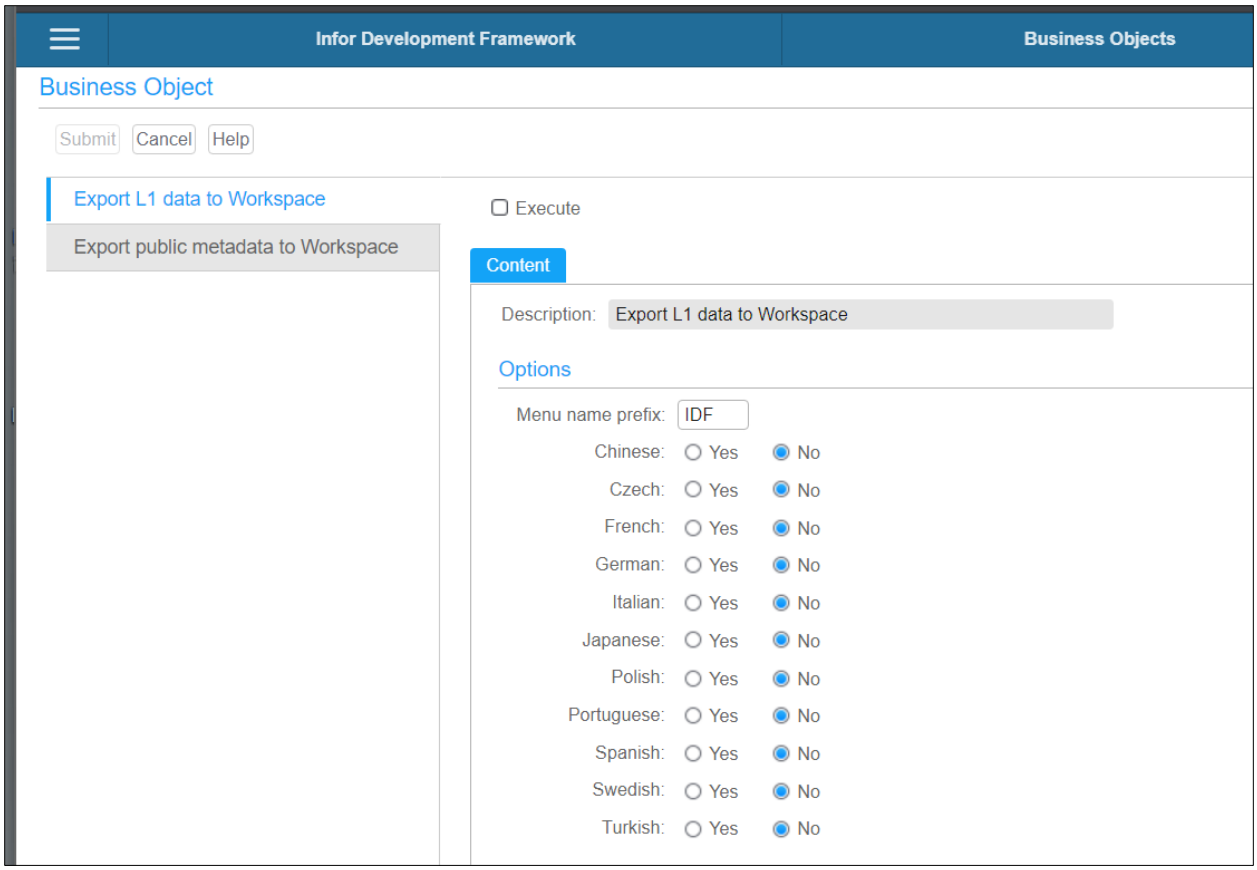
2 Navigate to the Business Objects object on the Integrator card.

3 Select **File > Host Jobs**.

4 Select the **Export L1 data to Workspace** tab. The tabs are displayed in alphabetical sequence.

5 Select the **Execute** check box.

The **Description** attribute is for the logs and does not affect the exported data.



6 Specify the prefix to use for the generated menus in the **Menu name prefix** field. Using the same value as in the public or private metadata job is recommended. The generated menu names may have the same prefix, which is not an issue.

7 Select **`Yes`** for each language only if translated card file, card, and object descriptions must be exported. Otherwise, leave as **`No`**.

8 Click **Submit**.

The **Export L1 data to Workspace** host job runs on the iSeries and generates a report that can be located using WRKUSRJOB.

When the export is complete, you must run the Export public or private host job again.

In the first run of the export, the links to the L1 menus are dropped as the L1 metadata is not available. After the L1 export, the metadata is available but not linked to the other menus. In the second run of the public or private metadata, the links are established.

Exporting users to Workspace

In XA, an environment might be unlocked and therefore the environment can be accessed by anyone with a valid IBM i user profile. For SiW, all the users must be authorized to use System i Manager.

Users are exported to Workspace using the Export public metadata to Workspace host job or the Export private metadata to Workspace host job.

If you have XA users who are not defined in the User Profiles object, we recommend that you define the users before you run the **Export users to Workspace** host job. Otherwise, you must define the users in System i Manager and authorize suitable menu authority. To define these users, select **`User Profile Maintenance`** on the **Security Maintenance** in Cross Application Support, menu AMZM38 option **5. Work With XA User Profiles**.

If you use SiW to run tasks exported from IDF and run the public or private version of the Export metadata to Workspace host job for the first time, you must set the **Set user attributes** to **`Yes`**.

Otherwise, the initial menu is not displayed for the users in the workspace. This is applicable for most XA users. You can change this attribute to **`No`** for subsequent Export users to Workspace host jobs unless you have defined additional users or additional private card files and cards.

Additional metadata maintenance

If cards or card files are changed in IDF, then you must export the metadata again if you have made any of these changes:

- Added an object to a card
- Removed an object
- Changed the workspace of an object on a card
- Added a new card, a new card file, or changed the cards in a card file

The only Integrator change that requires a rerun of the export is a change to the business object title.

If you have not added or changed L1 user options, then you do not have to run the L1 export again. A single run of the public or private metadata export job meets the requirement.

Re-exporting metadata from IDF to Workspace

If you make changes in IDF that affect the IDF cards such as adding additional objects or IDF L1 Tasks such as adding additional user options, then you must run the appropriate Export host jobs again.

If your change does not affect L1 tasks, then you can run the **Export public metadata to Workspace** host job or the **Export private metadata to Workspace** host job. Use the public or private version depending on whether you require public cards or public and private cards file or cards.

If your change affects L1 tasks, for example, an additional user defined L1 task, then you must run the **Export L1 data to Workspace** host job. You might have to run the **Export public metadata to Workspace** host job or the **Export private metadata to Workspace** host job afterwards. Your action depends on whether the change requires a new link from an L2 menu to an L1 menu. We recommend that you run the **Export public metadata to Workspace** host job or the **Export private metadata to Workspace host job** regardless.

After these jobs, you must run the **Export users again to Workspace** host job to configure the authority of the exported tasks in SiW. You are not required to use **Set user attributes** when re-exporting users, the job sets the menu authority whether this attribute is used. If you have deliberately changed a user's initial menu in System Manager, then you must specify **No** for **Set user attributes**.

Because most of the export jobs do not support subsets, you may export more metadata than required. This result is not usually a problem because unchanged objects, card files, and cards export the same data as previously. If you have changed any of the exported data in System Manager, these changes may be overwritten by a re-export. Therefore, we recommend that you do not modify System Manager data created by an export host job. System Manager warns you if you attempt to modify System Manager data created by an export host job but does not stop you. If you must build your own menus in System Manager that refer to exported data, we recommend that you create new menus rather than modify exported ones. Avoid the menu prefix that you used in the exports, for example, IDF, to prevent a conflict.

After you run the export host jobs, you must refresh the System i Workspace data.

See "Updating Workspace Application Manager in SiW" in this guide.

Exporting multiple environments

Environments are usually independent of each other in both IDF and System Manager. You can export different IDF environments independently and with different options.

If a user in System Manager has the same initial menu identifier in all environments, then the environments interact. That is, if a user's initial menu is IDFUS00123 in one environment, then the initial menu is IDFUS00123 in all other environments. In XA, the menu might or might not have the same definition in all environments and the menu might not even exist in all environments.

The **Export public metadata to Workspace** host job does not create user specific menus. The default menu is IDF. The default menu can be changed; however, the menu length must always be 3 characters.

The **Export private metadata to Workspace** host job creates specific user menus that allow access to the user's private card files and cards. The names of these menus are the selected prefix, **IDF** by default, followed by **US** and a number. The numbers are assigned sequentially, for example, 00001, 00002, 00003, in the first run of the host job. When the job is run for a second or later environment or rerun for the first environment, any previously exported user is assigned the same number. Users not previously exported are assigned a new number. Therefore, the user menu numbers may not be consecutive on the second or subsequent export.

Problems can occur if private metadata is exported in one environment and not another since one environment assigns an initial menu such as IDFUS00123 and the other environment, IDF.

To avoid problems with initial menus, we recommend these guidelines:

- If you export private metadata in one environment, do so in any other environments as well. If necessary, re-export environments that were previously exported with only public data.
- Use the same menu prefix in all environments. We recommend that you use the default menu prefix, IDF, unless a clash with existing menus occurs.
- If some users have an incorrect initial menu because you changed from public to private export host jobs or changed the prefix, then run the **Export public metadata to Workspace** host job again or the **Export private metadata to Workspace** host job with **Set user attributes** specified as **`Yes`**.

If you are familiar with System Manager, you can use System Manager functions to specify or correct user's initial menus or authority. If you change user's initial menus or authority in System Manager, we recommend that you specify **`No`** for **Set user attributes** in the **Export public metadata to Workspace** host job or the **Export private metadata to Workspace** host job.

Example of exporting multiple environments

Menus are defined in environments. For example, the menu SOMEMENU in environment AA is not necessarily the same as the menu SOMEMENU in environment BB and the menu might not exist in environment CC. However, the initial menu for a user does not specify an environment. So, if you change the initial menu for SOMEUSER to SOMEMENU, then you need to ensure that SOMEMENU exists in all the environments that SOMEUSER accesses. SOMEMENU is not required to be the same in all the environments, but it must exist. Because of this requirement, you must either use the Export public metadata to Workspace host job in all environments or Export private metadata to Workspace host job in all environments.

For example:

- The Export public metadata to Workspace host job is run for environment AA. The menu IDF is exported and specified as the initial menu for all users. At this point, all users must be able to access SiW for environment AA and see the menu IDF.
- The Export private metadata to Workspace host job is run for environment BB. User specific menus such as IDFUS00123 are generated and specified as the users' initial menus. For example, user JOHNDOE has his initial menu specified as IDFUS00123. JOHNDOE can successfully access SiW for environment BB and see his personal menu but gets an error when he tries to access environment AA since there is no menu IDFUS00123 in environment AA.

If the two export host jobs had run in the reverse order, then the problem is different. If the Export public metadata to Workspace host job is run second, the initial menu for JOHNDOE and other users is changed to **`IDF`**. JOHNDOE can access SiW in both environments but only sees menu IDF. He does not see his personal menu IDFUS00123 in environment BB.

This example assumes that the **Default** menu prefix has been used in all exports and that **Set user attributes** is **`Yes`**. The result is different with other settings but in all cases problems happen. Your only solution is to either use the public job for all environments or the private job for all environments.

The Export private metadata to Workspace host job ensures that the same menu name is used in all environments. If JOHNDOE is assigned IDFUS00123 in environment AA, then he is assigned IDFUS00123 in BB.

Note: Refer KB 2105811 on Export Metadata log and Export L1 data log for further reference.

Updating Workspace Application Manager in SIW

After the completion of Export metadata, the users must update the Workspace Application manager to update the definitions, exported from IDF to System Manager, in SiW.

1 Open the utility by specifying this URL for SiWA:

https://<hostname>:<port>/<web-contextname>/admin.html

2 Navigate to **Update Definitions** under Application Manager.

3 Choose the respective profile from the **Choose Profile** list.

4 If you are performing this process for the first time after environment setup or after metadata export, then select **Update main Application Manager definitions** and click **Update**.

5 Click **`Select all`** to select all users and roles or select a specific user.

6 Select the **Update main Application Manager definitions** check box to ensure all definition updates in System Manager are reflected in System i Workspace.

7 Click **Update**.

Note: See “System i Workspace additional configuration” in the *System i Workspace AnyWhere Installation & Administration Guide*.

Chapter 6 Additional configuring in SiW

Additional configuration is required in SiW after you export your metadata.

Changing System i properties

1 Locate the SiWA WebSphere system.properties file as documented in the *System i Workspace AnyWhere Installation Guide*.

2 Add this property to enable SiWA to launch from Infor OS:

- **Property**: com.infor.siw.cloud.mingle.url
- **Description**: The URL, minus any context path, of the Infor OS server that is hosting SiWA. This URL must be correct to prevent ClickJacking, or the browser will not let System i Workspace execute inside Infor OS. For example: https://mingle.your-enterprise.com

3 Restart System i Workspace. For an IBM i deployment, ensure the server1 application server and HTTP server are also restarted.

Configuring Single Log Out

If using SiWA FP 14 or above, these settings are discontinued and will not be available for you.

To configure Single Log Out (SLO) in the System i Workspace, go to System i Workspace AnyWhere Administration interface (admin.html) **> Workspace Configuration > Profiles > Xi Platform Integration settings > Single Log Out Behaviour**.

This table shows the SLO options within the System i Workspace.

Setting	Description
Allow and terminate all System i Emulator sessions	The **Sign Out** option inside the System i Workspace AnyWhere Application menu is hidden. To sign out, the user must use the Infor OS **Sign out** option. If the user signs out of Infor OS while having active 5250 AnyWhere Emulator sessions, the sessions are disconnected from the client, but preserved on the System i Workspace server. The sessions are automatically recovered and restored when the user next signs into System i Workspace If the user signs out of Ming.le while having active System i Emulator sessions, the sessions are terminated unless using the System i Workspace Telnet Proxy, which can cause object and record locks within your system. Customers, that do not use the System i Emulator, must use this setting. **Note**: This option is the recommended setting for customers who use the 5250 AnyWhere Emulator for running the daily SIM tasks in the enterprise.
Block if any active System i Emulator	The **Sign Out** option inside the System i Workspace AnyWhere application menu is displayed. Users must manually exit any System i Emulator tasks, and then sign out of System i Workspace before signing out of Infor OS. This is the default setting.

System i Workspace additional configuration

System i Workspace is configured during the installation process so, by default, no additional configuration is needed to start and use System i Workspace.

However, you may want to add additional environments and additional profiles by referring to the *System i Workspace AnyWhere Installation & Administration Guide*.

Chapter 7 Configuring XA in Infor OS

Use the steps provided in this section to configure XA with Infor OS On-Premises and using Ming.le.

As mentioned in “Post installation,” we recommend that you have one System i Workspace profile for each XA environment that you intend to configure and to match each profile with one Infor OS application. For example, you can have an XA test environment and an XA production environment, each with their own **Application** tab.

To configure the integration, log on to Infor OS with a user ID that is assigned Administrator role for the Infor OS application. We recommend that you use the same user ID used to install Infor OS, that is, SPInstall.

You can use the Infor OS environment to access the IDF views and screens. Users can access the Net-Link windows to which their user profile has authorization. Users can view all the IDF options that were exported whether the user profile has authority to the options.

Infor Ming.le uses Infor ION terminology. If you have installed Infor ION and configured ION to work with XA, use the same values that you used in that installation. If you are configuring Infor Ming.le but have not yet implemented Infor ION, note the values that you use and then use these same values when you install Infor ION.

These terms are common to Infor Ming.le, Infor ION, and integrations that use Infor ION:

- **Tenant**

  The tenant is the container for accounting entities and locations. No data is ever shared or accessible between two tenants. Your production environment and your test environments are separate tenants. The default tenant is **Infor**.
- **Accounting entity**

  The accounting entity is the lowest level for financial reporting. In an XA implementation, a Financial Divisions, Companies, Sites, and Warehouses are accounting entities. Accounting entities are defined as an organization node in the Financial Division, Company, Site, and Warehouse Objects.
- **Location**

  Location is a geographic site of an organizational facility or function associated with a user, typically a warehouse or an office.
- **Logical ID (lid)**

  The logical ID is the identifier used to locate the environment. The ID is generated based upon the hostname and environment and takes the form **lid://infor.xa.{mysystemi}-{xy}**. **mysystemi** is the System i name in lower case and **xy** is the environment code also in lower case.

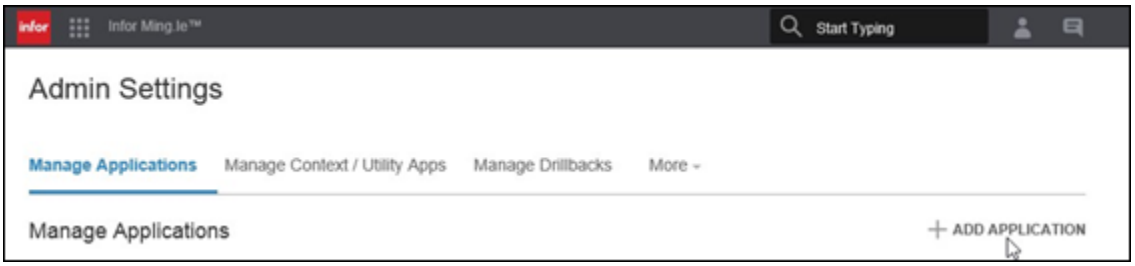
You can configure XA as an application in Infor OS by using **Admin Settings** option in Infor Ming.le. After configuring XA in Infor Ming.le, users can view XA as an application in **App Menu**, similar to other Infor applications such as CRM and EAM. User can launch XA by clicking on the XA specific option in **App Menu**.

Adding the XA application in Infor OS On-premises

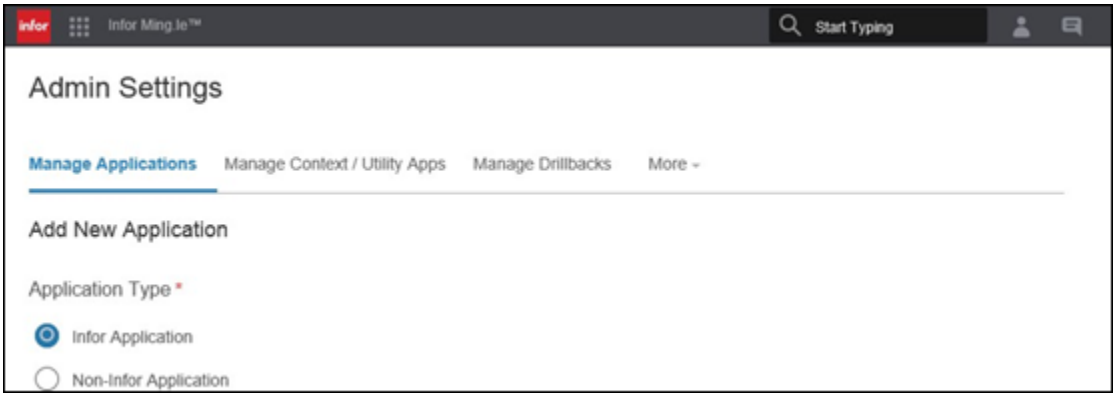
1 Login to Infor OS using the account setup for IFS administration.

2 Click the **User** option in the top right-hand corner and select **Admin Settings**.

3 Click the **+ Add Application** option.



4 Select **`Infor Application`**.



5 Specify this information to create the XA application option:

Application Name

Select **`XA 9.1`** or **`XA 9.2`** application from the list.

Display Name

Specify a display name for this application.

Application Icon

Select an icon for the application.

Logical ID

Specify in the XA environment, which is appended to the logical make-up, the logical ID. For example, *lid://infor.xa.<environment>*.

Use HTTPS

Ensure that this setting is enabled to use HTTPS.

Host Name

Specify the fully qualified host name of your System i Workspace server.

Port

Specify the port number used by System i Workspace. By default, this field is set to **`443`**.

Context

Specify the web context name that was defined for the System i Workspace. By default, this field is set to **`systemi`**.

Default Tenant

Specify the profile name defined within System i Workspace. We recommend that this field is set to the **`XA Profile ID`**, which is case sensitive.

6 Click **Save**.

7 Click **OK**.

8 Select the **Permissions** tab.

9 Click **Add New Users and/or IFS Security Roles**.

10 Refer to the “Create a new application security role”, as displayed, to create a new security role specific to XA. Search and select the role created.

11 Click **Done**.

12 Click **Save**.

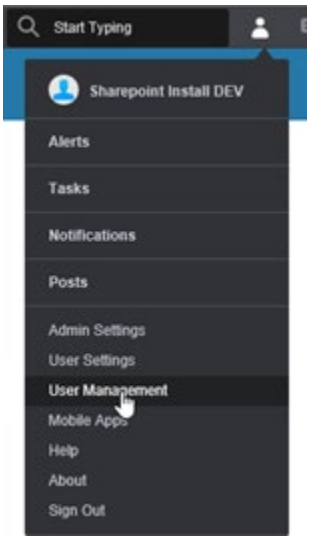
13 Click **OK**.

14 Click **Cancel** to exit.

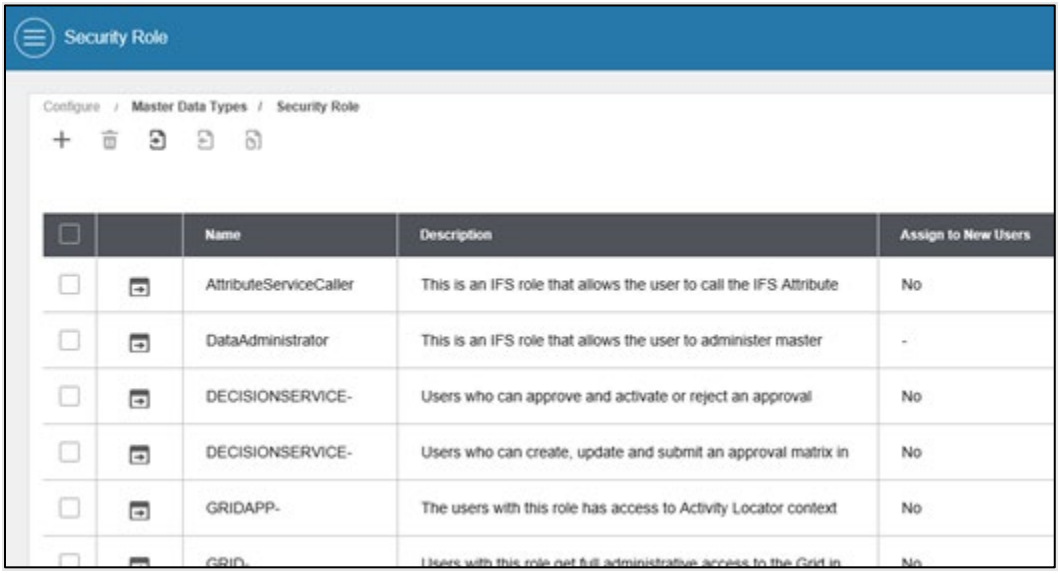
Create a new application security role

1 Log into Infor OS using the account setup for IFS administration.

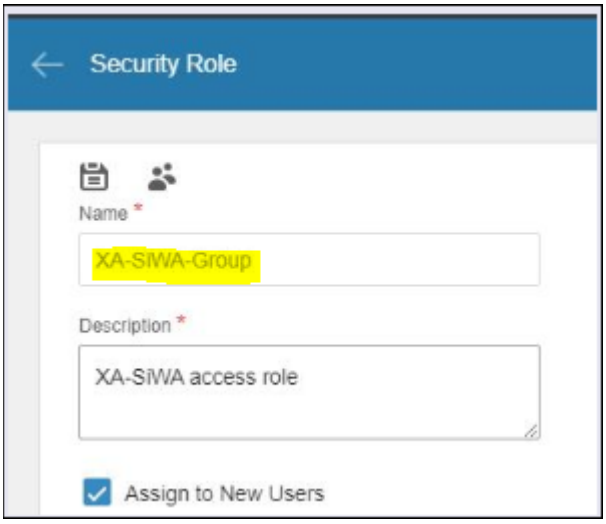
2 Click the **User** option in the top-right corner and select **`User Management`**.



3 On the **Application** menu, select **Configure > Master Data Types > Security Roles**.



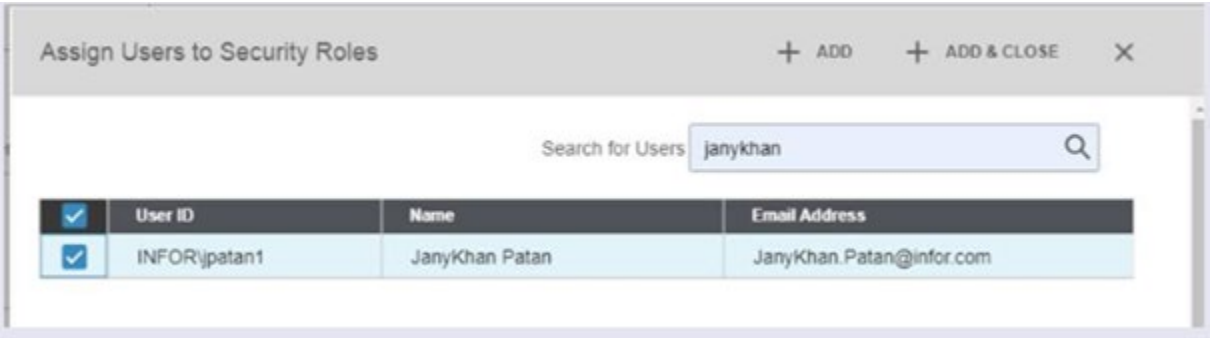
4 Click the **+** option to add a new security role.



5 Specify a name and security role for the **Description**.

6 Select the **Assign to New Users** check box so that, in future, any new users that you add to Infor OS can automatically get access to this new security role.

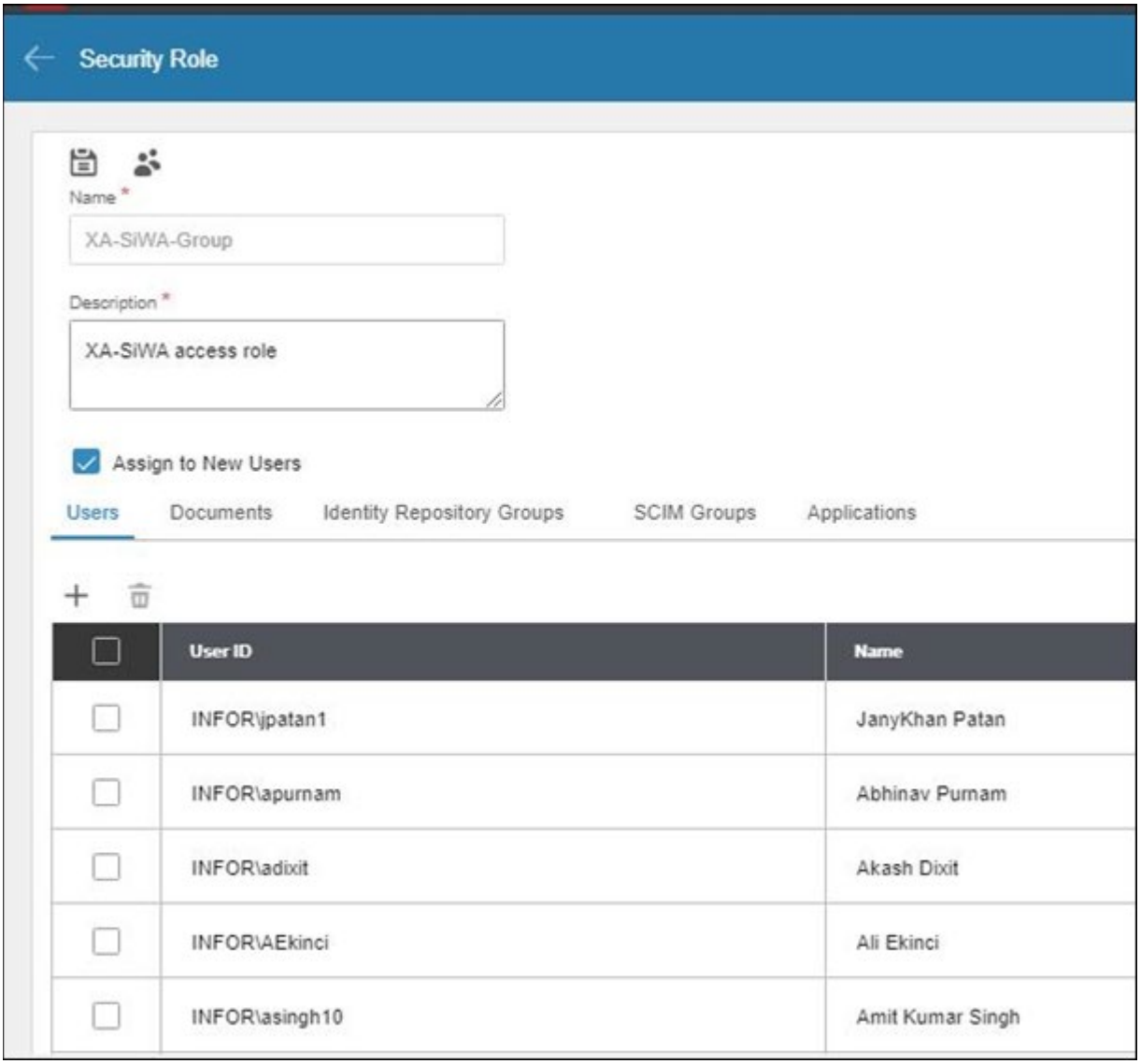
7 Click the **+** option to add users to the security role. If you have not yet added any users, then refer to “Adding users” for adding users into Infor OS.



8 Specify the username you want to add to the security role in the **Search for Users** prompt, as displayed in the screen shot, and then click the magnifying glass option.

9 Select the user to add from the table and click **Add**.

10 Repeat the search to include each user, and then click **Add & Close** to return to the main interface.

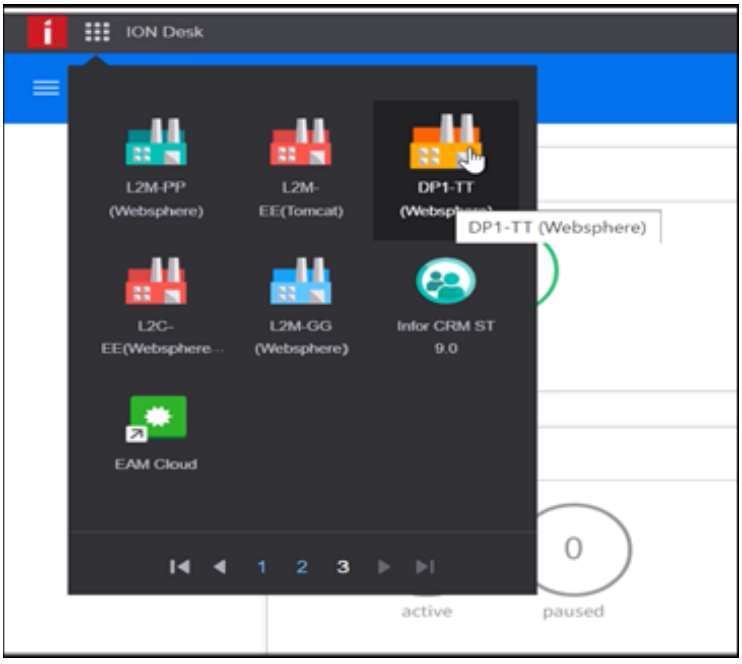


The table is updated with the selected user profiles.

