Infor XA Configuration Guide for Infor OS Portal using SiW AnyWhere

Infor XA 9.2,10.0 & 11.0
Infor OS Portal

Publication Information

Release: Infor XA 9.2,10.0 & 11.0

Publication date: August 7, 2025

Contents

About this guide

This document describes the integration of Infor XA On-premises with Infor Operating Service Portal (Infor OS Portal) using System I Workspace AnyWhere (SiWA). This guide explains the integration requirements, installations, configuration tasks and troubleshooting information.

Intended audience

This guide is intended for the system administrator or customer service consultant who configures the integration between System i Workspace AnyWhere and Infor OS Portal.

Required knowledge

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

Before you read this guide, ensure that you are familiar with the other guides listed in "**Related documents**".

Related documents

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

- Infor System Manager Quick Installation Guide for Infor XA
- Infor IDF Setup Guide for Secure Net-Link
- Infor OS Portal Administration Guide
- Infor OS Portal User Guide
- Infor Si System Manager Installation Guide
- System i Workspace AnyWhere Installation & Administration Guide
- *KB1365947* – Need Authorization codes
- *KB1136739* – System Manager and Work Management PTFs
- *KB1963350* – 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.

If we update this document after the product release, we will post the new version on the docs.infor.com.

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

Chapter 1 Introduction

Infor OS Portal is an application framework that provides a common user interface for integrated Infor ERP applications.

The navigation panel accesses several elements of the Infor OS Portal. This includes the navigation menu, used to display Infor ERP applications.

The smart panel is a collapsible tray that hosts contextual and non-contextual widgets. The widgets display content based on application screen data to help users work smarter. You can share content between widgets.

Users can customize their experience with Workspaces by creating shortcuts to frequently used application screens and widgets.

Additionally, Infor OS Portal supports drill-back capability among Infor applications. Users can navigate from one application to another to track transactions, transfer data, and report updates.

System i Workspace AnyWhere (SiWA) is the user interface for XA. This document describes the process to launch System i Workspace Anywhere from within Infor OS. Consequently, the benefits for both systems are enhanced. With this integration, the user interface of Infor XA can be accessed as an application in Infor OS Portal.

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
- Infor System i Workspace Anywhere (SiWA), an intermediate layer. This is required because XA user interface is not displayed directly within the frame of Infor OS Portal. SiWA receives information about XA from System i Manager (SiM). As part of the configuration, you export XA tasks, menus, and users to SiM.
- Within SiWA, Net-Link, and 5250 Emulator user interfaces are supported by XA.

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

This is the recommended sequence for a complete installation and

configuration:

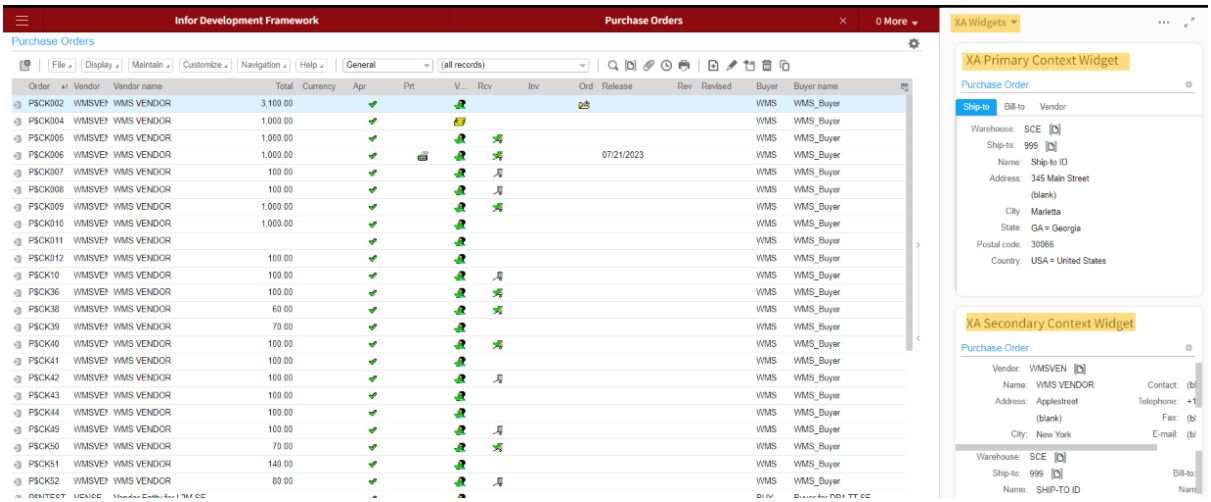
1 Infor XA server and client with Net-Link

2 Infor System i System Manager

3 Infor System i Workspace AnyWhere

4 Infor Operating Service (OS) Portal

The screenshot displays the System i Workspace AnyWhere in Infor OS Portal:


Infor Development Framework
Purchase Orders
0 More
Purchase Orders
XA Widgets
XA Primary Context Widget
Purchase Order
Ship-to
Bill-to
Vendor
XA Secondary Context Widget
Purchase Order

Chapter 2 Requirements

This chapter describes the requirements for configuring Infor XA within Infor OS Portal using SiWA.

Infor XA Server and Client with Net-Link Requirements

When XA is installed and configured with an available IBMi, you must install System Manager on each IBMi which runs XA environments that you intend to use in System i Workspace or Infor OS Portal.

- 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 9.2.2.3 client software build must be 02.09.02.02.61 or higher.
- Infor XA IDF 9.2.2.3 server PTFs is PCM SH SH16252 (XA 9.2.2.3 with PTF level 25457).
- Infor XA IDF 10.0.1.1 client software build must be 03.10.00.01.34 or higher.
- Infor XA IDF 10.0.1.1 server PTFs is PCM SH16275 (XA 10.0.1.1 with PTF level 00502).
- Infor XA IDF 11.0.0 client software build must be 03.11.00.01.01 or higher.
- IBMi standard software set option 5770SS1: Option 8 – AFP Compatibility Fonts (required for TIFF image support).
- IBMi standard software set option 5770TS1 on V7R3/R4 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 (with latest PTFs applied)

  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 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. By default, the profile name of this profile is called “default” and the server “server1”.

Infor System i System Manager Requirements

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

To install and perform required setup on SiM, Sign on to your iSeries as **QSECOFR** or a user with ***SECADM** and ***ALLOBJ** authority.

Caution: QSECOFR or any other IBMi supplied user profile that starts with ‘Q’ or ‘q’ are not allowed to access XA application via Single Sign on through SiWA. The IBMi supplied user profiles are for IBMi administration purpose. It is not recommended to perform IBMi administration from SiWA or Infor OS Portal.
You can create users with different names and provide them required SECOFR authority to use them with SiWA or Infor OS Portal, if there is any valid business needed.

Infor System i Workspace AnyWhere Requirements

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

Note: System i Workspace AnyWhere with latest Feature/Fix Packs and latest Tomcat Upgrade if Windows Deployment need to be used.

To understand the Software, Hardware, and Security requirements or recommendations for SiW AnyWhere installation and configuration, please refer to Chapter 2 Preparing for the installation from ***System i Workspace AnyWhere Installation & Administration Guide.***

Refer the Chapter 8 Client settings **in *System i Workspace AnyWhere Installation & Administration Guide*** for specific configuration that may be required for the client browsers.

Infor Operating Service Portal Requirements

You are expected to have latest version of Infor OS Portal provisioned with all required applications and Authorizations.

Client prerequisites

This section describes the software requirements for clients of the Infor OS Portal.

Refer to Chapter 2: Accessing Infor OS Portal from ***Infor OS Portal User Guide*** for details on supported browsers and recommended client settings.

Chapter 3 Installation

This chapter provides information on System Manager and System i Workspace AnyWhere installations.

Installing System Manager

For the complete set of instructions required to install System Manager, see *the* ***Infor System Manager Quick Install Guide for Infor XA*** in the Docs.infor.com.

Note: For additional information, refer to the ***Infor Si System Manager Installation Guide***.

Installing System i Workspace AnyWhere

Microsoft Windows deployment

For installation and configuration of SiW AnyWhere on Tomcat Web Server, refer to Chapter 4 Installation instructions in ***System i Workspace AnyWhere Installation & Administration Guide*** and follow all the steps mentioned in Microsoft Windows deployment section.

For Secure Sockets Layer (SSL) configuration, follow the process described in the Secure Sockets Layer (SSL) section in Chapter 14 Security in the ***System i Workspace AnyWhere Installation & Administration Guide***.

Note: If you want to install and run multiple instances of SiW AnyWhere Tomcat in a single Windows server using unique ports for each individual installation, please follow the required additional settings mentioned in Appendix E in this guide.

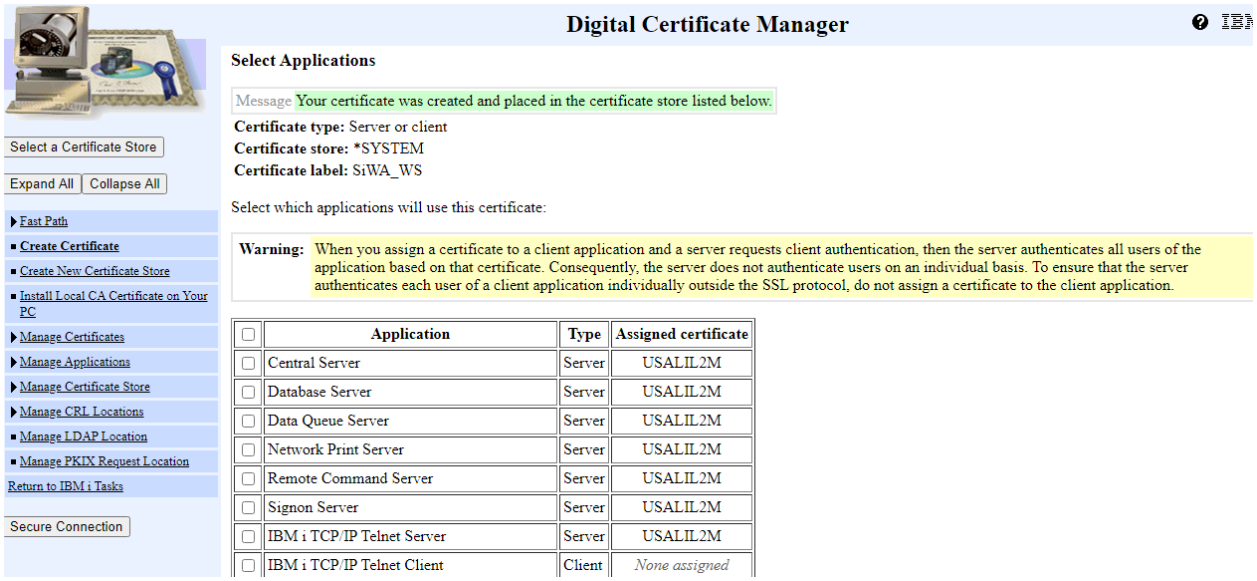
IBMi deployment

For installation and configuration of SiW AnyWhere to run on WebSphere Application Server, refer to Chapter 4 Installation instructions in ***System i Workspace AnyWhere Installation & Administration Guide*** and follow all the steps related to IBMi deployment section.

For Secure Sockets Layer (SSL) configuration, follow the process described in the Secure Sockets Layer (SSL) section in Chapter 14 Security in the ***System i Workspace AnyWhere Installation & Administration Guide***.

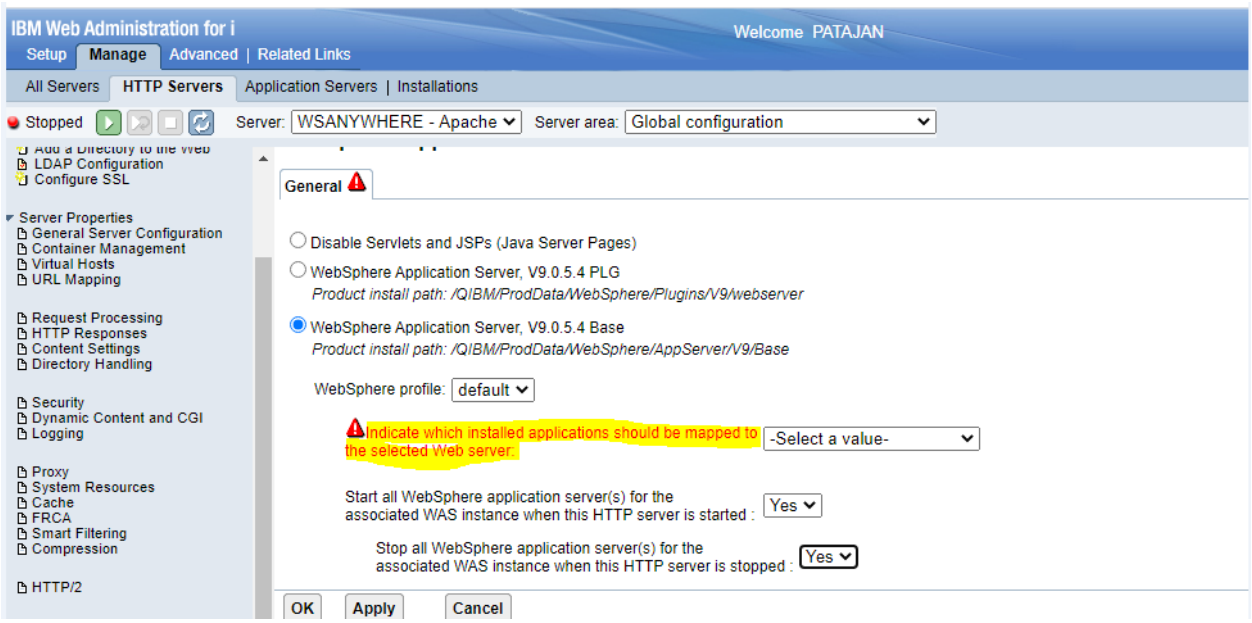
Refer these for any issues or missing steps observed during this deployment process:

- When working on step no 6, in Creating a local Certificate of Authority section, if you observe "**Select Applications**" page that requests to ***Select which applications can use the certificate***, as displayed in the screenshot, then select all the applications having XA IBMi server in "**Assigned Certificate**" Column. For example, select all applications having "USALIL2M" in "Assigned Certificate" column as displayed.



- When working on step no 34, in ***Creating an IBM HTTP Server instance*** section, if the "**default**" WebSphere profile is not displayed in the drop down of the application, then refer Appendix B in this guide and create the "**default"** profile in WebSphere.

- After selecting the “default” WebSphere profile, if application displays a message as “**Indicate which installed application should be mapped to the selected Web Server**”, select the value as **'Default Applications only**'.



- After successful installation of SiW Anywhere on WebSphere, if you encounter “**Internal Server Error**” when you try to launch the SiW AnyWhere for the first time, then refer Appendix C in this guide.

Note: If you want to install and run multiple instances of SiW AnyWhere WebSphere in a single IBMi server using unique ports for each individual installation, please follow the required additional settings mentioned in Appendix F in this guide.

Integration datasheet

During the installation and the configuration tasks, you are prompted for information. Print the data listed in this table and fill in the information that is applicable:

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

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 logins, before you begin the installation. The remaining data can be filled in the data sheet as you proceed through the installation to ensure that you have the data when prompted.

Provisioning Infor OS Portal

It is recommended to use XA with System i Workspace using Infor OS Portal. You can use XA with System i Workspace but without Infor OS Portal. You can omit the Infor OS Portal provisioning and configuration but complete the other steps: install System Manager, install System i Workspace and the export of the metadata. You can then access System i Workspace directly using standalone URL as described in the System i Workspace documentation. Even if you plan to use Infor OS Portal, you must verify the System i Workspace function.

Chapter 4 Post installation

This chapter provides the post-installation information for System i Workspace AnyWhere.

System i Workspace AnyWhere

Each of the tasks in this section refers to the ***System i Workspace AnyWhere Installation & Administration Guide*** that can be accessed from docs.infor.com.

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***.

Note: Validate both SiWA admin and install verify url after successful installation.

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

Note: If SiWA admin page is not loading properly when you hit above url, then follow the Appendix G in this guide.

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

Note: If an Internal Server Error message is displayed on screen when above URL is hit, then follow Appendix C in this guide.

iASP

If your XA Environment is on an iASP, execute these processes to ensure whether iASP group is set to the right iASP :

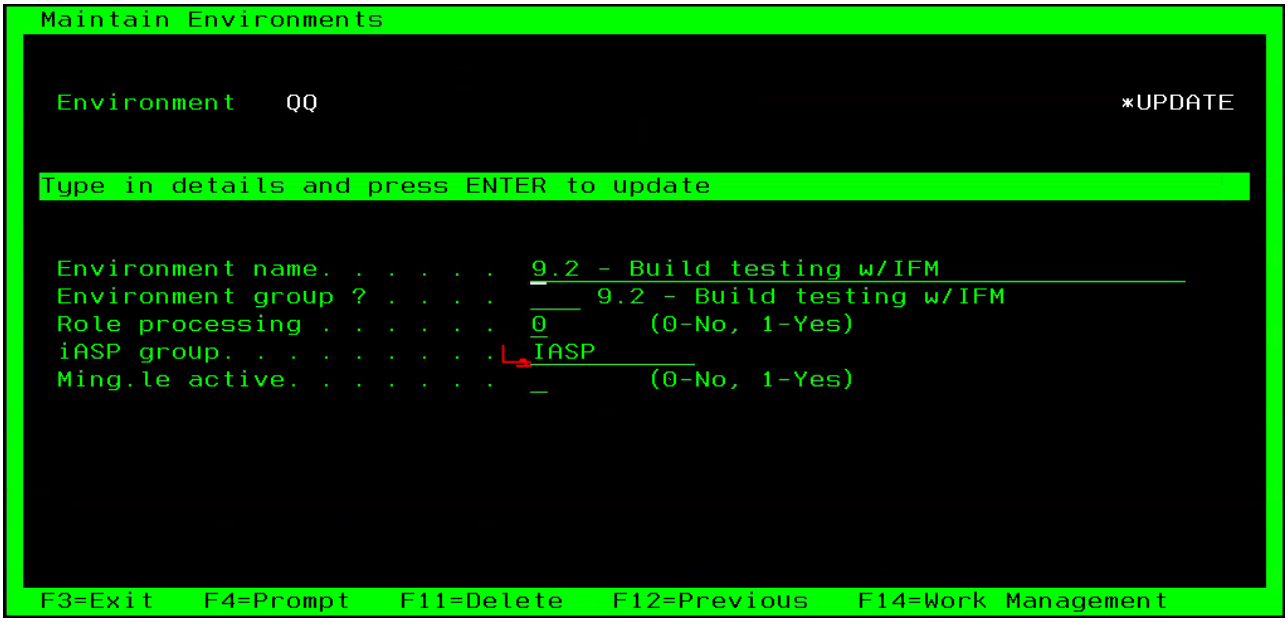
1 Specify STRM400 on the AS400 screen to start the System Manager.

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 right iASP.



Securing Net-Link and Secure Socket Layer (SSL) configuration

The standard installation process involves secure socket layer (SSL) configuration and accessing the Net-Link through a URL to the IBMi due to which users are confined to a secure network.

Microsoft Windows deployment

To configure the secured Net-Link application on Tomcat refer to *Chapter 3 Net-Link WAR file Generation and Deployment on Tomcat* in the ***Infor IDF Setup Guide for Secure Net-Link** guide*.

IBMi deployment

The recommended way of accessing Net-Link web server components is using Reverse Proxy configuration on IBM HTTP server.

The reverse proxy implementation is simple to set up and easy to maintain. Unlike WAR deployments, it does NOT require generating and redeploying Net-Link WAR files whenever WAR updates or changes are delivered with fixes. To implement above deployment, refer to

Chapter 2 Reverse Proxy configuration in IBM i HTTP Server to access default Net-Link in the ***Infor IDF Setup Guide for Secure Net-Link*** *guide*. Using

Client Settings

This section explains about the client settings that need to be configured on each client PC that accesses the System i Workspace AnyWhere. Follow the procedure described in Chapter 9 Client Settings in the ***System i Workspace AnyWhere Installation & Administration Guide***.

System i Workspace Profiles

It is recommended that you set one System i Workspace AnyWhere Profile for each XA Environment to be configured.

This means that for each System i Workspace AnyWhere Profile, only one Environment is configured, and this one profile relates back to one application inside Infor OS Portal. Currently, the Tenant is used, which is associated with each Infor OS Portal application to link back to the XA Workspace profile.

Chapter 5 Exporting Metadata

This section describes steps that are required to export the metadata from IDF to SiW. This metadata describes the card and card files and the contents in IDF. This 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. On the green screen, specify **STRXA** at the command to start your XA environment, and select the correct 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:

- Login with a user ID that has supplemental group authority AULUSER and AULSECOFR.
- System Manager and SiW PTFs must be the latest.

Exporting metadata from IDF to Workspace

After installation, the users need to export the metadata from IDF to SiW. The metadata describes the card and card files and the contents in IDF. It is used by SiW to construct the menus and the options.

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 which 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 must use Power-Link to invoke the Export process.

Exporting 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 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. Else, authorization to access the menu is no longer 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:

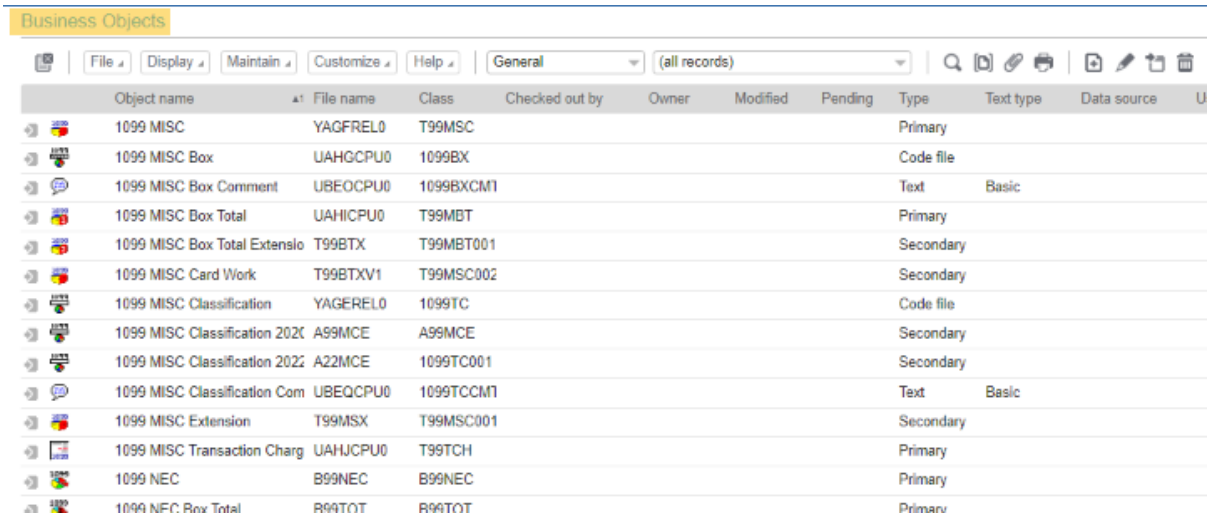
- Business Objects object on the Integrator card
- User Profiles object on the Integrator card
- User Profiles object on the Environment card.

This provides users without Integrator access to the job. 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 job is only available on the User Profiles object. It is very similar but allows the selection of the users, to be exported.

1 Start XA Environment.

2 Navigate to the Business Objects object on the Integrator application card or the User Profiles object on the Integrator or Environment.