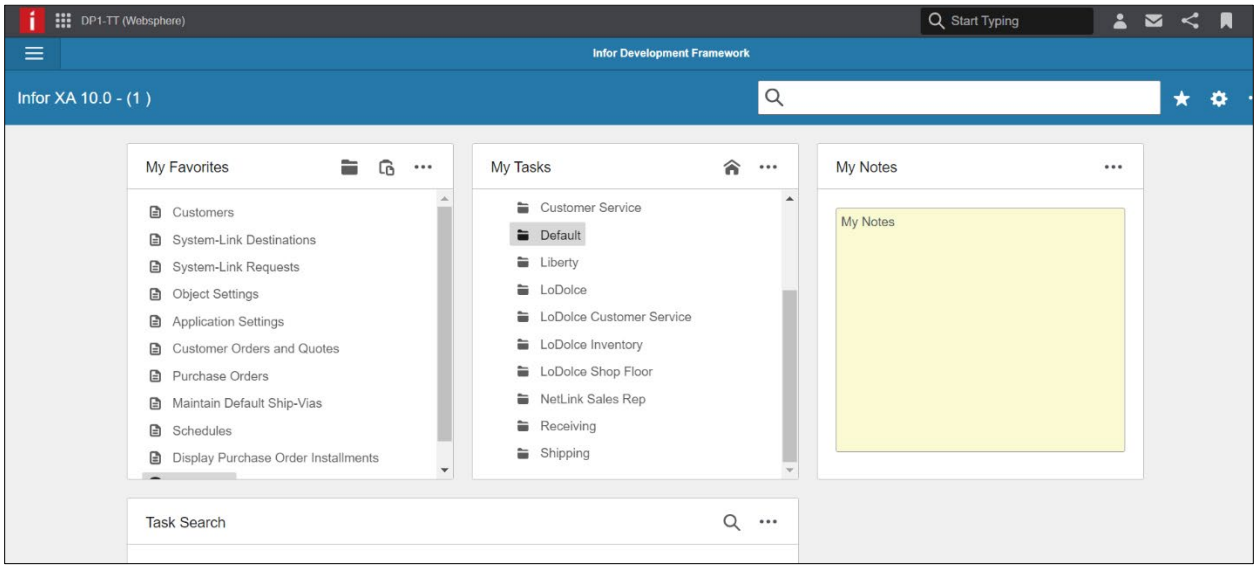
11 Click the **Save Item** option to apply the users to the security role.

Launch XA in Infor OS On-premises

Go to **App Menu** and click the **XA application** option.



The XA application is launched with menu and other details to access.



Chapter 8 Single Sign-On within Infor OS On-premises

SiWA is the user interface for Infor XA. If you intend to use SiWA with Infor OS on-premises. This chapter describes the steps to enable the Single Sign-On (SSO) functionality to launch SiWA from within Infor OS On-Premise using ADFS or STS.

Note: SiWA should be running on FP 13, at least, and latest Infor OS for SSO with Infor OS to work without any issues.

This chapter covers SSO enablement for these combinations:

- SiWA with Windows deployment (Tomcat) on Infor OS On-premise using Kerberos SSO.
- SiWA with Windows deployment (Tomcat) on Infor OS On-premise using SAML SSO.
- SiWA with IBMi deployment (WebSphere) on Infor OS On-premise using Kerberos SSO.
- SiWA with IBMi deployment (WebSphere) on Infor OS On-premise using SAML SSO.

If users are going to be using SSO for both SiWA and a 3rd Party 5250 Emulator such as IBM Access for I, then we recommend that each IBMi user has its **Set password to expired set** field set to **`*NO`** and the **User password** set to a random GUID password which cannot be guessed.

Note: If IBMi users have their **Set password to expired** set to **`*YES`**, this causes the **Change Password** window to appear during a SSO if the user's password has expired.

Kerberos SSO

To implement Kerberos SSO, refer to the process described in the *"*Enabling SSO with Microsoft AD and IBMi EIM*"* section of the *System i Workspace AnyWhere Installation & Administration Guide*.

Security Assertion Markup Language SSO implementation

Use these steps for Infor OS On-premises implementation.

Obtaining the setup zip file

To obtain the setup zip file, download the **InforOS_SSO_Setup zip** file from the SiWA solution KB 1963350 in Infor Concierge.

This file must be extracted or copied to the root directory of a Microsoft Windows PC or Server that has Amazon Corretto Java 8 installed and has the **JAVA_HOME** environment variable and **PATH** variable correctly configured to point to a valid Amazon Corretto Java 8 executable.

Updating the service provider metadata

1 Copy the file **sp_XA.properties** to **sp.properties**.

2 Update the following properties within the **sp.properties** file.

Property	Description
sp.entityid	Replace **TENANT** with the environment code being used within SiWA: **ERP_XA_TENANT**
sp.common.name	Replace **siwa-hostname.domain.com** with the hostname and domain of the SiWA server.
sp.sso.url	Replace **server-name.domain.com** with the hostname and domain of your SiWA server: **https://siwa-hostname.domain.com:443/systemi/CloudIntegrationServlet**
sp.slo.url	Replace **server-name.domain.com** with the hostname and domain of your SiWA server: **https://siwa-hostname.domain.com:443/systemi/fedletSloPOST**
sp.fedletadapter.class	Specify **com.geac.xtrane.servlet.http.CloudSLOFedletAdapter**.

3 To continue implementing your SAML SSO, see the next set of task steps for the Infor OS OP you are using:

- Infor OS OP ADFS: “Creating the Infor OS OP ADFS identity provider and fedlet metadata”
- Infor OS OP STS: “Creating the Infor OS OP STS identity provider and fedlet metadata”

Creating the Infor OS OP ADFS identity provider and fedlet metadata

1 Copy the file **idp_ADFS.properties** to **idp.properties**.

2 Launch this URL from any browser, replacing **adfs-server-name.domain.com** with the hostname and domain of your ADFS server:

https://adfs-server-name.domain.com/federationmetadata/2007-06/federationmetadata.xml

You are asked to download the **FederationMetadata.xml** file.

3 Open this file in Microsoft Windows Notepad and locate the Signing Certificate, which can be found under the element *<KeyDescriptor use="signing">* and between these elements *<X509Certificate>Signing Certificate</X509Certificate>*.

4 Copy the signing certificate without the elements.

5 Update these properties within the **idp.properties** file:

Property	Description
idp.adfs.entityid	Replace **adfs-server-name.domain.com** with the hostname and domain of your ADFS server: **http://adfs-server-name.domain.com/adfs/services/trust**
idp.adfs.location	Replace **adfs-server-name.domain.com** with the hostname and domain of your ADFS server: **https://adfs-server-name.domain.com/adfs/ls/**
idp.adfs.certificate	Paste in the IDP Signing Certificate that you copied.

6 Run the build-metadata.bat command with the following parameters: **build-metadata.bat /OP /ADFS sp.properties idp.properties**.

This command creates a populated set of fedlet metadata in the fedlet_config folder.

7 Go to Copying the fedlet metadata folder.

Creating the Infor OS OP STS identity provider and fedlet metadata

1 Copy the file **idp_STS.properties** to **idp.properties**.

2 From any browser launch this URL, replacing **sts-hostname.domain.com** with the hostname and domain of your InforSTS server:

https://sts-hostname.domain.com:9553/inforsts/rest/metadata/00000000000000000000000000000000/wsfed/idp

You are asked to download the **sts-metadata-idp-wsfed.xml** file.

3 Open this file in Microsoft Windows Notepad and locate the Signing Certificate, which can be found under the element <KeyDescriptor use="signing">, and between these elements <X509Certificate>Signing Certificate</X509Certificate>.

4 Copy the signing certificate without the elements.

5 Update these properties within the **idp.properties** file:

Property	Description
idp.sts.entityid	Replace **sts-hostname.domain.com** with the host name and domain of your InforSTS server: https://sts-hostname.domain.com:9553/inforsts/infor/00000000000000000000000000000000
idp.sts.sso	Replace sts-hostname.domain.com with the host name and domain of your InforSTS server: https://sts-hostname.domain.com:9553/inforsts/infor/00000000000000000000000000000000/idp/samlSSO
idp.sts.slo	Replace sts-hostname.domain.com with the host name and domain of your InforSTS server: https://sts-hostname.domain.com:9553/inforsts/infor/00000000000000000000000000000000/idp/samlSLO
idp.sts.certificate	Past the IDP Signing Certificate you copied.

6 Run the build-metadata.bat command with these parameters: **build-metadata.bat /OP /STS sp.properties idp.properties**.

This command creates a populated set of fedlet metadata in the fedlet_config folder.

7 Continue with the fedlet metadata folder.

Copying the fedlet metadata folder

Copy the fedlet_config folder to the root folder of your SiWA server. For an IBM i deployment of SiWA, this folder will most likely be the ROOT folder of the IFS.

Note: For IBMi deployments, after copying the fedlet_config folder to the IFS, check that the encoding of the idp.xml file is in ANSI format. We have observed instances where this file is created in UTF-8 format, which seems to cause issues with the OpenAM API. If the idp.xml file is in UTF-8 format, then the lead bytes are not converted correctly during the copy to the IBM i IFS. If the format is UTF-8, then open in Microsoft Windows Notepad and use **Save As** to change the encoding to ANSI. Do not change the idp.xml file name.

Java runtime changes

After copying the fedlet metadata folder, you need to add an additional Java runtime property for SiWA to identify the location of the fedlet metadata folder:

```
-Dcom.sun.identity.fedlet.home=<Path to fedlet metadata folder>
```

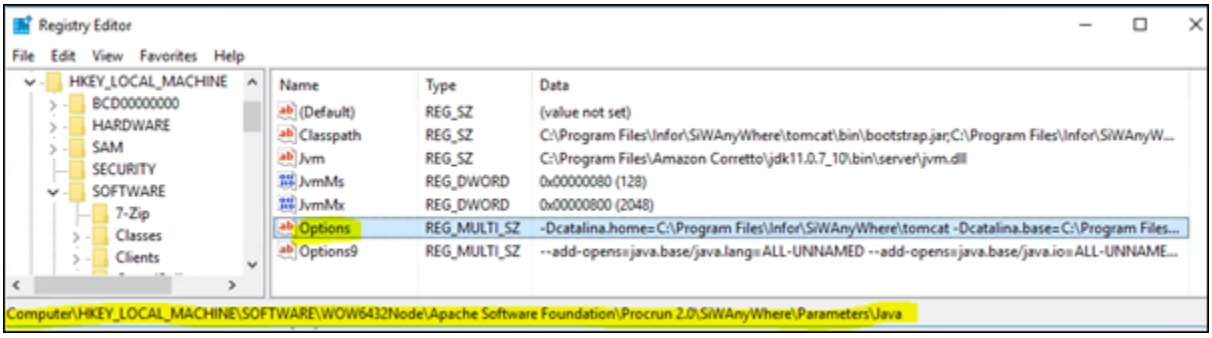
For Windows SiW deployment, see “Adding Java runtime properties to Windows SiW deployment.”

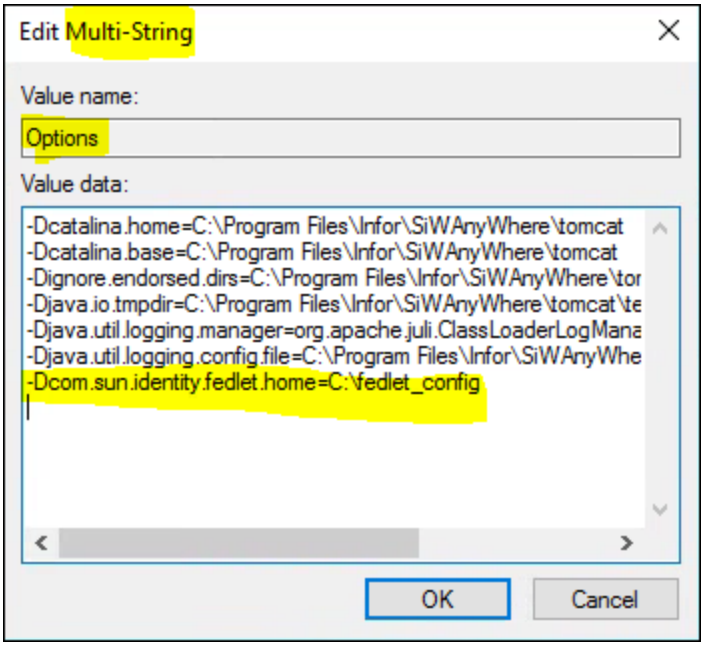
For IBMi SiW deployment, see “Adding Java runtime properties to IBMi deployment.”

Adding Java runtime properties to Windows SiW deployment

Using RegEdit, update this registry key to add in the additional -D parameter:

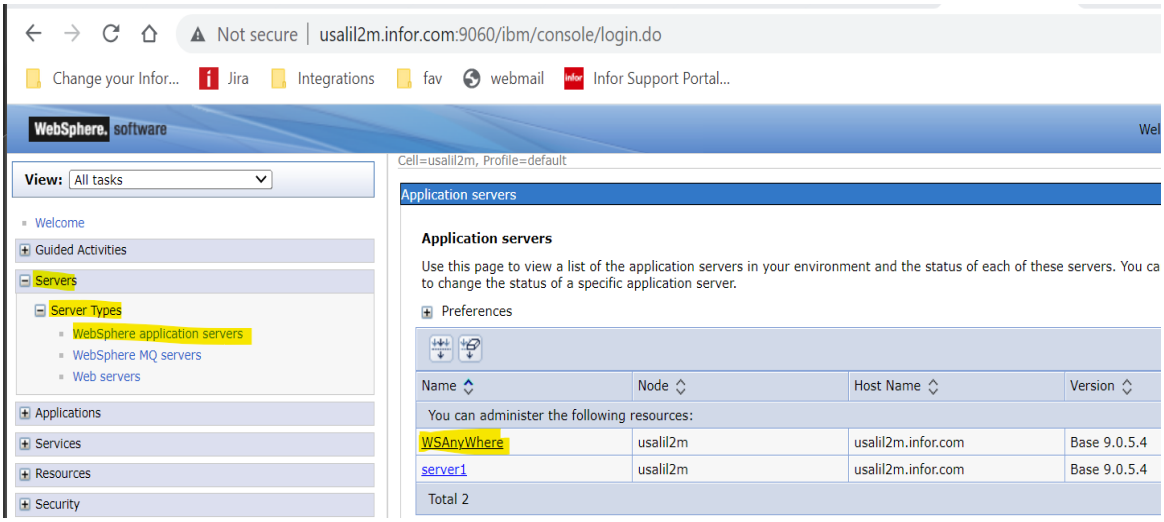
```
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\SiWAnyWhere\Parameters\Java\Options
```





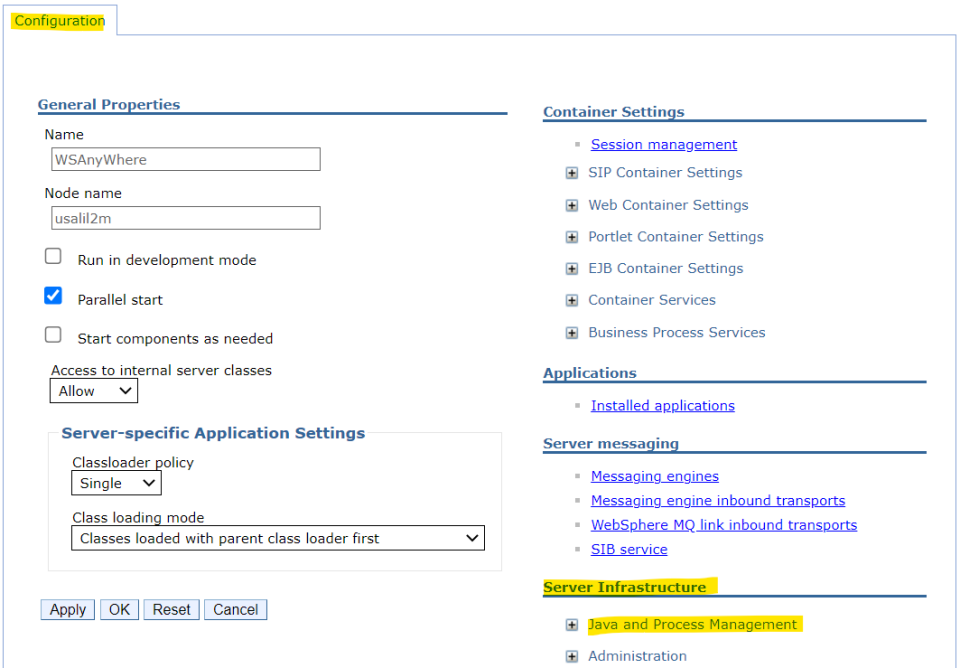
Adding Java runtime properties to IBMi deployment

1 Use the IBM WebSphere Administrative Console to make configuration changes. From the menus, select **Servers > Server Types > WebSphere Application Servers**.

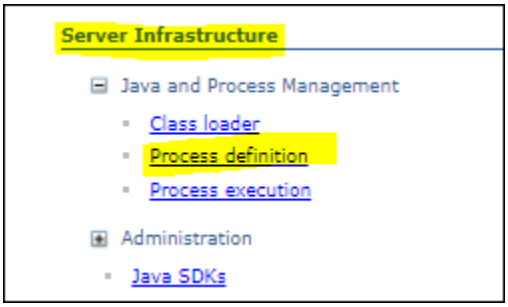


2 Select your System i Workspace AnyWhere Application server, usually WSAnyWhere for a default installation.

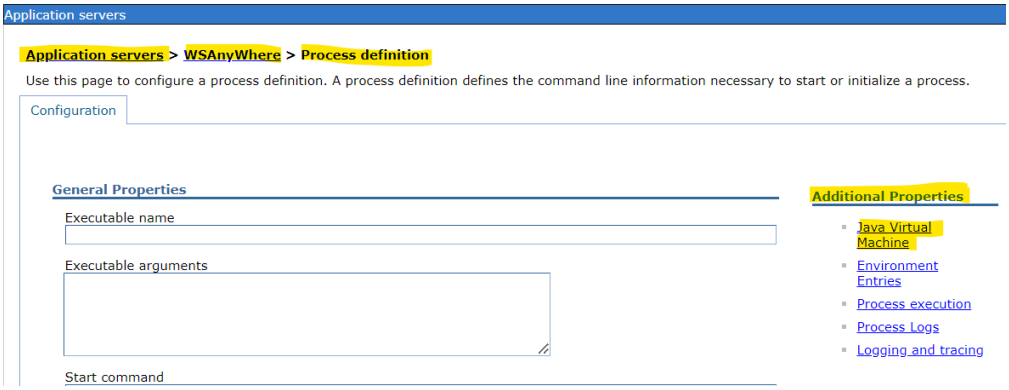
3 On the **Configuration** window, under the **Server Infrastructure** section, expand the **Java and Process Management** option.



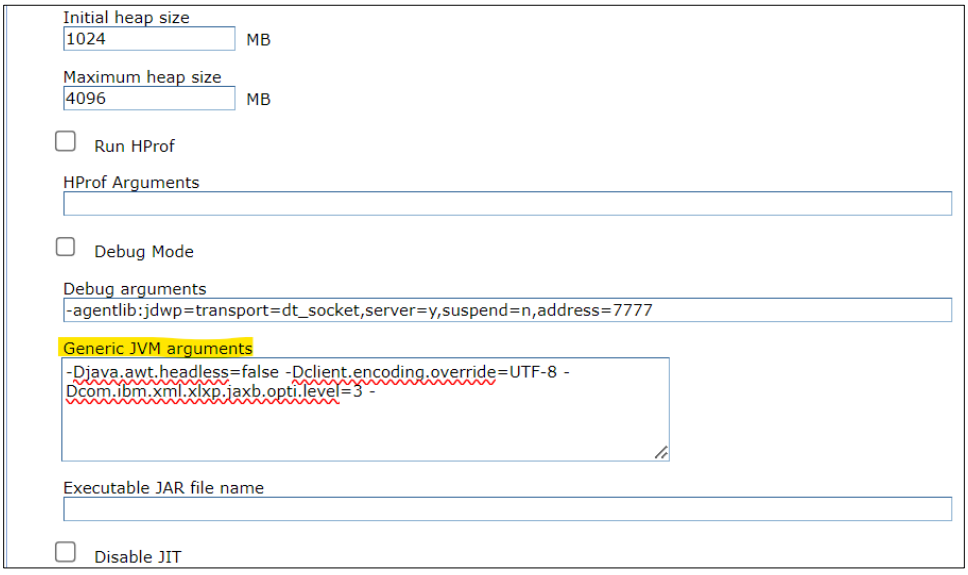
4 Select **Process definition**.



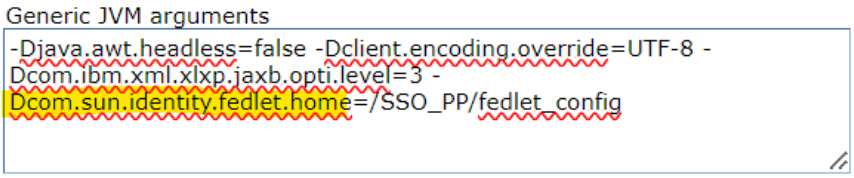
5 Under the Additional Properties, select **Java Virtual Machine**.



6 Locate the **Generic JVM arguments** field towards the bottom of the window. This field may have existing values.



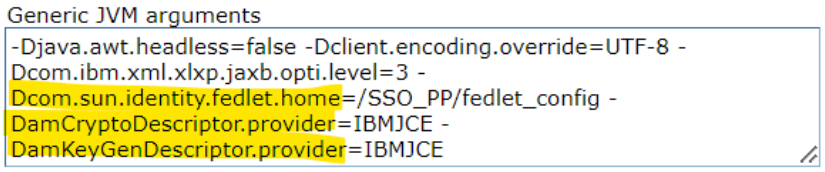
7 At the end of the existing arguments, add a space followed by the path to your fedlet_config folder:



8 After this setting, add these space-separated additional arguments to configure the OpenAM classes to use the IBMJCE for certificate decryption:

-DamCryptoDescriptor.provider=IBMJCE

-DamKeyGenDescriptor.provider=IBMJCE



9 Click **Apply** and **Save**.

Changing system properties

1 Locate the System i Workspace AnyWhere WebSphere system.properties file as documented in the *System i Workspace AnyWhere Installation Guide*.

2 Add these properties:

Property	Description
com.infor.siw.cloud	Set to `1` to enable SSO via Infor OS.
com.infor.siw.cloud.idp.properties	Specify the path to the SAML metadata folder used by SiWA to extract values from the metadata needed at runtime such as the Epoch Cookie name and domain. Example for SiWA Windows deployment: ***com.infor.siw.cloud.idp.properties=C:/fedlet_config*** Example for SiWA IBMi deployment: ***com.infor.siw.cloud.idp.properties=/fedlet_config***
com.infor.siw.cloud.mingle.url	The URL, minus any context path, of the Infor OS server that is hosting SiWA. This is used to prevent ClickJacking so the URL must be correct, or the browser will not let SiWA execute inside Infor OS. For example: *com.infor.siw.cloud.mingle.url=https://IOS-hostname.domain.com*

Property	Description
com.infor.siw.cloud.mingle.slo.url	The URL, minus any context path, from either the idp.adfs.location, idp.sts.slo or idp.saml.slo.url property value from the file idp.properties. This is used to prevent ClickJacking so it must be correct, or the browser will not let SiWA log out correctly from InforOS, For example: *com.infor.siw.cloud.mingle.slo.url=https://slo-hostname.domain.com*

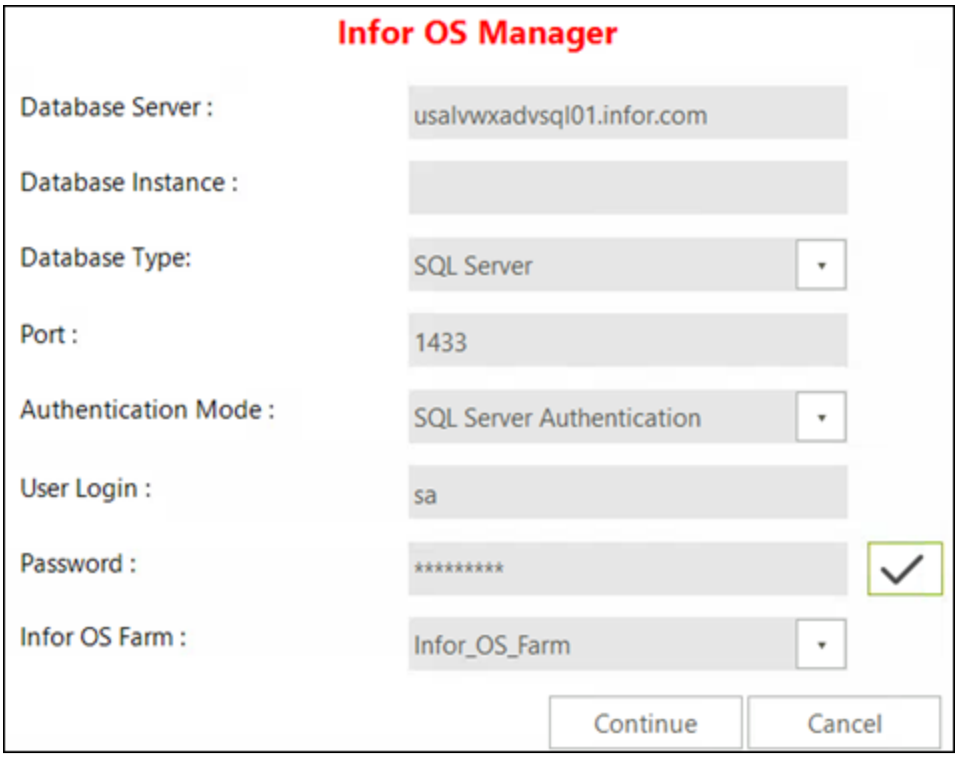
3 Save the changes. SiWA can now be restarted.

For an IBM i deployment, ensure the server1 application server and HTTP server are also restarted.

You can now only access pages within SiWA after signing into the Infor OS platform. Direct access is now disabled.

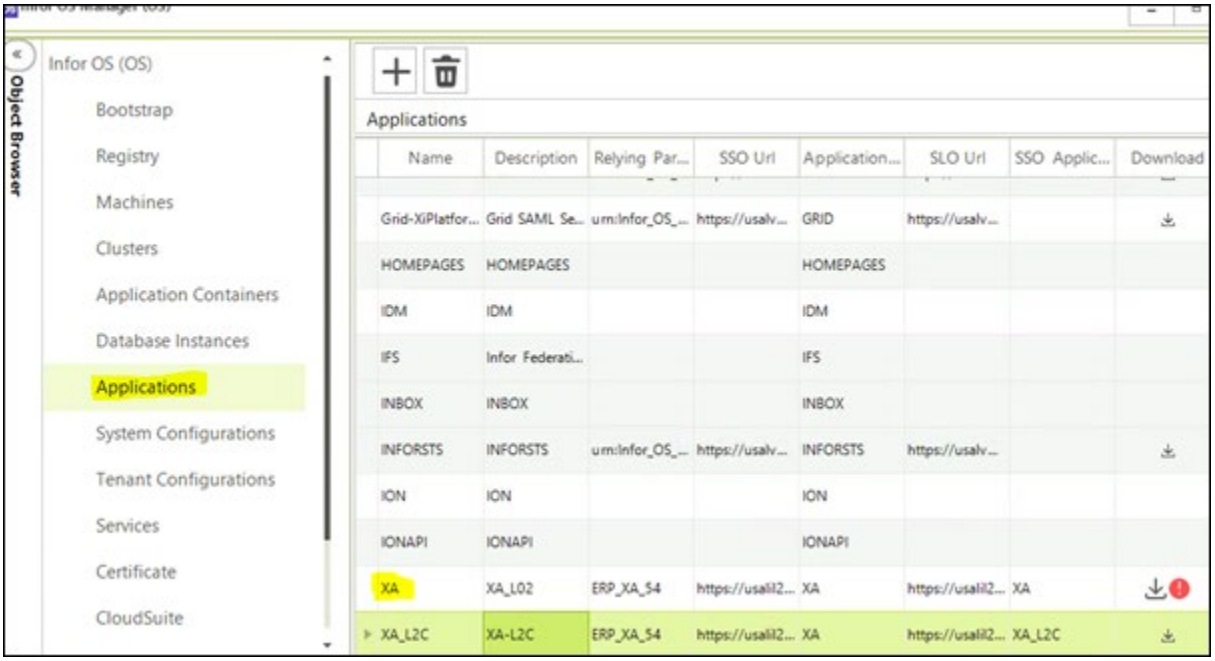
Updating Infor OS Manager application

1 Log into the Infor OS Manager from your Infor OS server as displayed and click **Continue**.



2 Click **Applications** and locate the XA application.

3 Double-click the XA application.



4 Specify this information:

Relying Partner Identifier

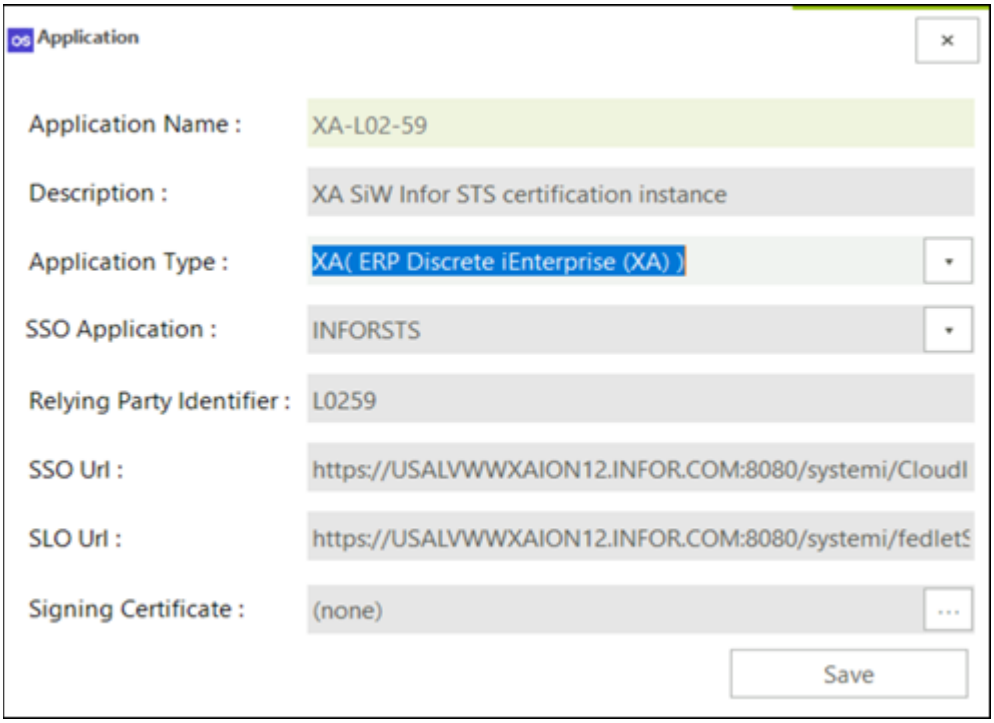
Specify the value that matches the value of the property **sp.entityid** from the **sp.properties** file.

SSO URL

Specify the value that matches the value of the property **sp.sso.url** from the **sp.properties** file.

SLO URL

Specify the value that matches the value of the property **sp.slo.url** from the **sp.properties** file.



5 Click the button for the **Signing Certificate** field to select the certificate **SiW_Certificate1.cer** found in the root of the fedlet_config folder.

6 Click **Open**.

7 Click **Save**.

To continue implementing your SAML SSO, see the next set of task steps for the Infor OS OP you are using:

- Infor OS OP ADFS: See “Updating the Infor OS OP ADFS server through the ps1 file.”
- Infor OS OP STS: See “Updating the Infor OS OP STS through the InforSTS .”

Updating the Infor OS OP ADFS server through the ps1 file

1 Click the **Download** option for the XA application.

2 Specify a download path or use the **Search** button to find the path.

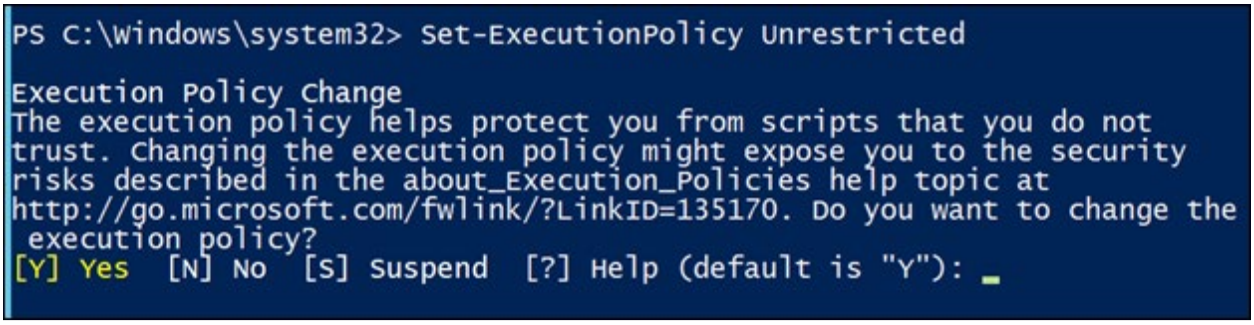
3 Click **Download**.

4 Copy the .ps1 file to the root of your ADFS server.

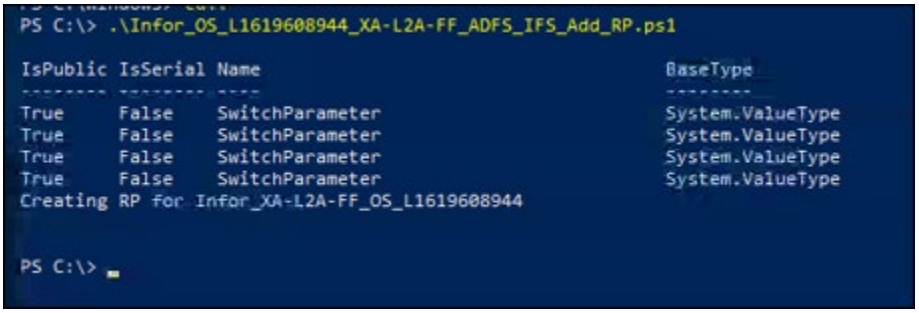
5 Log on to the ADFS server.

6 Open the Windows PowerShell as an Administrator.

7 Run the command **`Set-ExecutionPolicy Unrestricted`** and confirm the execution policy by typing **`Y`** and pressing **Enter**, if required to do so.



8 Locate the .ps1 file downloaded in above steps and then run as displayed.

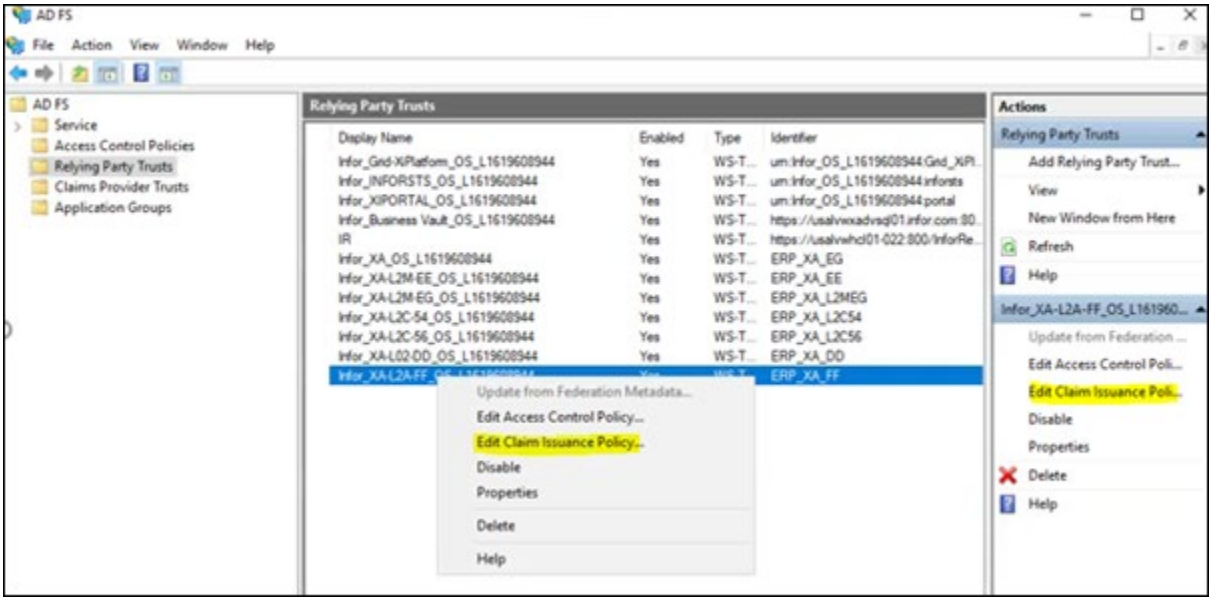


9 Launch the ADFS Management console.

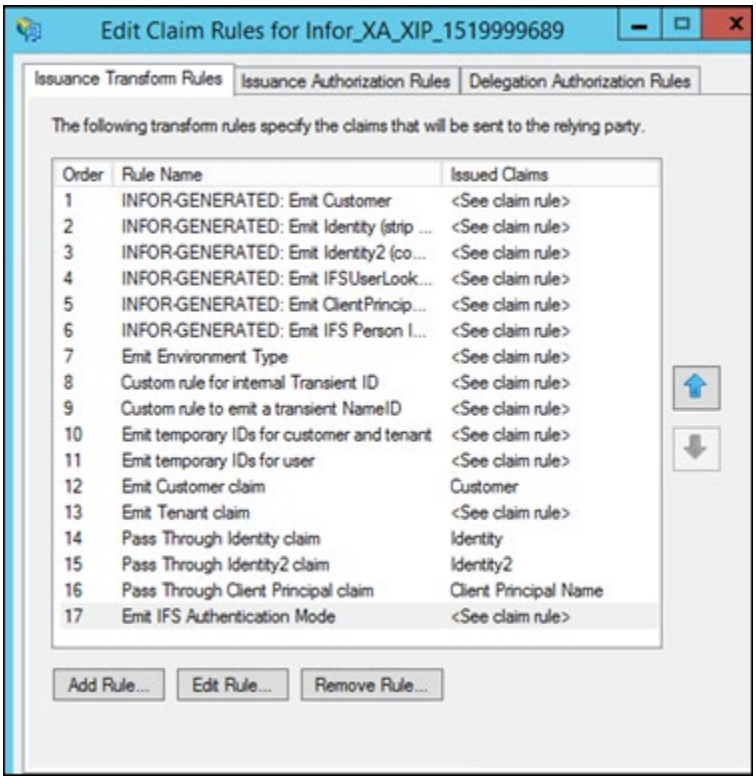
10 Select **Trust Relationships > Relying Party Trusts** and locate your application.

11 Note the reference ID of your application. For example, OS_L1619608944.

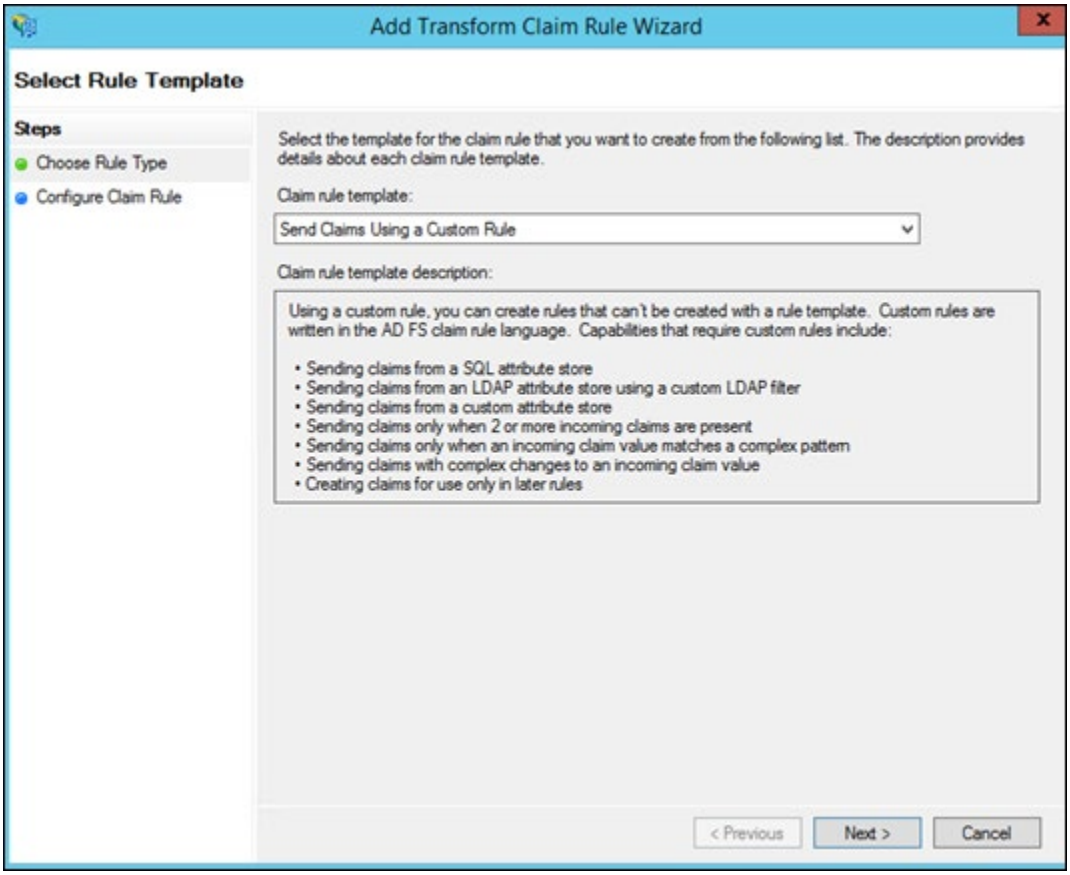
12 Right-click your application and select **Edit Claim Issuance Policy**.



13 Click **Add Rule**.



14 Select the **Send Claims Using a Custom Rule** option from the list.

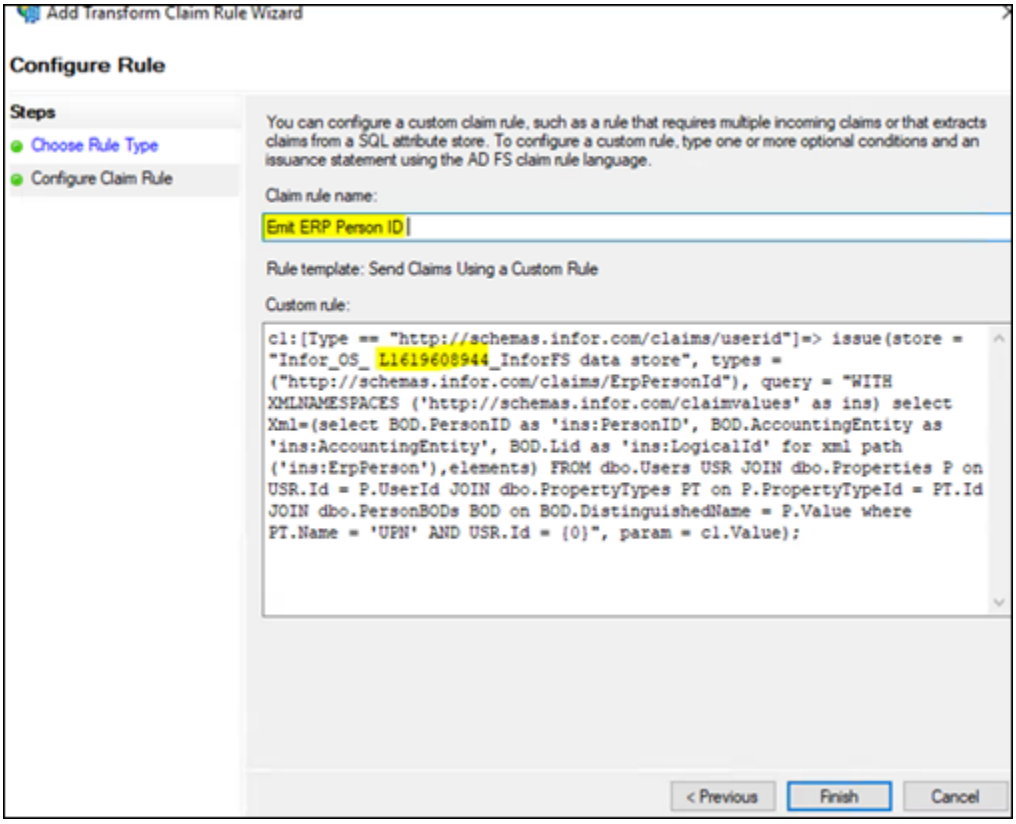


15 Click **Next**.

16 Specify **`Emit ERP Person ID claim`** for the **Claim rule name**.

17 Add this information into the **Custom rule** field. Change the reference ID to the reference ID of your application, which you made a note of earlier from **Relying Party Trusts** on the ADFS console:

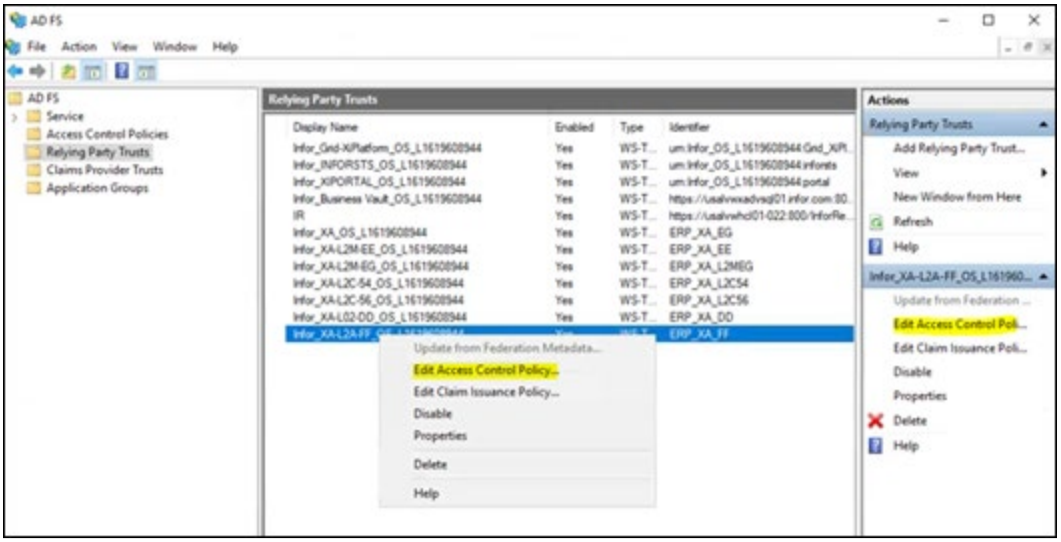
c1:[Type == "http://schemas.infor.com/claims/userid"]=> issue(store = "Infor_OS_L1619608944_InforFS data store", types = ("http://schemas.infor.com/claims/ErpPersonId"), query = "WITH XMLNAMESPACES ('http://schemas.infor.com/claimvalues' as ins) select Xml=(select BOD.PersonID as 'ins:PersonID', BOD.AccountingEntity as 'ins:AccountingEntity', BOD.Lid as 'ins:LogicalId' for xml path('ins:ErpPerson'),elements) FROM dbo.Users USR JOIN dbo.Properties P on USR.Id = P.UserId JOIN dbo.PropertyTypes PT on P.PropertyTypeId = PT.Id JOIN dbo.PersonBODs BOD on BOD.DistinguishedName = P.Value where PT.Name = 'UPN' AND USR.Id = {0}", param = c1.Value);



18 Click **Finish**.

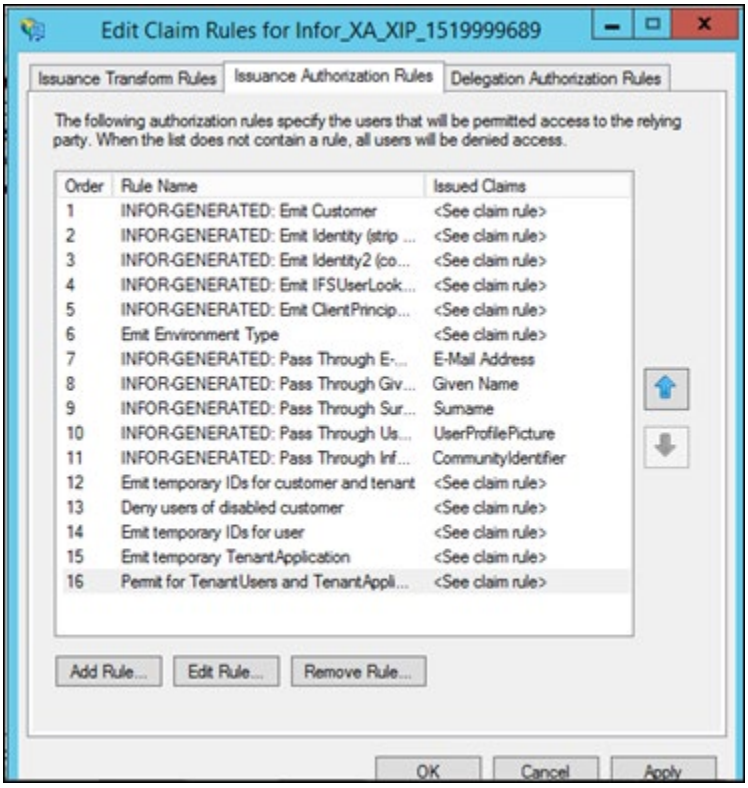
19 Click **Ok**.

20 Right-click your application and select **Edit Access Control Policy**.

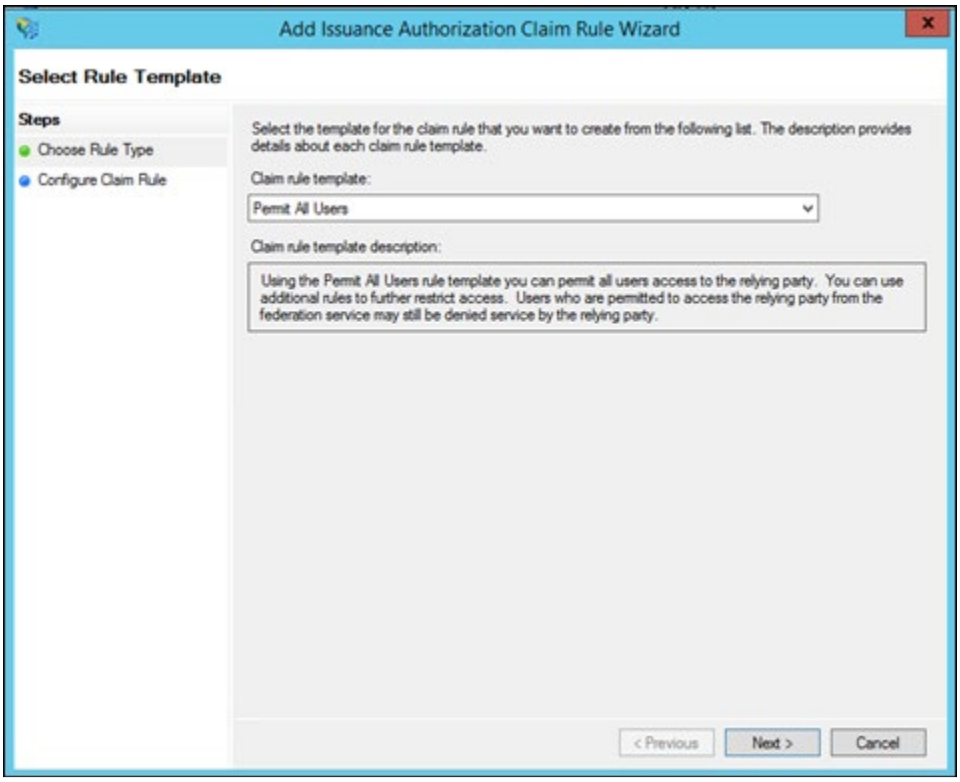


21 Click the **Issuance Authorization Rules** tab.

22 Click **Add Rule**.



23 Select the **Permit All Users** option from the list.



24 Click **Next**.

25 Click **Finish**.

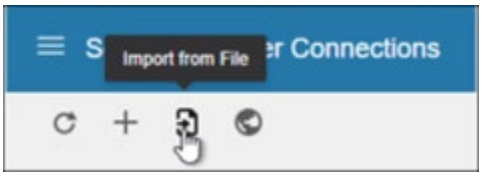
26 Click **OK**.

Install service provider in Infor STS

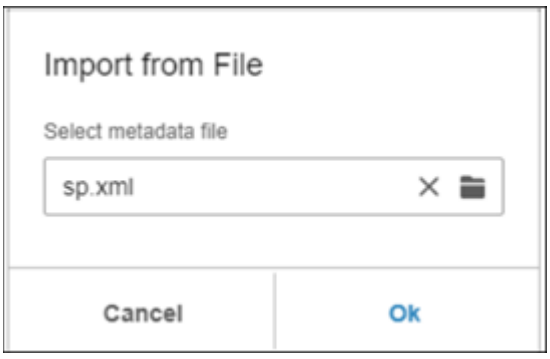
1 Launch the STS Admin UI from your Infor OS server.

2 Click on **SP connections**.

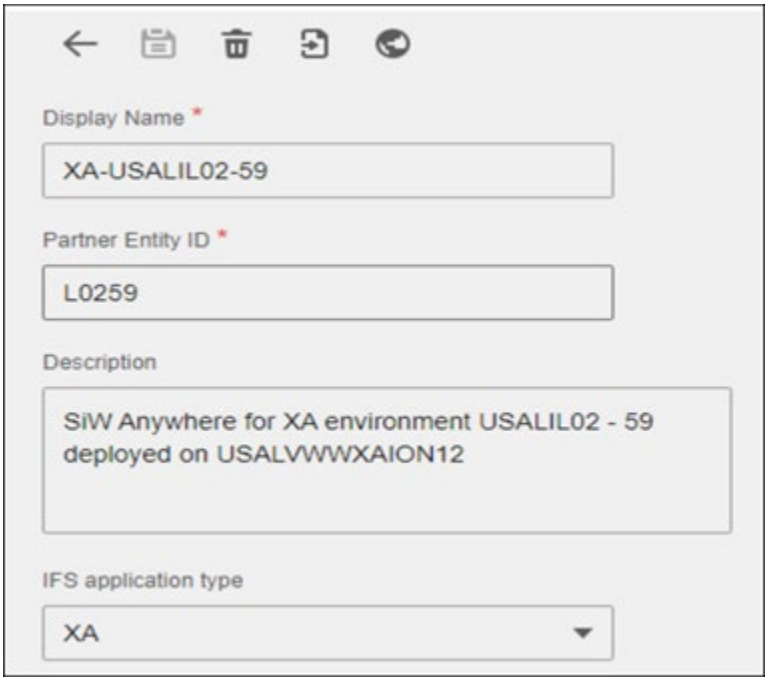
3 Click the **Import from File** icon.



4 Select the file sp.xml found in the root of the fedlet_config folder and then click **Ok**.



5 Specify a unique value for the **Display Name**.



6 Ensure that **Partner Entity ID** is **sp.entityid** from SP properties.

7 Select **XA** for the **IFS application type**.

8 Click the **Save** icon, and then click the **Back** icon.

Migration from ADFS to Infor STS as Identity Provider

To use Infor STS as Identity provider in place of ADFS, see “Appendix L: Upgrading Infor OS with Infor STS as identity provider” in the *Infor Operating Service Installation Guide* for information on upgrade your existing Infor OS.

Follow these steps when ADFS is already configured and used as Identity Provider for SSO.

1 Stop the SiWA service if running.

2 Go to SiWA installation folder and take a backup of existing fedlet_config folder used for SSO.

3 Delete the fedlet_config folder from the root location.

4 Reusing existing InforOS_SSO_Setup folder for generating fedlet_config for ADFS.

5 Go to InforOS_SSO_Setup folder, open and delete the existing fedlet_config folder.

6 Copy the file idp_STS.properties to idp.properties.

7 From any browser launch the following URL, replacing sts-hostname.domain.com with the hostname and domain of your InforSTS server:

https://sts-hostname.domain.com:9553/inforsts/rest/metadata/00000000000000000000000000000000/wsfed/idp

8 Download the file sts-metadata-idp-wsfed.xml.

9 Open this file in Microsoft Windows Notepad and locate the Signing Certificate, which can be found under the element <KeyDescriptor use="signing"> and between these elements <X509Certificate>Signing Certificate</X509Certificate>.

10 Copy the Signing Certificate without the elements. You will use this certificate in the next step.

11 Update the following properties within the idp.properties file:

Property	Description
idp.sts.entityid	Replace **sts-hostname.domain.com** with the host name and domain of your InforSTS server: https://sts-hostname.domain.com:9553/inforsts/infor/00000000000000000000000000000000
idp.sts.sso	Replace sts-hostname.domain.com with the host name and domain of your InforSTS server: https://sts-hostname.domain.com:9553/inforsts/infor/00000000000000000000000000000000/idp/samlSSO
idp.sts.slo	Replace sts-hostname.domain.com with the host name and domain of your InforSTS server: https://sts-hostname.domain.com:9553/inforsts/infor/00000000000000000000000000000000/idp/samlSLO
idp.sts.certificate	Paste the IDP Signing Certificate you copied.

12 Run the build-metadata.bat command using these parameters: **build-metadata.bat /OP /STS sp.properties idp.properties**. This command creates a populated set of fedlet metadata in the fedlet_config folder.

13 Copy the fedlet_config folder to the root folder of your SiWA server or for an IBM i deployment of SiWA. The root folder to use should be the ROOT folder of the IFS.

Note: This path is already mentioned in the Java runtime changes completed in the “Copying the fedlet metadata folder” section.

System property changes

1 Locate the System i Workspace AnyWhere system.properties file as documented in the *System i Workspace AnyWhere Installation & Administration Guide*. Add the following properties and change the slo url:

```
com.infor.siw.cloud.mingle.slo.url=https://slo-hostname.domain.com
```

Note: You can use the URL, minus any context path, from any of these locations:

- idp.adfs.location
- idp.sts.slo
- idp.saml.slo.url property value from the file idp.properties

2 Save your changes.

Updating InforOS manager application

1 Log into the InforOS Manager from your InforOS server, then click **Applications** and locate the XA application you configured with ADFS in an earlier step.

2 Change the SSO Application to INFORSTS.

The **Relying Party Identifier** should match the value of property sp.entityid from the file sp.properties.

The SSO URL should match the value of the property sp.sso.url from the file sp.properties.

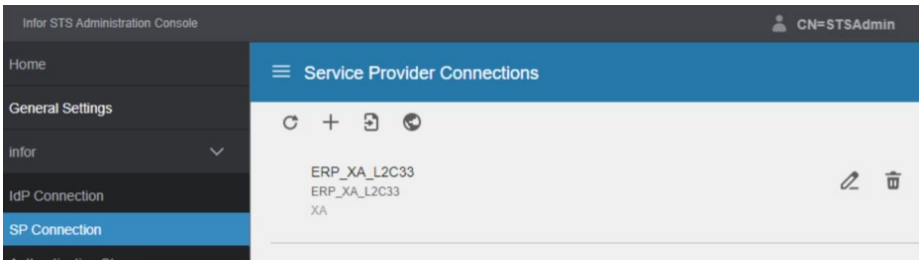
The SLO URL should match the value of the property sp.slo.url from the file sp.properties.

3 Click … on the **Signing Certificate** and select the certificate **SiW_Certificate1.cer** found in the root of the fedlet_config folder.

4 Click **Open** and click **Save**.

Updating the InforSTS server

1 Follow “Install service provider in InforSTS” section and install the service provide in Infor STS using sp.properties file.

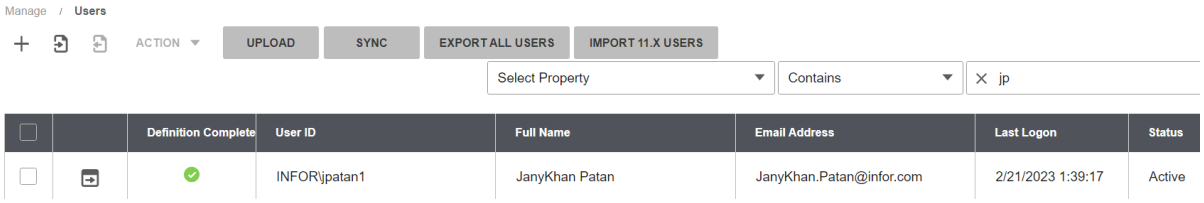


2 Start the SiWA service and validate the SSO functionality.

Configuring ERP Person IDs in Infor OS for SSO

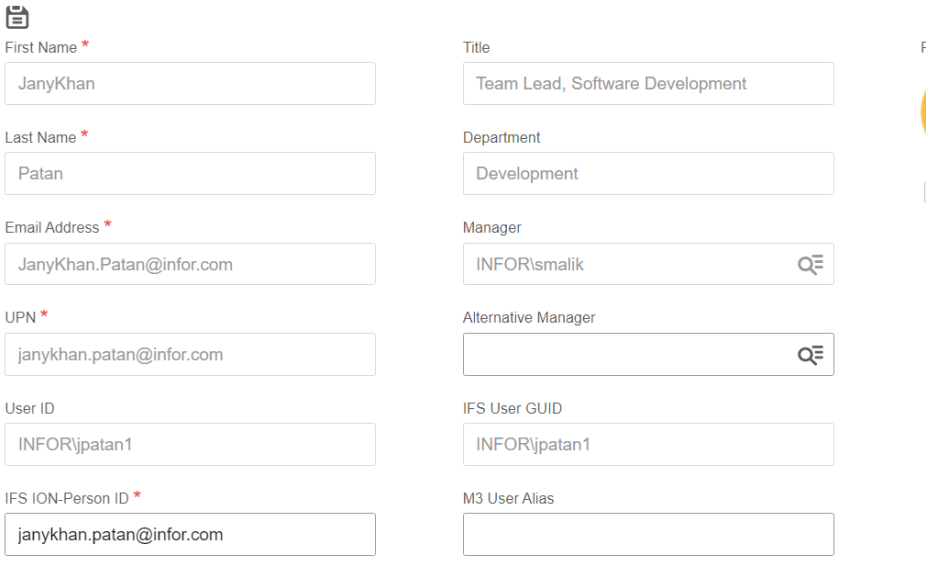
Each user that needs access to SiWA must be configured to add a mapping from the Infor OS platform to their ERP user, which is their IBMi profile ID. Mapping the IBMi profile ID to ERP Person ID is done through the User Management interface.