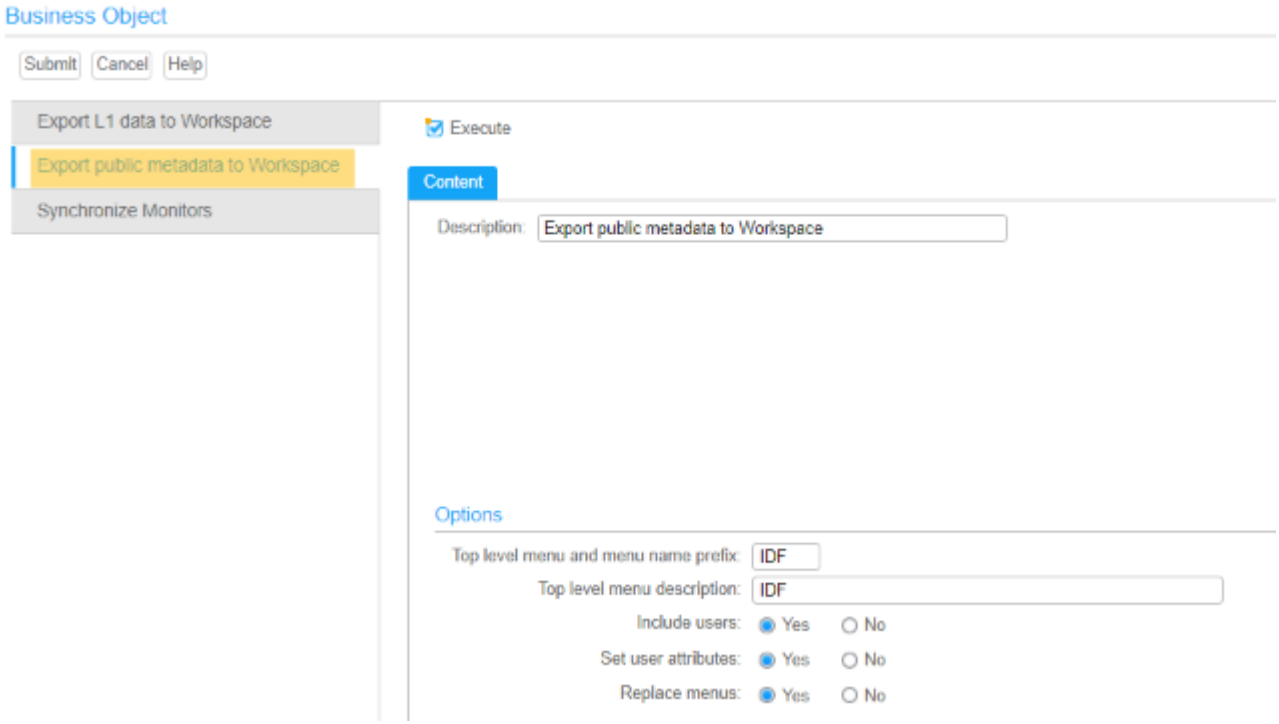
1 Select **File** > **Host** Jobs**.**

2 **Note:** 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.

3 Select the **Export public metadata to Workspace** tab. The tabs are displayed in alphabetical order which is not the best sequence to run them.

4 Select the **Execute** check box.

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



1 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. It is recommended that you use IDF unless IDF clashes with an existing menu. It is also recommended that you do not run the job multiple times with different Top level menu names, because this creates many similar menus in System i Manager. If you have to delete redundant menus, use System i Manager functions.

2 Specify the description of the Top level menu in System i Manager, in the **Top level menu description** field.

3 Specify if the users must be included, in the Export process in the **Include Users** field. If you do not include users, you must run the Export again later 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 **Include users**. Else, the authority to the menus and options is not available in Workspace.

4 Specify if user attributes must be set, in the **Set User Attributes** field. 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.

5 Specify if the menus are replaced in the **Replace Menus** field. Select **Yes** to delete 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 might remain in System i Manager.

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

6 Specify if translated card file, card, and object descriptions must be exported. 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. Else, the previous translations are lost.

7 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.

Exporting 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, in Power- Link. The Export L1 data to Workspace host job is also available in the User Profiles object on the **Integrator** or **Environment** application cards. This provides access to the Export L1 data to Workspace host job without an Integrator license.

You must run either the Export public or private metadata job before executing this job. Else, the Export L1 data to Workspace host job fails.

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.

1 Start Power-Link**.**

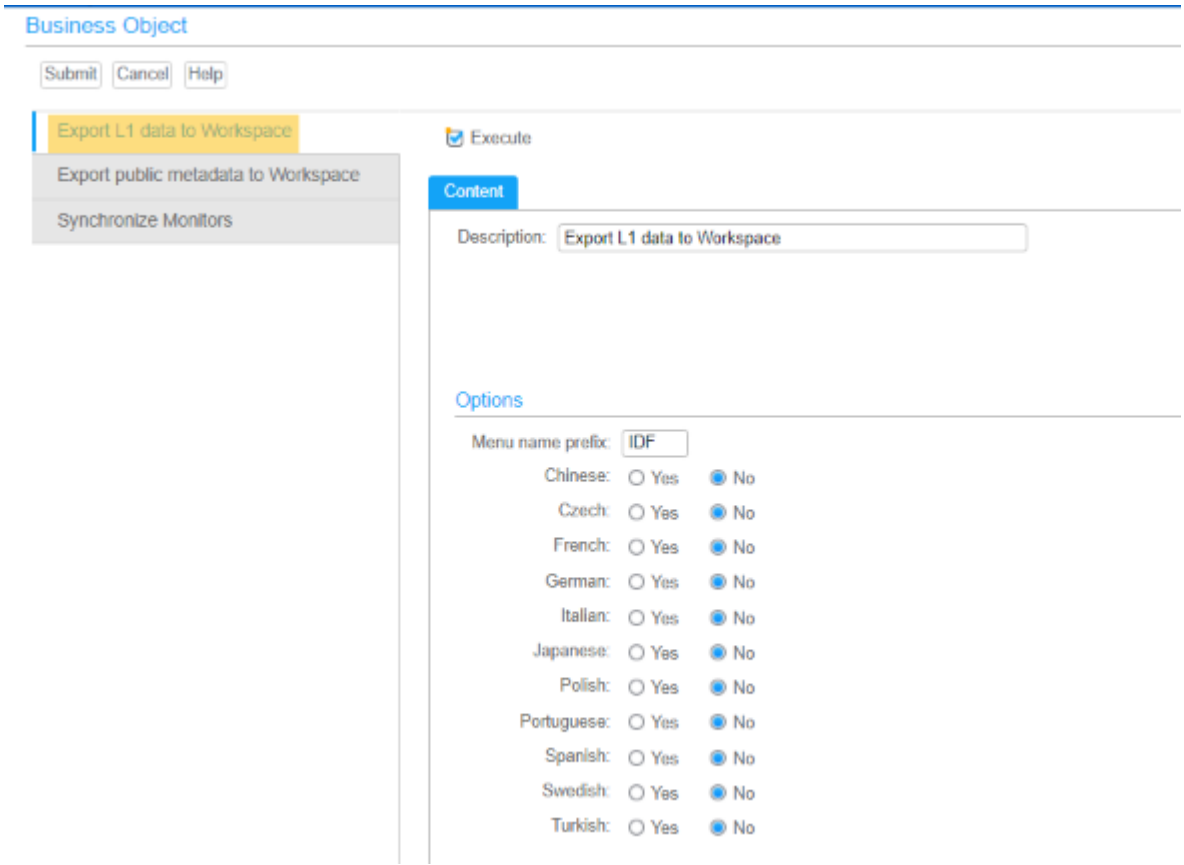
2 Navigate to the **Business Objects** object on the Integrator card.

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.

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



1 Specify this information:

- **Menu name prefix:** Specify the prefix used for the generated menus. 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.
- **Language attributes:** Specify the translated menu and option descriptions to be exported to SiW.

2 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, it is necessary to 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, it is recommended 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 it is necessary to export the metadata again. This is required if you:

- Add an object to a card
- Remove an object
- Change the workspace of an object on a card
- Add a new card, a new card file, or change 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, it is not necessary 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 (for example, additional objects) or IDF L1 Tasks (for example, additional user options), you must run the appropriate Export host job(s) 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. It is recommended 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 might 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, it is recommended 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, it is recommended 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 job(s), you must refresh the System i Workspace data. See "Updating Workspace".

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.

There is one situation in which the environments interact: a user in System Manager has the same initial menu identifier in all environments. 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 and, if the default prefix is used, all users are assigned the initial menu (which by default is **IDF**). This means the identifier of the initial menu is **IDF** in all environments, but the menu is not necessarily the same in all environments, the options may vary.

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, it is recommended:

1. If you export private metadata in one environment, you can do so in any other environments as well. If necessary, re-export environments that were previously exported with only public data.
2. Use the same menu prefix in all environments. It is recommended you use the default menu prefix, **IDF**, unless a clash with existing menus occurs.
3. 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, it is recommended 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, so 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 *KB2105811* 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 in SiW.

To update the definitions (exported from IDF to System Manager) in SiW:

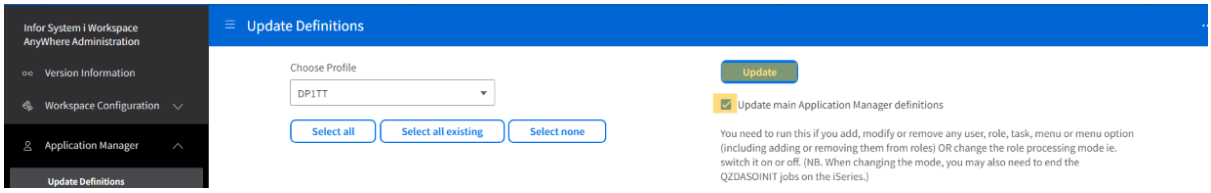
1 Open the utility by specifying this URL for SiW Anywhere:

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

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

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

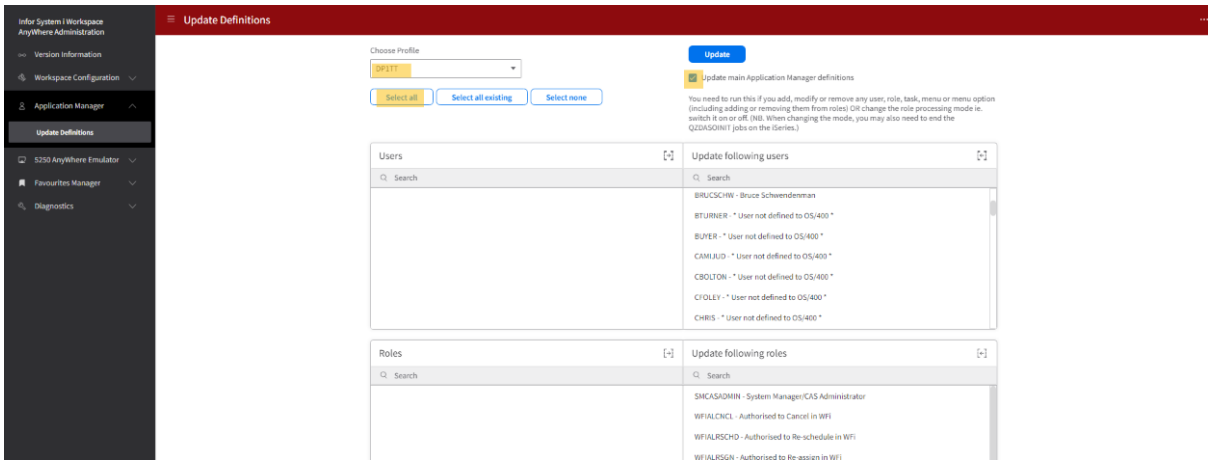
4 If you are performing this process for the first time after environment setup or after metadata export, then select **Update main Application Manager definitions** and click **Update**.



5 Click **Select all** to select all users/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 Select **Update**.



Note: Refer the Application/System Manager Synchronisation section in the Chapter 11 System i Workspace additional configuration in the ***System i Workspace AnyWhere Installation & Administration Guide*** for more information.

Chapter 6 Additional configuring in SiW

System properties changes

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

2 Add this property to enable System i Workspace AnyWhere to be launched from Infor OS Portal:

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

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

Allow cross-domain cookies

Due to further browser security restrictions, cookies set within iframes are now being treated as third-party cookies which breaks System i Workspace AnyWhere from functioning when integrating with **Infor OS Portal**. To get around this issue we must enable the Same Site Cookie flag which alters how the browse treats these cookies.

Windows SiWA Deployment:

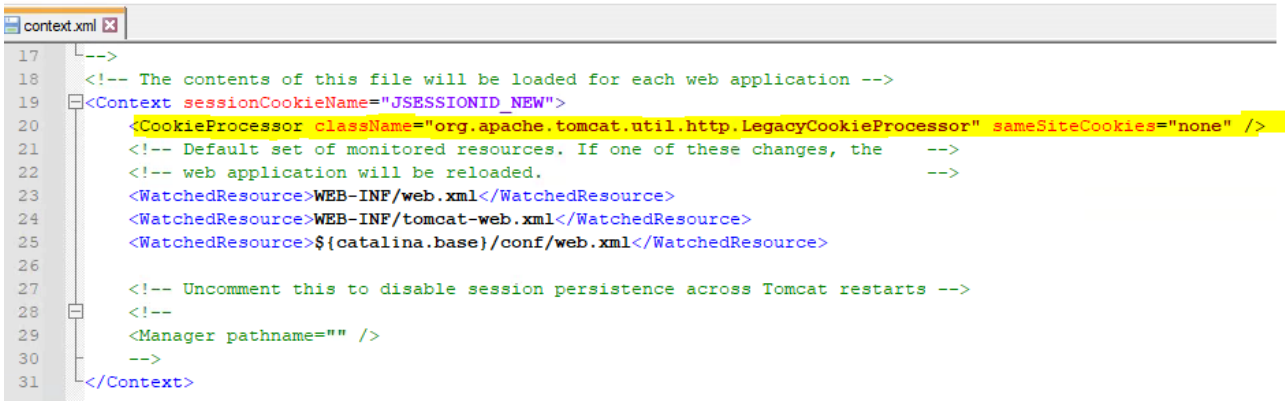
1 Edit file ***conext.xml*** which can be located in the ***tomcat\conf*** folder:

(For example: *C:\Program Files\Infor\SiWAnyWhere\tomcat\conf)*

2 Add the following line to the <Context> element:

<CookieProcessor className="org.apache.tomcat.util.http.LegacyCookieProcessor" sameSiteCookies="none" />

3 Save the file.



IBMi SiWA Deployment:

1 Use the following URL (replacing <hostname> with your IBMi server FQDN or IP Address):

http://<hostname>:2001/HTTPAdmin

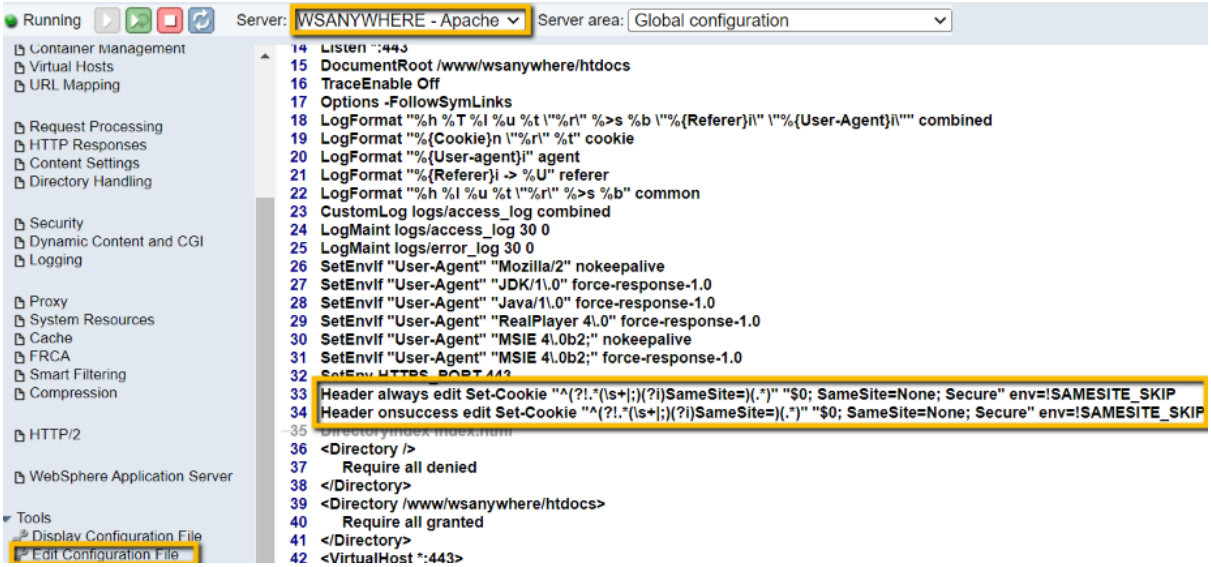
(for example: http://usalil2a.infor.com:2001/HTTPAdmin)

2 Navigate to SiWA specific HTTP server and click on “Edit Configuration File” option under “Tools” Menu.

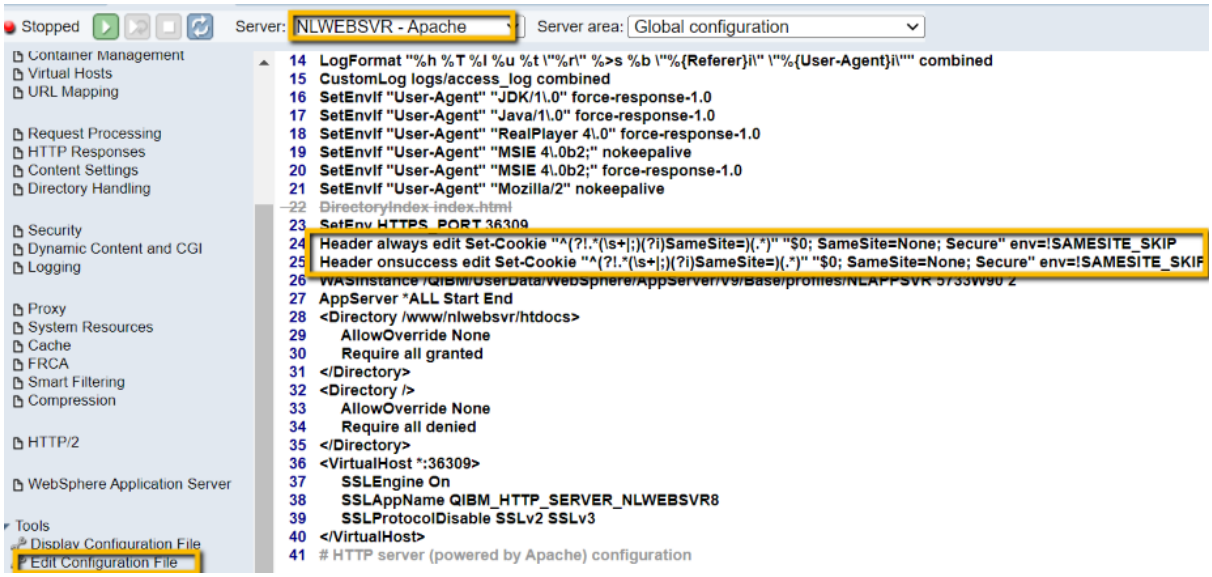
Add the following lines as shown below. Click on “Apply” and “OK”.

Header always edit Set-Cookie "^(?!.*(\s+|;)(?i)SameSite=)(.*)" "$0; SameSite=None; Secure" env=!SAMESITE_SKIP

Header onsuccess edit Set-Cookie "^(?!.*(\s+|;)(?i)SameSite=)(.*)" "$0; SameSite=None; Secure" env=!SAMESITE_SKIP



3 Navigate to Net-Link specific HTTP server and click on “Edit Configuration File” option under “Tools” Menu. Add the same lines, click on “Apply” and “OK”.



Restart both the HTTP servers and its associated Application servers.

Note: It is highly recommended to configure both WSANYWHERE and Net-Link to using same hostname and port as WSANYWHERE to avoid issues while using context apps or widgets in Infor OS Portal. Follow the steps in “Appendix B” in this guide and configure same.

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 by referring the Adding extra environments sections in the Chapter 5 Post installation tasks and other configuration, such as adding additional profiles, can also be performed if you wish to have different profiles by referring the Configuring System i Workspace **and** Application/System Manager Synchronisation sections in the Chapter 11 System i Workspace additional configuration in the ***System i Workspace AnyWhere Installation & Administration Guide***.

Chapter 7 Launching XA in Infor OS Portal

Use the steps provided in this section to configure XA with Infor OS Portal

As mentioned in "**Post installation**" chapter in this guide, it is recommended 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 Portal 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 Portal application.

You can use the Infor OS Portal environment to access the IDF views and screens. Users can access the Net-Link screens 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 OS Portal 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 OS Portal 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 OS Portal, 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 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. It 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 application in Infor OS Portal by using Portal option in Infor OS Portal.

After configuring XA in Infor OS Portal, users can view the 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 Portal

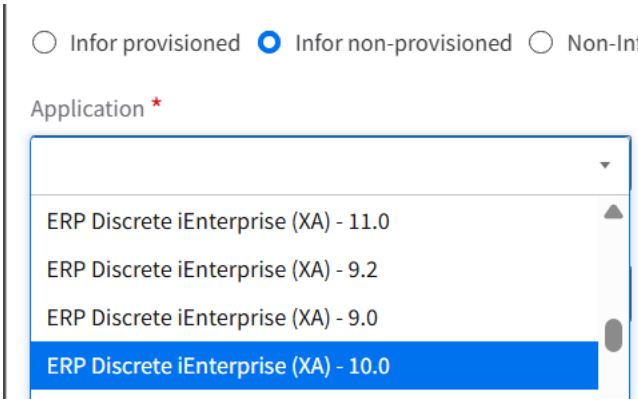
To configure for Infor OS Portal:

Login to Infor OS Portal using the account setup for administration.

4 Go to Navigation Menu, **OS** -> **Portal** -> **Applications**.

5 Click the **+ Add Application** option on the right-hand side.

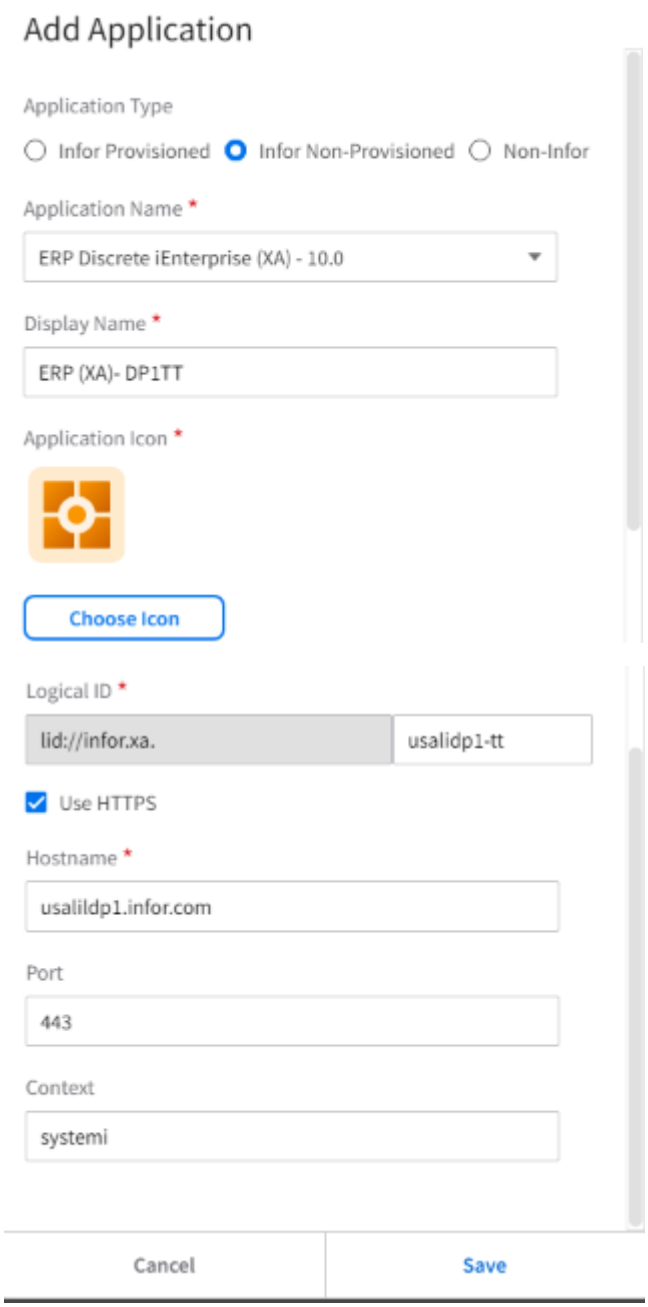
6 Select the Application type as **Infor Non-provisioned** and Application Name for an example as **ERP Discrete iEnterprise (XA) – 9.2 or 10.0 or 11.0 (based on version of XA being used)**



7 Specify this information to create the XA application option:

Field Name	Field Description
Application Name	Select from the drop-down either the **XA 9.2 or 10.0 or 11.0** application.
Display Name	Specify a display name for this application.
Application Icon	Choose 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	This setting must be enabled to use **HTTPS**.
Hostname	Specify the fully qualified hostname 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 which was defined for the System i Workspace. By default, this field is set to **systemi**.