1 Log into Infor OS and select **Users > User Management**.



2 Use the table navigation or **Search** function to locate each user profile that you need to change.

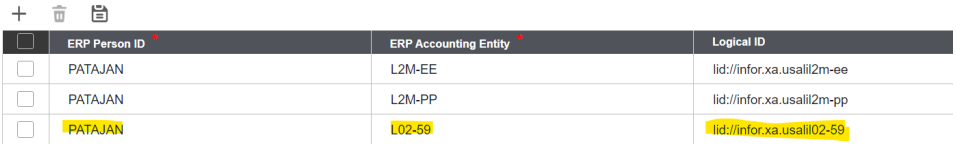
3 Click the drill-down option next to the username display their properties.



If you are using Role-based authorization for access to the SiWA application, then ensure that the user is authorized to the correct role.

4 Select the **ERP Person IDs** tab.

5 Create a mapping between the Logical ID of the SiWA application and the IBMi username.



In this example, when a user logs in to Infor OS and accesses the Infor IBMi based application that runs inside SiWA, uses the ERP Person ID which is the IBMi profile ID of the user.

6 Specify the ERP person ID, ERP accounting entity, and ERP logical ID for the environment, and then click **Save**.

7 Repeat for each user profile that needs access to SiWA.

Chapter 9 Drill-back configuration

Drill-back configuration requires the deployment of a configuration file within Infor Ming.le and Infor ION. This file is supplied by XA for drill-back support.

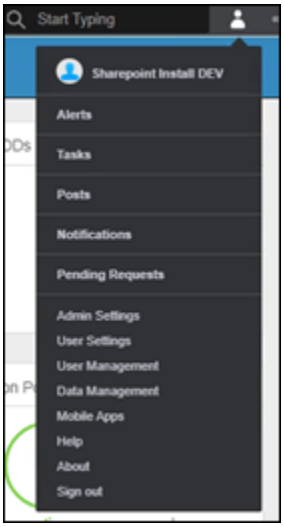
Configuring Infor Ming.le drill-backs

To configure drill-backs in Infor Ming.le, you must import the XA_Standard_Views.xml Drillback Definition File.

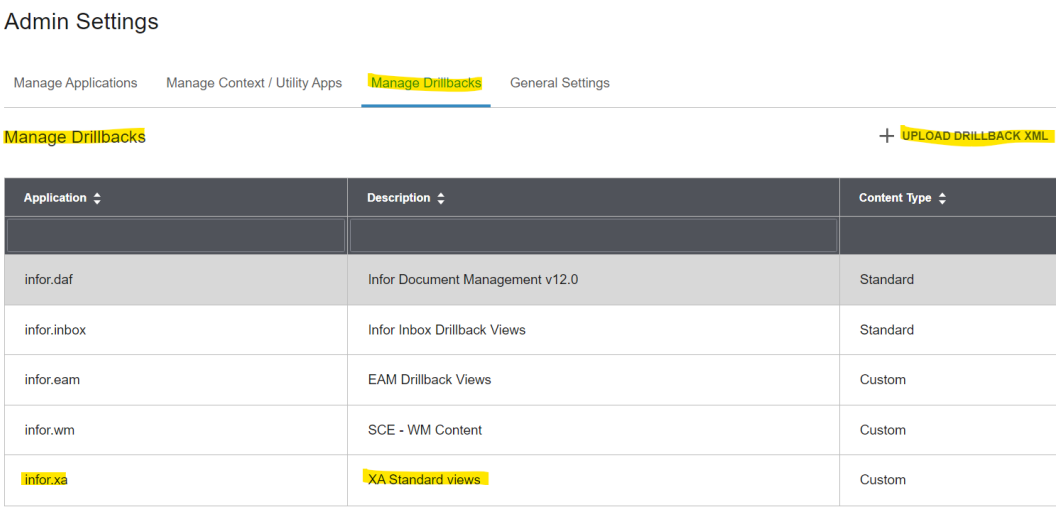
1 Navigate to the **infor\vlib\Ming.le** folder in the client IFS directory, which is the location of the XA sample solution files used for integrations through Infor OS and save the **XA_Standard_Views.xml** file.

2 Log on to Infor OS as the administrator.

3 Click your profile picture and select **Admin Settings**. You require an Admin profile to manage drill-backs.



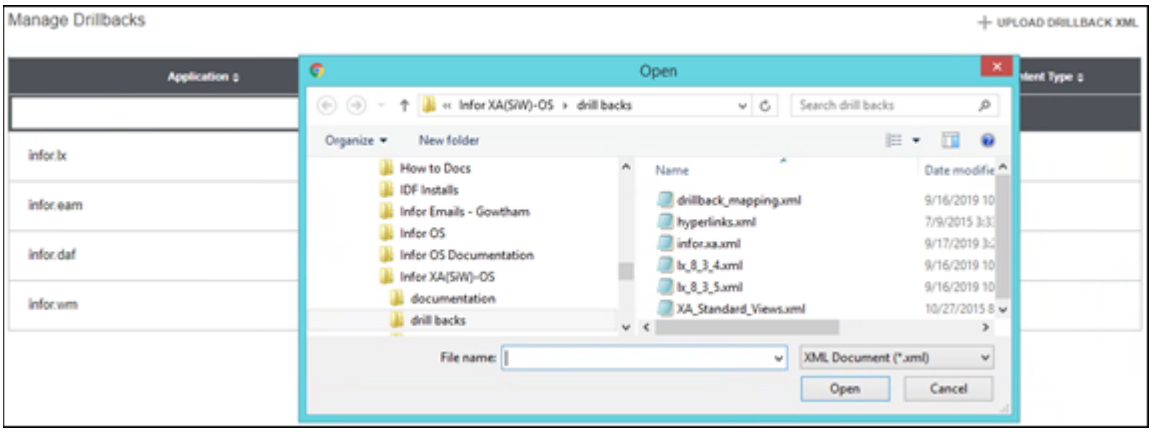
4 When the Admin Settings load, click **Manage Drillbacks**. A list of drill-back definition files that are uploaded is displayed. Upload latest drillback xml if needed.



5 Click **UPLOAD DRILLBACK XML** and browse to select the **Drillback Definition**.

6 Click **Open**.

7 Click **OK**. This step will override the old with new drillback defiintions.



Drill-back definitions

These Drillback Definition files are used in Infor Ming.le to generate the drill-back links for ION tasks/alerts.

Drill-backs are supported from InforBusinessContext messages which are shared in SocialSpace or subscribed to by other Infor Ming.le applications. Each InforBusinessContext message supported by XA IDF includes a drill-back URL the receiving product can use to drill back into XA. These drill-backs are often referred to as InforBusinessContext Drillback.

Drill-backs are also supported from products integrated with XA using ION and BOD messages. Products such as Infor Reporting and ION analytics require additional configuration; see their

respective guides. A drill-back can be requested to XA and the appropriate related task can be launched. These drill-backs are often called BOD DrillBacks.

This table shows the ERP XA supported drill-backs that include these BOD nouns:

BOD	Infor XA object
AccountingEntity	Accounting Entity
AccountingChart	General Ledger Account Administrative Division
AdvanceShipNotice	Shipment Notice Shipment Container Shipment Container Item
BillToParty	Entity Financial Division Vendor Customer Company Account
Carrier Party	Carrier
ChartOfAccounts	General Ledger Account Nature
CodeDefinition	Business Information Services Financial Division Company Payment Term Code File Unit Warehouse Site
ContactMaster	Contact
Contract	Customer Quote Customer Contract Quote
CustomerPartyMaster	Customer
FinancialCalendar	Financial Division
FinancialPartyMaster	Entity Financial Division Vendor Customer Company Account
ItemMaster	Item Revision Item Warehouse Item

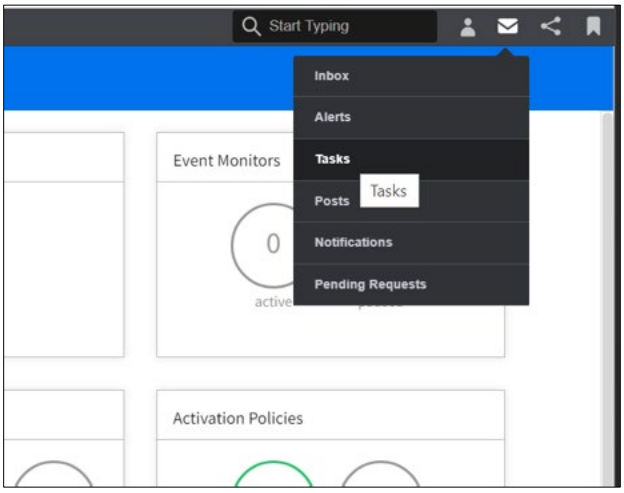
BOD	Infor XA object
Invoice	Financial Transaction Customer Invoice
Location	Company Site Financial Division Warehouse
Opportunity	Opportunity
PayableTransaction	Financial Transaction Vendor Invoice
PayFromPartyMaster	Entity Financial Division Vendor Customer Company Account
Person	Buyer Sales Representative
ProductionOrder	Manufacturing Order
PurchaseOrder	Purchase Order Purchase Order History
Quote	CustomerQuote Quote
RemitToPartyMaster	Entity
Requisition	Purchase Request
SalesOrder	Customer Order or Quote Customer Order History
ShipFromPartyMaster	Entity Customer Ship To
SourceSystemGLMovement	GL Account Period Balance GL Account Period Budget General Ledger History General Ledger Activity
SupplierInvoice	Financial Transaction Vendor Invoice Customer Receivables
SupplierPartyMaster	Entity Vendor
SupplierQuote	Quote

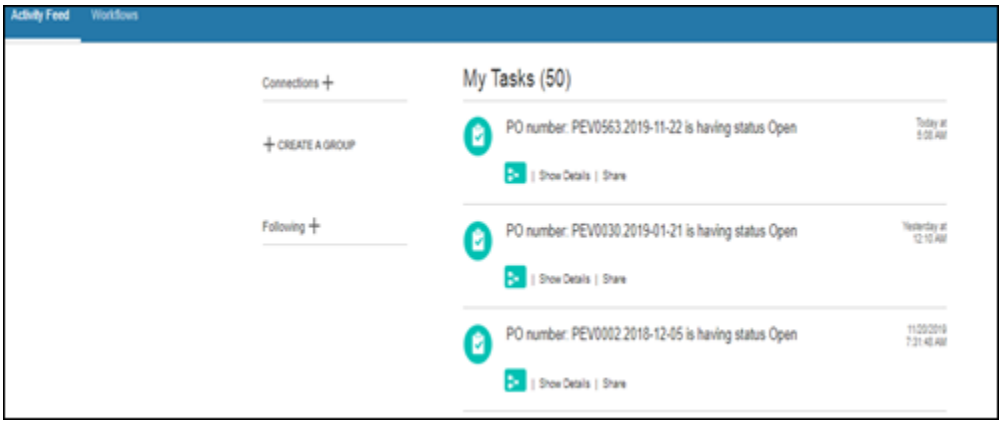
BOD	Infor XA object
SupplierShipmentSchedule	Purchase Order Purchase Order History
TradingPartner	Entity Financial Division Vendor Customer Company Account

Using drill-backs in Infor Ming.le and context/utility app

To use the drill-back functionality in Infor Ming.le and Tasks Context/Utility Apps, configuring drill-backs and enabling Tasks Context/Utility app for that XA environment in Infor Ming.le is a prerequisite.

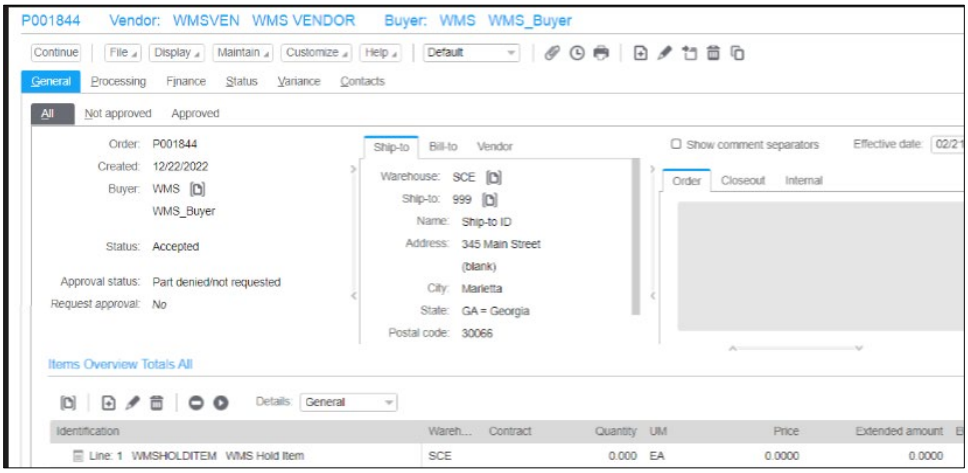
1 Click **Inbox > Tasks** in Infor OS to view **Activity Feed > My Tasks**.





2 Click **Show Details** to open and select the **Drillback** link as highlighted in this screenshot.

3 Click the **Drillback** link. The page is redirected to the specific XA object. In this example, the page is Purchase order.



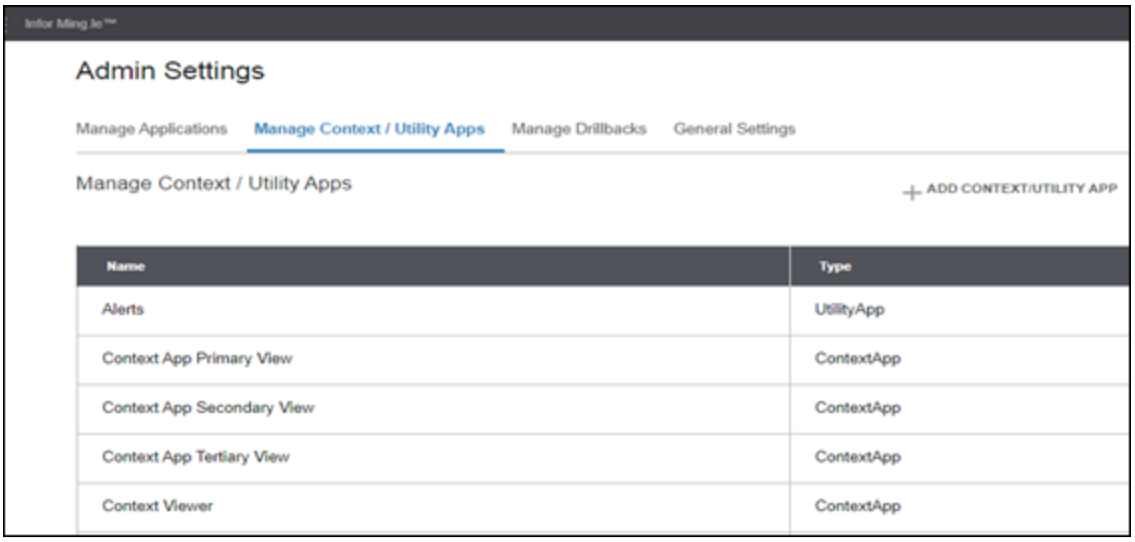
Configuring the IDF Context application

You can configure the IDF Context application in Infor Ming.le. When configured, the application is displayed on the right-side of the window.

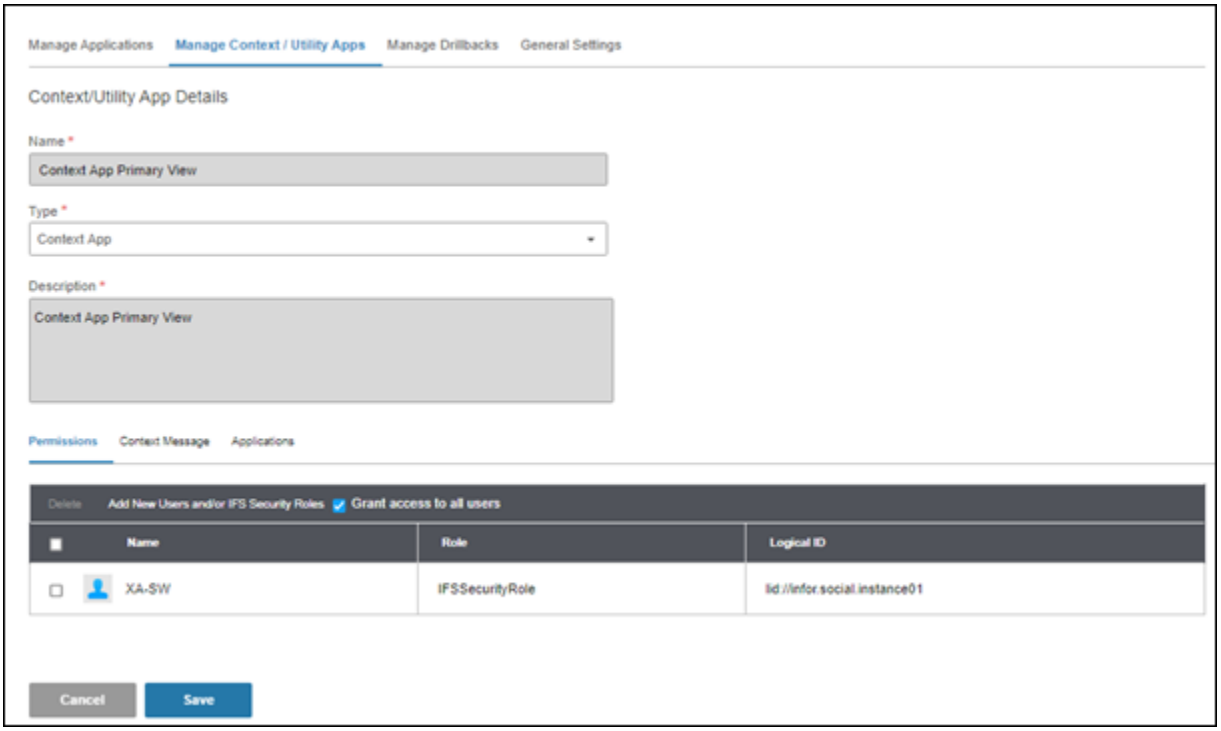
To use the IDF Context application, System i Workspace must be at PTF level 16 or later.

Enabling IDF Context applications

1 In Infor OS, go to **Admin Settings > Manage Context/Utility Apps**. Context App Primary View, Context App Secondary View, and Context App Tertiary View are displayed.

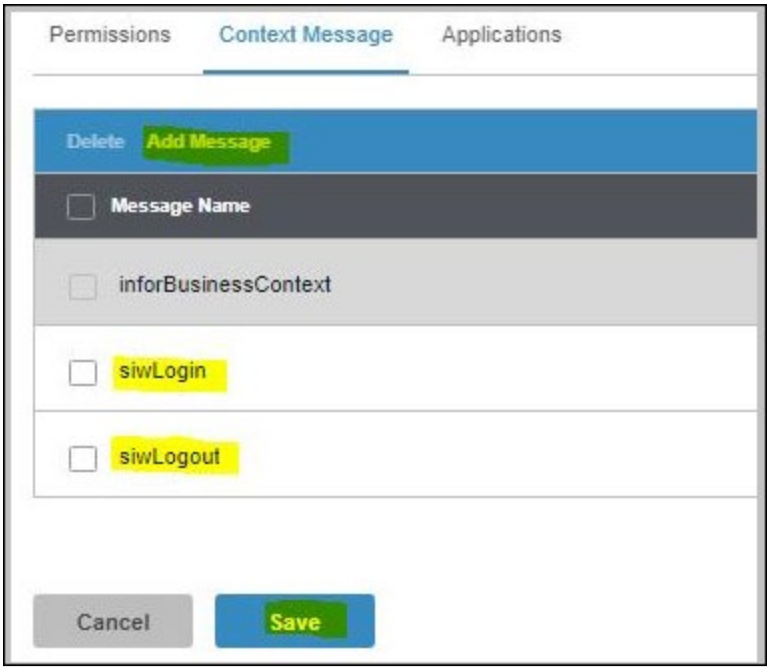


2 Click **Context App Primary View** to view the details.

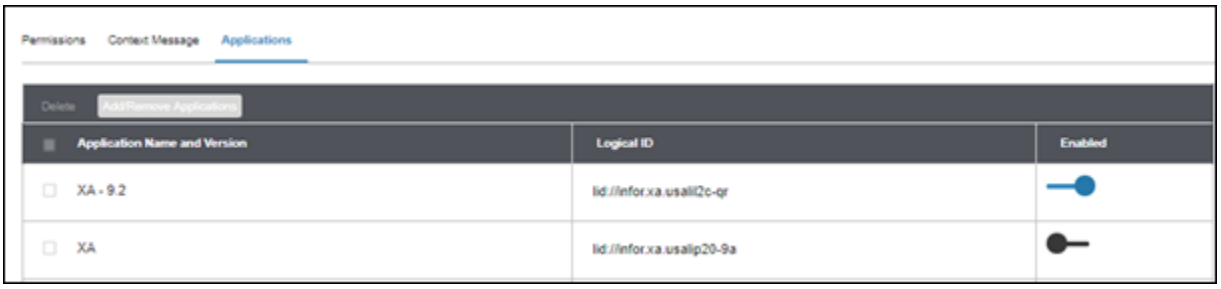


3 In the **Permissions** tab, add the security role created for XA in “Create a new application security role”. All the users under this security role can view this Context App while accessing XA.

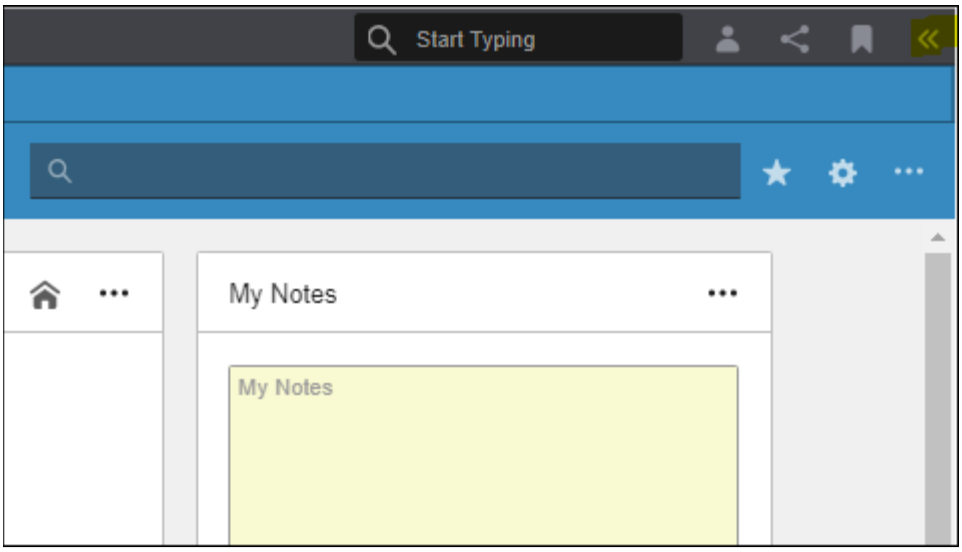
4 Select the **Context Message** tab and add these messages as displayed. Refer KB 2046253 for more details.



5 Select the **Applications** tab and enable the toggle for required XA application.



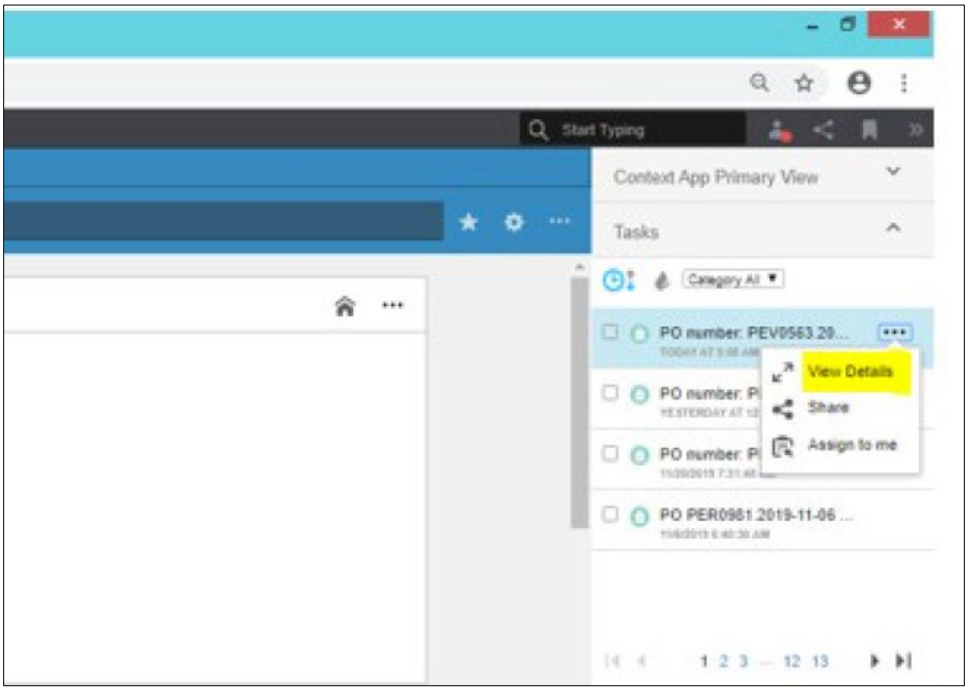
6 Launch XA and click the double arrow option in the top right corner to launch Context apps.



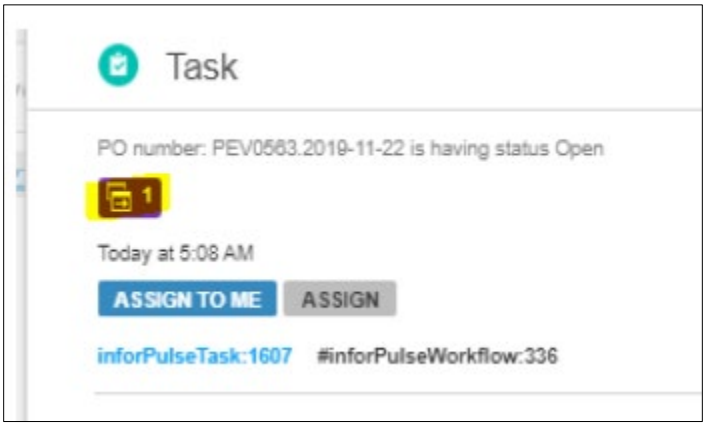
Drill-backs in Task Context/Utility app

Tasks Utility App enabled in **Manage Context/Utility App** enables users to view the tasks in the right-side corner of SiWA System i window. A list of tasks available for the current user is displayed.

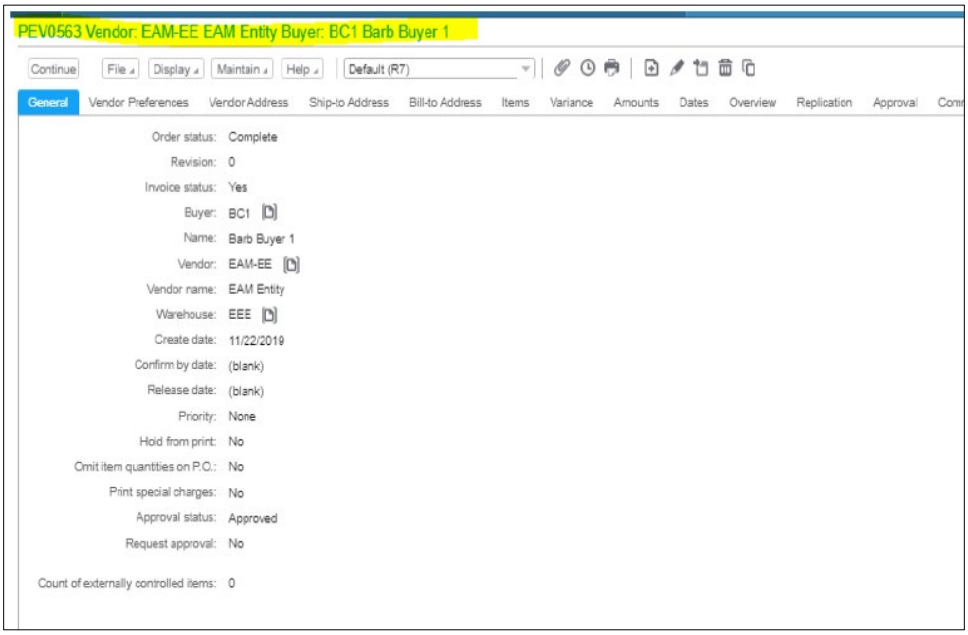
1 Click **More > View Details**. The **Task details** window is displayed.



2 Click on the drill back symbol to view the drillback link.



3 Click the drillback link to launch and redirect to PO details in XA.


PEV0563 Vendor: EAM-EE EAM Entity Buyer: BC1 Barb Buyer 1
Continue
File
Display
Maintain
Help
Default (R7)
General
Vendor Preferences
Vendor Address
Ship-to Address
Bill-to Address
Items
Variance
Amounts
Dates
Overview
Replication
Approval
Order status: Complete
Revision: 0
Invoice status: Yes
Buyer: BC1
Name: Barb Buyer 1
Vendor: EAM-EE
Vendor name: EAM Entity
Warehouse: EEE
Create date: 11/22/2019
Confirm by date: (blank)
Release date: (blank)
Priority: None
Hold from print: No
Omit item quantities on P.O.: No
Print special charges: No
Approval status: Approved
Request approval: No
Count of externally controlled items: 0

Chapter 10 Infor Business Context

The Infor Business Context (IBC) message is an Infor Ming.le standard message that broadcasts the status of an application. The message consists of the identity of the application and the view that is being displayed along with a list of entities.

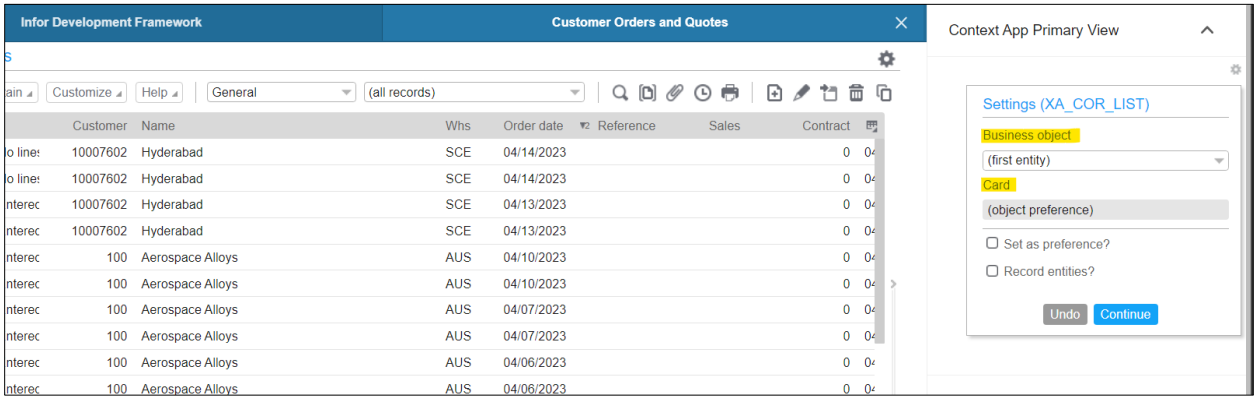
All Infor applications running inside Infor Ming.le send these messages. In IDF, the entities correspond to the business objects that are currently being displayed.

In list view, the IDF always sends a message when the selection changes. The message contains an entity for each selected row.

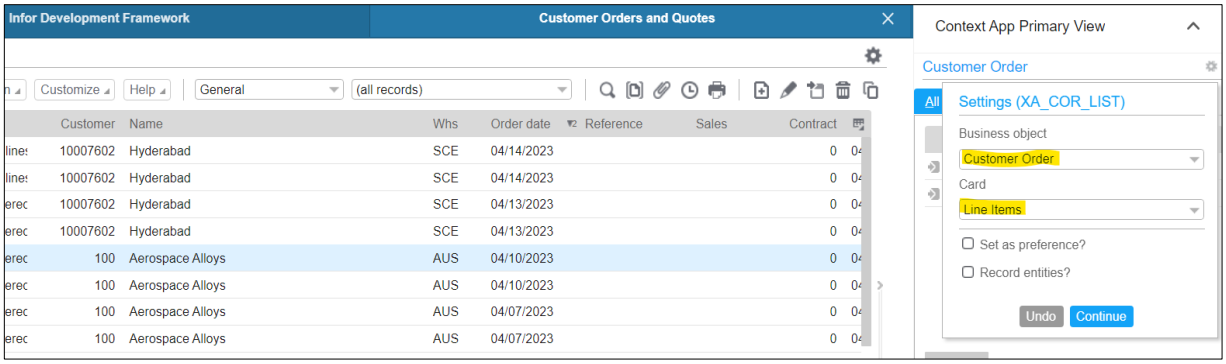
In object view, the IDF sends a message containing the displayed object and any many-to-one related objects. When the user selects a row from a list card, the currently selected object is added to the message.

Context applications or web parts can be added to any application page in Infor Ming.le. These context applications display data that is appropriate for the message.

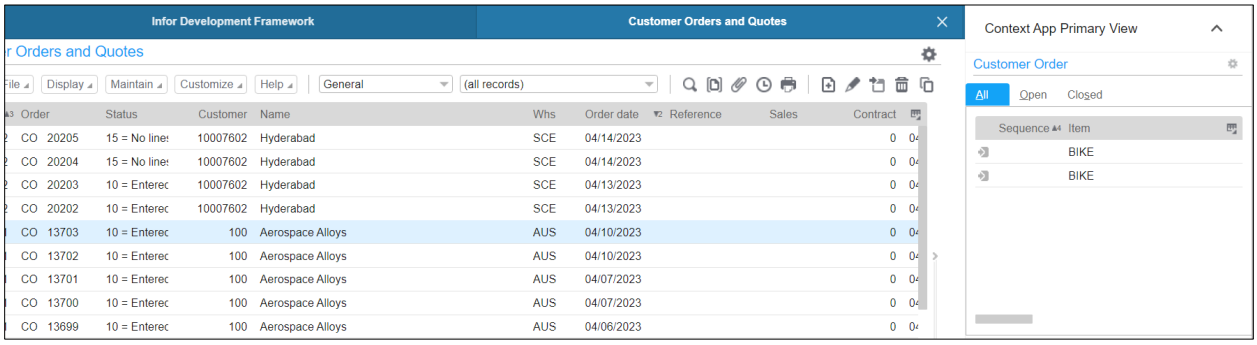
The IDF context application listens for IBC messages and when the context application receives a message and recognizes the first entity, the context application looks at the preferences for the corresponding business object to see if a card preference has been defined. If a card preference is defined, then the IDF context application displays the object using that card preference.



You can select the **Settings** option and select a business object and a card from the list. In this example, **`Customer Order`** and **`Line Items`** are selected, respectively.



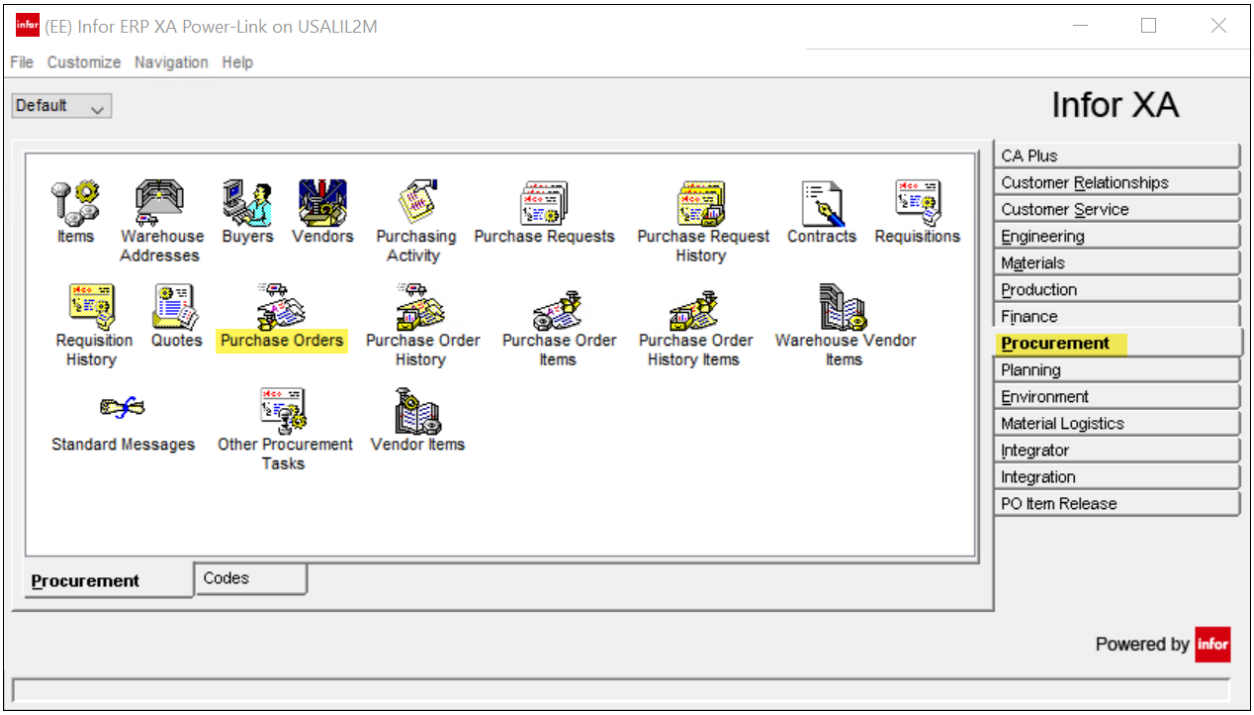
Line items are displayed when you click on the customer order as displayed in the screenshot.



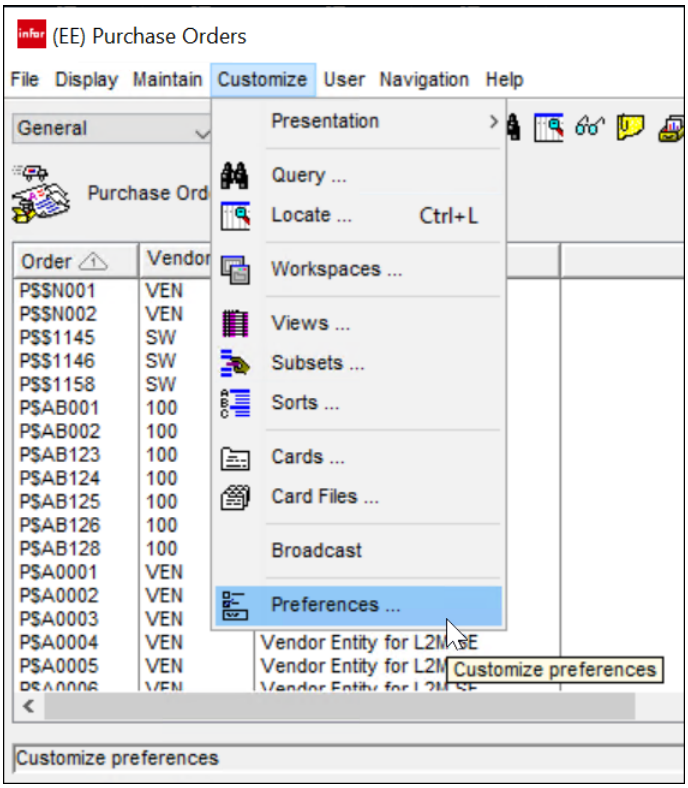
Preference definition in XA 9.2

Preferences for the context application for any business object are defined in Power-Link.

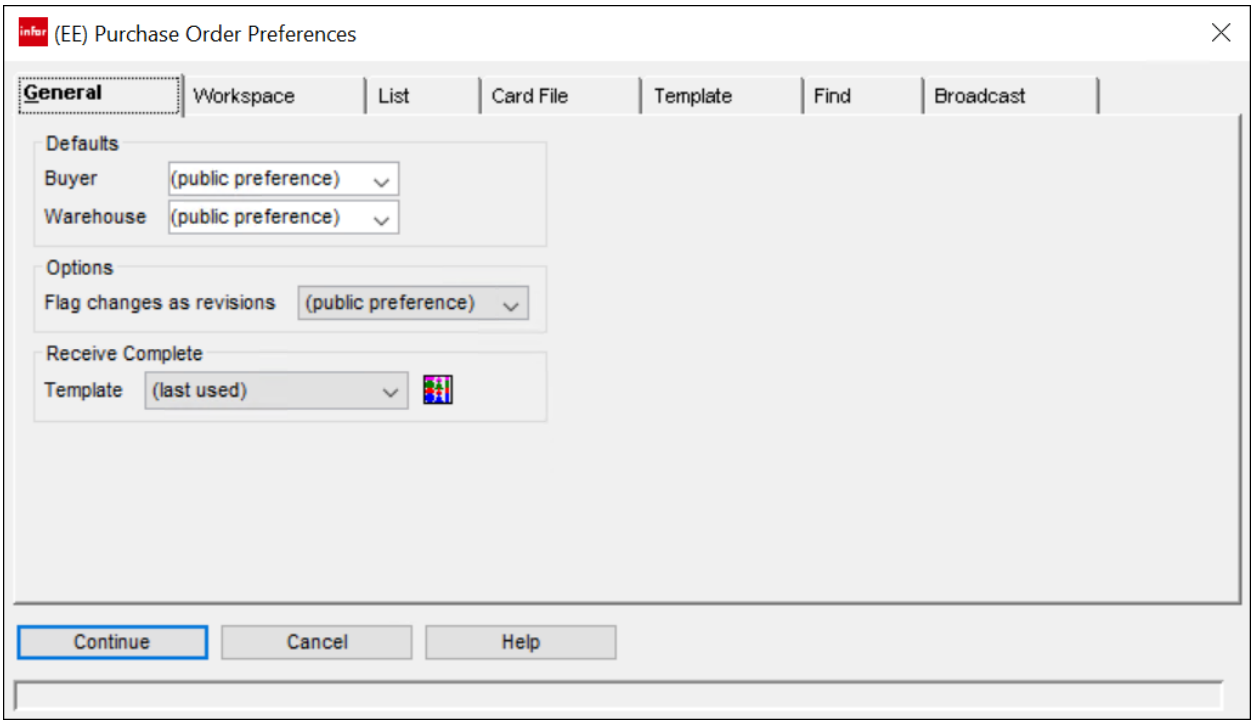
1 From the main browser, double-click **Business Object** to configure the context application.



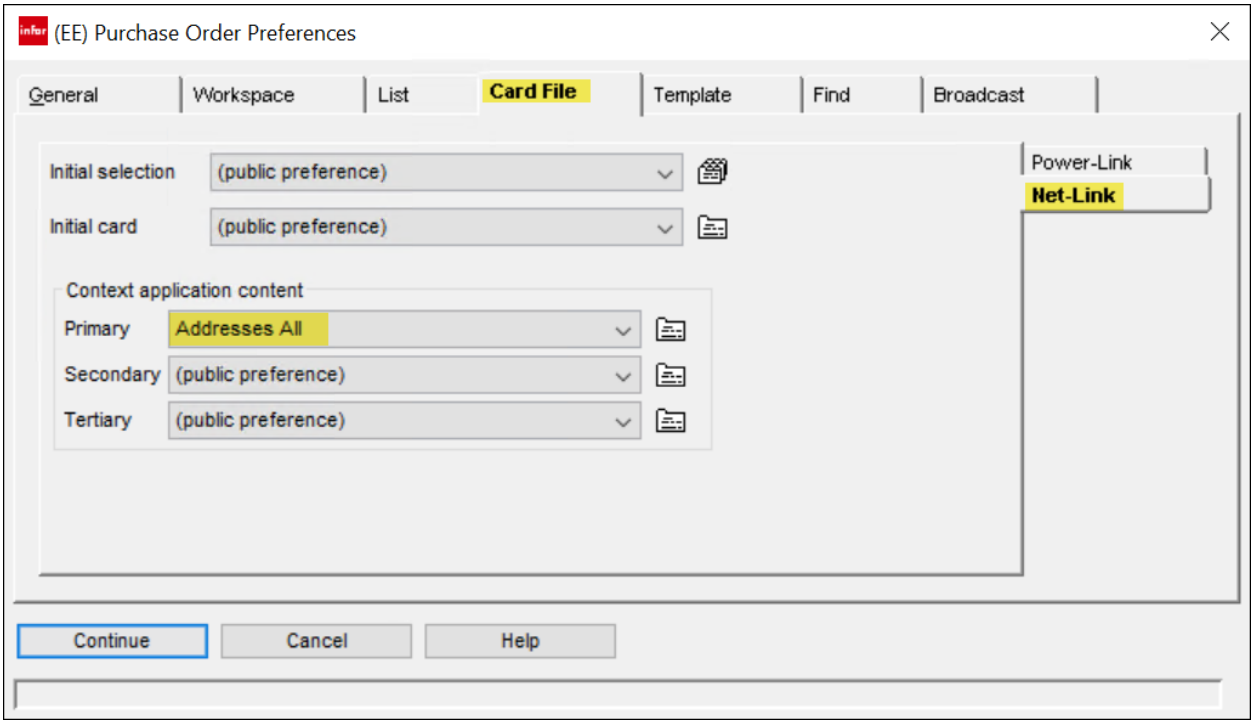
2 Select **Customize > Preferences**.



The **Purchase Order Preferences** screen is displayed.



3 Select the **Card File** tab, and then select the **Net-Link** tab.



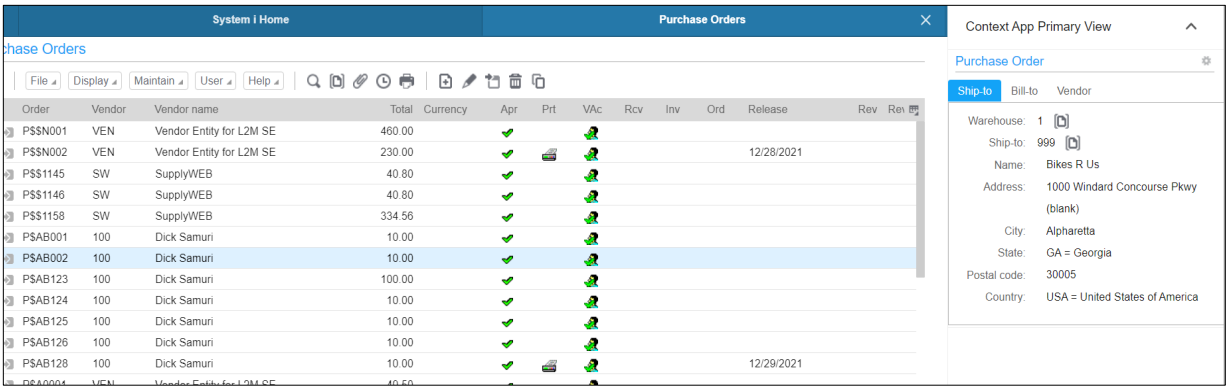
4 Specify the preferences for the context application. In the example, **Addresses All** is selected.

The context application content area is where the cards that are to be used by the IDF context application are defined. You can use any cards, but most cards are designed to be used in a full screen and may result in unwanted scrollbars when presented in the limited space available to the context application. We recommend that you define specific cards using the customization features of Power-Link specifically for the context application. See the context help of Power-Link for guidance about how the customization facilities are used.

See the “Export Metadata from XA” section in *Infor System Manager Quick Installation Guide for Infor XA* after setting up preferences in Power-Link to reflect the changes made in Power-Link export Private metadata.

After exporting the metadata, Workspace must be updated for the existing or new users. See the *“Updating Workspace”* section in *Infor System Manager Quick Installation guide for Infor XA.*

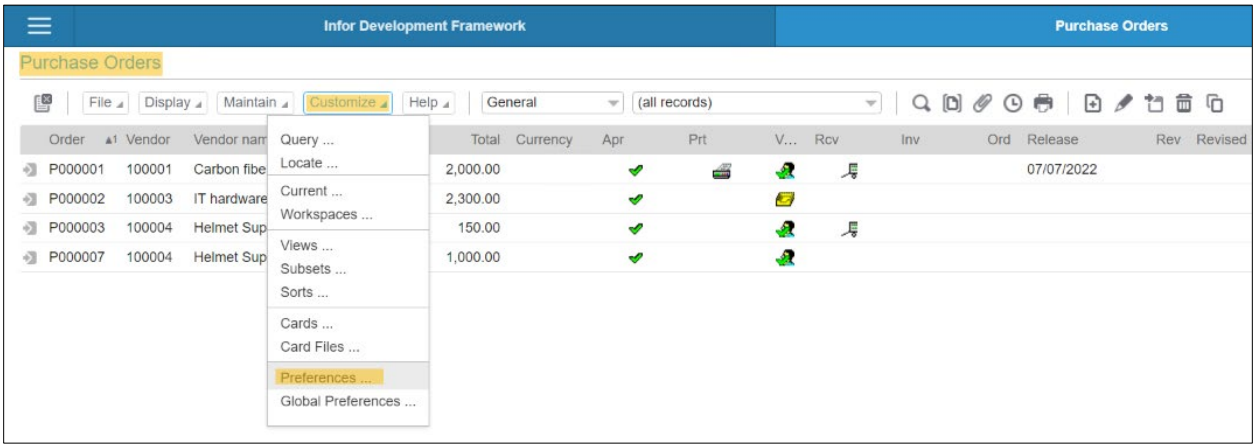
5 Launch XA in Infor OS to see the Context App Primary View with Addresses. Select a purchase order in the Context App Primary View to display the Purchase orders Addresses.



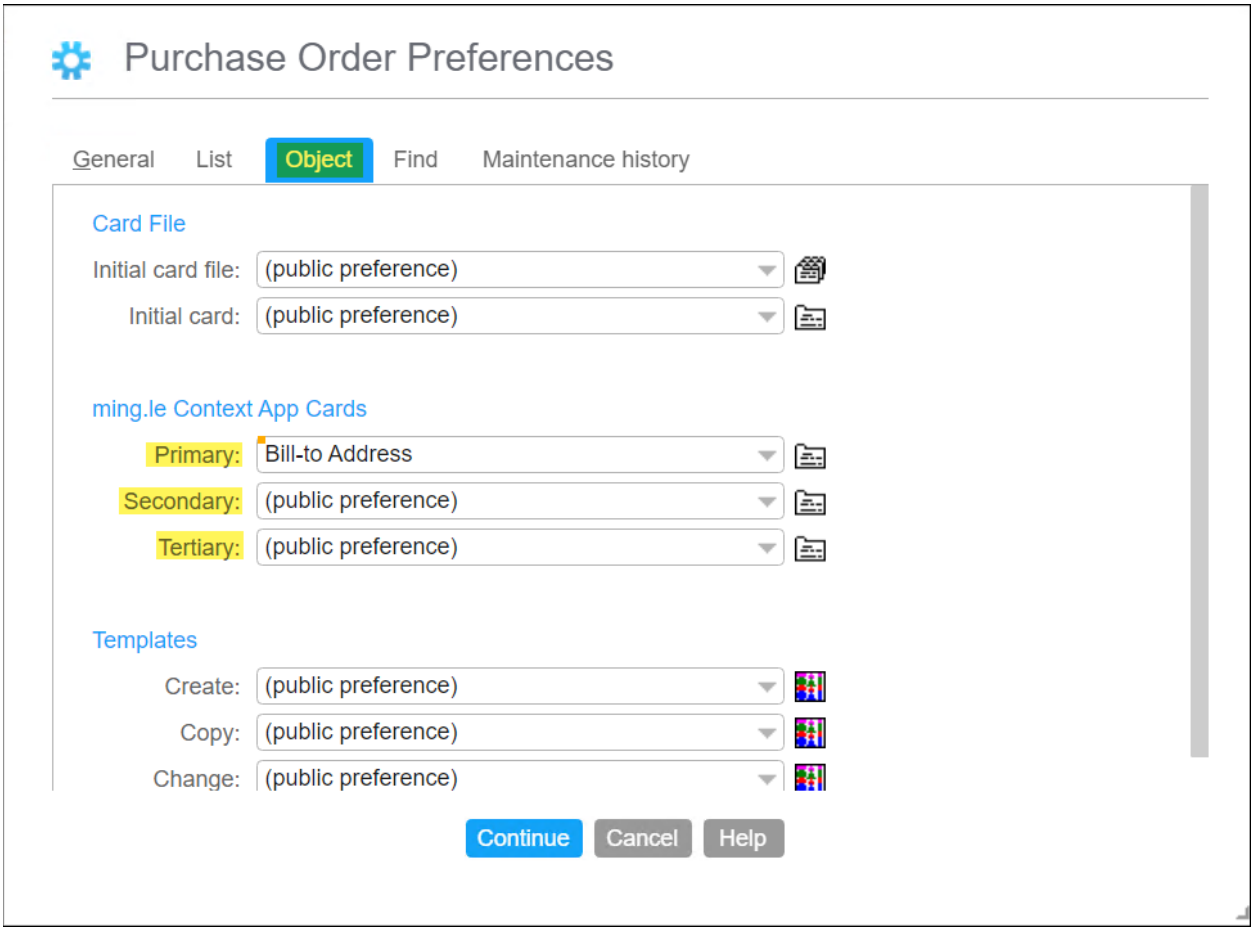
Preference definition in XA 10

Preferences for the context application for any business object are defined in Net-Link and can be configured in SiWA.

1 Open the Business Object and select **Customize > Preferences** to configure the context application.

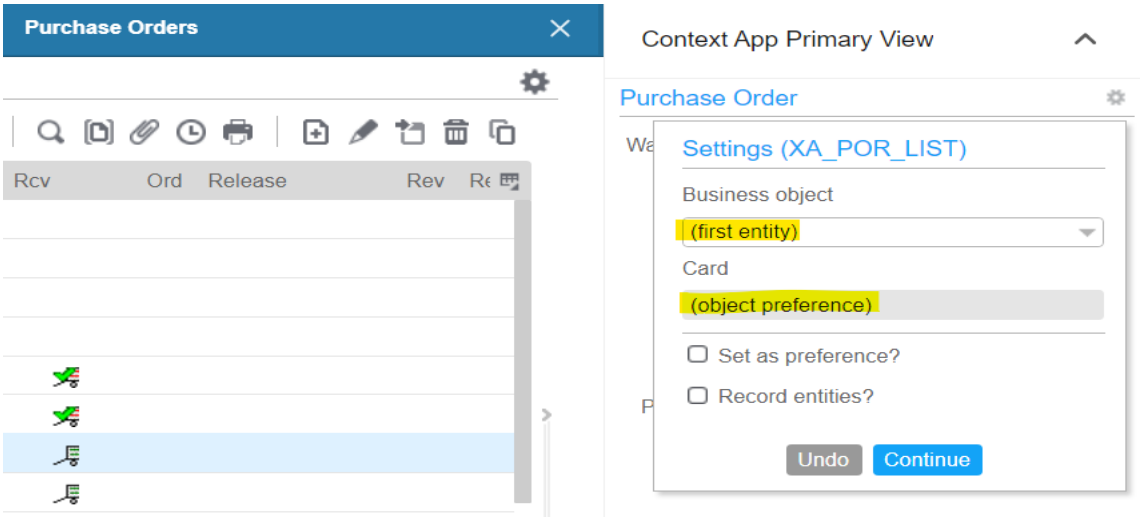


2 Select **Object** tab. Under ming.le Context Apps Cards you can select the required preferences for Primary, Secondary, and Tertiary applications. Bill-to-Address is selected as Primary Application preference in this example.



3 Click **Continue**.

4 From the Purchase Orders list select a PO. Go to settings for Primary Context App on right side. Ensure that no Business Object and Card details are selected before.



5 Click **Continue**.

6 From the Purchase Orders list, select a PO to see bill to address details in **Context app Primary View**.

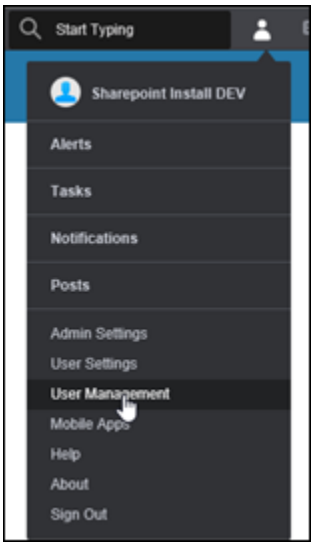
Chapter 11 User maintenance

This chapter only covers minimal user maintenance. You must refer to the *Infor OS Administration Guide* for the complete documentation of the features described here.

Adding users

1 Log into Infor OS using the account that you set up for IFS administration.

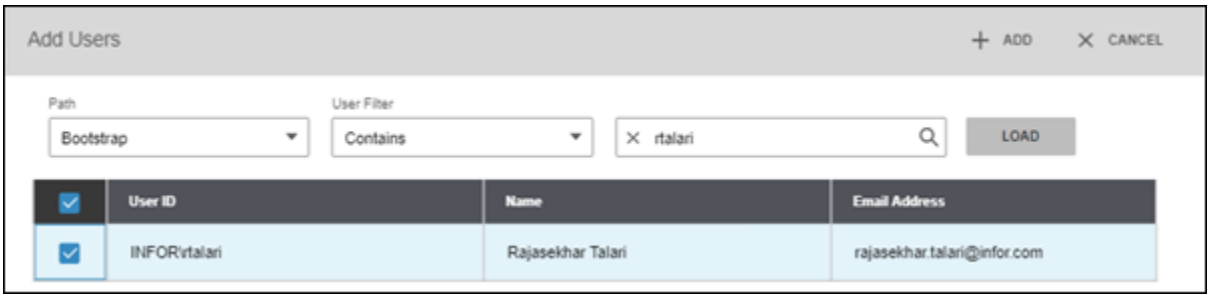
2 Click the **User** option in the top-right hand corner, and then select **User Management**.



3 Select **Users**.

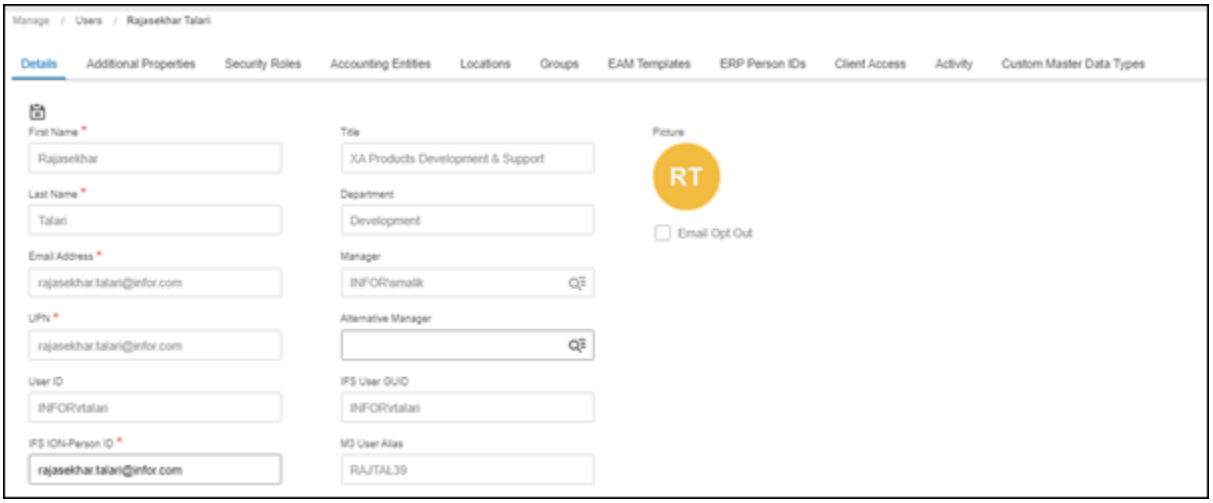
4 Click the **+** option to add a new user.

5 Specify a name in the search box and click **Load**.

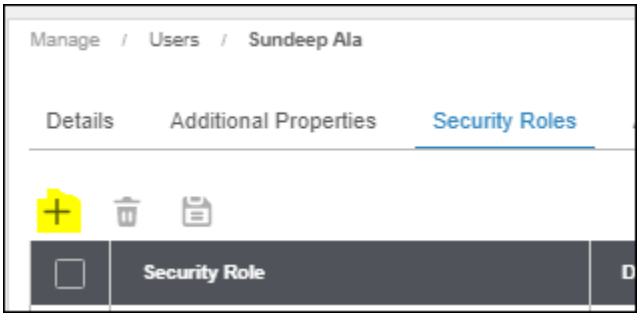


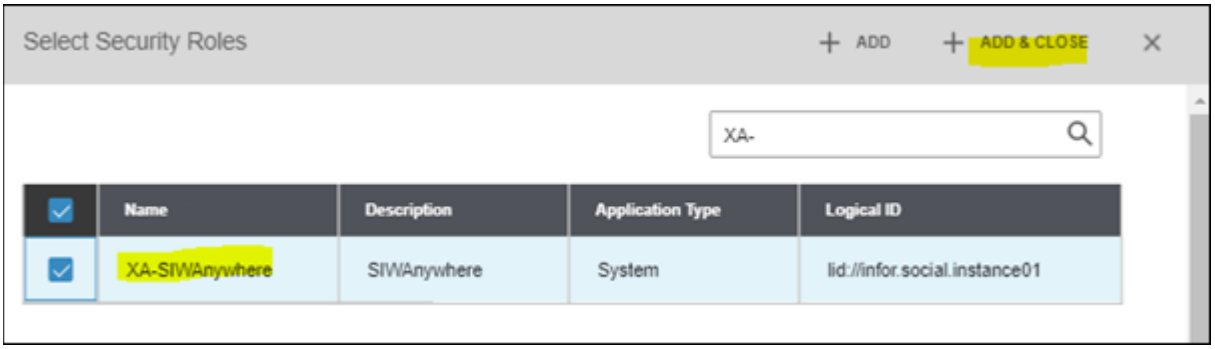
6 Select the user from the list and click **Add**.