8 Click Save and Click OK.

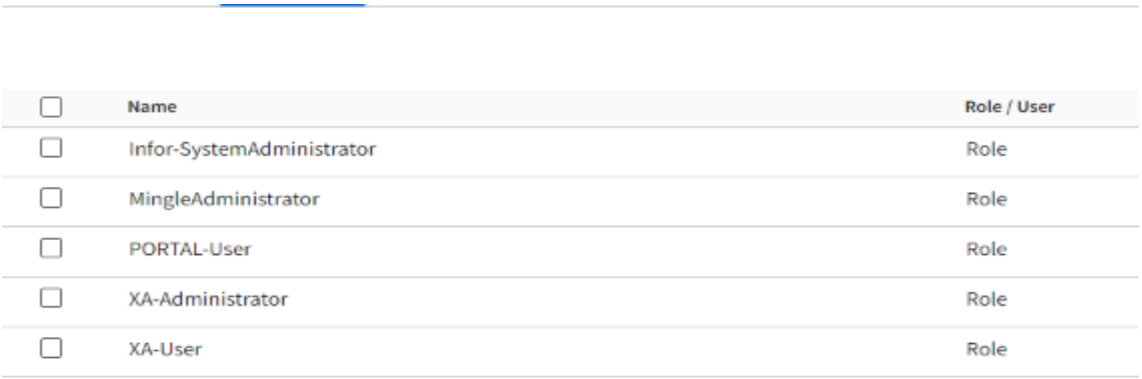
9 Select the Permissions tab.

10 Click Add New Users and/or IFS Security Roles.

11 Otherwise, refer “Create a new application security role” in this Chapter. Search and select the role created.

12 Click **Done**.

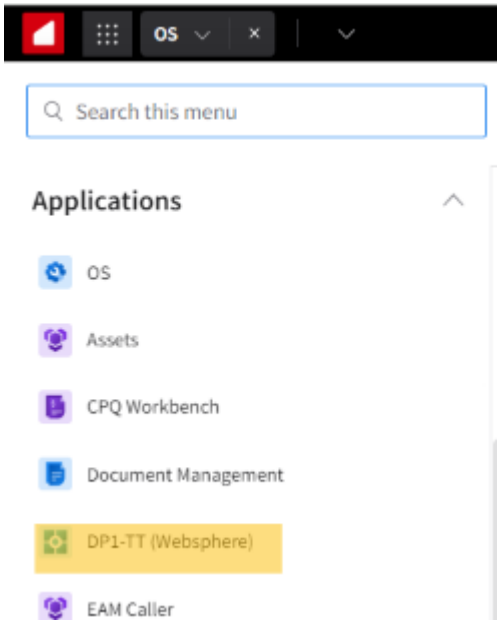
13 Click **Save and OK**.



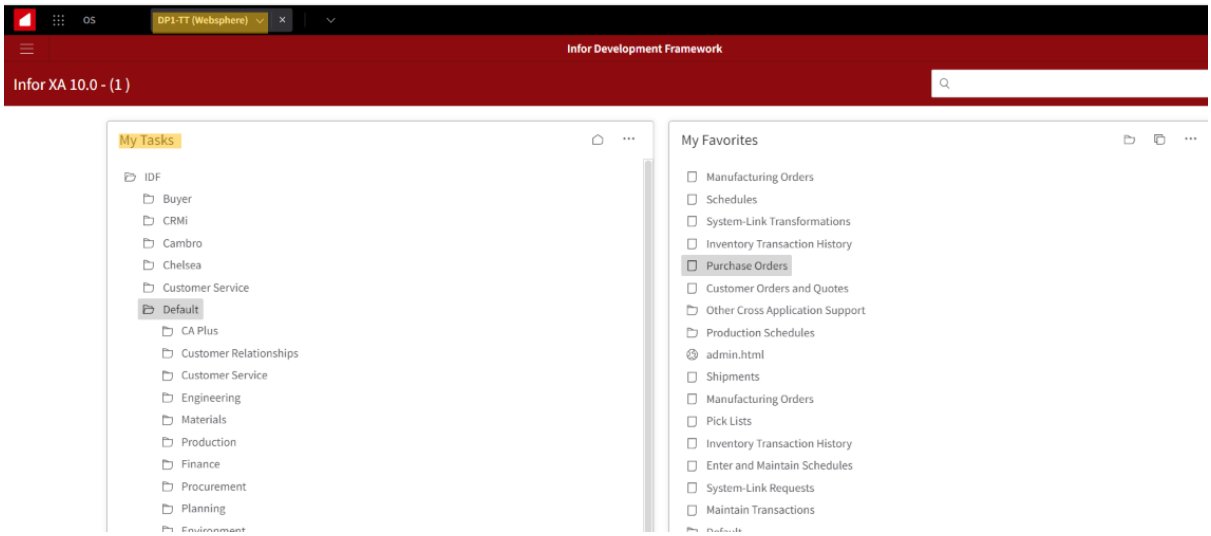
For enabling XA Context Widgets, refer Configuring Drillbacks Section under Chapter 10 Using Infor OS Portal in this guide. For adding the tab on screen, add the group/users to permissions in Admin settings of Manage XA Context Widgets.

Launch XA application in Infor OS Portal

1 Go to “**Navigation Menu**” and select the configured XA application icon in the Dropdown.



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

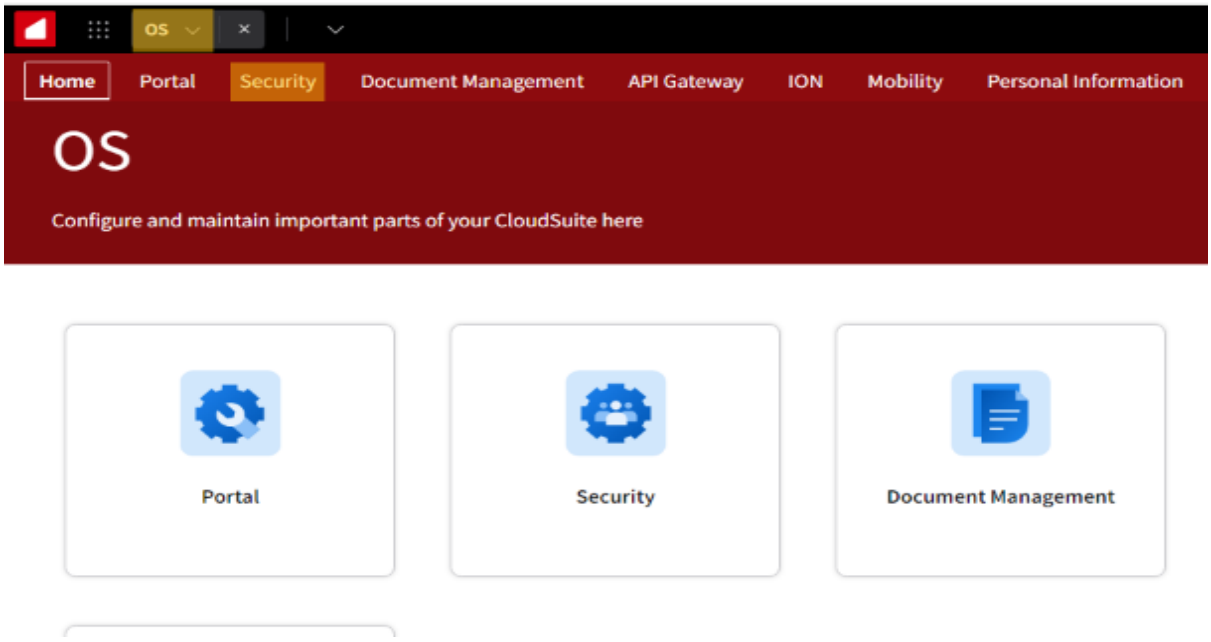


Create a new application security role

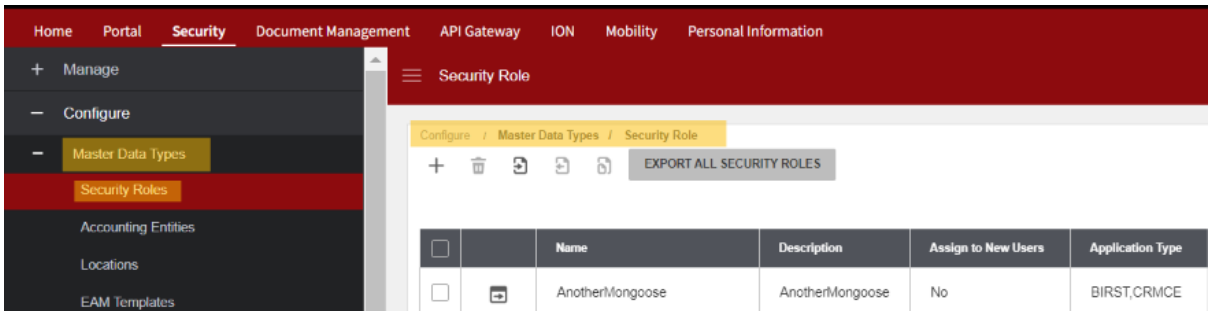
Caution: This step is not required if you are using automated user-provisioning functionality mentioned in Chapter 9 User Provisioning Implementation.

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

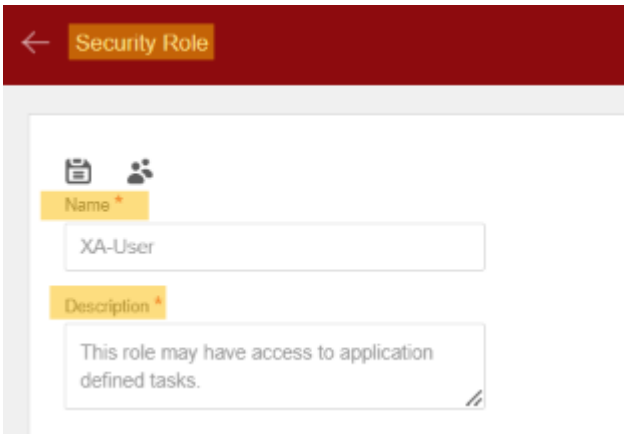
2 Click the **OS** option in Dropdown and select **Security**.



3 **Goto Security >Configure > Master Data Types > Security Roles**



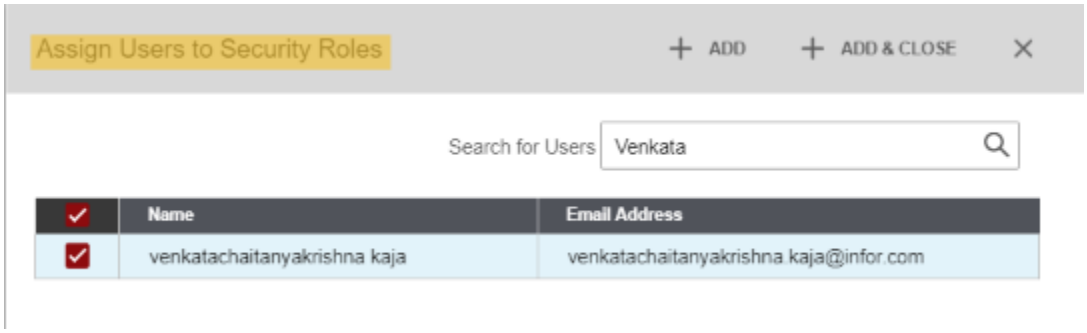
4 Click the **+** option to add a new Security Role:



5 Enter **Name** and *Security Role* for the **Description**.

6 Check the **Assign to New Users** field so that, in future, any new users that you add to Infor OS Portal can automatically get access to this new Security Role.

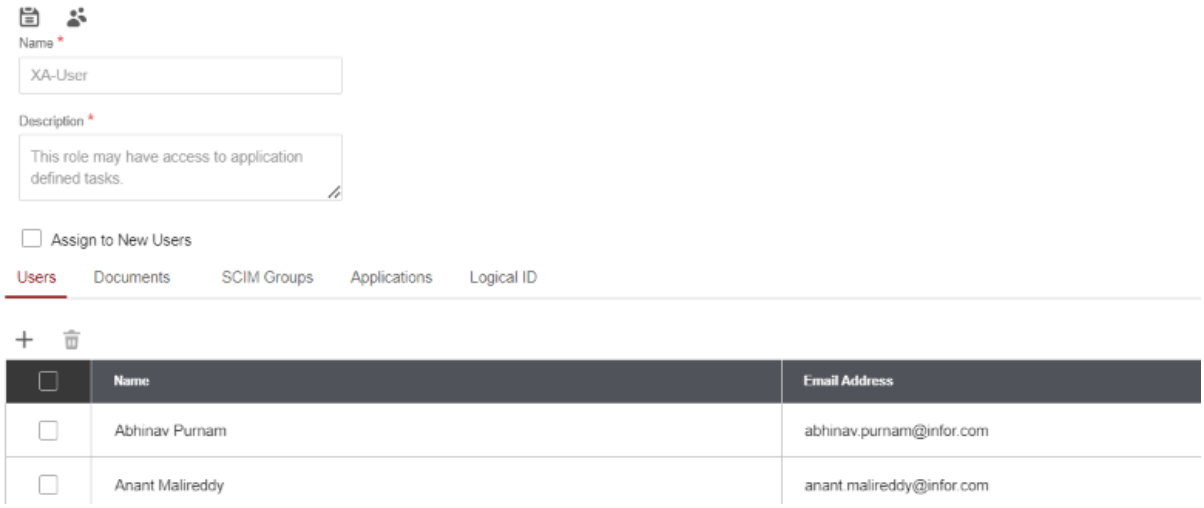
7 Click the **+** option to add users to the Security Role. If you have not yet added any users, then refer Chapter 12 – User maintenance *for* adding users into Infor OS Portal.



8 Specify the username you want to add to the Security Role in the Search for Users prompt box, as displayed in the previous example, and then click the magnifying glass option.

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

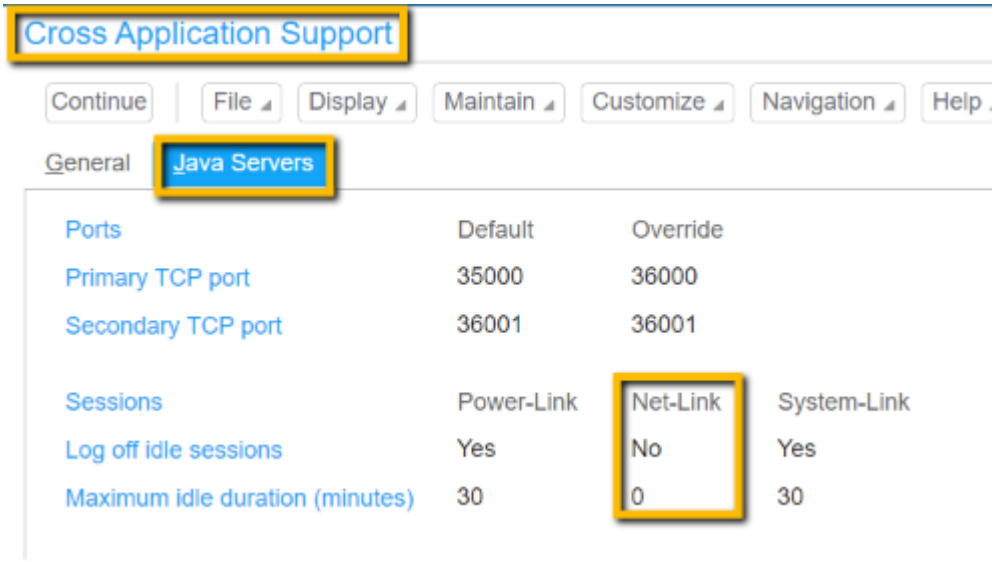
10 Repeat the search for each user you wish to include, and then click **Add & Close** to return to the main interface.



11 The table is updated with the selected user profiles. Click the **Save Item** option at the top of the page to apply the user(s) to the Security Role.

Disable Net-Link Log off idle sessions

To avoid session logout issues in Portal due to inactivity, go to Environment -> Settings -> Application Settings -> Cross Application Support -> Java Servers. Set "**Log off idle sessions**" to "**No**".



To configure other functionalities like Widgets, Drillbacks and Bookmarks refer to Chapter 10 Configure and Use Infor OS Portal.

Chapter 8 Single Sign-On (SSO)

This chapter describes the steps to enable the Single Sign-On functionality to integrate Infor XA, using System i Workspace AnyWhere with Infor OS Portal.

Note: SiWA should be running on FP 13 (minimum) and latest Infor OS for SSO with Infor OS Portal to work without any issues.

Throughout this guide we are referring to the following specific deployment options, please only follow instructions which are relevant to your deployment:

Single Sign-On Combinations:

This chapter covers SSO enablement for these combinations:

a. System i Workspace AnyWhere with IBM deployment (WebSphere) on **Infor OS Portal** using ***SAML SSO.***

b. System i Workspace AnyWhere with Windows deployment (Tomcat) on **Infor OS Portal** using ***SAML SSO.***

If users are going to be using Single sign-on for both System i Workspace AnyWhere and a 3rd Party 5250 Emulator (such as IBM Access for i) then it is also recommended 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 screen to appear during a Single sign-on if the user’s password has expired.

Software

The following software should have been installed and tested independently before proceeding with these integration instructions:

- System Manager 3.0 (with latest PTFs applied)
- 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 03.10.00.01.30 or later.
- Infor XA IDF R10.0.1.1 server PTFs is PCM SH16275 (XA R10.0.1.1 with PTF level 00502).
- Infor XA IDF 11.0.0 client software build must be 03.11.00.01.01 or later.
- System i Workspace AnyWhere (with latest Feature/Fix Packs applied – at least FP13)
- Infor OS Portal

Caution: Latest silver copy of System i Workspace AnyWhere (FP7 Build 200331 GA (Silver) - plus the latest Feature/Fix Packs applied) is needed, which comes with Apache Tomcat 9.0.34, if you wish to integrate with Infor OS Portal (Windows SiW Deployment).

Please make sure to complete the steps mentioned in Chapter 6 Additional configuring in SiW.

Security Assertion Markup Language (SAML) SSO on Infor OS Portal

This SSO implementation is recommended as this is easy to implement and maintain.

Migration from PingFederate to InforSTS for single-sign-on (SSO)

Infor applications that leverage SSO functionality through Infor OS Portal previously integrated with PingFederate using the SAML/WS-FED and OPENID protocols, now uses InforSTS as Service Provider.

Note: To migrate from PingFederate to InforSTS, please redo the below SSO steps for all your applications running on Infor OS Portal.

Obtaining the setup ZIP file

1 Find the latest ***InforOS_SSO_Setup.zip*** file, from the System i Workspace AnyWhere solution on the Infor Support website (*KB1963350*).

2 This 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. Rename 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 System i Workspace AnyWhere: ERP_XA_TENANT
sp.common.name	Replace *siwa-hostname.domain.com* with the hostname and domain of the System i Workspace AnyWhere server.
sp.sso.url	Replace *server-name.domain.com* with the hostname and domain of your System i Workspace AnyWhere server: *https://siwa-hostname.domain.com:443/systemi/CloudIntegrationServlet*
sp.slo.url	Replace *server-name.domain.com* with the hostname and domain of your System i Workspace AnyWhere server: *https://siwa-hostname.domain.com:443/systemi/fedletSloPOST*
sp.fedletadapter.class	com.geac.xtrane.servlet.http.CloudSLOFedletAdapter

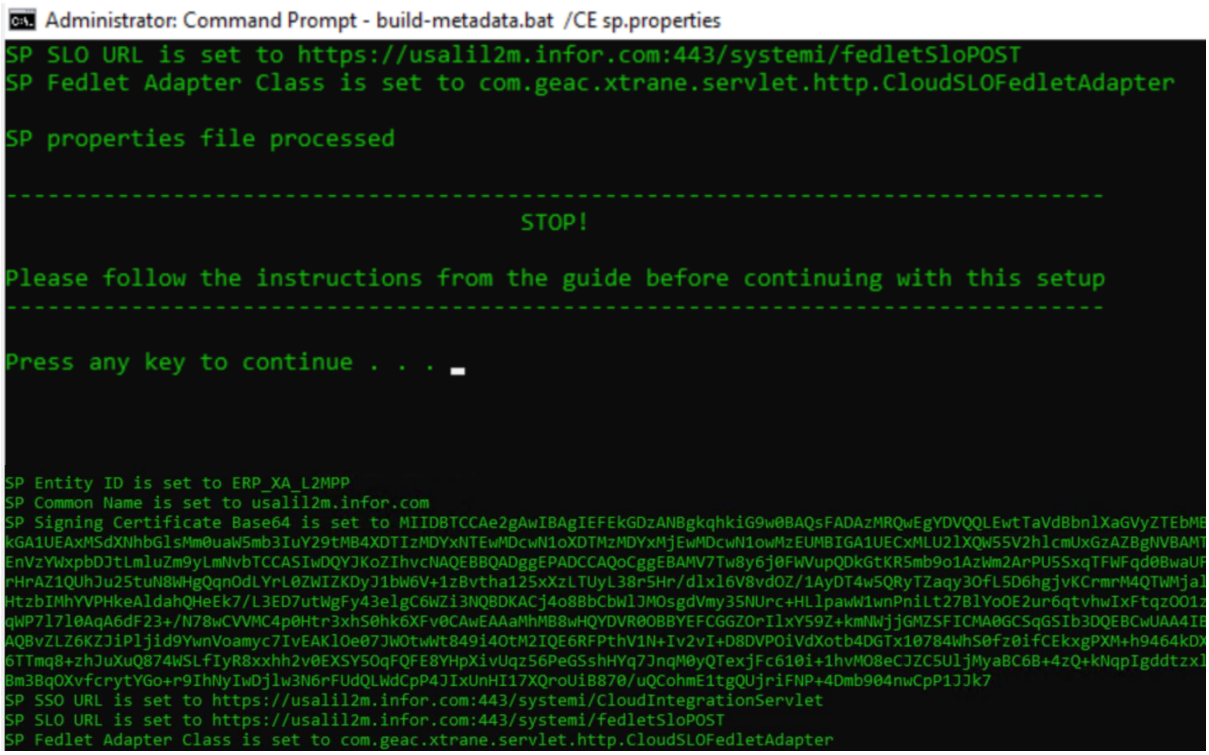
Creating the identity provider and fedlet metadata

1 Run the build-metadata.bat file giving it the following parameters:

build-metadata.bat /CE sp.properties

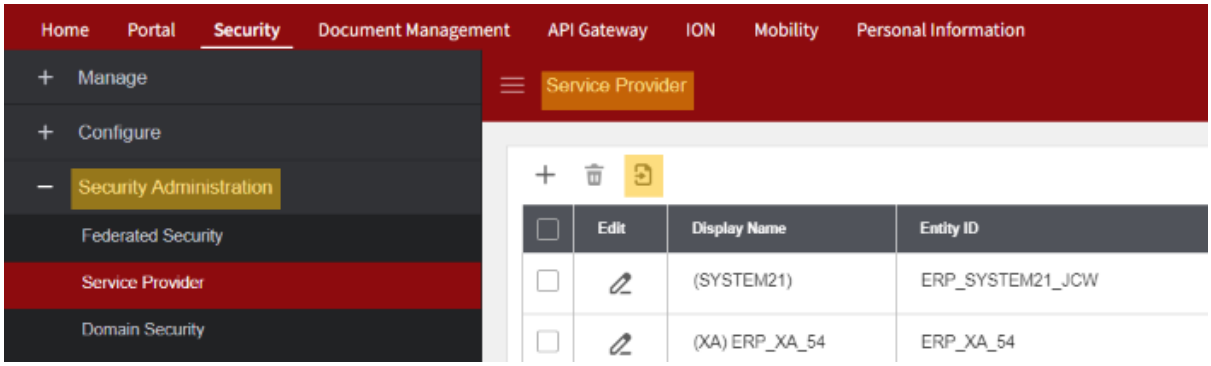
2 This creates a populated set of Fedlet Metadata in the folder ***fedlet_config*** at the end of the process.

3 During the build the build-metadata.bat is paused, do not continue until you have completed the following:

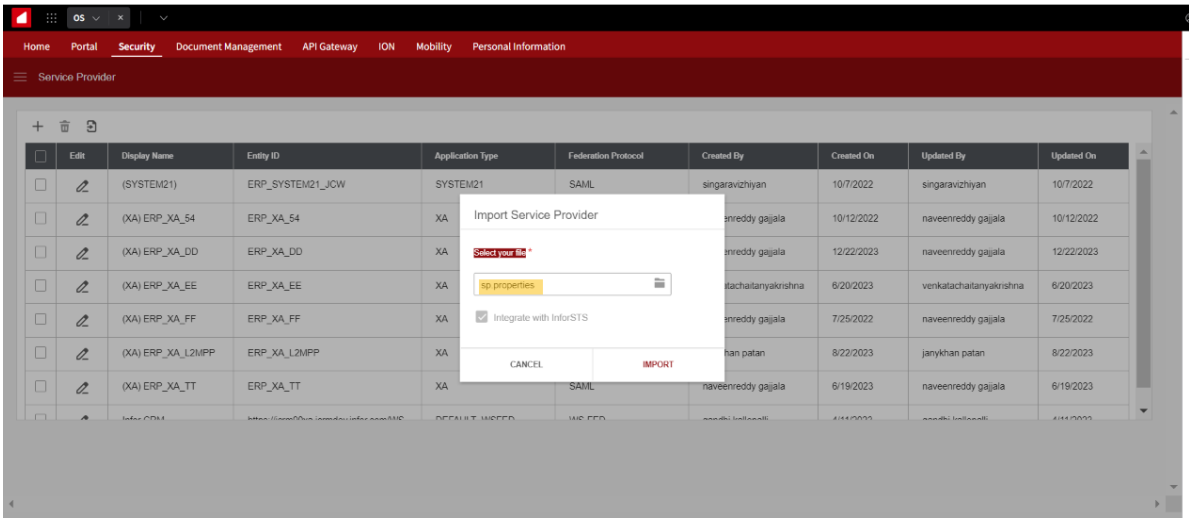


a. Log into Infor OS Portal using the account setup for IFS administration authority.