7 Verify the user information and update as per the business requirement.



8 Navigate to security roles and click the **+** option to add the required security roles to a user as per the business requirement.





9 Click **Save**, as highlighted, to save the changes to the user profile.

Chapter 12 Net-Link WAR file redeployment

This section explains about the procedure on Net-Link WebArchive (WAR) file redeployment. We perform this section only when we want to redeploy the Net-Link war file with new changes.

System i Workspace AnyWhere with Windows deployment

Refer “WAR file Generation” and “Tomcat (version 7.0 +)” sections in the *Infor XA Setup Guide for Secure Net-Link*, which describes the Net-Link WAR file redeployment with SiWA using Windows deployment.

System i Workspace AnyWhere with IBMi deployment

Refer “WAR file Generation” and “WebSphere (version 9.x)” sections the *Infor XA Setup Guide for Secure Net-Link*, which describes the Net-Link WAR file redeployment with SiWA using IBMi deployment.

Appendix A Publishing BODs

Use this appendix to understand how to publish business object definitions (BODs).

Business Information Services

The BIS Organization node setting in XA is used by all BODs as a base accounting entity for many different BOD elements including document ID's. The Code Definition BOD is used to send the list of accounting Entities to the Business Vault.

It is recommended the BIS organizationNode ("machineName.EnvironmentCode") on the Business Information Services card in the Application Settings object is not more than ten characters. For example, if machine name is USATLD06 and environment is AB, you can use either USATLD06 or D06.AB or any other combination of characters that is less than or equal to ten characters.

If you change the Organization node attribute for the root Organization Node accounting entity, the PUB* files storing published data for many objects are not changed. Also, the root Organization Node accounting entity in the Business Vault is not updated even if you run the Publish Business Information Services host job on the Business Information Services card in Application Settings.

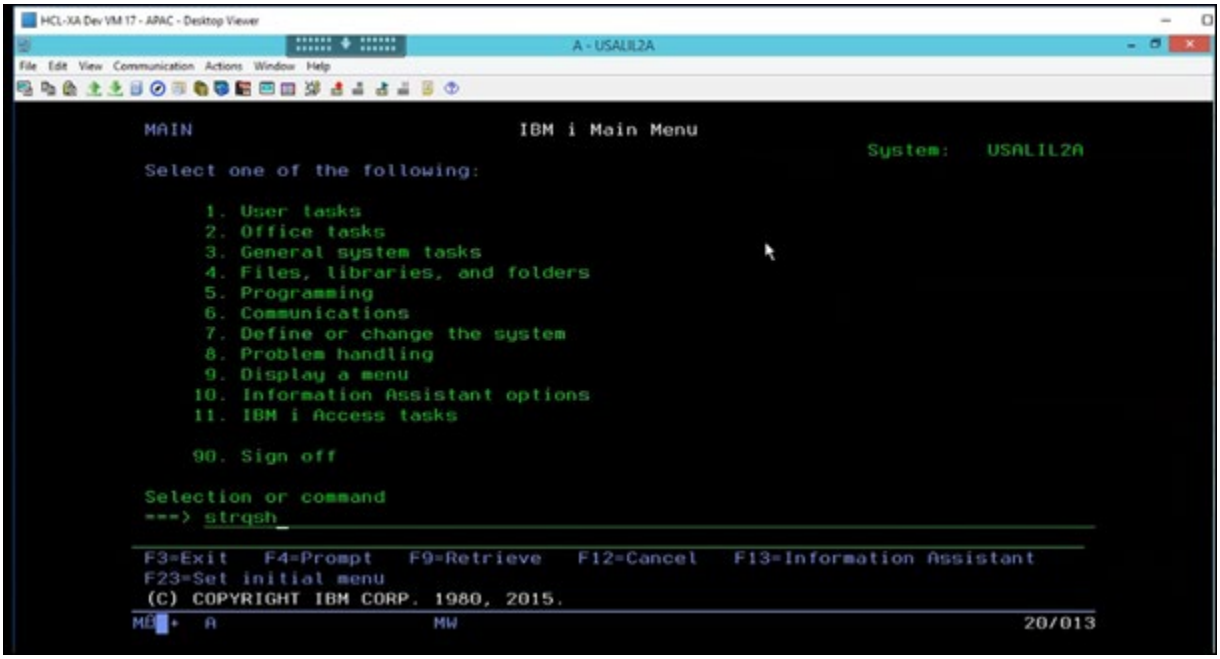
If the root Organization Node accounting entity is changed in BIS, you must do these steps:

1. Clear all published data files (PUB***) for the environment.
2. To rebuild the PUB* file data as well as re-sync of BV data, re-publish all published objects including objects that publish Code Definitions and Accounting Entity.
3. Use the **Publish** host job on each object to publish BODs.

Appendix B Creating a default WebSphere profile

If you are unable to get the default profile from WebSphere profile dropdown while creating an IBM HTTP Server instance, follow these steps to create default WebSphere profile:

1 Start a QSH session in iseries.



2 Run these commands:

$ cd /QIBM/ProdData/WebSphere/AppServer/V9/BASE/bin

$ ./manageprofiles -create -serverName server1 -nodeName <hostname> -cellName <hostname> -hostName <hostname.domain.com> -templatePath /QIBM/ProdData/WebSphere/AppServer/V9/BASE/profileTemplates/default -profileName default

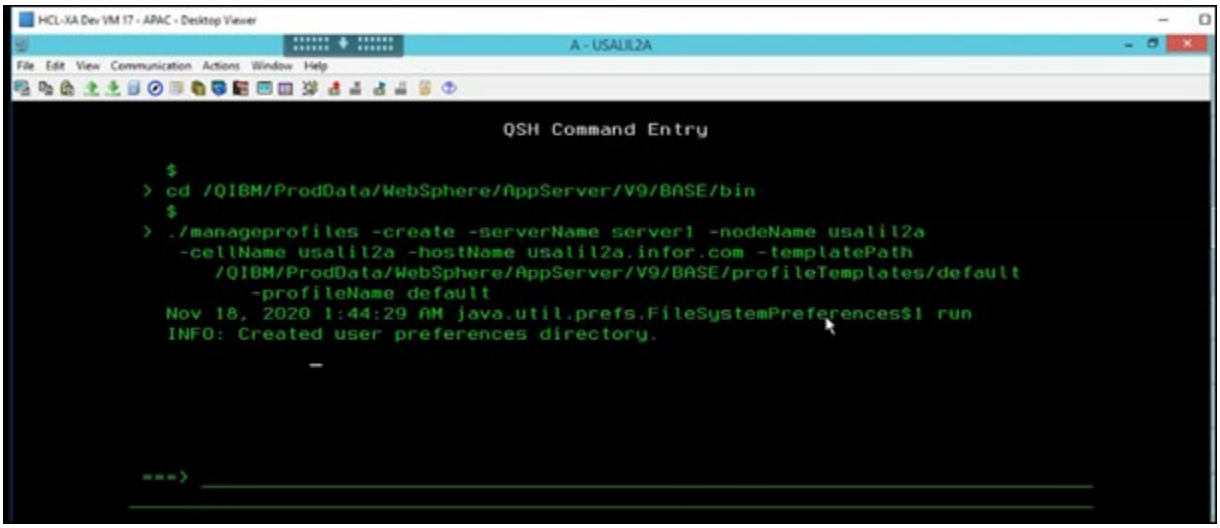
Replace *<hostname>, <hostname.domain.com>* with the relevant iseries hostname.

For example:

```
$ cd /QIBM/ProdData/WebSphere/AppServer/V9/BASE/bin

$ ./manageprofiles -create -serverName server1 -nodeName usalil2m -cellName usalil2m -hostName usalil2m.infor.com -templatePath
```

```
/QIBM/ProdData/WebSphere/AppServer/V9/BASE/profileTemplates/default -
profileName default
```



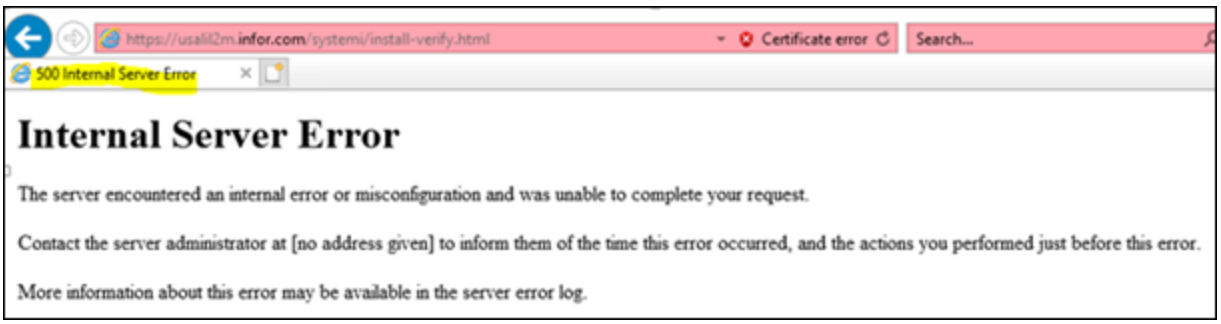
Note: In some severs the folder “**BASE**” is “**Base**”. Check the folder structure before running the command.

3 Return to the **WebSphere HTTP admin -> HTTP servers -> WebSphere** applications server. The default profile is listed in the list.

If you still have issues while creating the default profile, check with IBMi support and get this resolved.

Appendix C Internal server error resolution

At the end of SiWAnyWhere installation, try to verify the installation, if you are receiving an Internal Server Error.



Use these steps to resolve the issue:

1 Login to IBM i Web administrator console.

http://<hostname.domain.com>:<port>/HTTPAdmin

Replace *<hostname>, <hostname.domain.com>* with the relevant iseries hostname.

For example: http://usalil2m.infor.com:2001/HTTPAdmin

2 Stop the HTTP server and application servers related to SiWAnyWhere.

3 On the IBMi server (Ex: USALIL2M), check if the file - plugin-key.kdb is present in this location:

QIBM\UserData\WebSphere\AppServer\V9\Base\profiles\<profilename>\config\IHS_WSANYWHERE

4 If the file - plugin-key.kdb is not present, then copy the file from:

QIBM\UserData\WebSphere\AppServer\V9\Base\profiles\<profilename>\config\cells\<cellname>\nodes\<nodename>\servers\IHS_WSANYWHERE

To:

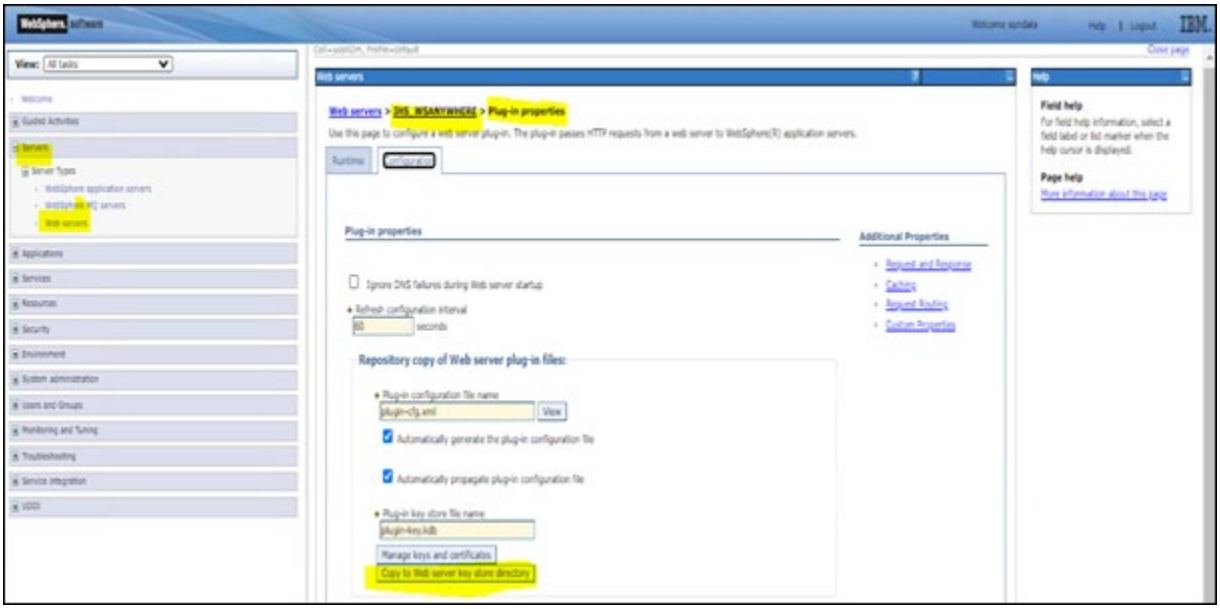
QIBM\UserData\WebSphere\AppServer\V9\Base\profiles\<profilename>\config\IHS_WSANYWHERE

Note: You must have QSECOFR authority to perform this action.

5 Start the HTTP server and application servers related to SiWAnyWhere.

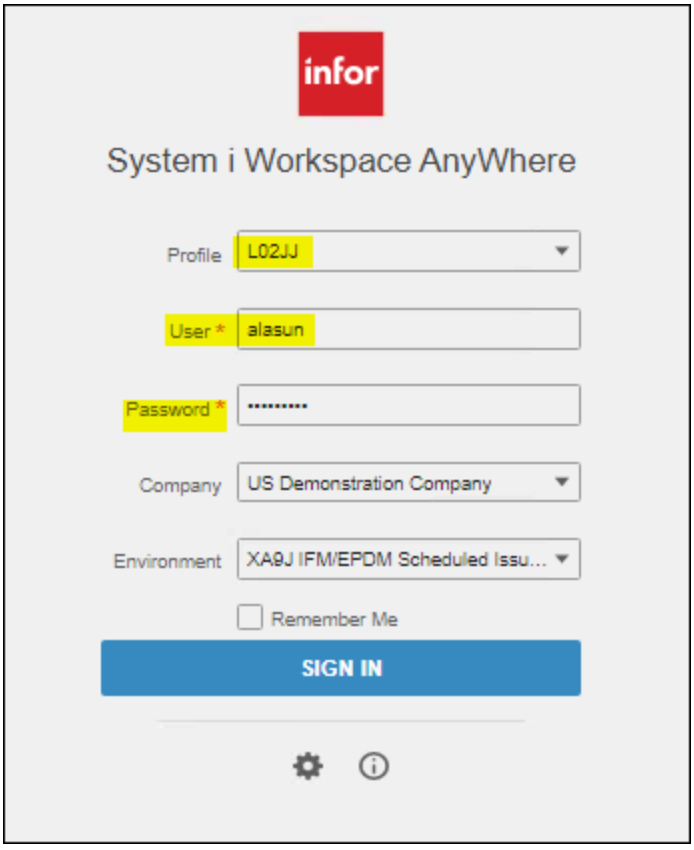
6 Launch https://usalil2m.infor.com/systemi/install-verify.html.

7 If you still receive an Internal Server Error, then navigate to the **WebSphere Application Server > Launch Administrative Console > Servers > WebServers > IHS_WSANYWHERE > Additional properties > Plug-in properties** and select **Copy to WebSphere KeyStore Directory > Apply** and click **Save**.



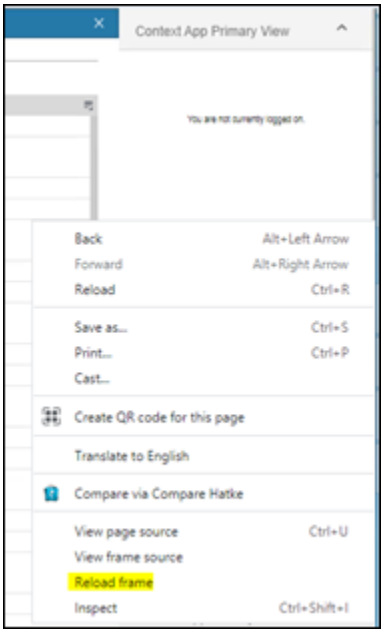
Appendix D Troubleshooting

- If a user is trying to login to Infor OS for the first-time using Infor credentials and the user is unable to login to the Infor OS successfully, then you must make sure the user profile is configured in Infor OS application. If not, then the user can request the Project Manager or XA Integration team for user provision in Infor OS with the user's Infor mail ID. The user will need to specify whether they need access to Infor OS Development or Infor OS QA environment.
- If a user logs in to Infor OS successfully but gets prompt again for credentials while launching the SiWA applications, then the user can enter the respective IBM i user ID and credentials. For example, in this screen, login prompt screen is displayed for USALIL02 IBM i machine.

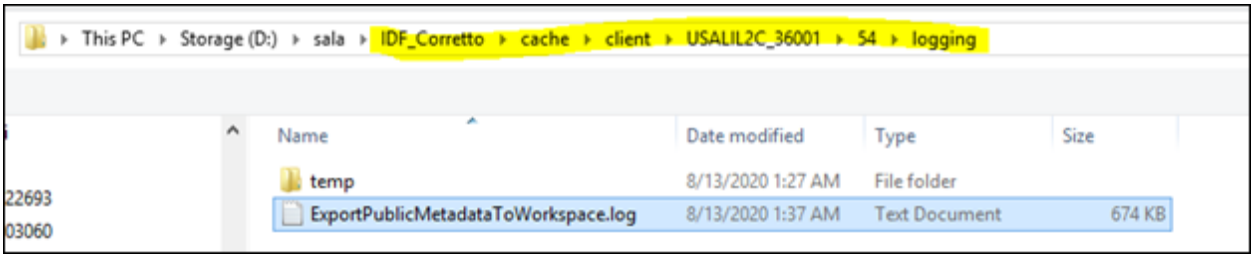


- If user can login to Infor OS and SiWA applications, but facing an issue at Context App Primary, Secondary & Tertiary Views with an error message *"You are not currently logged on"* displayed,

then as a workaround, right-click the respective Context App view and click the *"Reload frame"* as displayed.

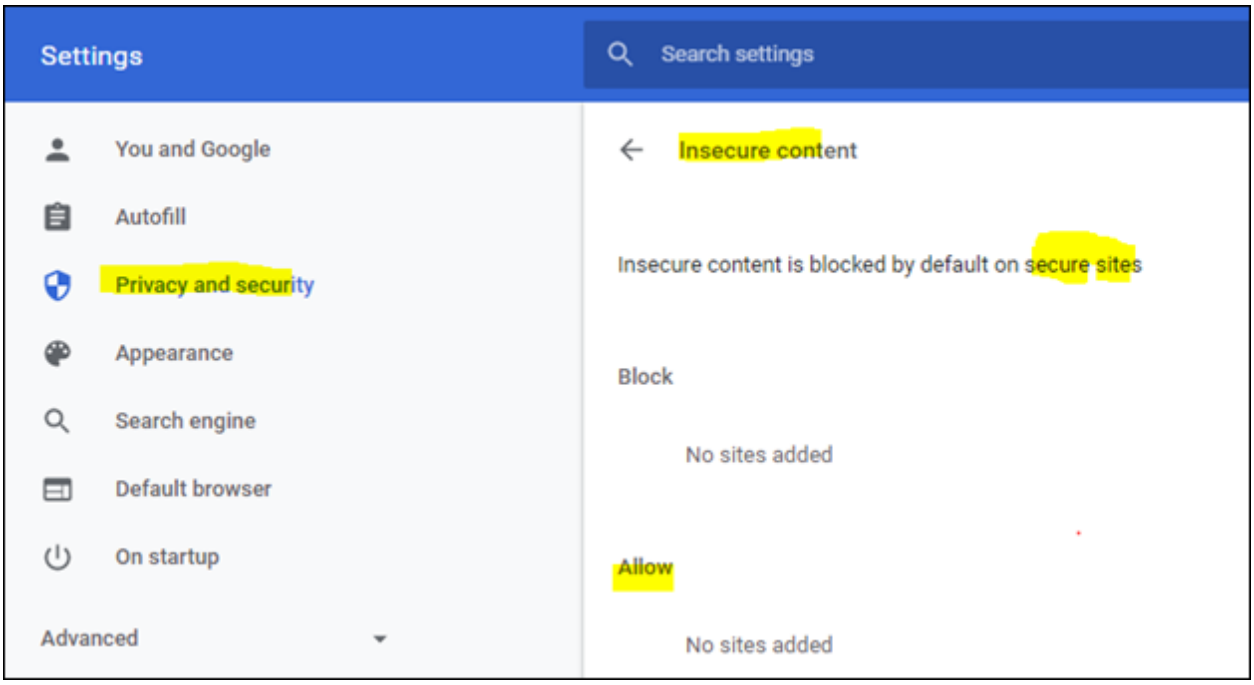


- Even after successful SIWA environment setup, if the environment is launching with no IDF tasks under My Tasks in home page, then you need to check whether exporting is done successfully or not in the ExportPublicMetadataToWorkspace.log at the local IDF logging folder. This is similar to going to **Power- Link > help > About > Ctrl + D > Ctrl + L** and going to logging folder.

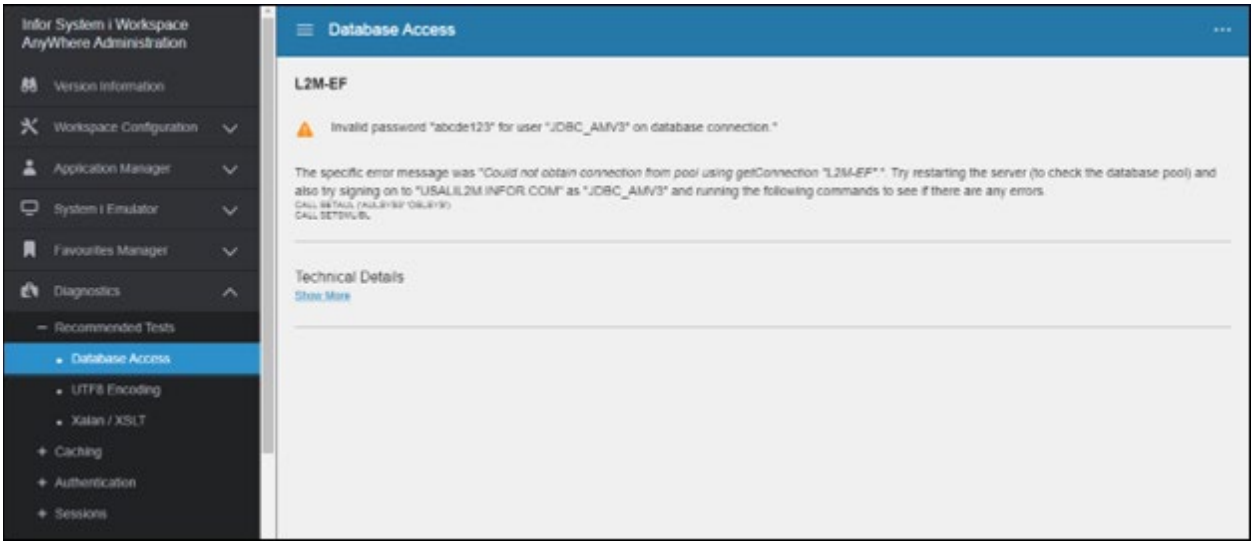


- If you find any errors, those need to be resolved and re-run export metadata again to ensure that you do not encounter any errors.
- If you encounter the "Language Code is not defined" error, then you need to cross check and update language code in SIM console.

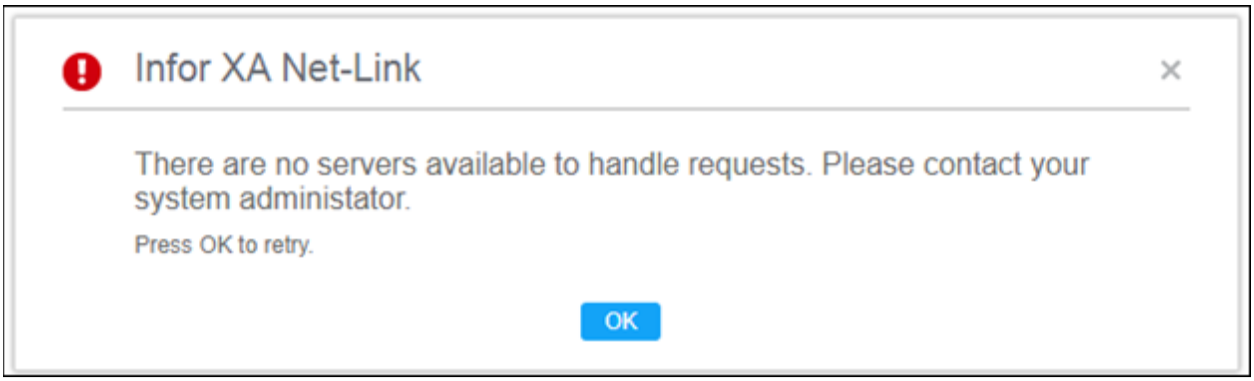
- When you try to open any business object from IDF using SIWA, if it displays a blank page, you need to add the SIWA URL to the insecure content and try to relaunch the application.

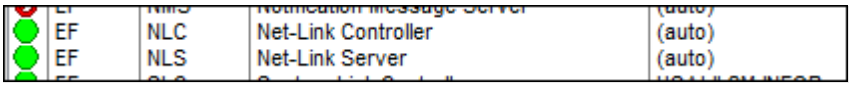


- Restart the server SIWA application installed server if this issue appears and recheck the Database access under diagnosis in SIWA admin page.



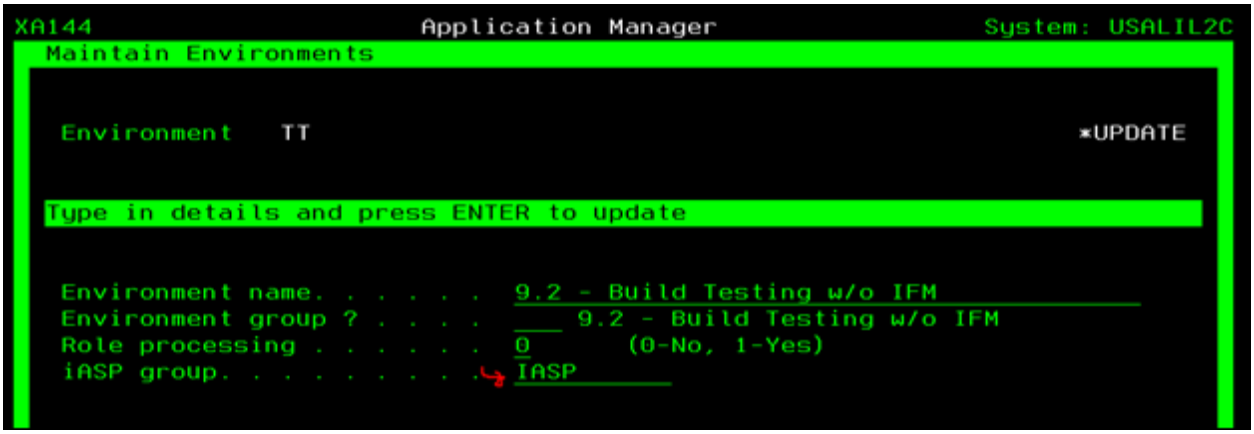
- If you receive this request, cross check whether the NLS and NLC processes are in active state or not, if not start the processes.





If you face an issue, as displayed, when launching L1 tasks, check if the environment is pointing to the correct iASP group or not by navigating to this path in System Manager Console:

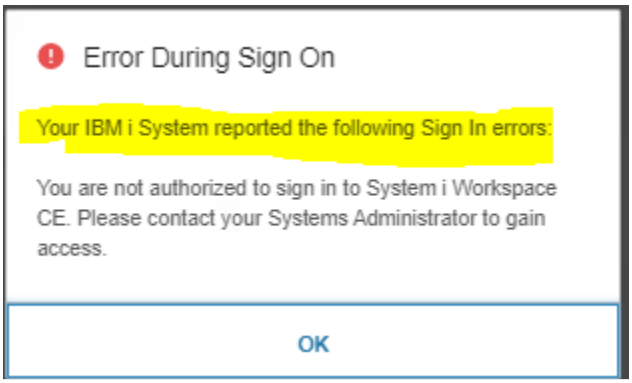
STRM400 → Application Manager → Maintain Environments



Due to maintenance activities on weekends and holidays, SiW and Net-Link related HTTP and Application servers in the IBMi Web Administration Console may go down similar to XA servers in Link Manager. You need to check and start them if you face any issues while launching SiWA application.

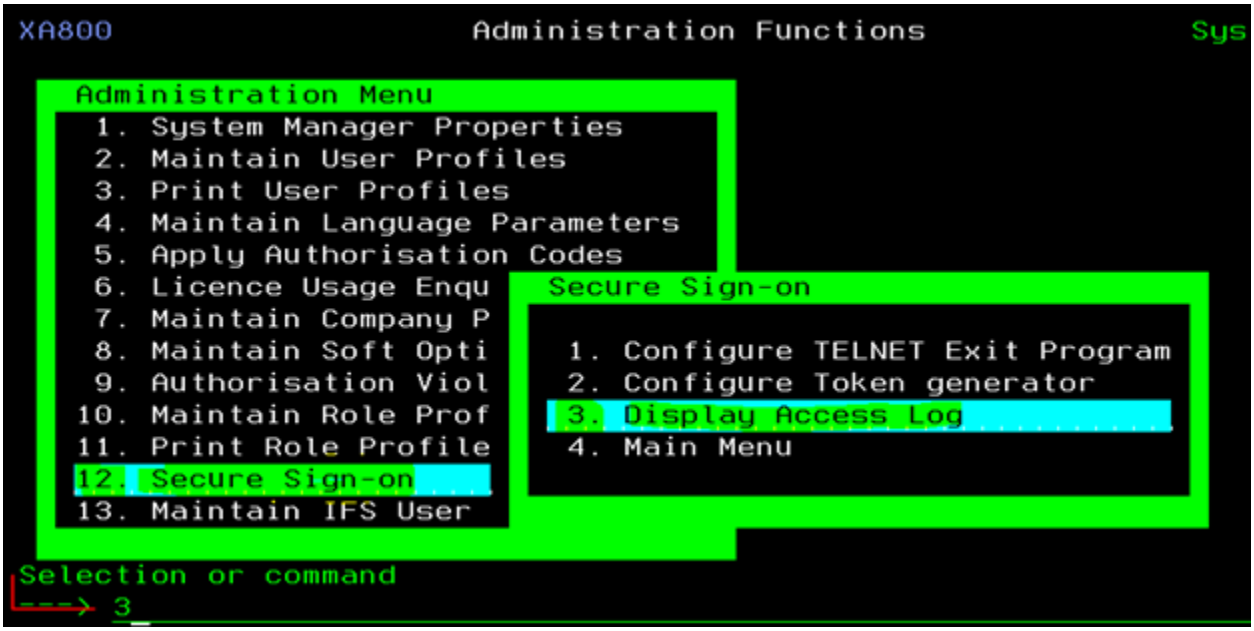
To secure Net-Link and launch the SiWA application in Infor OS, the Globals for the XA server must be on 9.2. If the globals are on 9.1, then the user cannot download Net-Link.war file and will fail to secure the Net-Link on SiWA. We do not recommend that you run SiWA on Infor OS without securing Net-Link.