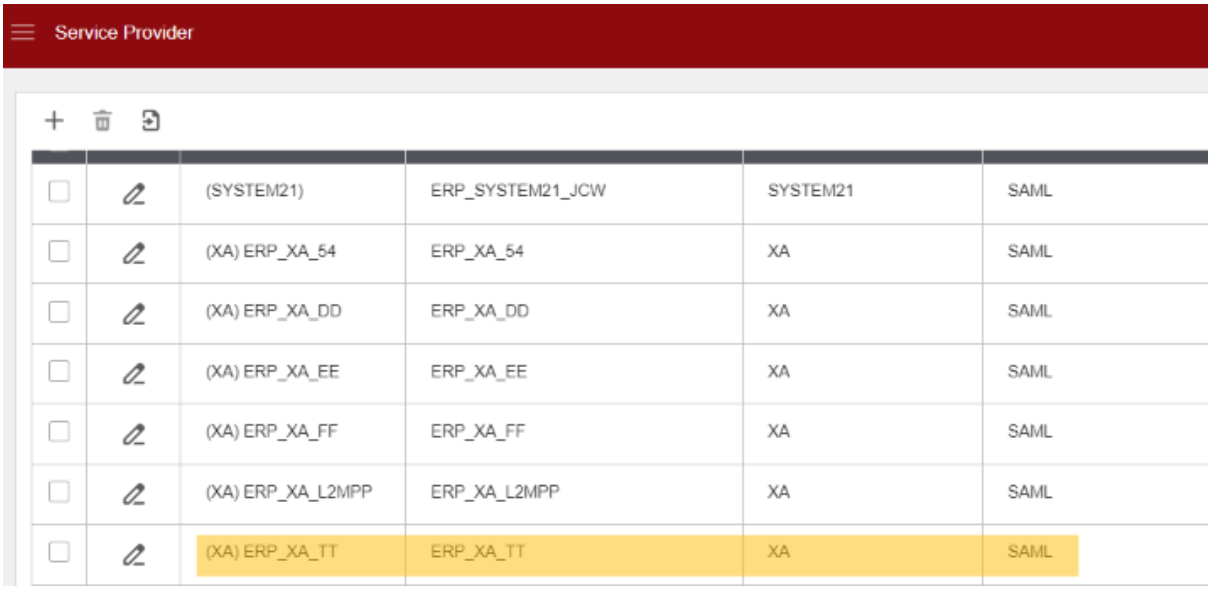
b. Click on the **Security tab** and then select ***Security Administration > Service Provider,*** click on ***Import Icon*** as shown below.



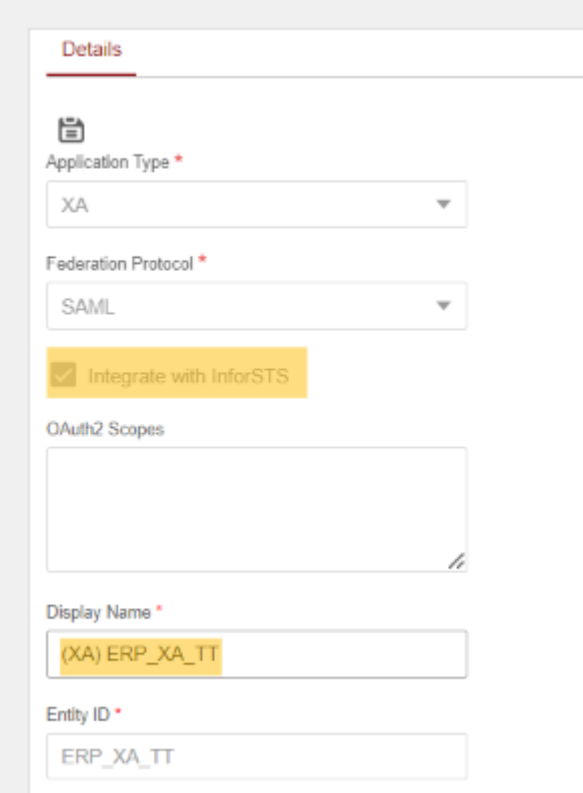
c. Select the file ***sp.properties*** from the populated folder ***fedlet_config,*** check the "***Integrate with InforSTS***" check box and Click ***Import.***

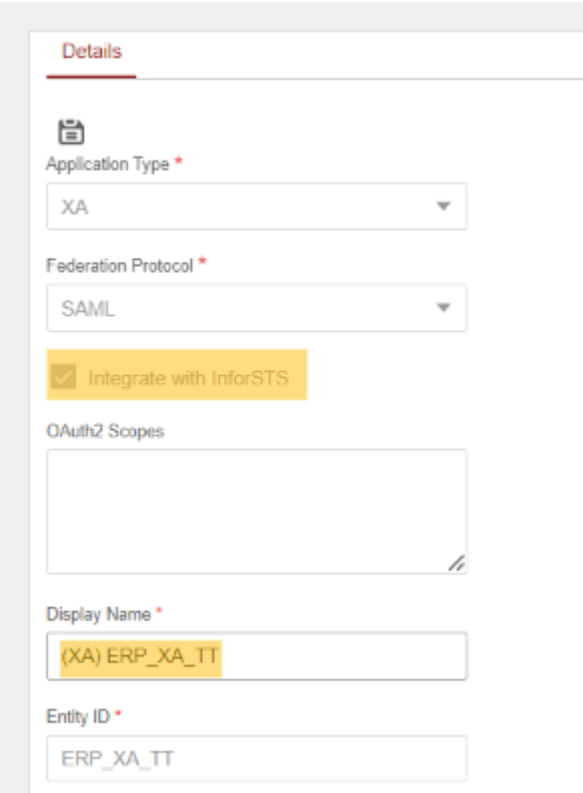


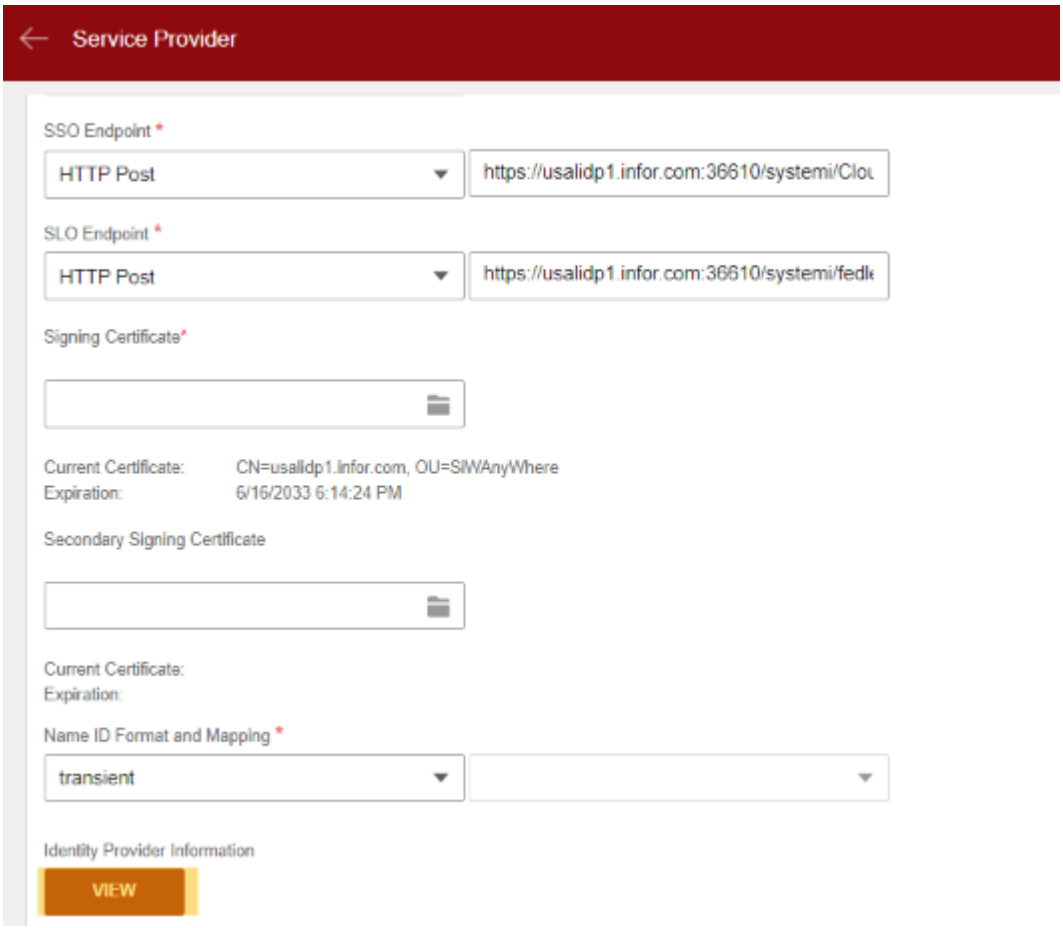
d. SP Entry is added successfully. Click on Edit, shown as below.



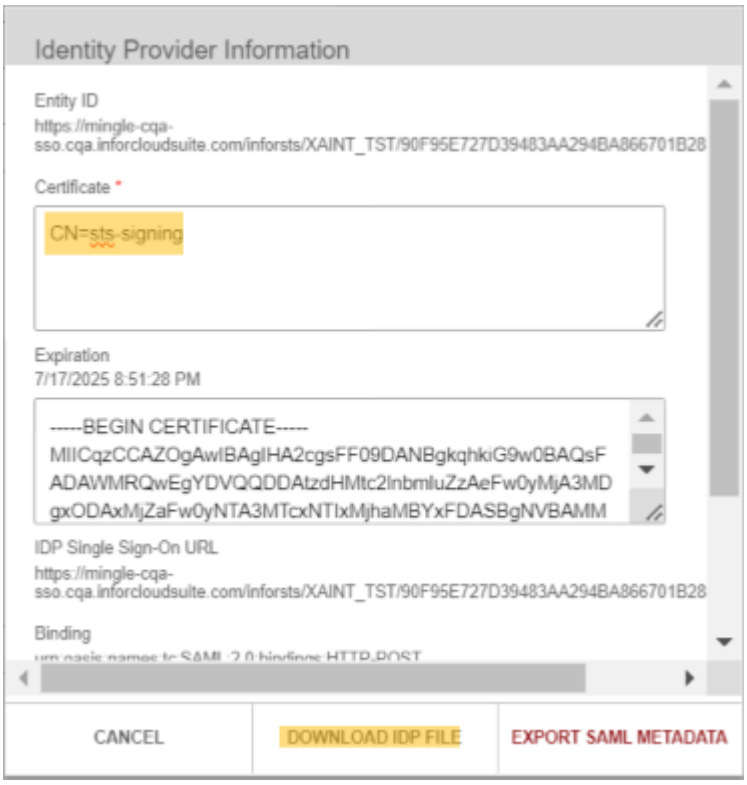
e. Scroll to the bottom and click on VIEW.


Details
Application Type *
XA
Federation Protocol *
SAML
Integrate with InforSTS
OAuth2 Scopes
Display Name *
(XA) ERP_XA_TT
Entity ID *
ERP_XA_TT


Details
Application Type *
XA
Federation Protocol *
SAML
Integrate with InforSTS
OAuth2 Scopes
Display Name *
(XA) ERP_XA_TT
Entity ID *
ERP_XA_TT

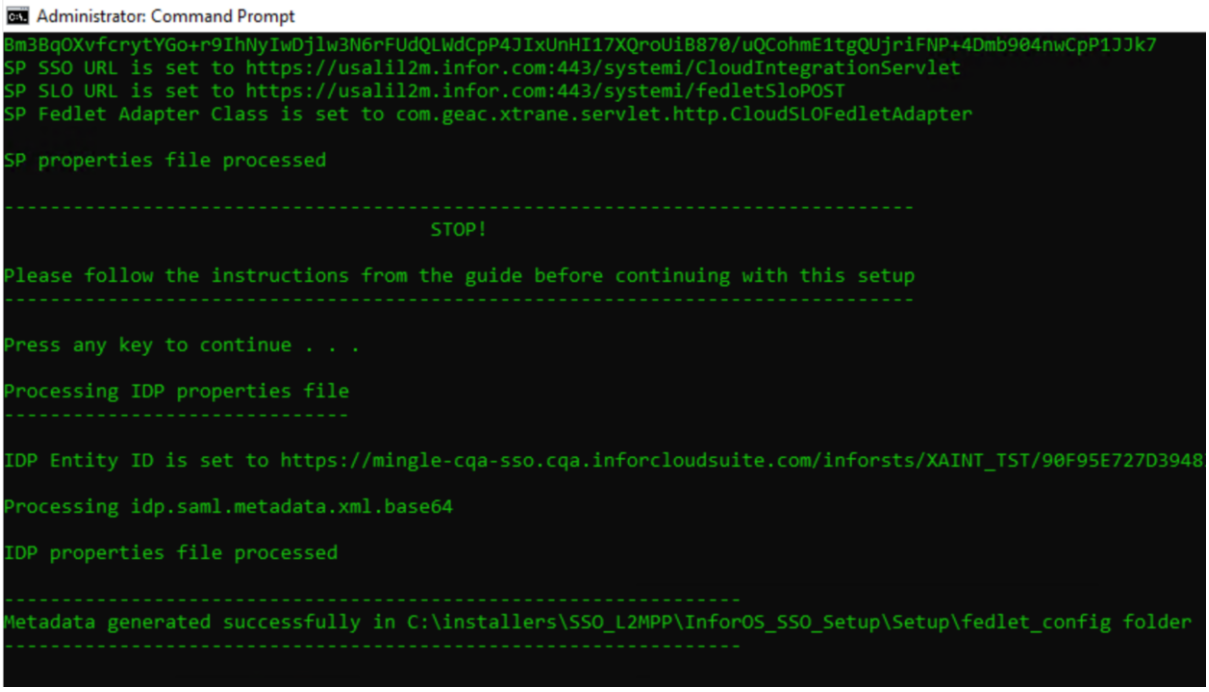


f. The Identity provider information pop-up is displayed with the details. Click the **Download IDP File** option as displayed.



g. This file needs to be renamed as idp.properties and copied to the setup folder overwriting the existing one.

4 You are now ready to continue with build-metadata.bat process, press any key to continue.



Copy the fedlet metadata folder

- Copy the ***fedlet_config*** folder to the root folder of your System i Workspace AnyWhere server or for an IBM i deployment of System i Workspace AnyWhere, this is most likely be the ROOT folder of the IFS

Note: For IBMi deployments, after copying the fedlet_config folder to the IFS, check 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 in UTF-8 format, the lead bytes are not correctly converted during the copy to the IBM i IFS. If it is UTF-8, open in Microsoft Windows Notepad and use Save As to change the encoding to ANSI (leave file name identical).

Java Runtime Changes

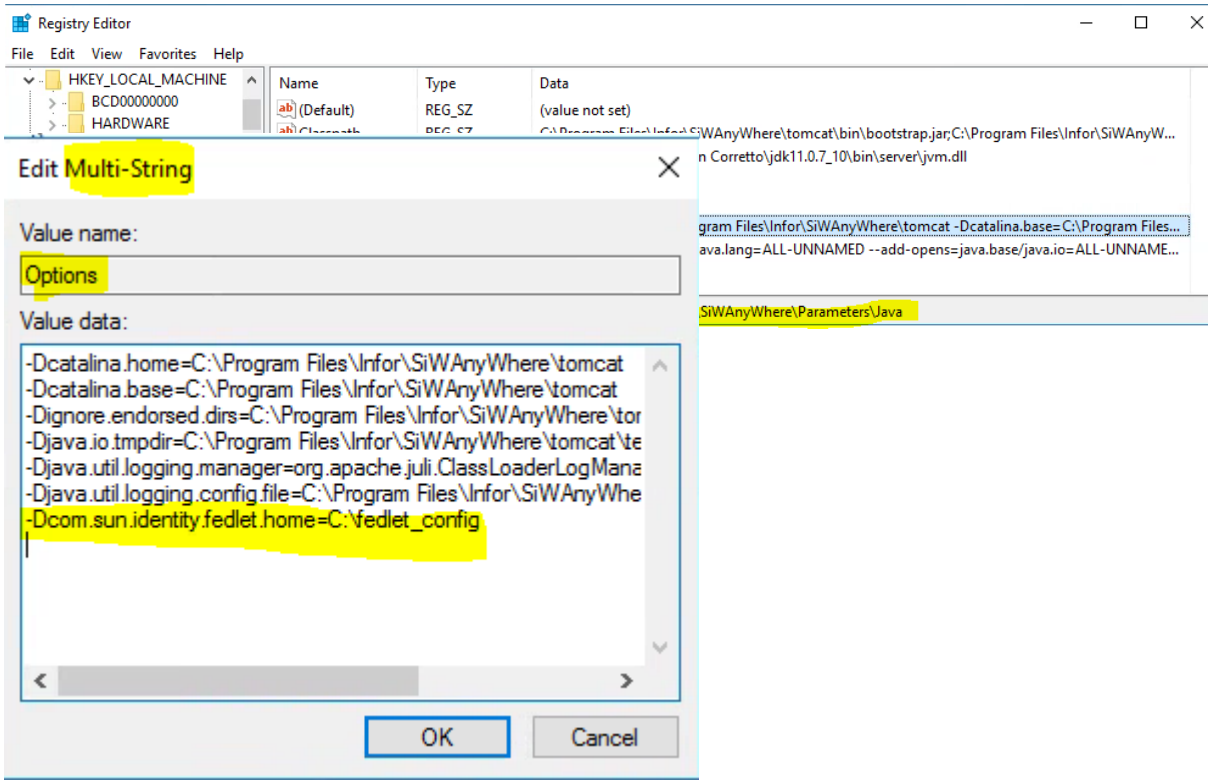
- An additional Java runtime property is required for the Web Server to identify the location of the SAML2 metadata folder created during the previous steps, For example,

-Dcom.sun.identity.fedlet.home=<Path to SAML2 metadata folder>

Windows Deployment

- Using RegEdit, update the following registry key below to add in the additional -D parameter, shown as below:

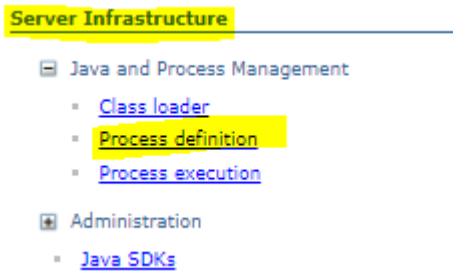
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Apache Software Foundation\Procrun 2.0\SiWAnyWhere\Parameters\Java\Options



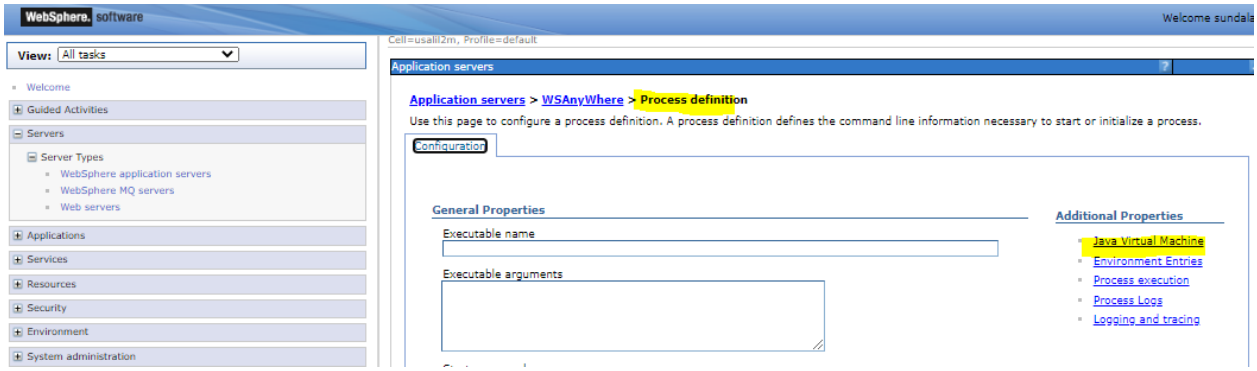
1 Use the IBM WebSphere Administrative Console to make configuration changes. From the menus on the left-hand side, select ***Servers -> Server Types -> WebSphere Application Servers.***

2 Select your System i Workspace AnyWhere Application server (usually WSAnyWhere for a default installation). On the next screen, expand the **Java and Process Management** option under Server Infrastructure section.

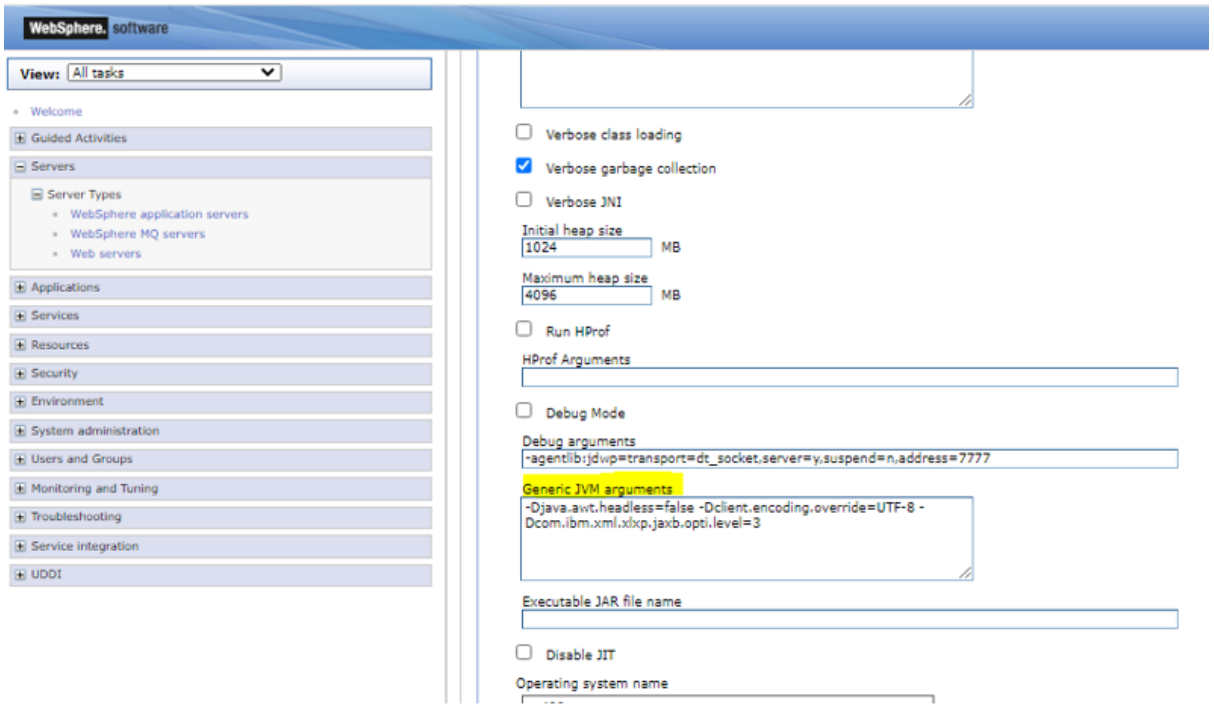
3 Select **Process definition.**



4 On the **Additional Properties** menu, select **Java Virtual Machine**.



5 Locate the **Generic JVM arguments** field, which may have existing values.



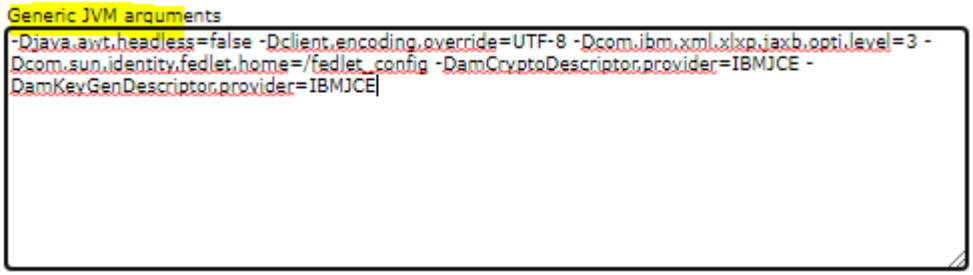
6 At the end of the existing arguments, type a space followed by the setting pointing to the path to your fedlet_config folder.