- If the client system is getting blocked at System Manager (SIM) or if you are receiving this error while accessing SIWA environments with or without SSO, you must add the IPv4 address of the client system in the allowed clients at SIM.



- Navigate to **STRM400 → Administration Functions**

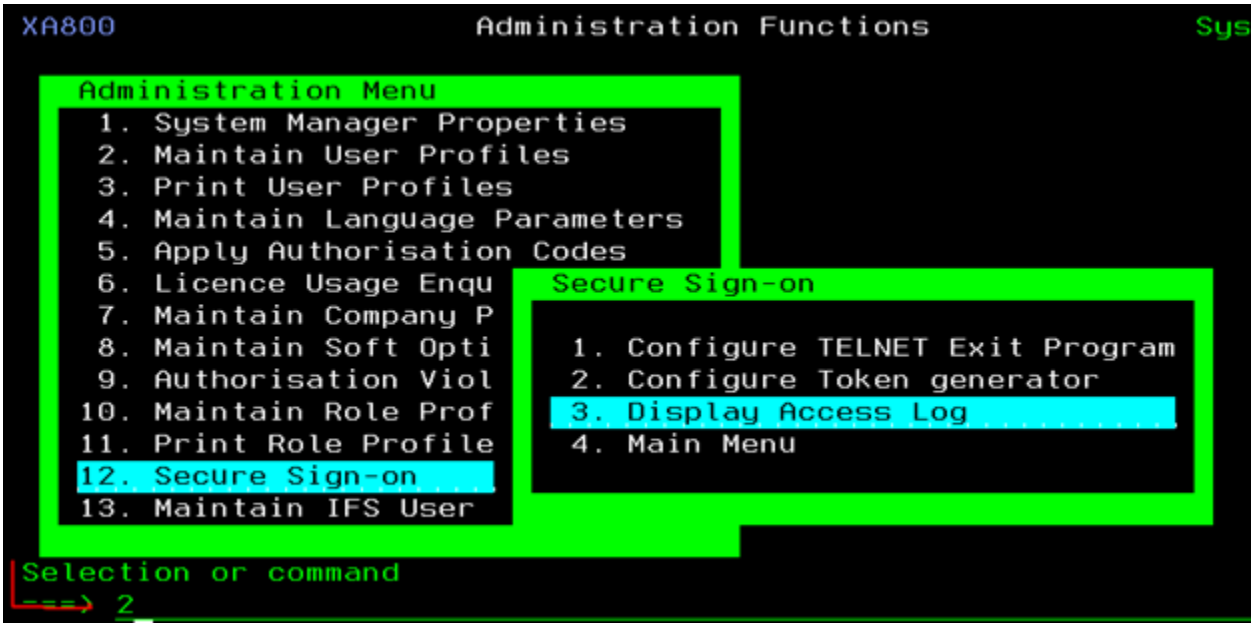
- Navigate to **Secure Sign-on option → Display Access Log**



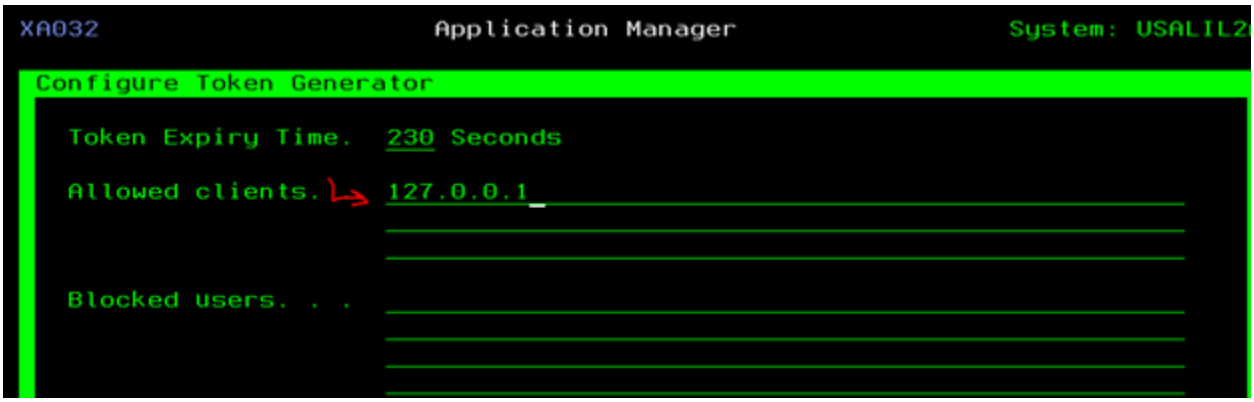
- Identify and copy the client IPv4 address with result as blocked, as displayed.

  For example: 127.0.0.1

- Press **F3** to exit.
- Navigate to **Secure Sign-on option → Configure Token generator**

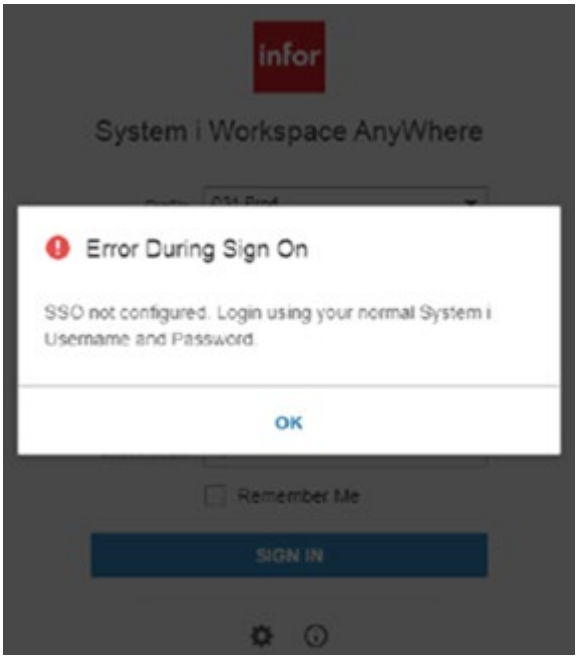


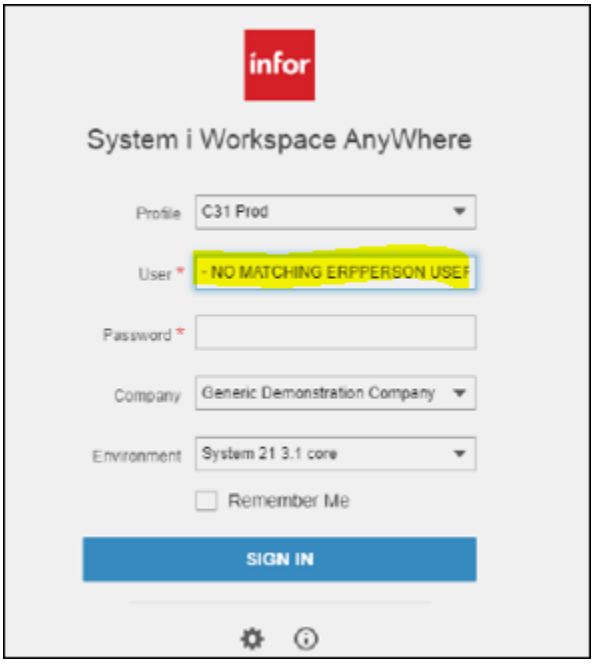
- Update the Client IPv4 address at Allowed clients, as displayed.



- Press **F8** to update.
- Press **F3** to exit.

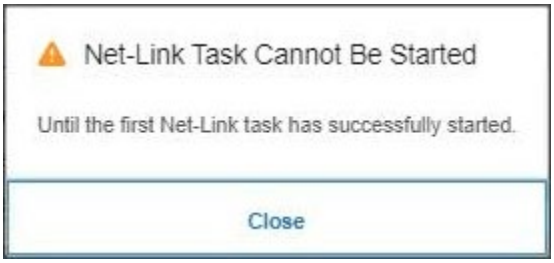
- If, on launching the XA application from InforOS, you see a blank screen or one, or both, of these screens, then Single Sign-On (SSO) is not correctly configured in InforOS, System Manager, SiWA, or all three.





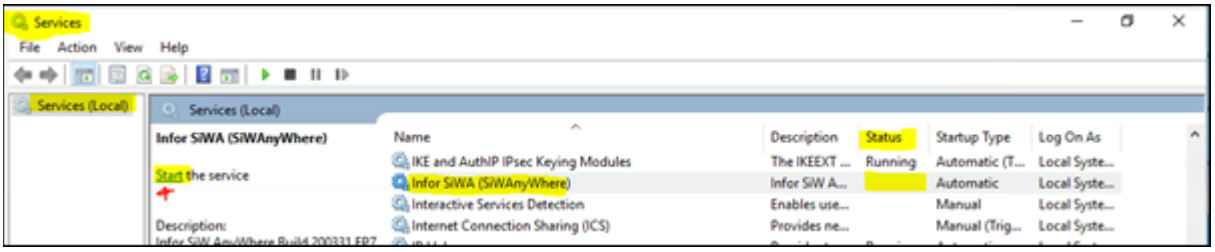
Note: Ensure that you have already tested SiWA as a stand-alone application, from a client PC, and resolved any issues with that setup before enabling any of the SSO features.

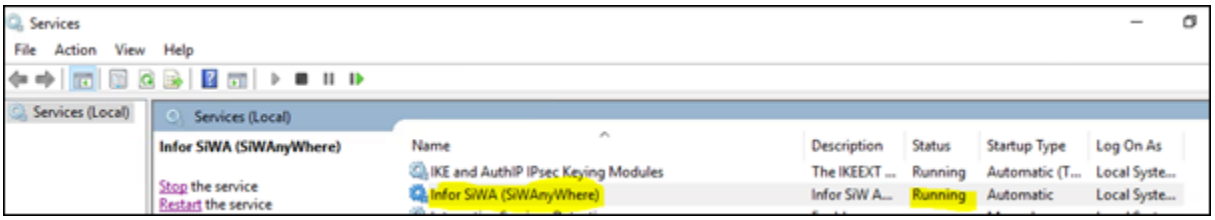
- If this message is displayed when you try to access any object in XA, you need to logout of SiWA environment and login to Net-Link environment of this same application. Navigate through couple of objects and check the objects in SiWA/Infor OS.



- If you encounter the error “abc.infor.com refused to connect,” where abc is SiWA installed server hostname, then review this information for your deployment.

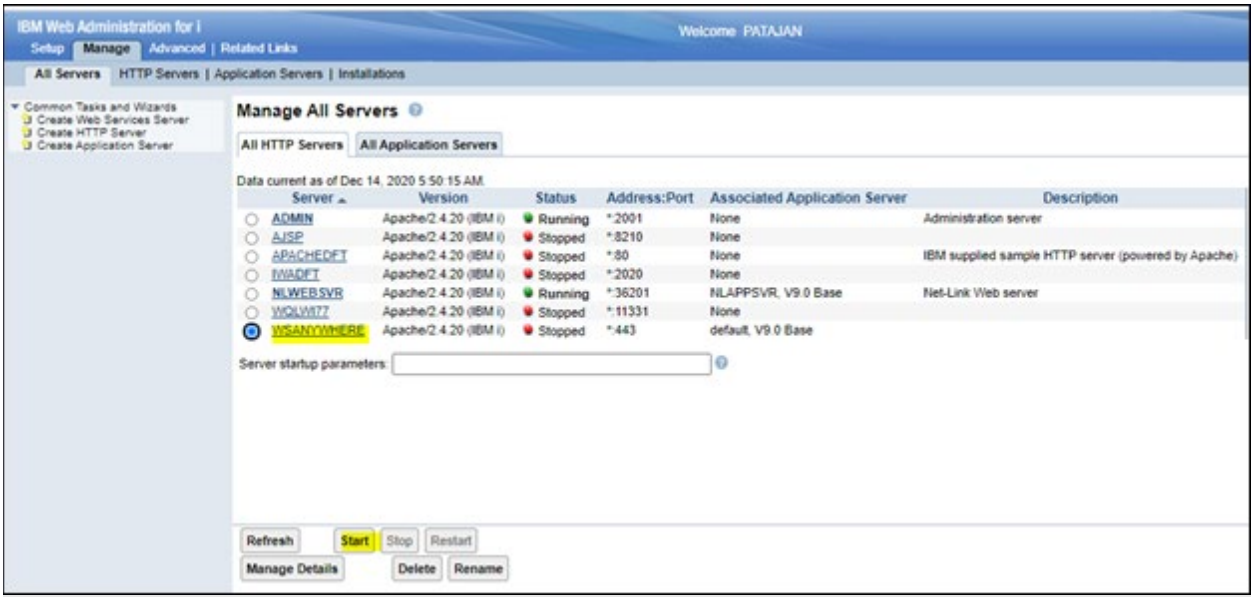
  - **For SiWA with Microsoft Windows deployment**: Login to the SiWA installed server with admin privileges, and from windows search **`open services`**, check if the Infor SiWA (SiWAnyWhere) service is in **Running** status. If not, then start the service by clicking on **Start** the service as shown.

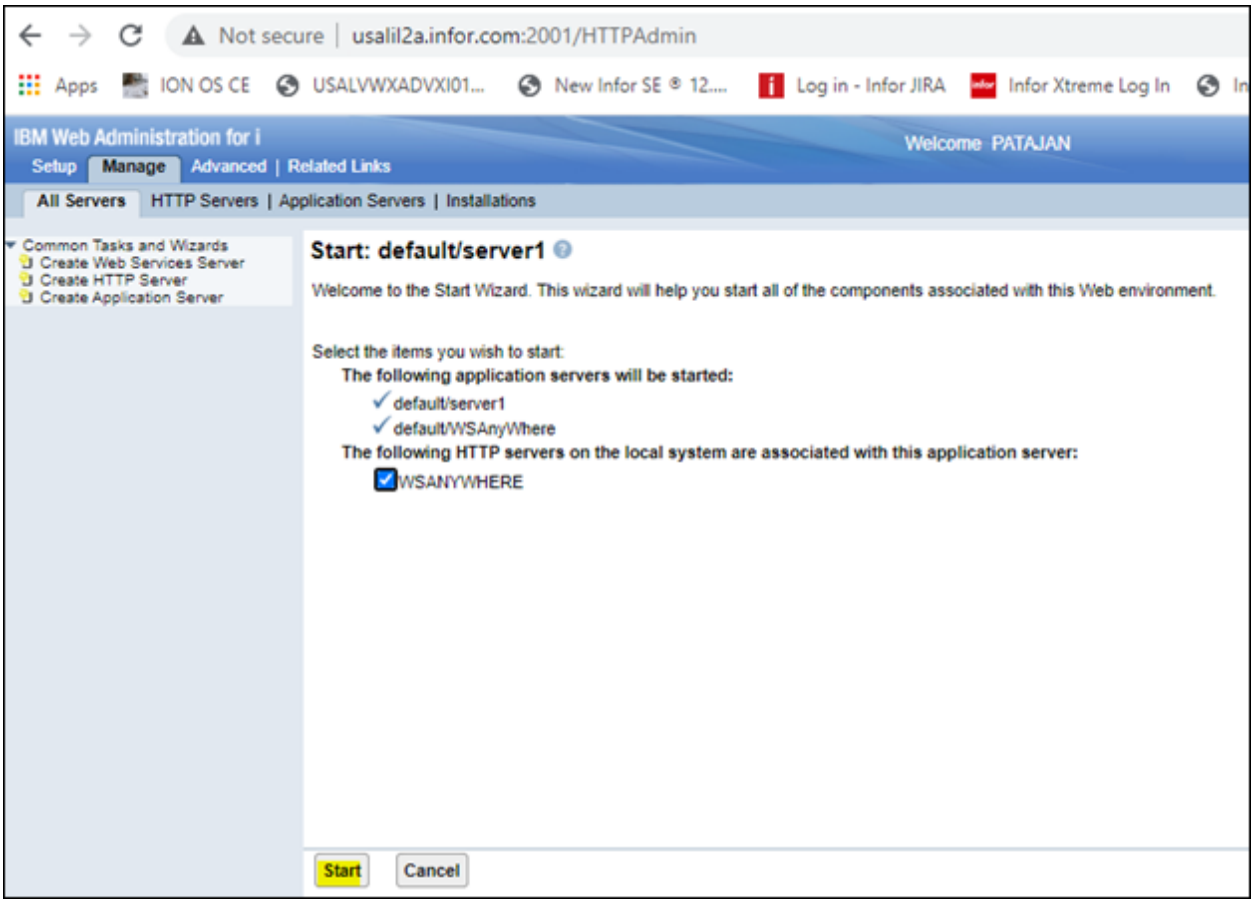




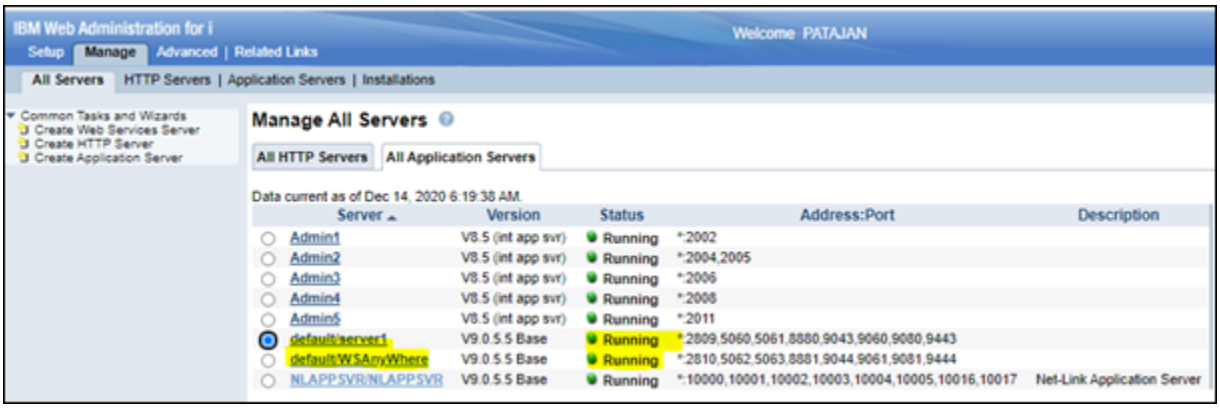
  - **For SiWA with an IBMi deployment**: Login to **IBM Web Administration** console and check if the HTTP & Application servers related to SiWA WebSphere and Net-Link are in **Running** status. If not, then start both the SiWA WebSphere and Net-Link server instances as shown.

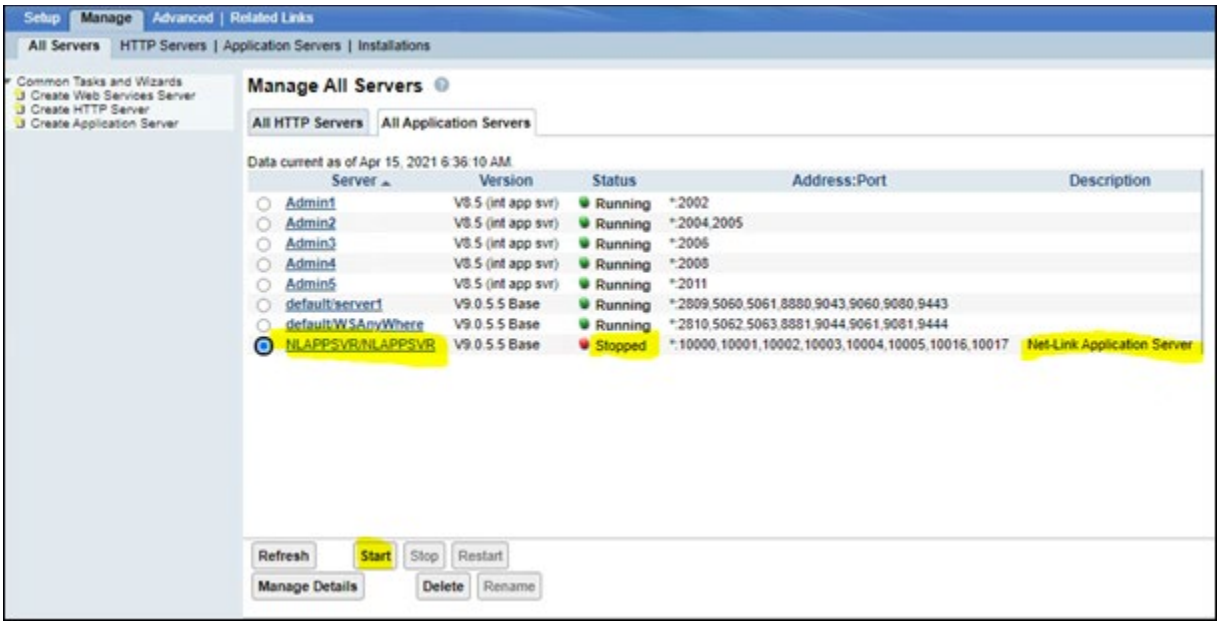
    Under **All HTTP Servers** tab, select the **SIWA WebSphere installed HTTP server** and click on **Start**.

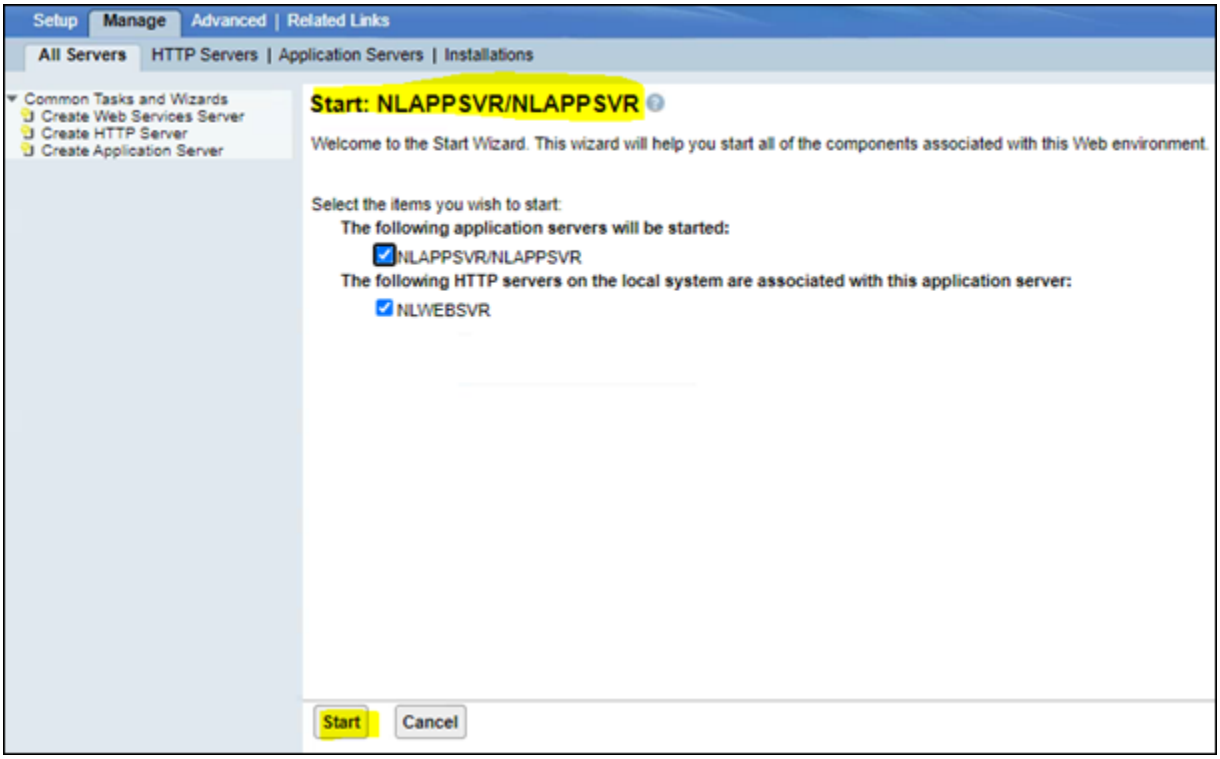

IBM Web Administration for i
Welcome PATAJAN
Setup
Manage
Advanced | Related Links
All Servers
HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Manage All Servers
All HTTP Servers
All Application Servers
Data current as of Dec 14, 2020 5:50:15 AM
Server
Version
Status
Address:Port
Associated Application Server
Description
ADMIN
Apache/2.4.20 (IBM i)
Running
*:2001
None
Administration server
AJSP
Stopped
*:8210
None
APACHEDFT
*:80
IBM supplied sample HTTP server (powered by Apache)
IWADFT
*:2020
NLWEBSVR
*:36201
NLAPPSVR, V9.0 Base
Net-Link Web server
WQLW77
*:11331
WSANYWHERE
*:443
default, V9.0 Base
Server startup parameters:
Refresh
Start
Stop
Restart
Manage Details
Delete
Rename

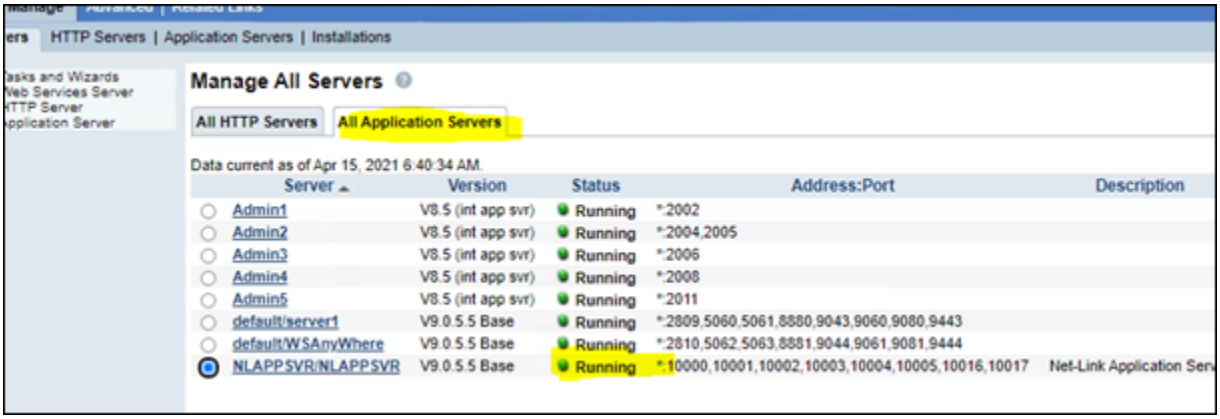

Not secure | usalil2a.infor.com:2001/HTTPAdmin
Apps
ION OS CE
USALVWXADVXI01...
New Infor SE ® 12....
Log in - Infor JIRA
Infor Xtreme Log In
IBM Web Administration for i
Welcome PATAJAN
Setup
Manage
Advanced | Related Links
All Servers
HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Start: default/server1
Welcome to the Start Wizard. This wizard will help you start all of the components associated with this Web environment.
Select the items you wish to start:
The following application servers will be started:
default/server1
default/WSAnyWhere
The following HTTP servers on the local system are associated with this application server:
WSANYWHERE
Start
Cancel

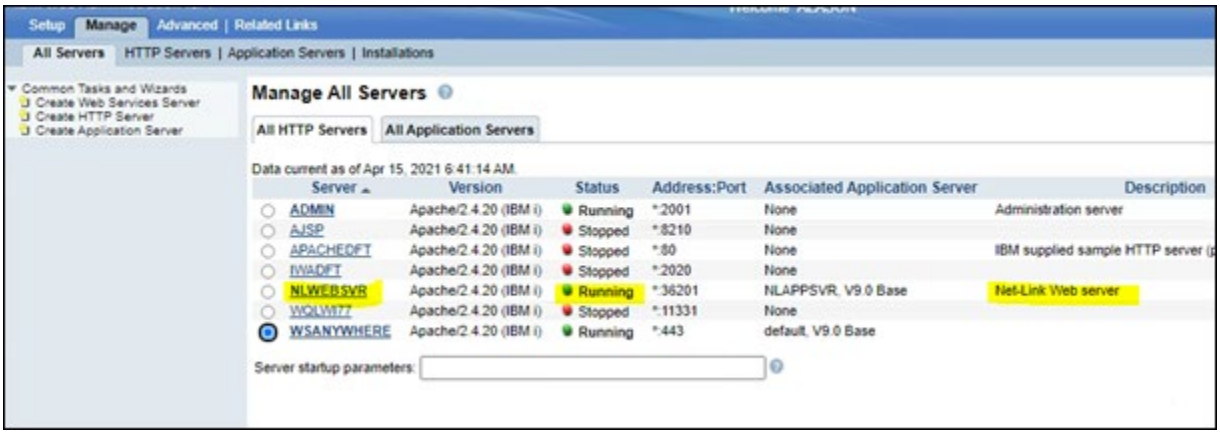

Not secure | usalil2a.infor.com:2001/HTTPAdmin
IBM Web Administration for i
Welcome PATAJAN
Setup | Manage | Advanced | Related Links
All Servers | HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Manage All Servers
All HTTP Servers | All Application Servers
Data current as of Dec 14, 2020 6:15:03 AM.
Server | Version | Status | Address:Port | Associated Application Server | Description
ADMIN | Apache/2.4.20 (IBM i) | Running | *:2001 | None | Administration server
AJSP | Apache/2.4.20 (IBM i) | Stopped | *:8210 | None
APACHEDFT | Apache/2.4.20 (IBM i) | Stopped | *:80 | None | IBM supplied sample HTTP server (powered by Apache)
IWADFT | Apache/2.4.20 (IBM i) | Stopped | *:2020 | None
NLWEBSVR | Apache/2.4.20 (IBM i) | Running | *:36201 | NLAPPSVR, V9.0 Base | Net-Link Web server
WOLWI77 | Apache/2.4.20 (IBM i) | Stopped | *:11331 | None
WSANYWHERE | Apache/2.4.20 (IBM i) | Running | *:443 | default, V9.0 Base
Server startup parameters:


IBM Web Administration for i
Welcome PATAJAN
Setup | Manage | Advanced | Related Links
All Servers | HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Manage All Servers
All HTTP Servers | All Application Servers
Data current as of Dec 14, 2020 6:19:38 AM.
Server | Version | Status | Address:Port | Description
Admin1 | V8.5 (int app svr) | Running | *:2002
Admin2 | V8.5 (int app svr) | Running | *:2004,2005
Admin3 | V8.5 (int app svr) | Running | *:2006
Admin4 | V8.5 (int app svr) | Running | *:2008
Admin5 | V8.5 (int app svr) | Running | *:2011
default/server1 | V9.0.5.5 Base | Running | *:2809,5060,5061,8880,9043,9060,9080,9443
default/WSAnyWhere | V9.0.5.5 Base | Running | *:2810,5062,5063,8881,9044,9061,9081,9444
NLAPPSVR/NLAPPSVR | V9.0.5.5 Base | Running | *:10000,10001,10002,10003,10004,10005,10016,10017 | Net-Link Application Server


Setup | Manage | Advanced | Related Links
All Servers | HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Manage All Servers
All HTTP Servers | All Application Servers
Data current as of Apr 15, 2021 6:36:10 AM.
Server | Version | Status | Address:Port | Description
Admin1 | V8.5 (int app svr) | Running | *:2002
Admin2 | V8.5 (int app svr) | Running | *:2004,2005
Admin3 | V8.5 (int app svr) | Running | *:2006
Admin4 | V8.5 (int app svr) | Running | *:2008
Admin5 | V8.5 (int app svr) | Running | *:2011
default/server1 | V9.0.5.5 Base | Running | *:2809,5060,5061,8880,9043,9060,9080,9443
default/WSAnyWhere | V9.0.5.5 Base | Running | *:2810,5062,5063,8881,9044,9061,9081,9444
NLAPPSVR/NLAPPSVR | V9.0.5.5 Base | Stopped | *:10000,10001,10002,10003,10004,10005,10016,10017 | Net-Link Application Server
Refresh | Start | Stop | Restart
Manage Details | Delete | Rename


Setup
Manage
Advanced | Related Links
All Servers
HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Start: NLAPPSVR/NLAPPSVR
Welcome to the Start Wizard. This wizard will help you start all of the components associated with this Web environment.
Select the items you wish to start:
The following application servers will be started:
NLAPPSVR/NLAPPSVR
The following HTTP servers on the local system are associated with this application server:
NLWEBSVR
Start
Cancel


HTTP Servers | Application Servers | Installations
Manage All Servers
All HTTP Servers
All Application Servers
Data current as of Apr 15, 2021 6:40:34 AM
Server
Version
Status
Address:Port
Description
Admin1 V8.5 (int app svr) Running *:2002
Admin2 V8.5 (int app svr) Running *:2004,2005
Admin3 V8.5 (int app svr) Running *:2006
Admin4 V8.5 (int app svr) Running *:2008
Admin5 V8.5 (int app svr) Running *:2011
default/server1 V9.0.5.5 Base Running *:2809,5060,5061,8880,9043,9060,9080,9443
default/WSAnyWhere V9.0.5.5 Base Running *:2810,5062,5063,8881,9044,9061,9081,9444
NLAPPSVR/NLAPPSVR V9.0.5.5 Base Running *:10000,10001,10002,10003,10004,10005,10016,10017 Net-Link Application Ser


Setup
Manage
Advanced | Related Links
All Servers
HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Manage All Servers
All HTTP Servers
All Application Servers
Data current as of Apr 15, 2021 6:41:14 AM
Server
Version
Status
Address:Port
Associated Application Server
Description
ADMIN Apache/2.4.20 (IBM i) Running *:2001 None Administration server
AJSP Apache/2.4.20 (IBM i) Stopped *:8210 None
APACHEDFT Apache/2.4.20 (IBM i) Stopped *:80 None IBM supplied sample HTTP server
IWADFT Apache/2.4.20 (IBM i) Stopped *:2020 None
NLWEBSVR Apache/2.4.20 (IBM i) Running *:36201 NLAPPSVR, V9.0 Base Net-Link Web server
WQLW877 Apache/2.4.20 (IBM i) Stopped *:11331 None
WSANYWHERE Apache/2.4.20 (IBM i) Running *:443 default, V9.0 Base
Server startup parameters:

Enabling debugging in System i Workspace AnyWhere

1 Locate the System i Workspace AnyWhere system.properties file as documented in the *System i Workspace AnyWhere Installation Guide*.

2 Add this property to enable SSO Debug mode in SiWA:

- **Property**: *com.infor.siw.cloud.debug*
- **Description**: Set to **`1`** to enable SSO debugging specific features of SiWA

3 Locate the server\xsl folder within your web application deployment.

4 Edit the logon-validate-global.xsl file using a text editor and change *<xsl:variable name="login-debug" select="""/>* to *<xsl:variable name="login-debug" select="'true'"/>*.

5 Save the file.

6 Locate the WEB-INF\classes folder within your web application deployment.

7 Edit the log4j.xml file using a text editor and change *<Root level="warn">* to *<Root level="debug">*.to

8 Save the file and restart SiWA to apply these changes.

Note: You may want to clear or backup any existing log files at this point.

The next time a user logs into SiWA through InforOS, debugging information is written to the Standard Output log file of your web application or server.

Enabling debugging of the identify provider

1 Locate the fedlet_config folder. If you followed the instructions in this document, this folder is in the root directory of your SiWA server.

2 Edit the FederationConfig.properties file contained within this folder using a text editor and locate this line: *com.iplanet.services.debug.level=error.*

3 Change the *com.iplanet.services.debug.level* setting to one of **`off`**, **`error`**, **`warning`**, or **`message`**.

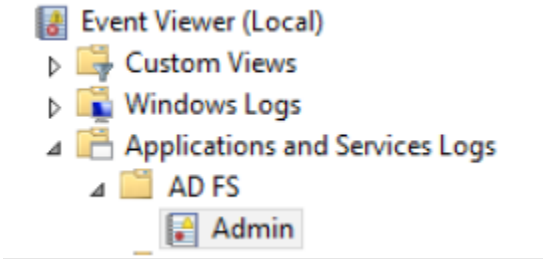
4 Save the file and restart SiWA to apply the change.

Note: You may want to clear or backup any existing log files at this point.

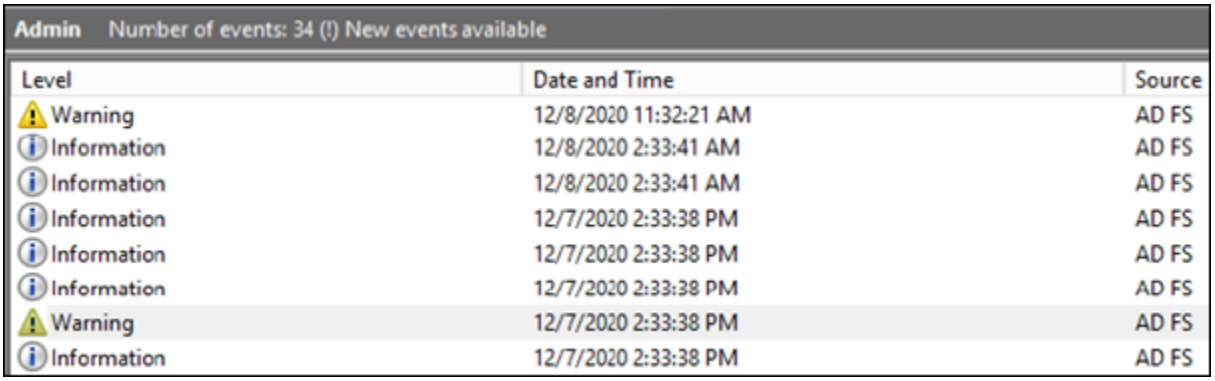
The next time a user logs into SiWA, via InforOS, debugging information is written to the debug folder located under the fedlet_config folder.

Viewing debugging on the ADFS server

1 Within the Windows Event Viewer locate the Applications and Services Logs > AD FS > Admin as shown.



2 Review all events with a logging level of Error.



Additional troubleshooting

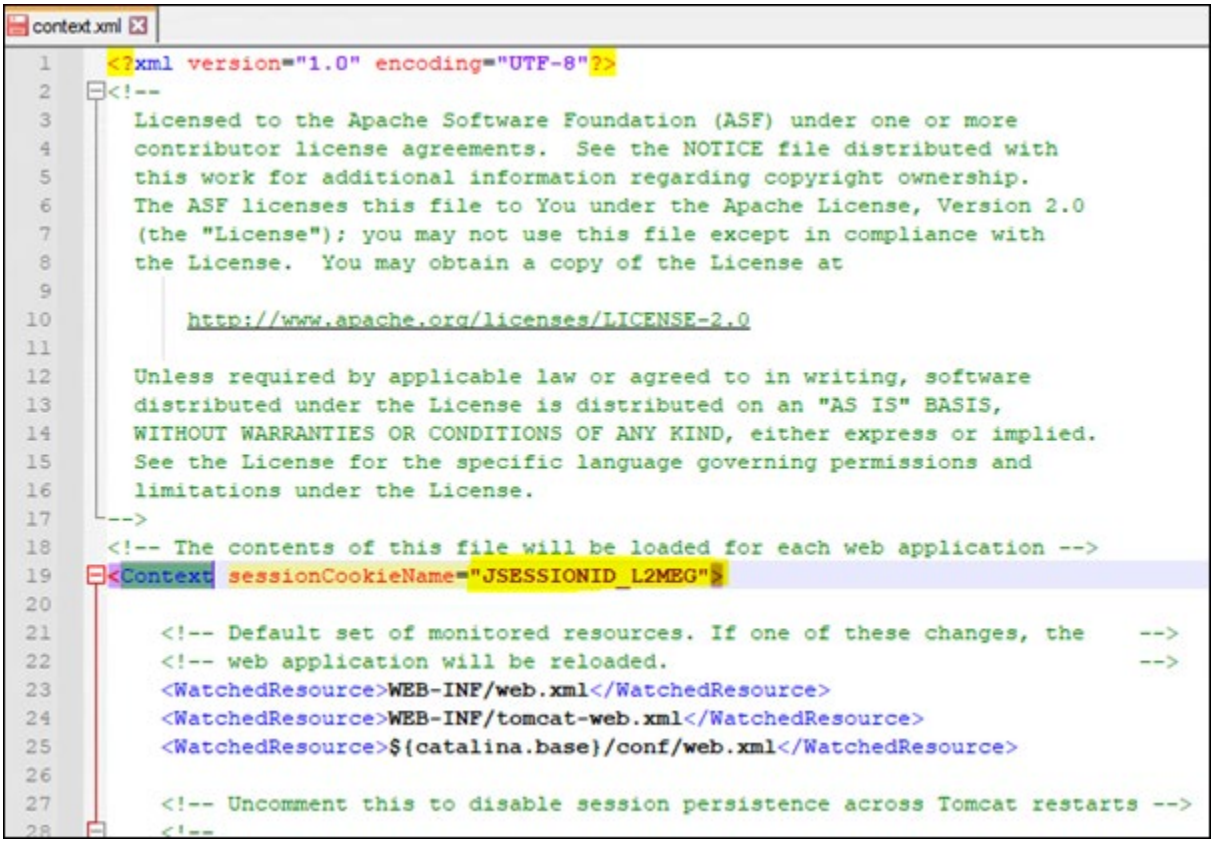
For any additional troubleshooting steps, see “Troubleshooting Techniques” in the *System i Workspace AnyWhere Installation & Administration Guide*.

Appendix E Multiple SiWA installations on a single Windows server

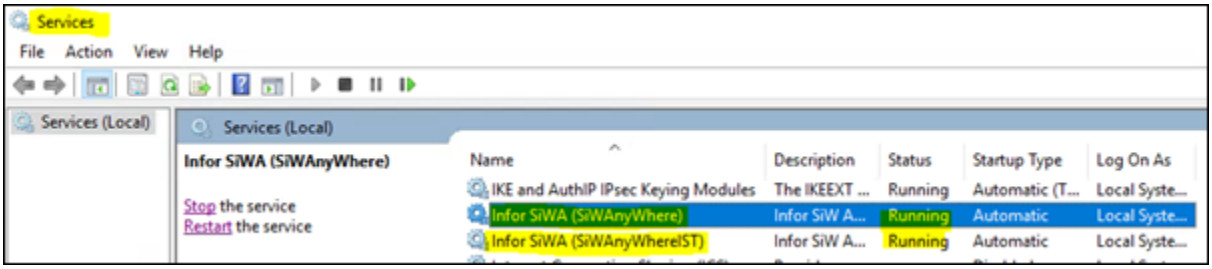
If you want to install and run multiple instances of SiWA on a single Windows server using unique ports for each individual installation, follow these additional settings for each SiWA installation.

1 Navigate to SiWA Installation folder. For example, /tomcat/conf/context.xml file.

2 Edit the context.xml file and change <*Context*> to <*Context sessionCookieName="JSESSIONID_{environmentID}"*> where *{environmentID}* is the ID of the environment.



3 Restart the SiWA Windows server and ensure that the status of SiWA services is running post server restart.


Services
File Action View Help
Services (Local)
Services (Local)
Infor SiWA (SiWAnyWhere)
Stop the service
Restart the service
Name
Description
Status
Startup Type
Log On As
IKE and AuthIP IPsec Keying Modules
The IKEEXT ...
Running
Automatic (T...
Local Syste...
Infor SiWA (SiWAnyWhere)
Infor SiW A...
Running
Automatic
Local Syste...
Infor SiWA (SiWAnyWhereIST)
Infor SiW A...
Running
Automatic
Local Syste...

Appendix F Multiple SiWAW WebSphere installations on a single IBMi server

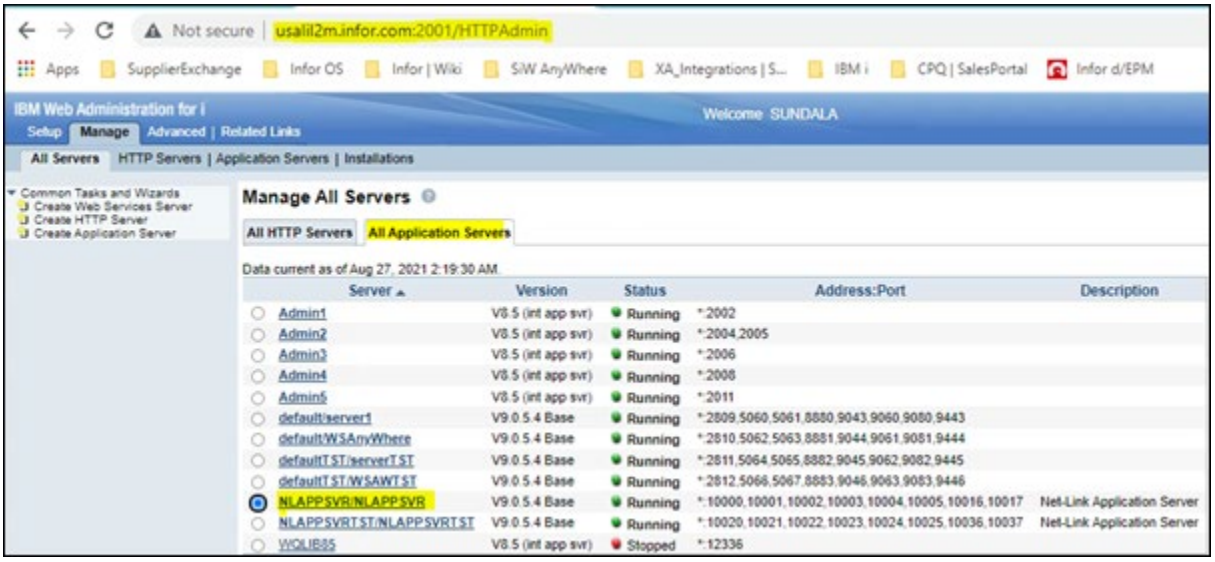
If you want to install and run multiple instances of SiWA WebSphere on a single IBMi server using unique ports for each individual installation, follow these additional settings for each SiWA installation.

1 Log in to IBMi Web Administrator for i using this URL, where <*hostname*> is the FQDN of the IBMi server:

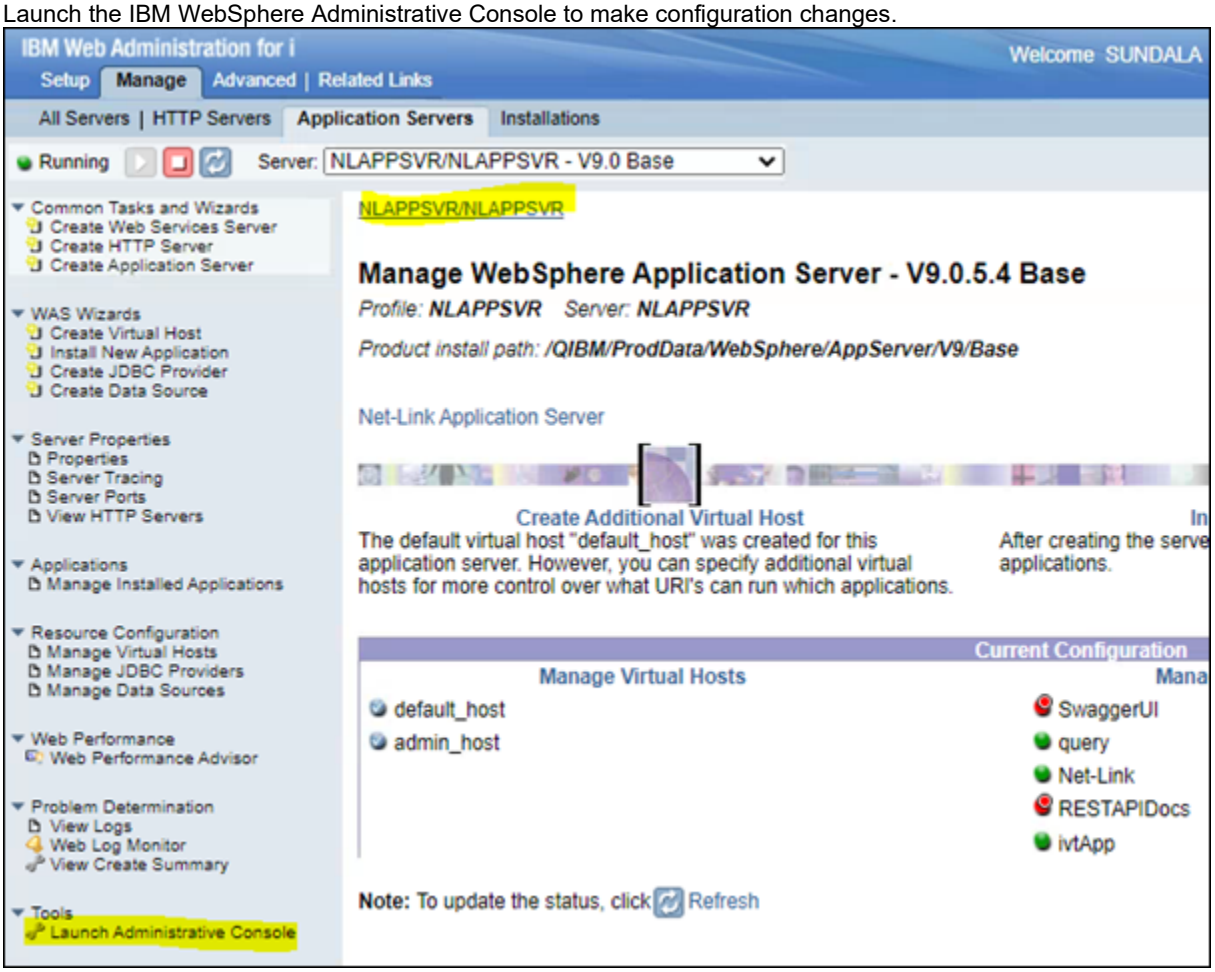
http://<hostname>:2001/HTTPAdmin

For example: *http://usalil2m.infor.com:2001/HTTPAdmin*)

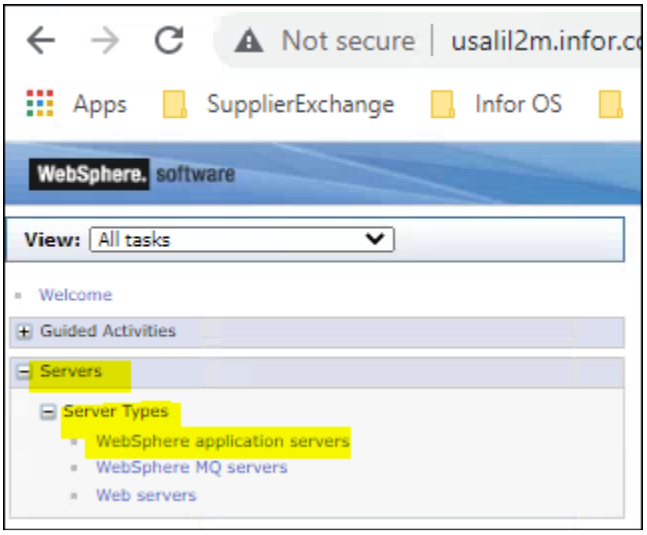
2 Navigate and select the Net-Link WebSphere Application server, which is used for securing Net-Link.



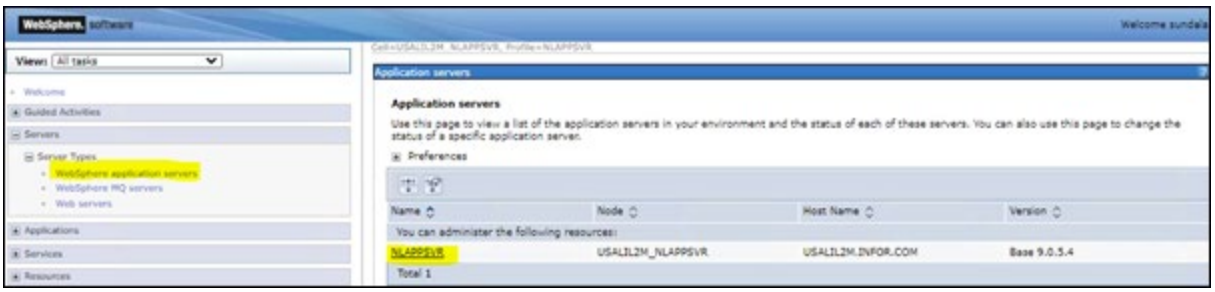
Launch the IBM WebSphere Administrative Console to make configuration changes.

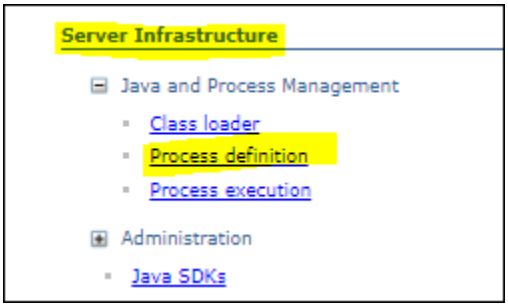


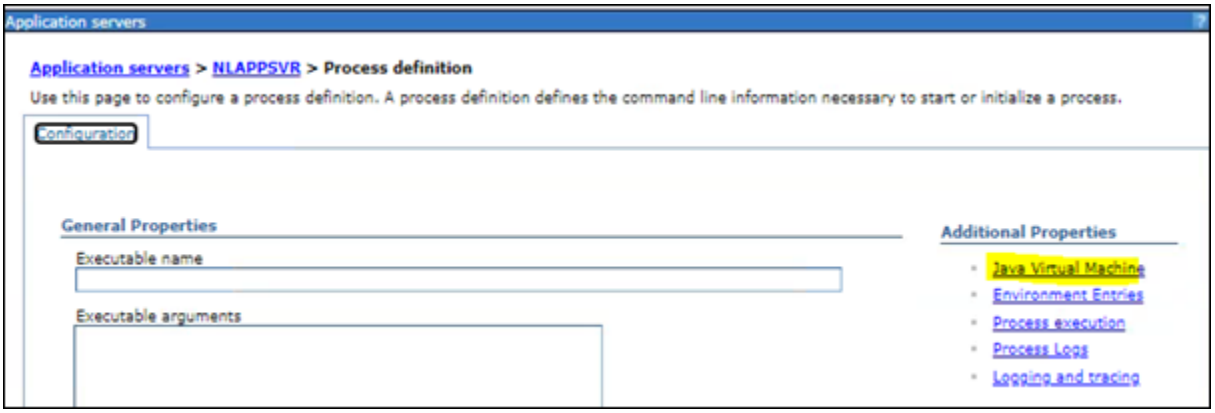
3 From the menus, select **Servers > Server Types > WebSphere Application Servers**.

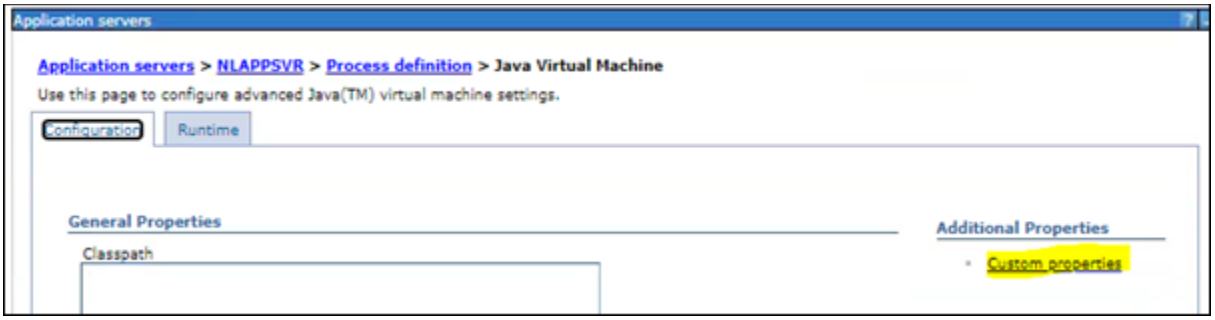


4 Click on the Net-Link configured **WebSphere Application server**, and then navigate to **Server Infrastructure > Java and Process Management > Process Definition > Java Virtual Machine > Custom Properties**.

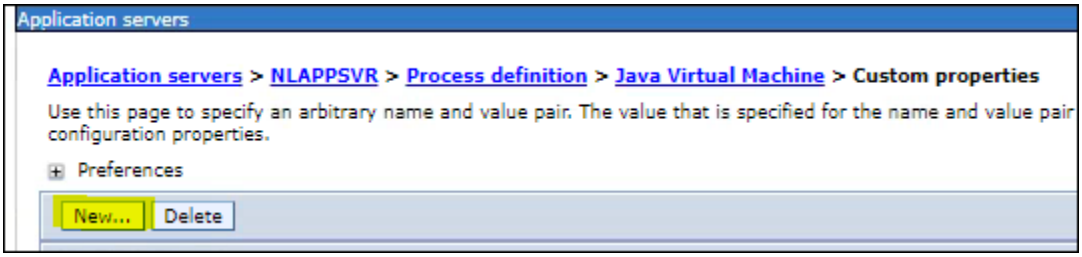








5 Click **New** and add a new Custom Property for the JVM to reuse the sessionId.



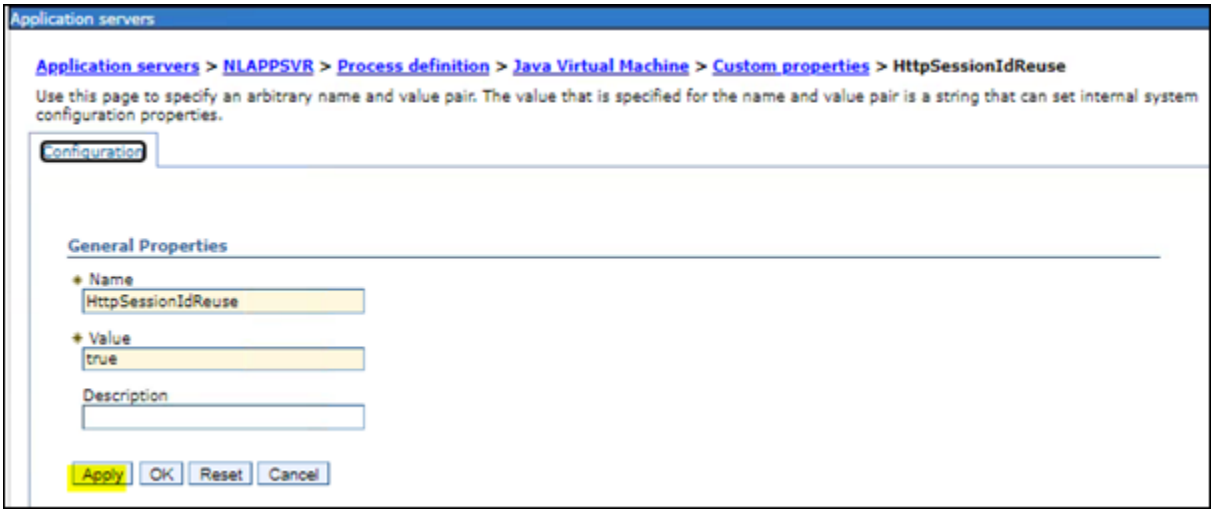
6 Specify this information:

Name

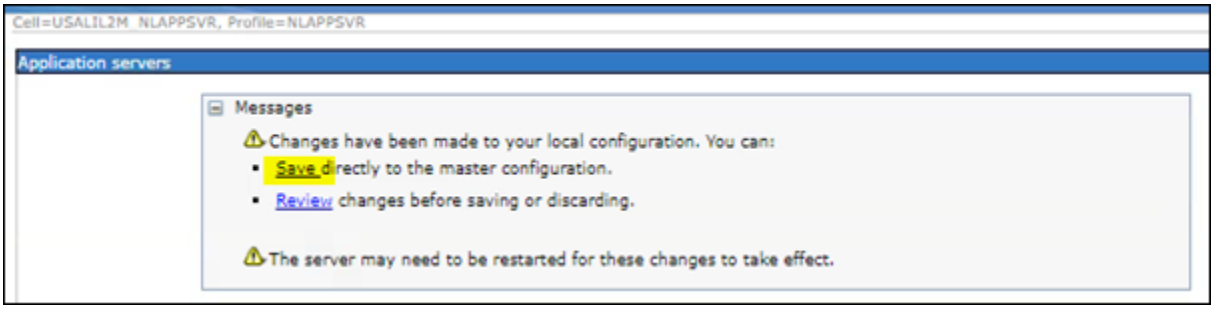
Specify **`HttpSessionIdReuse`** for the name of the system property.

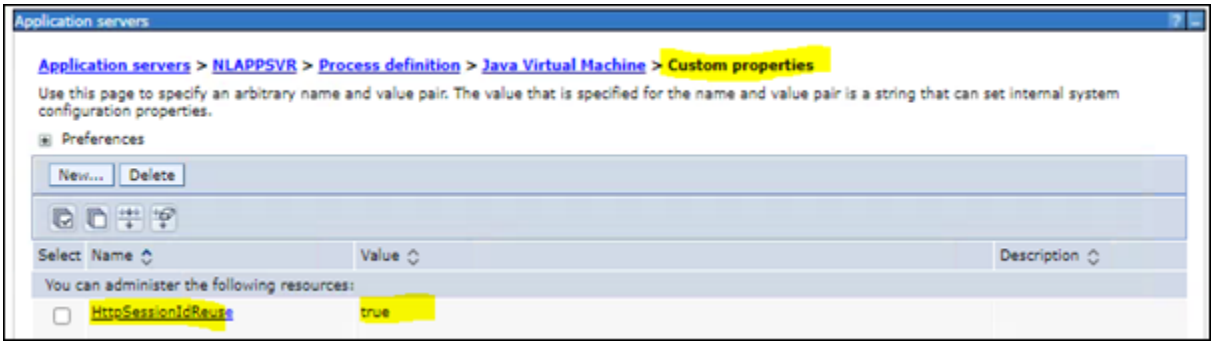
Value

Specify **`true`** for the value of the system property.



7 Click **Apply**, and then save your changes and restart the Application Server.





Note: SSO cannot be implemented for the second instance of SiWA, as we are using single WebSphere for 2 SiWA, which is a limitation.