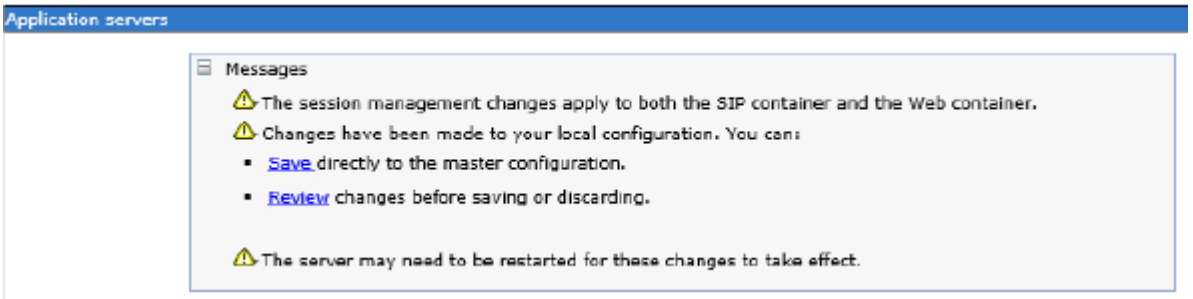
-Dcom.sun.identity.fedlet.home=/fedlet_config

7 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





8 Click Apply and then, click Save.

9 Exit the Administration Console.

System Properties 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:

Property	Description
com.infor.siw.cloud	Set to **1** to enable the cloud specific features of System i Workspace AnyWhere
com.infor.siw.cloud.idp.properties	The path to the SAML metadata folder. Used by System i Workspace AnyWhere to extract values from the metadata it needs 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 Portal server that is hosting System i Workspace AnyWhere. This is used to prevent ClickJacking so it must be correct, or the browser does not let System i Workspace AnyWhere execute inside Infor OS Portal. For example: ***com.infor.siw.cloud.mingle.url=https://IOS-hostname.domain.com***
com.infor.siw.cloud.mingle.slo.url	The URL, minus any context path, from either the *idp.adfs.location* 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 does not let System i Workspace AnyWhere log out correctly from InforOS, for example: ***com.infor.siw.cloud.mingle.slo.url=https://slo-hostname.domain.com***

com.infor.siw.session.cookie	The name of the session cookie used by the Application Server required so that any direct HTTPS requests from the System i Emulator share the same session ID as the System i Workspace AnyWhere web pages. The name of the session cookie is set during the installation of System i Workspace AnyWhere, though it may be overridden either at installation time, or via the IBM WebSphere Application Server console. The default session cookie name is JSESSIONID, so for example: ***com.infor.siw.session.cookie= JSESSIONID*** **Note:** Only required if the System i Emulator and Designer are provided to the customer. **Caution:** The “com.infor.siw.session.cookie” configuration is discontinued from SiWA FP14 or above,

2 Save the changes. System i Workspace AnyWhere can now be re-started. For an IBM i deployment, ensure the server1 application server and HTTP server are also restarted.

Note: You can now only access pages within System i Workspace AnyWhere after signing into Infor OS Portal. Direct or Standalone access to SiWA application is now disabled.

SiWA admin page also cannot be access directly when SSO is enabled.

But after login to SiWA inside Infor OS, we can access SiWA admin page in the same browser using new tab.

Caution: End of the SAML SSO implementation for Infor OS Portal.

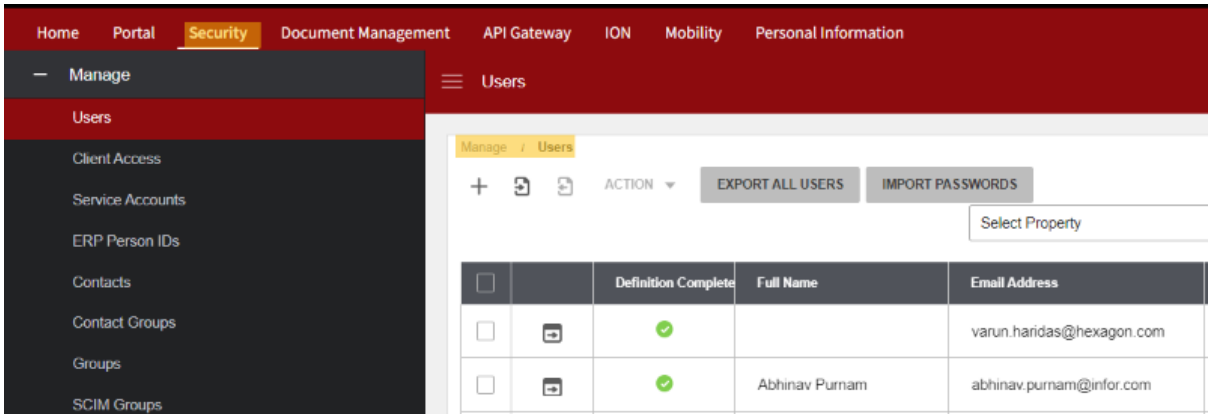
Note: QSECOFR or any other IBMi supplied user profile that starts with ‘Q’ or ‘q’ are not allowed to access XA application via Single Sign on through SiWA. The IBMi supplied user profiles are for IBMi administration purpose. It is not recommended to perform IBMi administration from SiWA or Infor OS Portal.
You can create users with different names and provide them required SECOFR authority to use them with SiWA or Infor OS Portal, if there is any valid business needed.

Configuring XA User IDs in Infor OS Portal for SSO Support

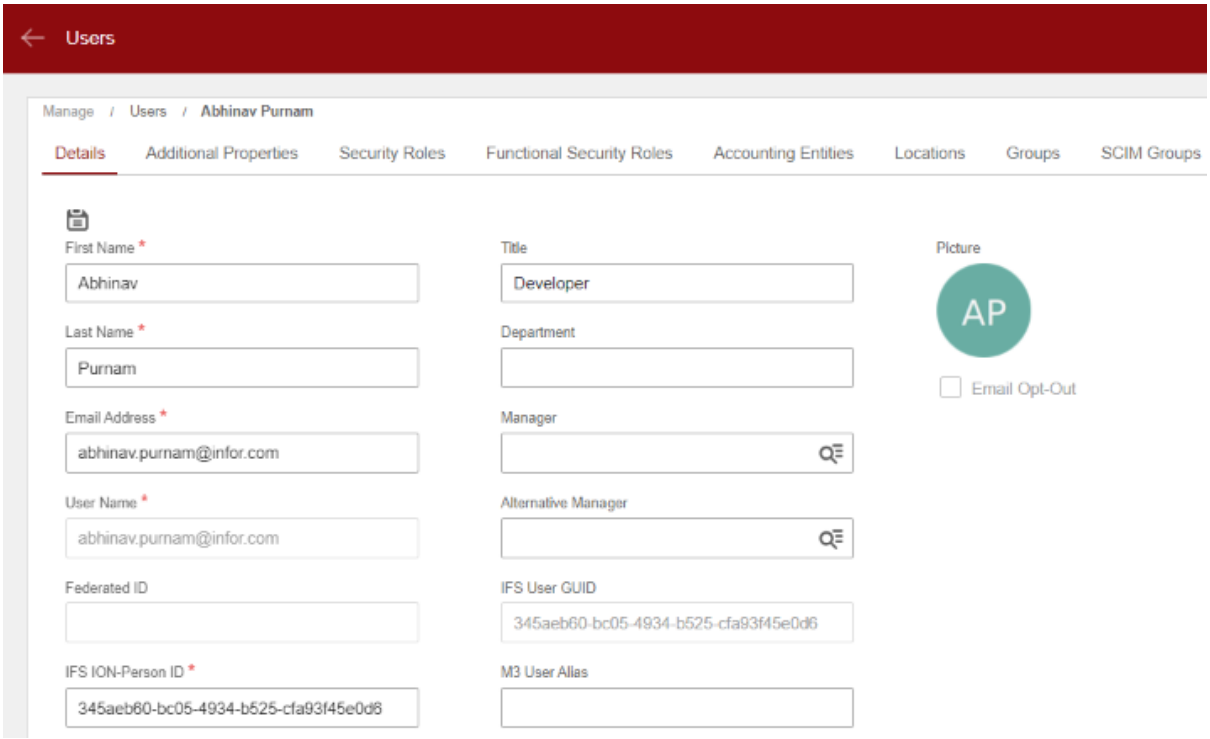
Caution: This step is not required if you are using automated user-provisioning functionality mentioned in Chapter 9 User Provisioning Implementation.

Each user that needs access to System i Workspace AnyWhere must be configured to add a mapping from the Infor OS Portal platform to their ERP User (i.e. their IBMi user account). This is done via the User Management interface.

1 Log into Infor OS Portal and select **Users** from the Security menu.

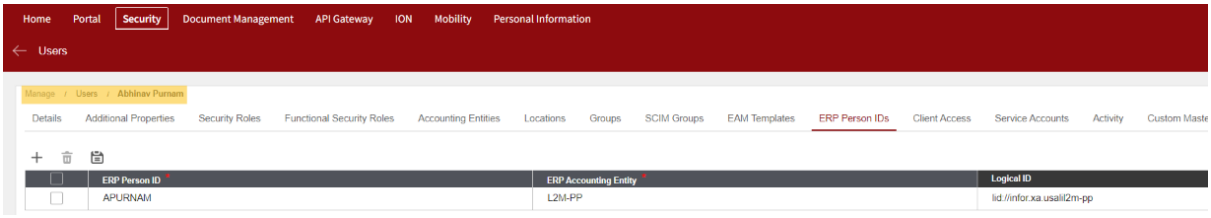


2 Use the table navigation or search to locate each user profile that needs changing. Click the drilldown option next to the username in the grid to display their properties



3 If you are using Role-based authorization for access to the System i Workspace AnyWhere application, then make sure the user is authorized to the correct Role.

4 Select the ERP Person IDs tab. In this tab, create a mapping between the Logical ID of the System i Workspace AnyWhere application and the IBMi username.



(For example, when abhinav.purnam@infor.com logs in to Infor OS Portal and accesses the Infor IBMi based application that runs inside System i Workspace AnyWhere, the IBMi profile ID of APURAM must be used.)

5 Click the **Save** option in the ERP Person IDs table to apply the changes to the user.

6 Repeat for each user profile that needs access to System i Work.

Chapter 9 User Provisioning Implementation

For a ‘new’ XA implementation where for all Infor applications user provisioning is in the Infor Federation Services domain. Provide the ability to create and maintain users in Infor applications from User Management in the IFS.

System i Manager is a pre-requisite and should be at a minimum PTF level of AMAG0176 to access the User Provisioning functionality.

SiWAnyWhere should be running on FP 13 to support SSO on Infor OS Portal.

Infor OS Portal should have the XA specific roles in IFS registry to assign to XA users.

To use this functionality,

XA 9.2.2 client should be at least on 02.09.02.02.57.

XA 10 client should be on 03.10.00.01.30.

XA 11 client should be on 03.11.00.01.01.

SH69855 and SH71181 PTFs should be applied on 9.2.2.

SH69855 and SH71633 PTFs should be applied on 10.0.1.

Overview

The primary usage of this functionality is, within IFS user management:

When a new user is created and assigned with XA specific Roles including any other application roles in IFS.

IFS publishes a Sync.SecurityUserMaster BOD to all Infor applications including XA.

XA subscribes to incoming Sync.SecurityUserMaster BOD and process the bod to create System Manager user, IBMi user, XA User Profile.

XA assigns XA specific Roles and publish Sync.Person BOD to IFS as an indication of successful user creation in XA.

IFS in Infor OS Portal subscribes to Sync.Person BOD and consume the bod received from XA.

IFS updates the XA User ID value in “ERP Person IDs” section in IFS user.

This helps XA User to directly login to XA environment using SiWA in Infor OS Portal via SSO.

Based on the XA Roles selected, the XA User can access XA functionality.

Limitations

Current implementation has below limitations or considerations:

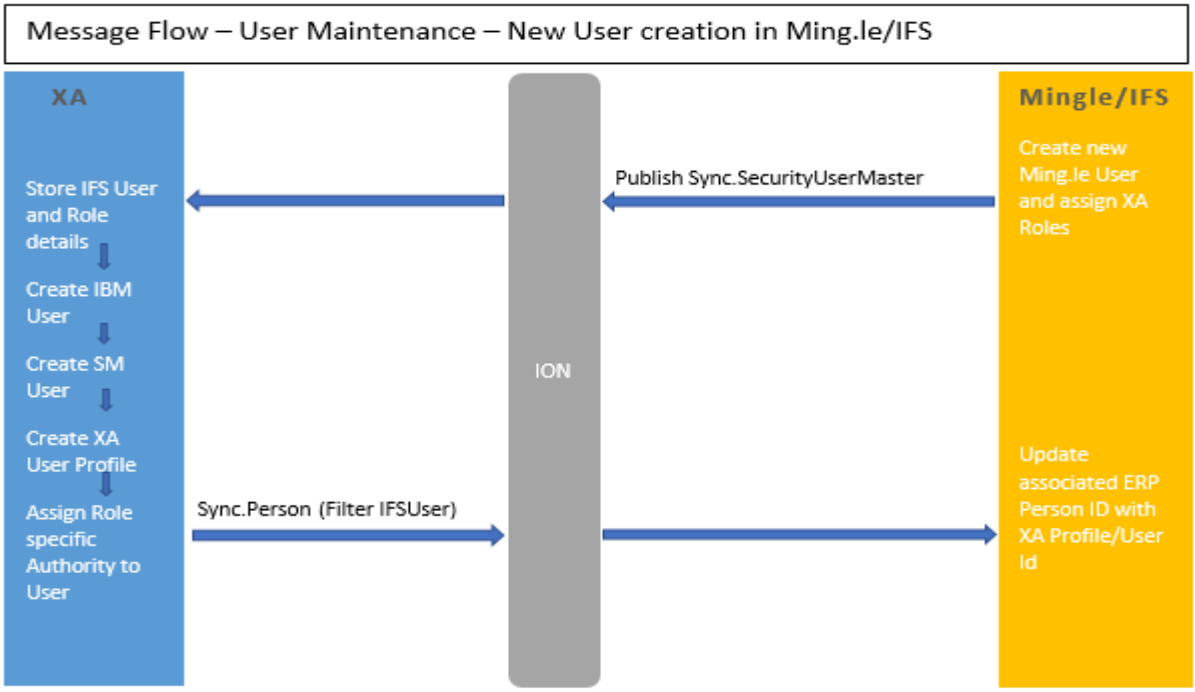
- XA environment is a one to one relationship to tenant on Infor OS Portal.
- This solution is best suited or intended for customers with freshly installed XA and Infor OS Portal applications and no existing users in both the applications.
- Creation of new users in XA does not trigger user creation in IFS. XA does not support Process.SecurityUserMaster bod to sync user in IFS from XA.
- New users created in IFS can be created/synced in XA using Sync.SecurityUserMaster bod from IFS to XA.
- XA does not have roles concept and does not support Sync.SecurityRoleMaster bod to publish roles from XA to IFS.
- Only XA-User and XA-Administrator need to be assigned as roles in IFS and sent to XA. These two roles are one-to-one mapped with security areas with same name in XA. Any new roles created in IFS cannot be recognized by this solution.
- A newly created user in IFS doesn't have any of the XA roles assigned to it. XA does support creation of user without any security roles. Roles in IFS can be added or modified at any point of time.
- The XA-User and XA-Administrator security areas in XA is empty when this solution is installed for the first time. It is System Administrator's responsibility to add the required security areas or tasks in these security areas in Cross Application Support based on business need.
- Removing XA specific roles for user in IFS, performs cleanup of security areas in XA as well. Roles can be swapped based on need.
- Exception handling is not supported in current implementation. If any failure occurs during user creation in XA, generic exceptions are observed in Transaction Status in MXABUS user and confirm bod is shown in ION with those exceptions.
- If the user creation fails in XA due to any reason for the first time, then republishing of Sync.SecurityUserMaster bod from IFS to XA can complete the user creation process.
- After successful user creation in XA, to login to XA (using SiWA in Infor OS Portal with SSO) the admin needs to manually run the "Update Definitions" for user in SIWA Administration page.
- Creation of IFM user profiles in XA is not in the scope in the current implementation. System Admin need to take care of required setup separately to get this done.
- In IFS if the user is disabled or deleted, then the user can be set as de-activated in XA and access to XA application is revoked.

IFS User Management

These are the currently supported functionality for maintaining and synchronizing users in the IFS and System Manager. Changes to functionality is updated in this Chapter.

New Users

7 New users are added in IFS and a GUID is automatically generated. IFS publishes a



Sync.SecurityUserMaster for the new IFS user with the GUID as the User ID.

For the new IFS user add the:

In Security Roles, the XA-User or XA-Administrator Role must be added for access to XA application and tasks.

8 ION routes the Sync.SecurityUserMaster to the XA environment associated with the Infor OS Portal Tenant as per active ION Document flows.

9 XA consumes Sync.SecurityUserMaster and stores all the user and roles data in XA tables. It creates a record in the SM file with SM user for IFS users, with the GUID as the key and other IFS details also stored. At this point there is no Person ID associated to the IFS user.

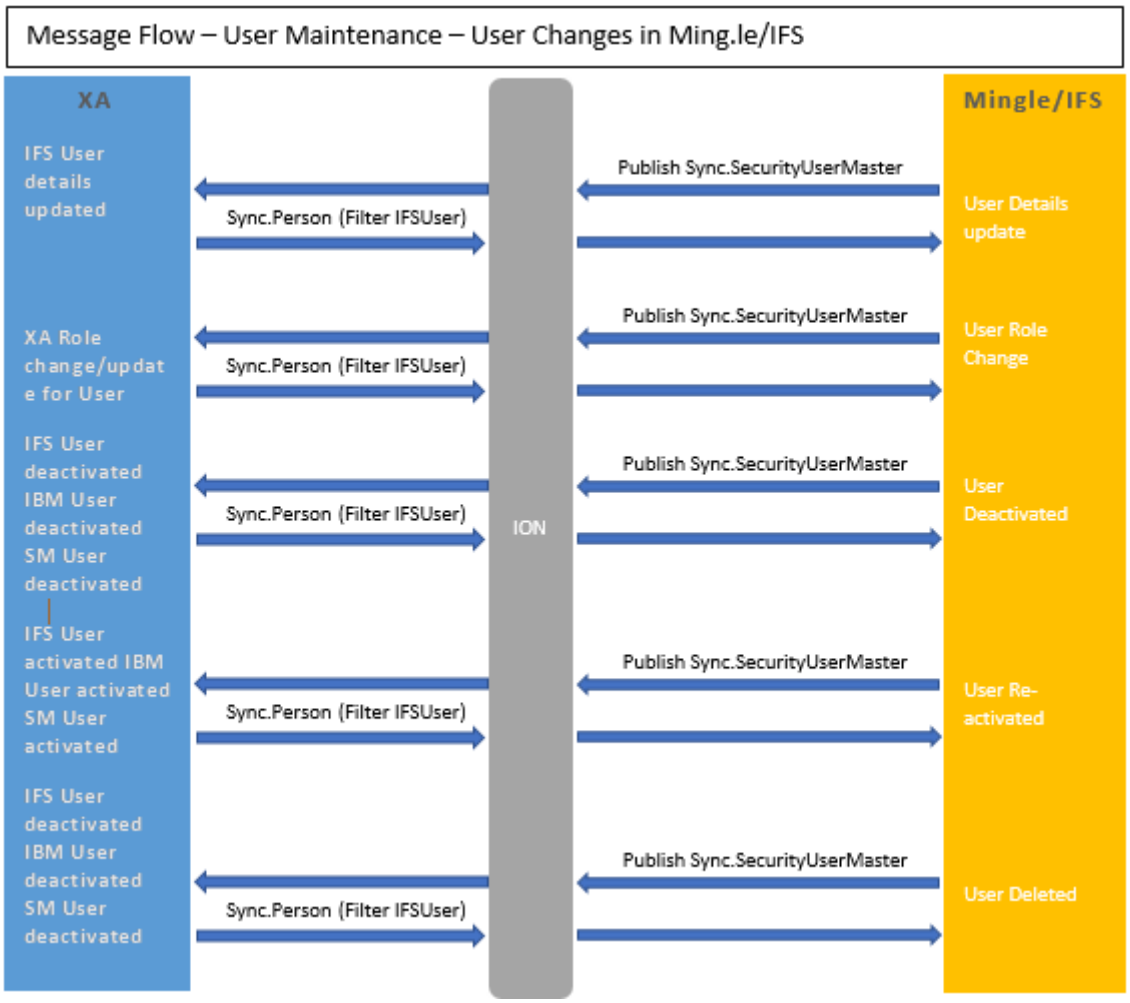
10 IBMi user is created automatically same as SM user. Same user is added into Cross Application Support -> XA User profiles in the current XA environment.

11 Having associated a XA user to the received IFS user, XA automatically publishes a Sync.Person BOD with the S21 user being a ‘Person’ associated to IFS security user via the GUID.

Note: The Person BODs required contains a Description of ‘IFSUser’, to avoid sending BODs of other types not required in the IFS it is suggested you add a filter to the ION Document Flow to only route the required type to the IFS.

12 IFS consumes Sync.Person BOD and updates XA user as the ERP Person ID.

User Changes in IFS



13 As well as creating new users in IFS as described in the previous processes, changes to the IFS user can also be in IFS User Management. Any change made results in Sync.SecurityUserMaster BOD being published and routed to XA. Any changes to the basic user profile are reflected on the System Manager copy of the IFS user.

14 If the activation status is changed via the IFS User Management Action menu the Active/Inactive status is reflected in System Manager.

15 If the user is deleted, then the System Manager record is updated with a status of deleted.

16 If roles are added or removed from the list of role assignments those details are also received on the SecurityUserMaster BOD. The XA tasks and authorization for the user is updated to reflect the select roles.

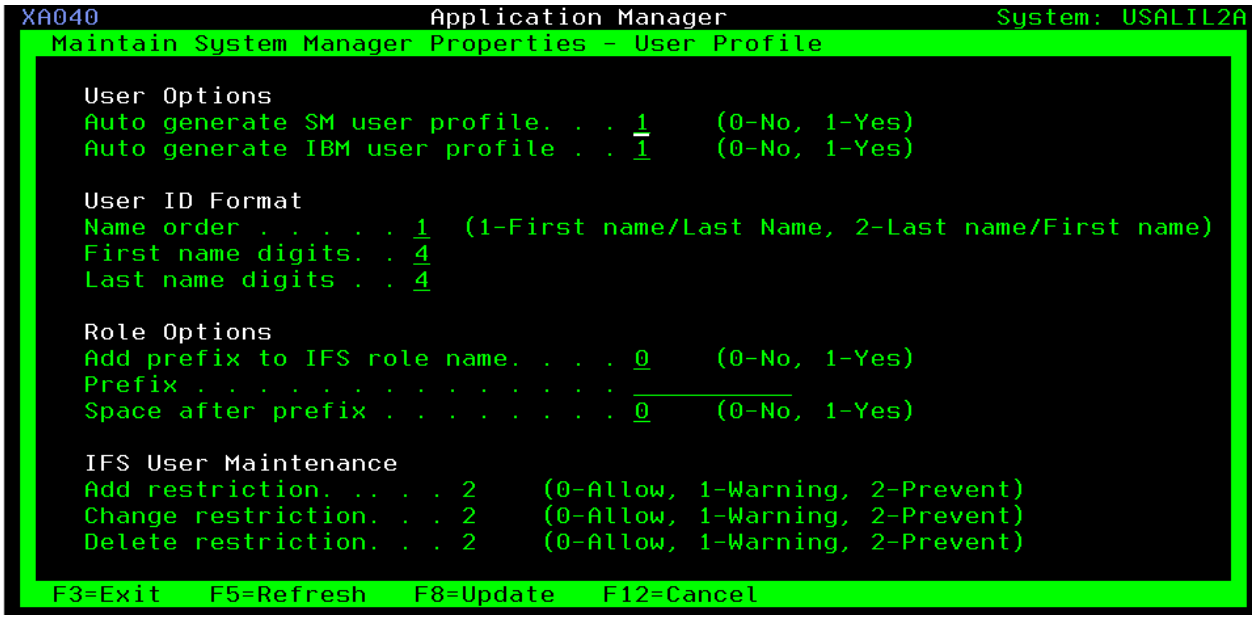
System i Manager Setup

The following are the required pre-requisite configurations in System i Manager.

NOTE: System i Manager should be at a minimum PTF level of **AMAG0176** to access user provisioning functionality.

User Profile

Establish the configurations for creating the System Manager & IBMi user profile.



Fields

Auto generate SM user profile

Identifies if a System Manager user profile should be created automatically on receiving a new user sent from IFS. The user ID can be derived from the supplied user name where the options below allow you chose how many characters are taken from the first and last names and in which order. A qualifying numeric count us then added to make the derived ID unique,

Set to 1, generate System Manager user profile automatically. The ID can be derived from the supplied user name. The recommended setting.

Set to 0, do not generate System Manager user profiles.

Auto generate IBM user profile

Identifies if an IBM user profile should be created automatically on receiving a new user sent from IFS.

Only applicable if you have chosen to create System Manager user profiles automatically.

Set to 1, generate an IBM user profile automatically. The User ID is the same as that allocated to the System manager user profile.

Set to 0, do not generate an IBM user profile.

Note: the password is a unique identifier and isn't available to the user, it is created from the IBMi API GENUUID.

Name order

This allows to decide which of the two parts of a name are used first.

Select option 1 to use first name then last name

Select option 2 to use last name then first name.

First name digits

This defines how many characters are taken from the leading characters of the First name. Chose to take from 0 to 8 characters.

Last name digits

This defines how many characters are taken from the leading characters of the Last name. Chose to take from 0 to 8 characters.

Add prefix to IFS Role name

Identifies whether an application prefix should be added to the Role Name to make the roll unique, or application specific in IFS.

Set to 1, add the application prefix.

Set to 0, add an application prefix.

Prefix

Enter the prefix if wanted on the IFS Role names. Must be entered if you have chosen to add an application prefix

Space after prefix

Identifies whether a space should be left between the prefix and the role name

Set to 1, leave a space.

Set to 0, leave no space.

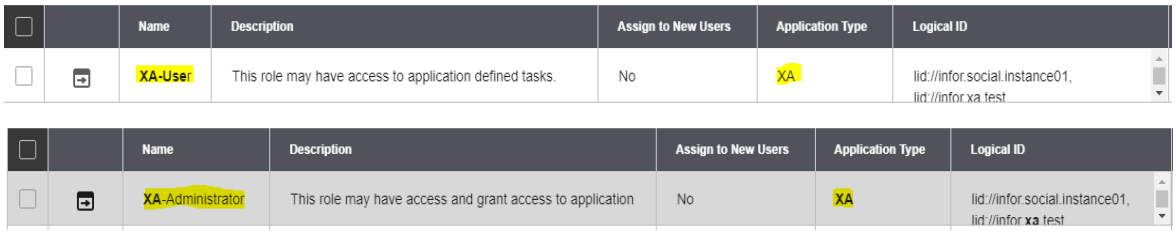
IFS user maintenance

Whether the System Manager copy of the IFS user can be maintained, currently not supported, and therefore prevented.

Infor Operating Services Setup

XA Security Roles

Infor OS Portal should have the XA application specific security roles in its IFS registry. You can see below roles in User Management -> Configure ->Master Data Types -> Security Roles.



	Name	Description	Assign to New Users	Application Type	Logical ID
☐	XA-User	This role may have access to application defined tasks.	No	XA	lid://infor.social.instance01, lid://infor.xa.test

	Name	Description	Assign to New Users	Application Type	Logical ID
☐	XA-Administrator	This role may have access and grant access to application	No	XA	lid://infor.social.instance01, lid://infor.xa.test

XA Initial Setup

This section explains the XA side setup need for this functionality to work. This is one-time setup and need to be done without fail.

BIS Organization Node Check

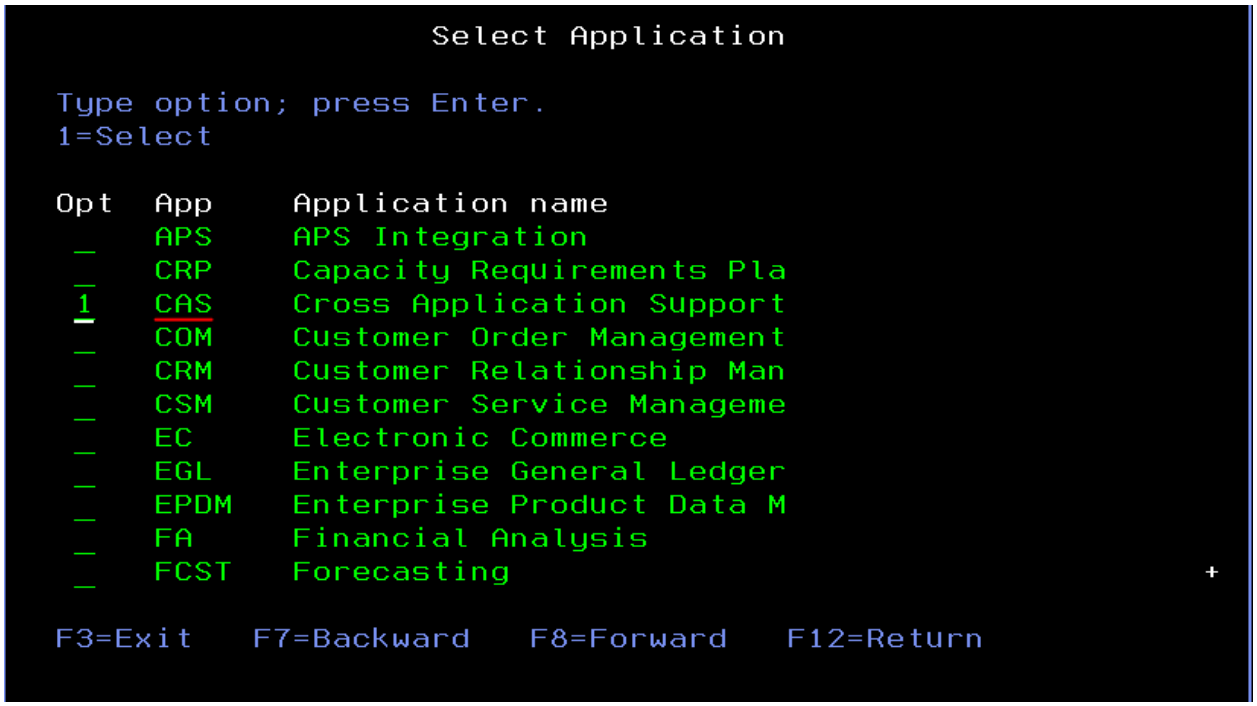
In XA Environment -> Application Settings -> Business Information Services -> Organization Node value need to be setup with proper value to reflect XA environment detail. This Organization Node value is sent as Accounting Entity value in Sync.Person BOD from XA to IFS and updated.

XA-User and XA-Administrator Role Setup

1 Go to CAS -> Maintenance/Change -> Security Maintenance.

2 Take option “1” and press ENTER to access Area and task authorizations.

1 At application selection screen, select Cross Application Support by taking option “1”, shown as below and press ENTER.



2 At Maintain Security Areas screen, navigate to ***Role: XA-Administrator*** and ***Role: XA-User***

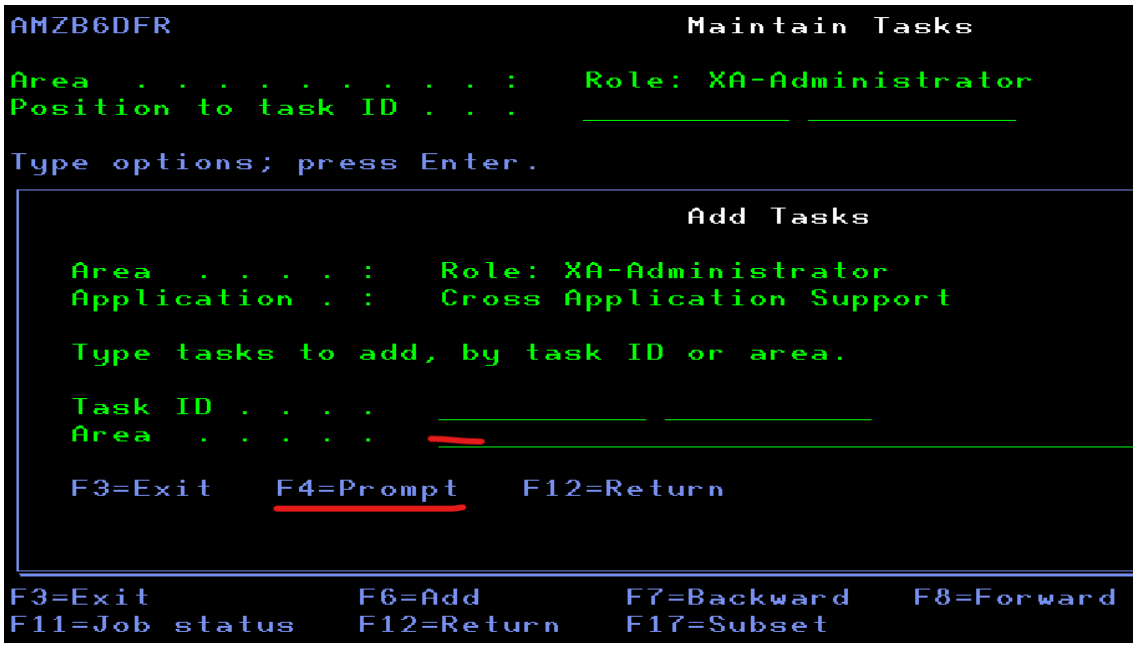
3 Take option “2’ and press ENTER to perform changes on Role: XA-Administrator security area.

```
AMZB5DFR                        Maintain Security Areas

Application  . . . . . :   CAS   Cross Application Support
Position to area . . . .   ____________________________________

Type options; press Enter.
  2=Change   4=Delete   5=Display   11=Authorize users

Opt  Area
__   Client Media File Tasks
__   Client Product Update
__   Client Publish Tasks
__   Client Report Tasks
__   Client System Preferences
__   Client Template Tasks
__   Client User Definitions
__   Inventory Status Tasks
_2   Role: XA-Administrator
__   Role: XA-User
```

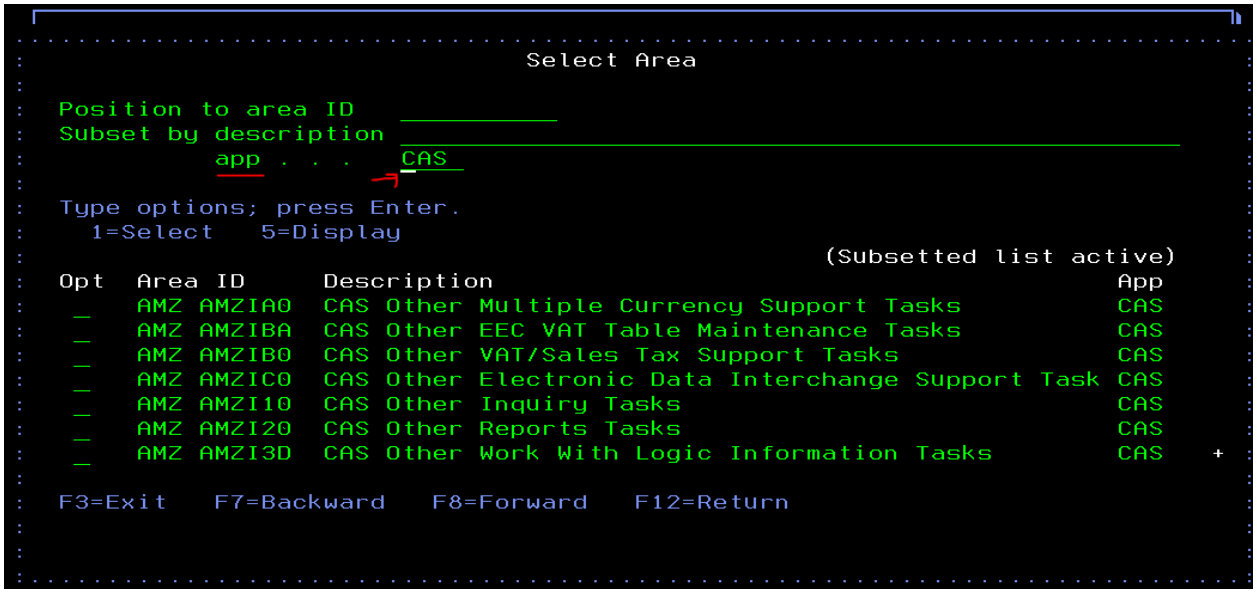
4 In Maintain Tasks screen, take “F6” to add new tasks, shown as below.

```
AMZB6DFR                          Maintain Tasks

Area  . . . . . . . . . . :   Role: XA-Administrator
Position to task ID . . .   __________ ____________

Type options; press Enter.
  4=Delete   11=Authorize users   22=Lock   23=Unlock

F3=Exit          F6=Add          F7=Backward   F8=Forward
F11=Job status   F12=Return      F17=Subset
No data to display.
```

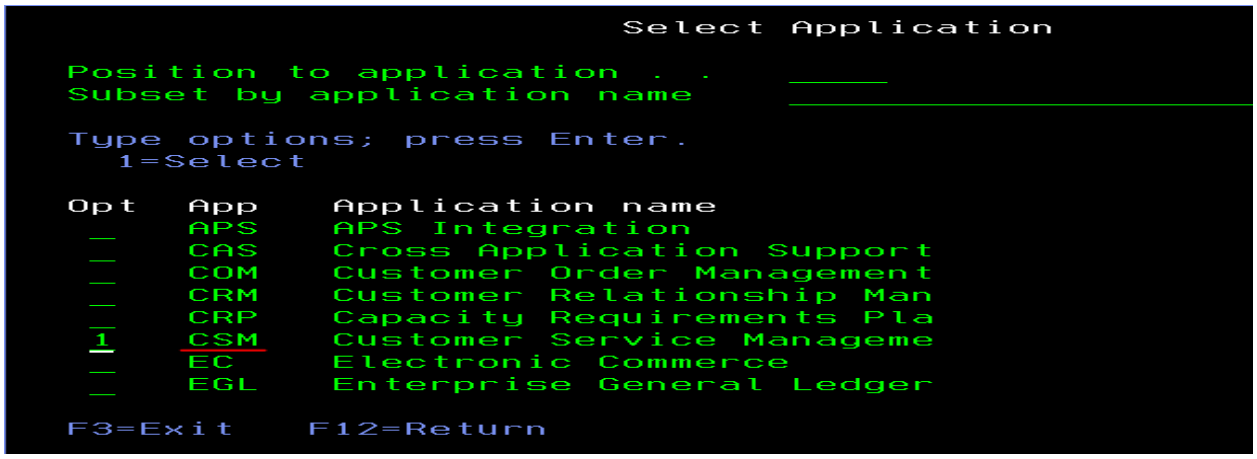
5 At Add Tasks screen, move cursor to Area and then take “F4” to Prompt the available options, shown as below.

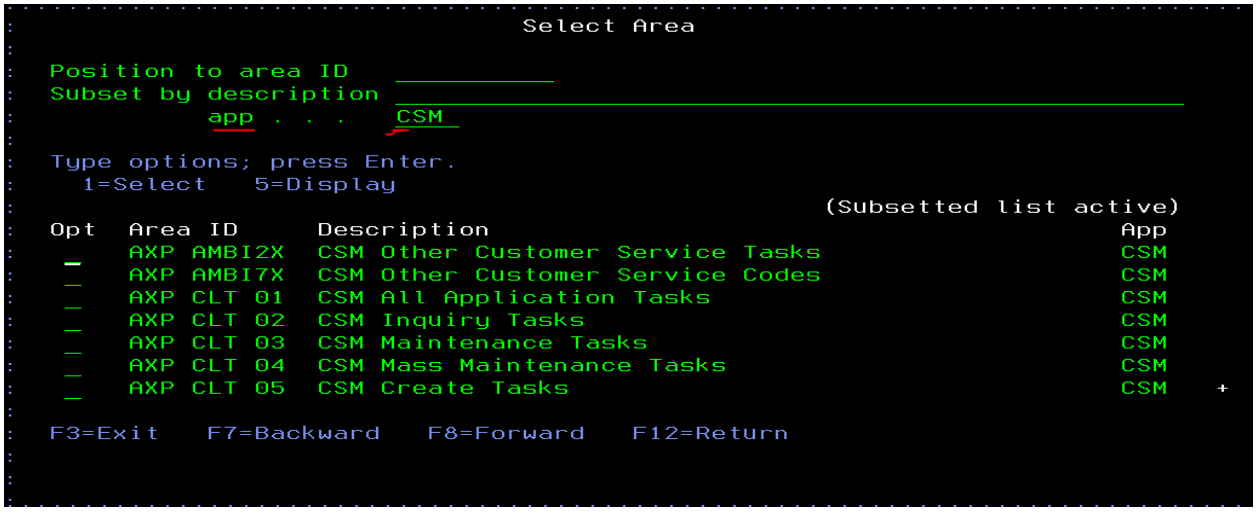


6 The below Select Areas screen shows the list of CAS application areas. If you want to get the other application areas, place cursor at app and take “F4”, shown as below.

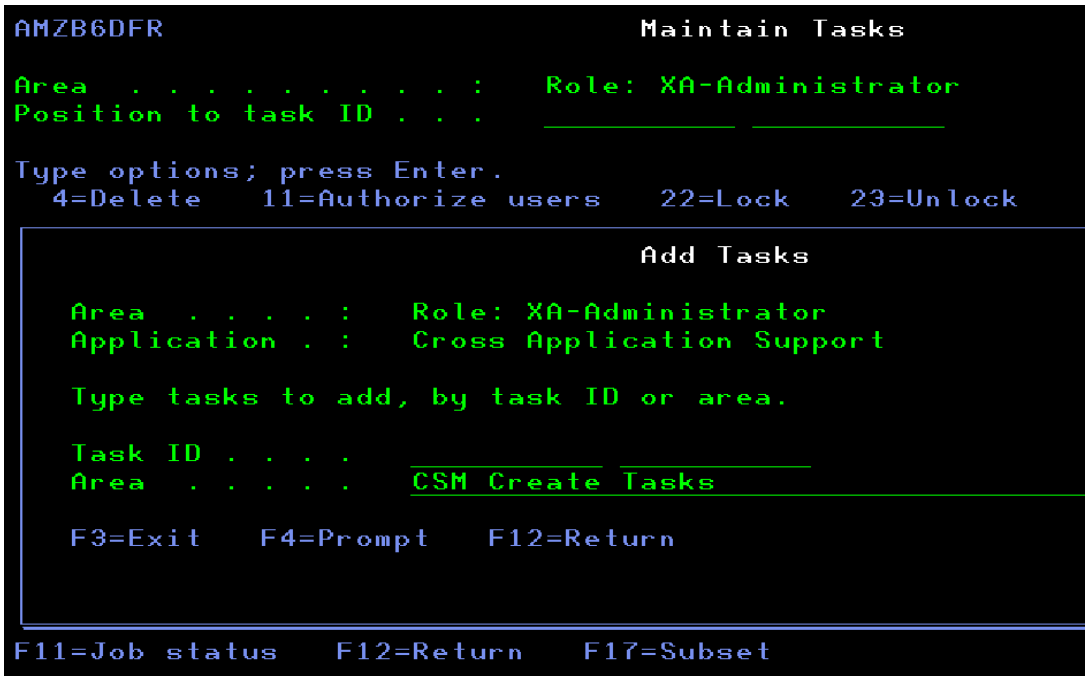


7 For an example: Here we are selecting the ***CSM*** application by taking option “1” and press ENTER, shown as below.

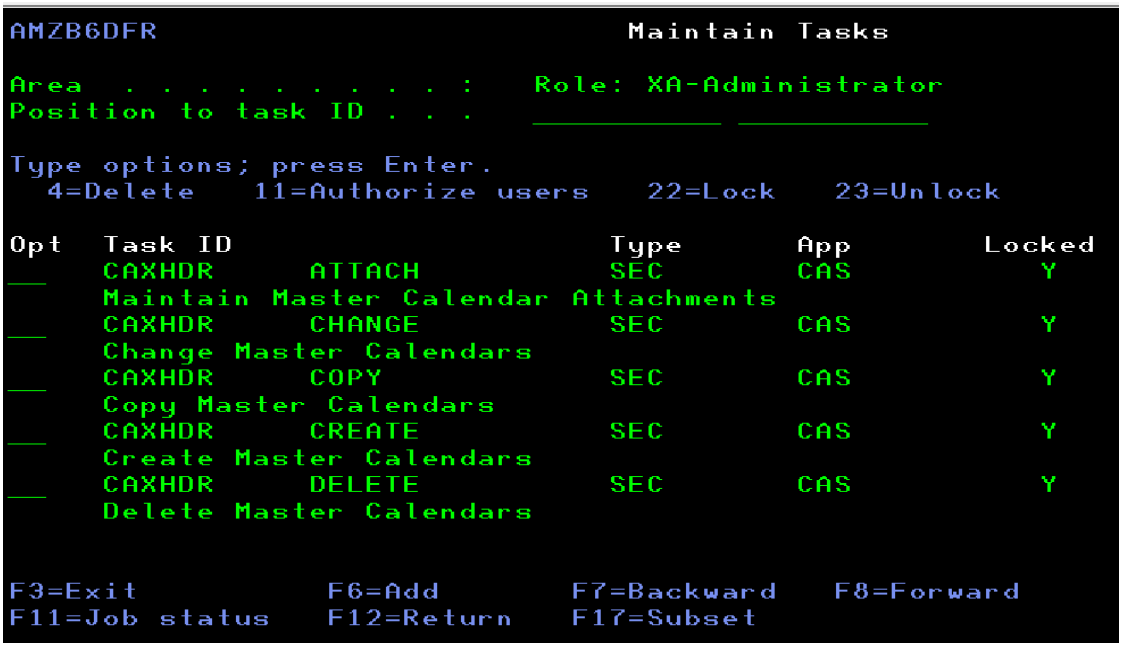




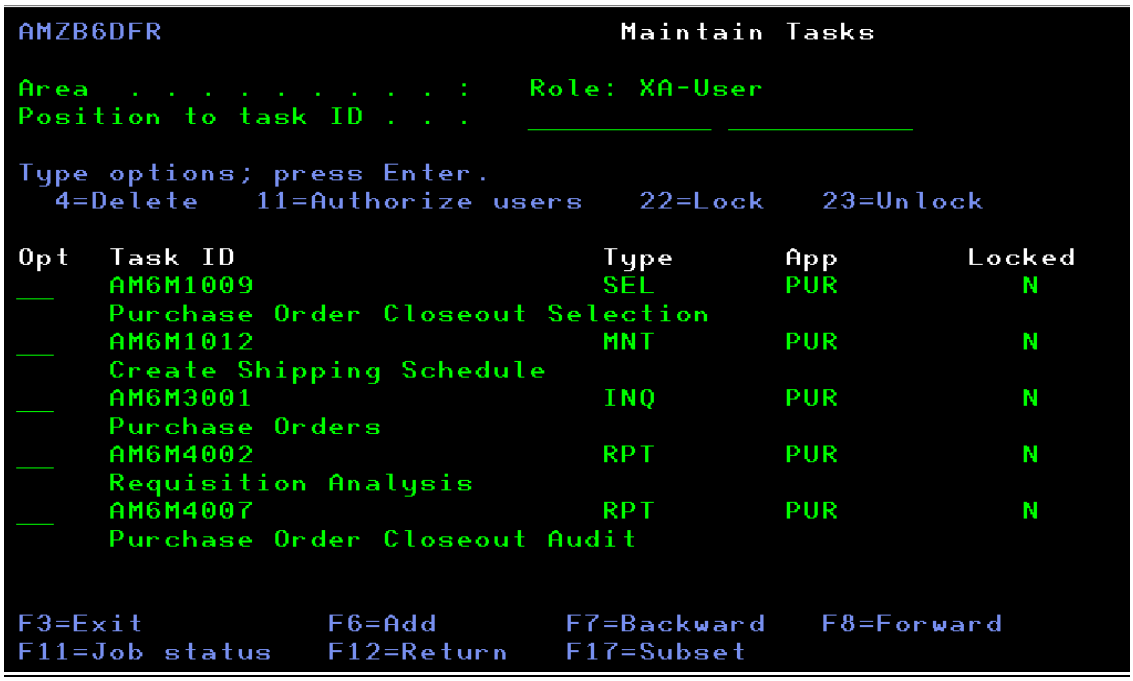
8 From the list of CSM application areas is displayed, select one of the application areas to which you would like to add as a task to ***Role: XA-Administrator*** security area.



Now the ***Role: XA-Administrator*** is authorized with required Tasks.



Follow same process to add tasks into ***Role: XA-User.***



Changes to APGBCPHY and APGBC01P objects

Login to XA and run command *EDTOBJAUT AULAMF3/APGBCPHY *FILE*

Add or change “AMAPICS” user with “*CHANGE” as Object Authority.

```
                           Edit Object Authority

Object . . . . . :   APGBCPHY        Owner . . . . . :   AULOWNER
  Library  . . . . :     AULAMF3     Primary group . . . :   AULAMDBUSR
Object type  . . . . :   *FILE       ASP device . . . . :   *SYSBAS

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . .   *NONE

                          Object
User        Group       Authority
*PUBLIC                 *EXCLUDE
*GROUP      AMAPICS     *CHANGE
*GROUP      AULAMDBUSR  *CHANGE
*GROUP      AULOWNER    *ALL
```

Similarly run *EDTOBJAUT AULAMF3L1/APGBC01P *FILE.*

Add or change “AMAPICS” user with “*CHANGE” as Object Authority.

```
Object . . . . . :   APGBC01P        Owner . . . . . :   AULOWNER
  Library  . . . . :     AULAMF3L1   Primary group . . . :   AULAMDBUSR
Object type  . . . . :   *FILE       ASP device . . . . :   *SYSBAS

Type changes to current authorities, press Enter.

  Object secured by authorization list  . . . . . .   *NONE

                          Object
User        Group       Authority
*PUBLIC                 *EXCLUDE
*GROUP      AMAPICS     *CHANGE
*GROUP      AULAMDBUSR  *CHANGE
*GROUP      AULOWNER    *ALL
```

BOD Setup

Below bods are supported by XA to implement this functionality.

Incoming BODs

Sync SecurityUserMaster

New and updated IFS user is published in the form of Sync.SecurityUserMaster bod from IFS to XA through ION.

Outgoing BODs

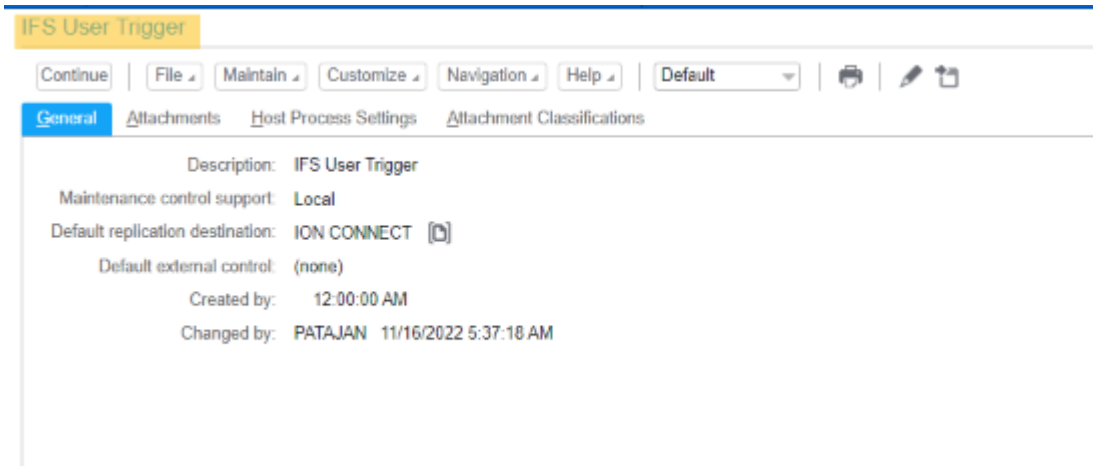
Sync Person (XA User)

New and updated XA user to be published as a Sync Person bod to IFS. The user id is updated as ERP Person ID for the User in IFS in Infor OS Portal.

Object Settings

Go to Environment ->Object Settings -> IFS User Trigger, set the “Maintenance control support” to “Local” or “Both” and select the “default replication destination” with respective destination meant for ION.

Sync Person bod is only published if this setup is done.



Activating the System-Link Transformations

The following SL transformation need to be activated in XA to use this functionality:

System-Link Request	System-Link Transformation
XA_Replicate_IFSUser	XA_Replicate_IFSUser_SyncPerson_BOD_2_12_0.xsl
XA_Sync_SecurityUserMaster	XA_Sync_SecurityUserMaster_BOD_2_12_0.xsl

Chapter 10 Configure and Use Infor OS Portal

This chapter provides information on how to use Infor OS Portal with XA using SiW AnyWhere application.

Infor OS Portal is an application framework that provides a common user interface for integrated Infor ERP applications.

The navigation panel accesses several elements of the Infor OS Portal. This includes the navigation menu, used to display Infor ERP applications.

The smart panel is a collapsible tray that hosts contextual and non-contextual widgets. The widgets display content based on application screen data to help users work smarter. You can share content between widgets.

Users can customize their experience with Workspaces by creating shortcuts to frequently used application screens and widgets.

Infor OS Portal supports drill-back capability among Infor applications. Users can navigate from one application to another to track transactions, transfer data, and report updates.

Additionally, Infor OS Portal supports Bookmarks and Recently closed functionality. Bookmarks enables you to save and access important pages or content links. Recently closed is where you can reopen your recently closed pages or applications.

To get familiarity with Infor OS Portal and the supported functionality go through the guides below at docs.infor.com.

Infor OS Portal Administration Guide
Infor OS Portal User Guide

Security Roles Specific to perform activities on Infor OS Portal

Infor-SuiteUser:

“Infor-SuiteUser” is the end-user role. This is the default role assigned to all the users. Users with this role have access to the portal only.

MingleAdministrator:

“MingleAdministrator” is the role assigned to users to have access to administration pages in Infor OS Portal. By design, the “MingleAdministrator" role is added to all applications in the tenant. The user with this role can view all application icons on the Navigation Menu panel. The user's ability to open the application and access functionality, however, is controlled by the application security. Users who have this role can see the Portal menu item in the Infor OS Portal application. Users who have this role can manage this content: **Applications, Widgets, Pages, Workspaces, Drillbacks, General Settings**.

Portal-ContentAdministrator:

Users with this role are content administrators in Infor OS Portal. Content administrative users have full permission to content-related tasks so that they can create published content and manage published content. They can create, edit, and delete any published workspaces or widgets, not only their own content. It is not mandatory to use this role as the administrator has full access to all content as well.

Users with this role have access to these Portal administration features: **Widgets, Pages Workspaces.**

Note: For regular Portal users “Infor-SuiteUser” role should be assigned. For admin users “MingleAdministrator” or “Portal-ConentAdministrator” roles should be assigned.

This chapter covers the following functionality supported by XA application in Infor OS Portal.

- Migration of data from Infor OS to Portal
- Disabling Context app views in Portal
- Accessing XA Application in Portal
- Accessing the Smart Panel
- Insight Group in Smart panel
- Deletion of Default Insight Group in Smart Panel
- Creating Insight Group to configure XA Context Widget(s)
- Pop-Out Insight Group with Widgets
- Publishing and Edit Permissions on Insight Group
- Publishing XA Context Widgets
- Configure and use Bookmarks
- Configuring Tasks and Context Viewer Widgets in Insight Group
- Configuring Drillbacks in Portal
- Using Drillbacks from Tasks in Inbox
- Using Drillbacks from Tasks List in Insight Group
- Using Recently Closed

Functionality not supported by XA in Infor OS Portal

Below section explains the functionality not supported by XA application in Infor OS Portal.

Workspaces

Workspaces help users boost productivity by providing shortcuts to application screens and combining relevant widgets.

A workspace can be a copy of an application created by a user, admin, or application, or a dedicated page for widgets only. By creating a copy of an application, you have more control over the application than the default application. The user can control the default settings or choose what page within the application opens upon launch. A widget workspace allows the user to set up a page for specific widgets, separate from any application. Workspaces can also be set as startup page to open upon launch.

Configuring and accessing XA applications in Workspace is not supported.
Configuring and accessing XA Context widgets in Workspace is not supported.

Context App Views

Primary, Secondary and Tertiary Context app views supported by XA are replaced by the new widget called “XA IDF Context” in the new Portal. Ther is no change in functionality when compared between old Context app views and new XA IDF Context Widget. Part of Widgets adoption requirement, the old Context app views are added as single Widget in Portal. Same widget can be configured as all 3 types of Context widgets by changing the Index value. For more information on how to use XA IDF Context widget refer to below sections in this Chapter.

Note: Once all the customer tenants are migrated from old Infor OS to new Portal, the Primary, Secondary and Tertiary Context Apps will be deleted (deprecated) from Infor OS registry and will not be available to use.

As of now the Admins on the Portal need to follow Disabling Context app views in Portal section below to disable the old Context app views in Portal. This will make them unavailable in Widget Catalog so that users can’t use while configuring in Insight Groups.

Migration of data from Infor OS to Portal

Migration is the process of pushing all the data (Applications, Context Apps, configurations etc.,) from old Infor OS to new Infor OS Portal.

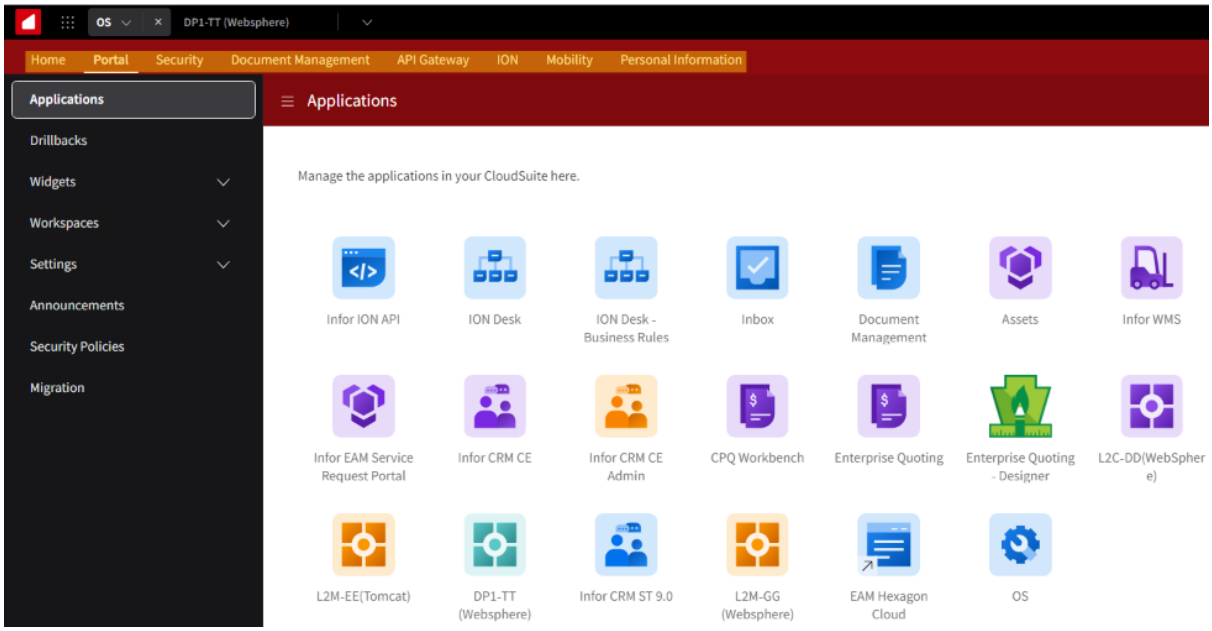
This step is required only when Customer is migrating from Infor OS to new Portal.

All Application data does not get migrated and will remain as-is in old Infor OS. The migration consists of user content and settings such as application settings, bookmarks, homepages and Infor Go favorites.

Follow KB2277419 in Service Now to perform migration process.

Note: It is recommended that you refresh the page after completion of migration. A refresh message will be displayed at the top of the portal page.

After successful migration, the "**OS** -> **Portal** -> **Applications**" section will be updated with all the applications from Infor OS Portal.

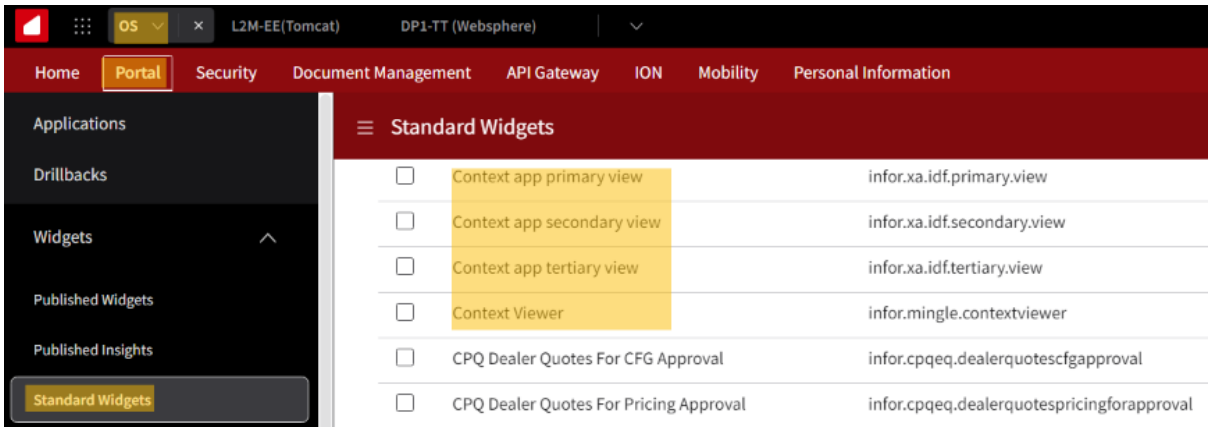


For more information on Applications, please refer to Chapter 3: Applications in ***Infor OS Portal Administration Guide.***

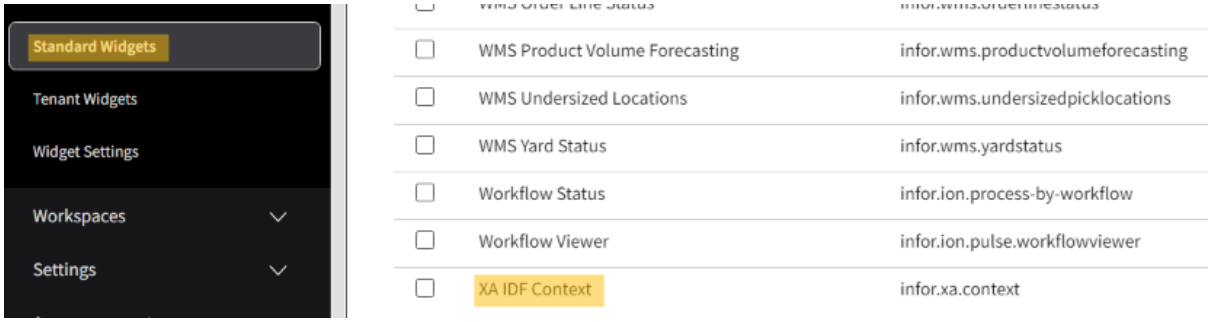
To view the XA Context Apps and widgets go to **OS** -> **Portal** -> **Standard Widgets**.

Primary, Secondary and Tertiary Context App views are replaced by the new XA IDF Context Widget in Portal.

Once all the customers are migrated from Infor OS to new Portal, the Primary, Secondary and Tertiary Context Apps will be deleted from Infor OS registry and will not be available to use.



The new "**XA IDF Context**" widget is also available here.



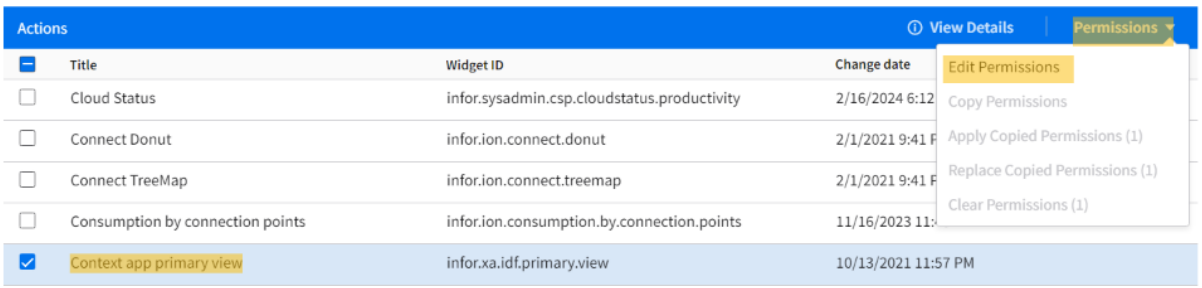
Disabling Context app views in Portal

As mentioned in limitations above, the Primary, Secondary and Tertiary Context App views are replaced by the new XA IDF Context Widget in Portal.

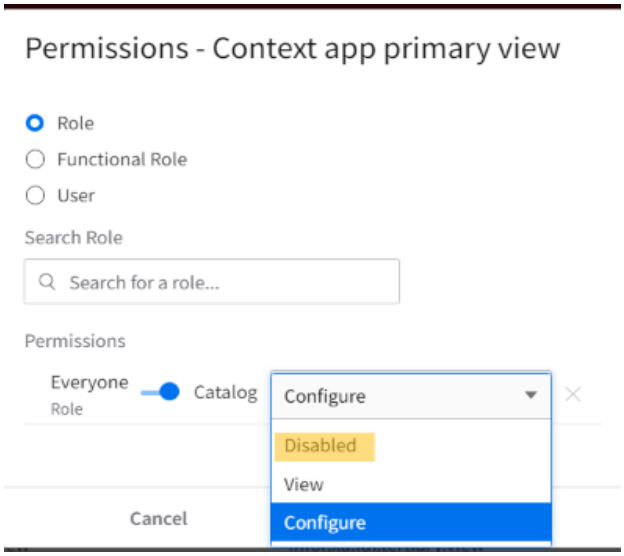
All the XA Users need to stop using these 3 widgets in Infor OS Portal.

To avoid further issues, the Administrator can disable the 3 Context Apps views in Portal by following below steps.

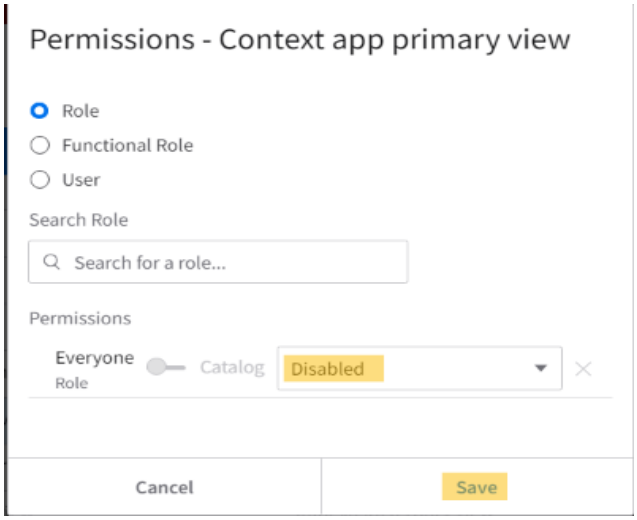
Go to **OS** -> **Portal** -> **Standard Widgets,** select the 3 context app views one by one and click on Permissions -> Edit Permissions.



In **Permissions** window, you can select the drop down. Change the Catalog from **Configure** or **View** to **Disabled**.



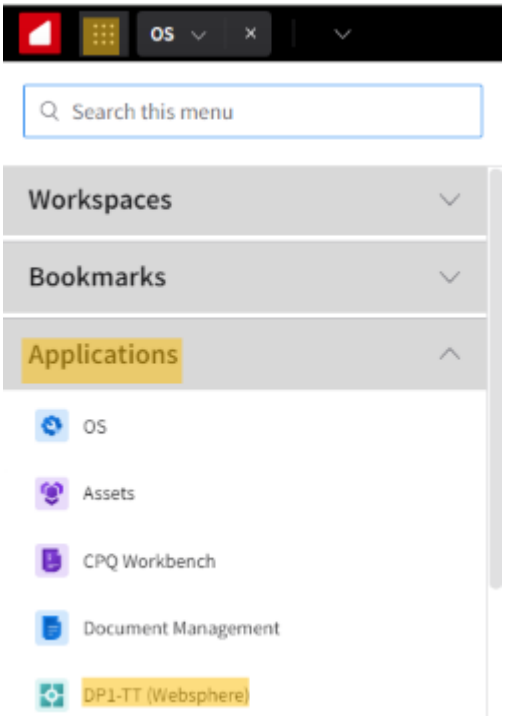
Click-On Save.



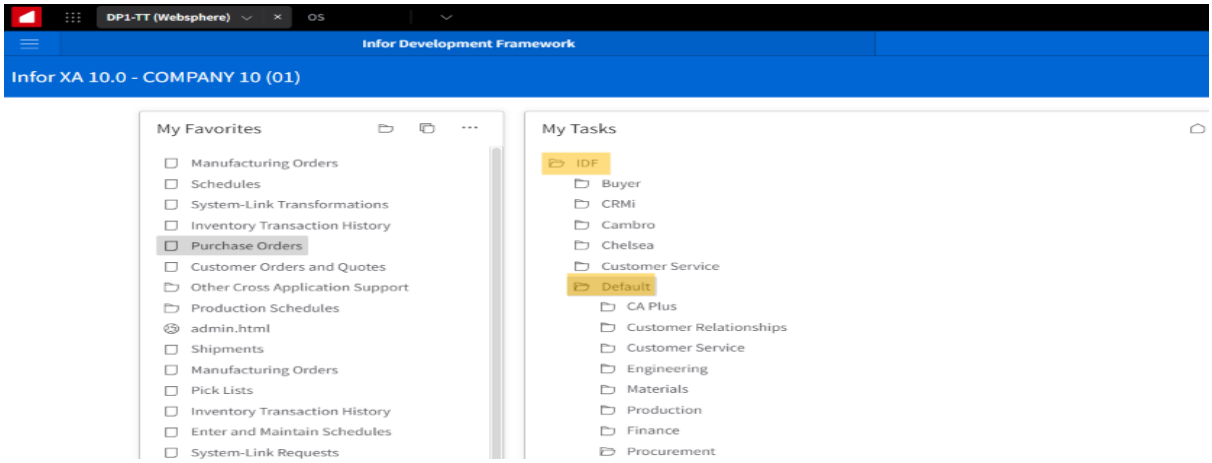
Note: Once disabled, these 3 Context app view widgets are disabled on this tenant and users cannot view or select them in Widget Catalog to add in Insight Groups.

Accessing XA Application in Portal

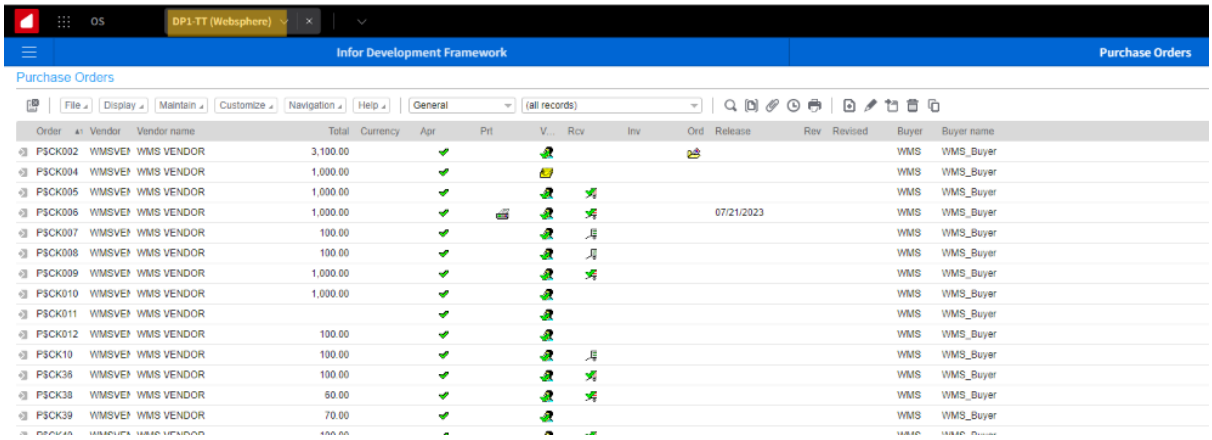
Goto **Navigation Menu** -> **Applications** -> Select the required XA Environment to Launch.



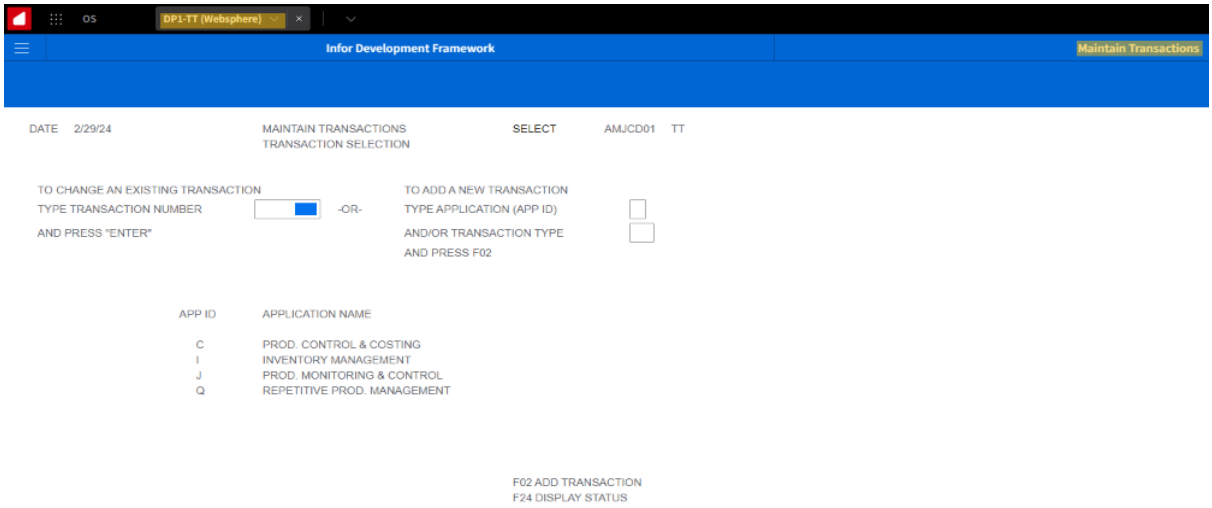
IDF Home page:



L1 or IDF tasks:

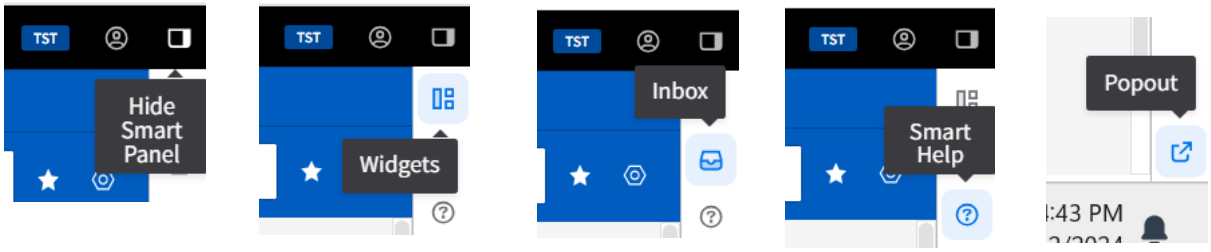


L2 or GS tasks:



Accessing the Smart Panel

The smart panel is collapsible tray which can contain Insights, Coleman DA, Inbox and Smart Help. The smart panel content can be accessed using the toolbar on the right of the application or workspace The content available in the smart panel depends on the current application.



For more information on Smart Panel, please refer to Chapter 4: Using the smart panel in ***Infor OS Portal User Guide.***

Insight Group in Smart Panel

An insight is like a small widget page contained within the smart panel. A published workspace can have both private and public Insights. A public insight will be displayed for all users using the Portal, while the private insights will only be visible to the user who added it. An insight can also be published or embedded. Published means it will be available in the Insight Catalog and can be added as insights to other applications and by other users. An embedded insight will only be available within this workspace.

All contextual applications will be ported over as contextual widgets and will be available inside the Smart Panel. Infor OS Portal provides the ability to group a set of Widgets in the Smart Panel. These are groups called Insight Groups. It can display a predefined group of widgets associated with the current application.

Note: if the option is not available, the feature has turned off. Contact your administrator for more information.

If an Insight Group is created with context widgets like "**XA IDF Context**" Widgets, then that Insight Group will belong to that specific XA application and will work only with that application.

The XA IDF Context Widgets will be using that XA application specific logical Id to retrieve and display the data.

Administrator can create a publish Insight Group for a specific XA application and publish it for other users to re-use.

If you have multiple XA applications configured on Portal, Insight Group created for one XA application and published cannot be used for different XA applications.

If an Insight Group is created with non-context widgets like Tasks List, Bookmarks etc., then that Insight Group can be published and used by different XA applications.

Based on business need and type of data need to be displayed in the Widgets in Insight Group, users can decide on using private or published Insight Groups and Widgets.

For more information on using Insight Groups, please refer to Chapter 4: Using the smart panel in ***Infor OS Portal User Guide.***

Note: If you have 1 or more Context App views configured for XA environment in old Infor OS. After migration of data from Infor OS to new Portal, default "Widgets" Insight Group is created

(containing Context App views migrated from old Infor OS) in new Portal. Users need to delete the “Widgets” Insight Group and created a new Insight Group with desired name using new IDF Context Widget(s) in new Portal.
If the XA environment is newly configured in Infor OS Portal after migration, then the new Insight group need to be configured as per business need.

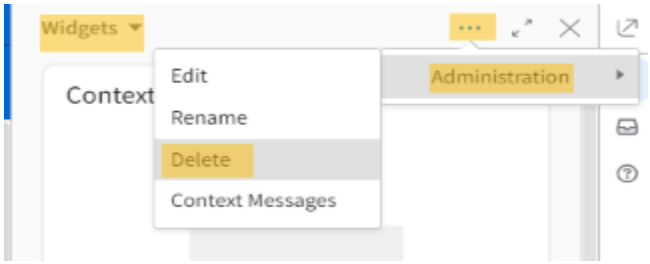
Deletion of Default Insight Group in Smart Panel

The migration process will create a default Insight Group called “**Widgets**” for each XA application migrated from old Infor OS to new Portal. All contextual applications migrated from Infor OS are added to this default group in Infor OS Portal in combination with the current configuration of Default Widgets in Infor Registry.

Note: The 3 XA Context app views (**Primary, Secondary and Tertiary**) are replaced by single Context Widget called “**XA IDF Context**” in Portal. Existing “**Widgets**” Insight Group need to be deleted and new Insight Group can we be created for that specific XA application by individual user or by Admin. While creating new Insight Group the new “XA IDF Context” widget need to be configured and used to setup 3 Context Widgets.

The Insight Group created by Administrator can be published to all the other users on the Portal tenant to re-use the Insight Group and the widgets configured in it.

To delete the default “**widgets**” Insight Group, open the required XA application, go to “Widgets” Insight Group ->Click-On Ellipsis (…) Under Administration select the delete option and Click-On confirm delete.



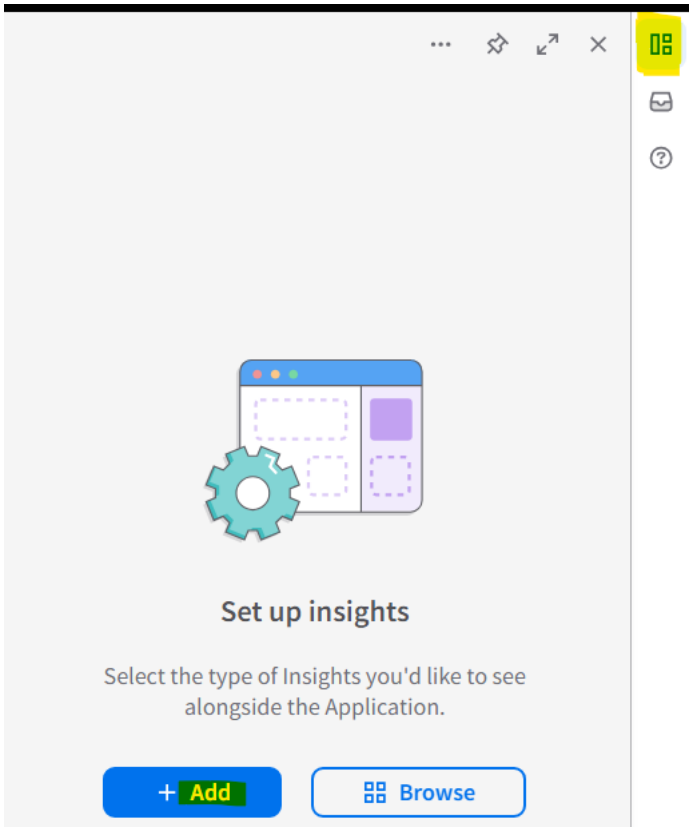
Creating Insight Group with new XA Context Widget(s)

An Insight Group can be created by a user (as private) or Administrator (as public) as per business need.

Created Insight Group can be used and published to different users on the same tenant as well.

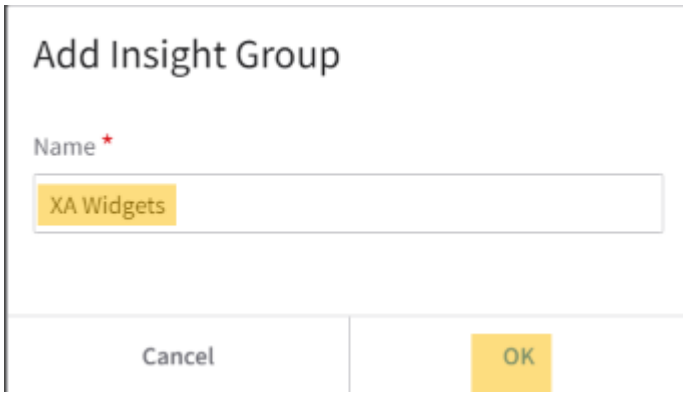
Creating Insight Group

Open required XA environment. Go to Widgets Insight Group on extreme right side in Smart

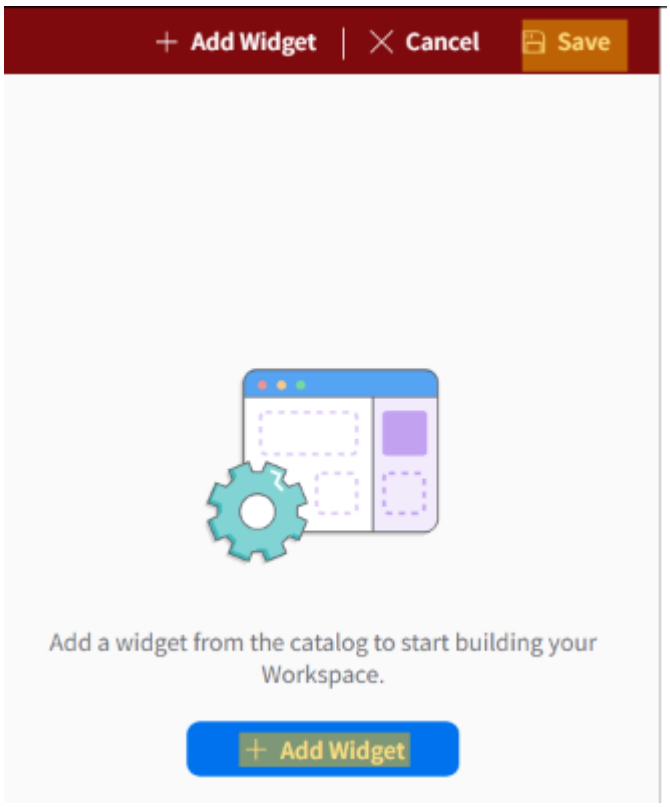


Panel. Click-On “+ Add”.

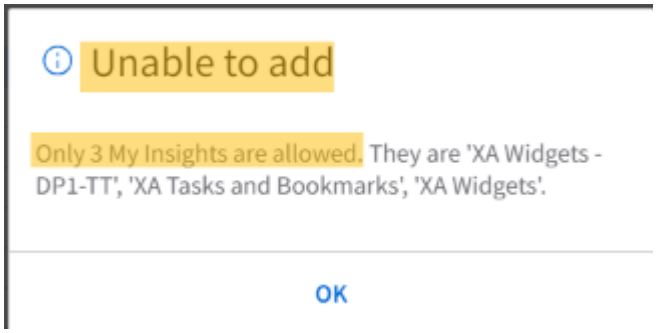
Provide desired Insight Group Name (Ex: XA Widgets) and Click-On “OK”.



Click on Save, to save the Insight Group or “+ Add Widget” to add widgets while creating Insight Group.



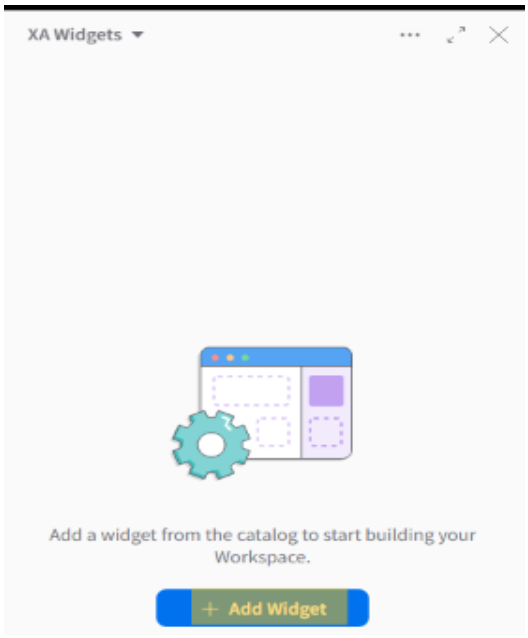
Note: Maximum of 6 (3 Private and 3 Public) Insight Groups can be add to an Application in Portal.



Adding Widgets in Insight Group

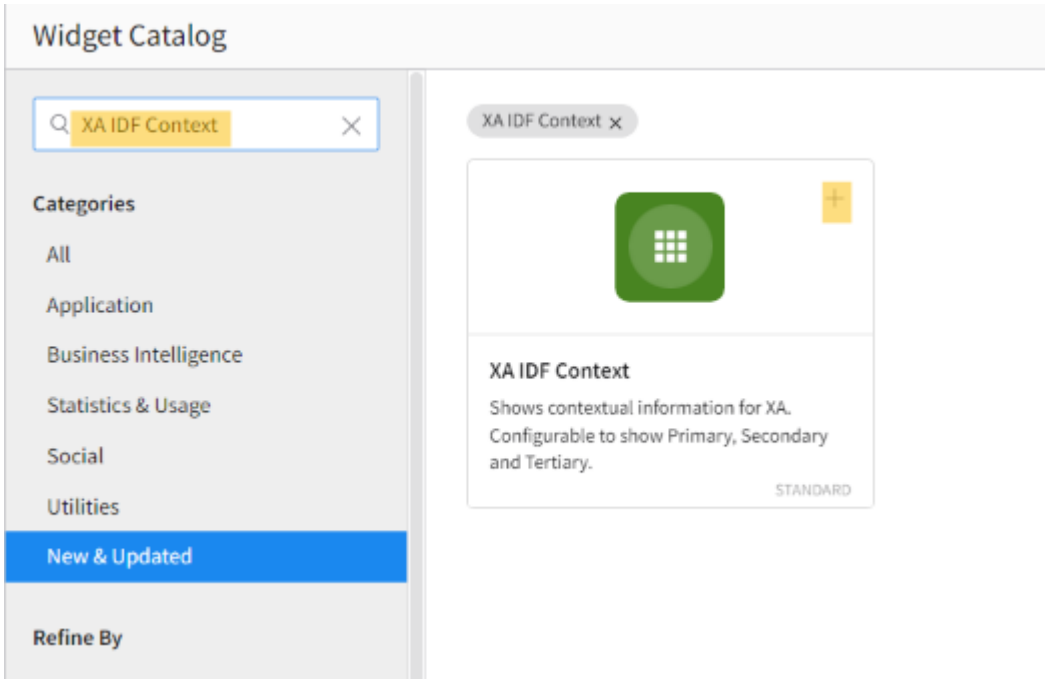
Before getting started with using Widgets in Portal go through Chapter 5: Widgets in ***Infor OS Portal Administration Guide.***

Open previously created Insight Group, click on **"+ Add Widget**" button to add Standard or Published Widgets into this Insight Group.

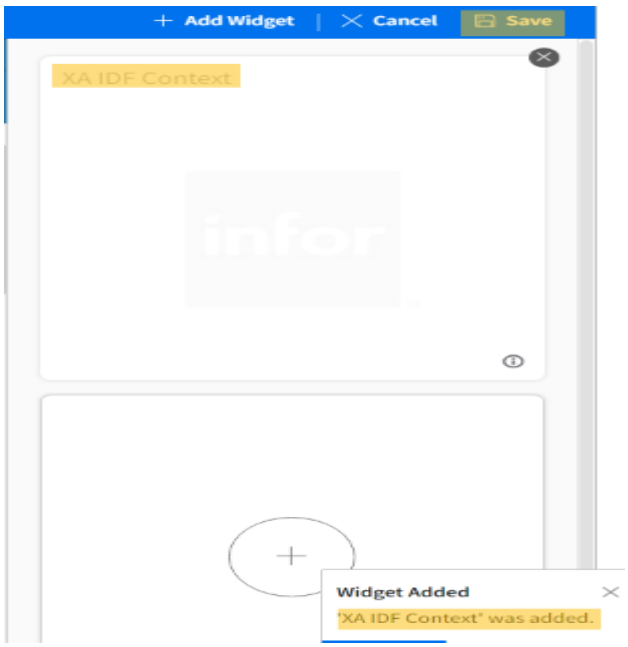


This will open “**Widget Catalog**” page to search and add the required widgets to the application.

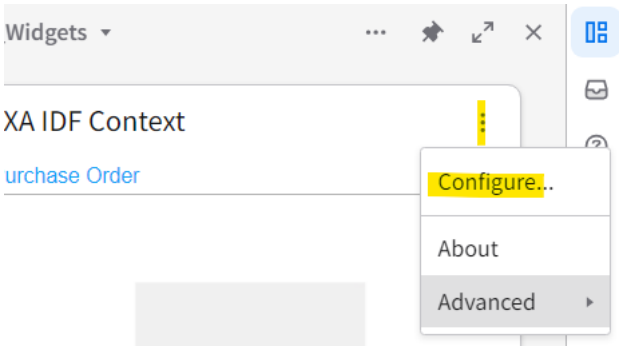
In this example we are use “**XA IDF Context”** Widget as Primary Context Widget. Search for “XA IDF Context” in the Widget Catalog and then Click-On “**+**” to add Widget to Insight Group. Closet the Widget Catalog page.



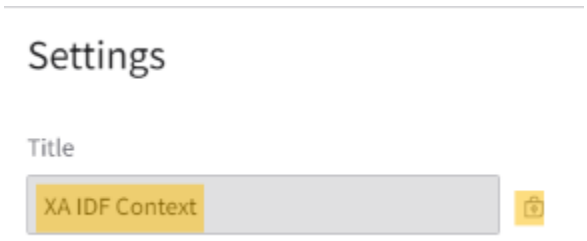
Now XA IDF Context Widget is added to Insight Group and Click-On “**Save**”



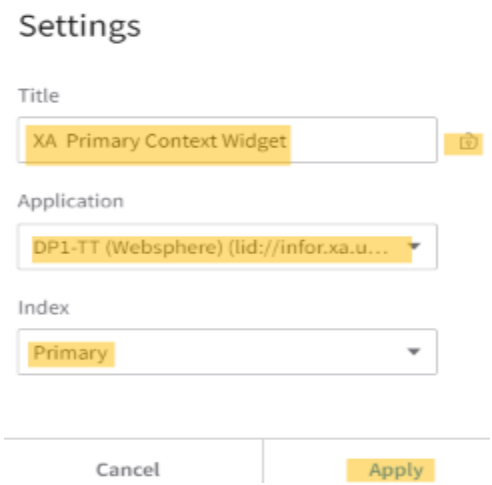
Now select the above added XA IDF Conext Widget and Click-On “**Configure**…” option” to modify the Widget Settings.



Click-On “**Lock**” Icon to change the default Title. Change the Title to desired one. Ex : “XA Primary Context Widget”. Click-On “**Lock**” Icon to save the changed Title.

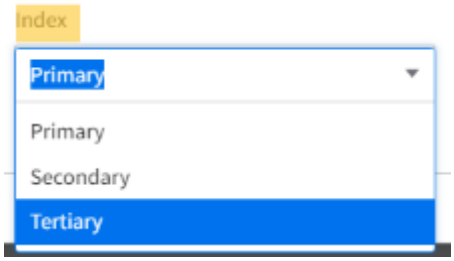


Select the valid application logical Id from “**Application**” drop down and “**Index**” as Primary from drop down and Click-On “**Apply**” to create XA Primary Context Widget.



For the same widget, you can find the “Secondary” and “Tertiary” **Index** in drop down. These indexes can be used to configure respective “Secondary” and “Tertiary” context Widgets.

Note: This single XA IDF Context widget with 3 different indexes is the replacement for Primary, Secondary and Tertiary Context Views in old Infor OS.

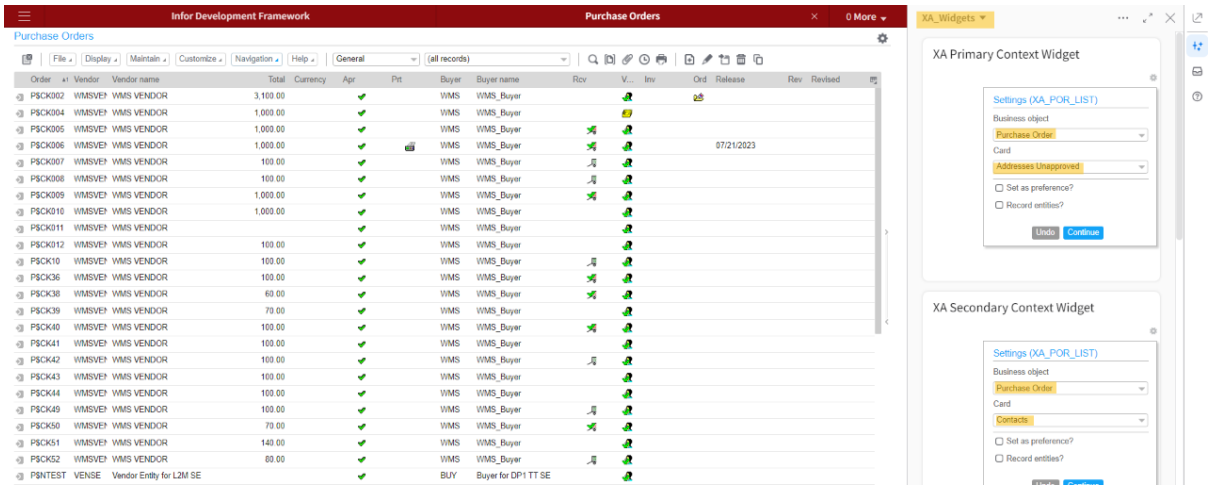


Similarly repeat the above steps to configure XA Secondary and Tertiary Context Widgets by selecting Secondary or Tertiary as Index.

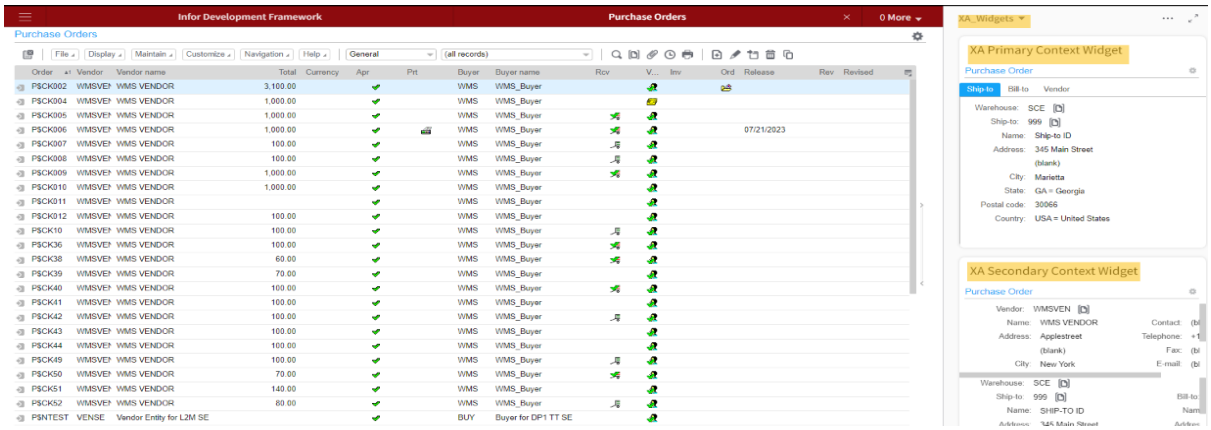
Follow below sections in Chapter 11 Infor Business Context IBC in this guide to configure these widgets to load and display data.

Configuring Business Object and Card in XA Context Widget

Configuring Preference definition in XA Business Object



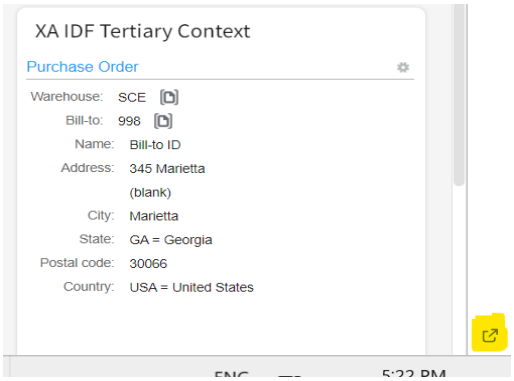
Purchase Order details displayed in XA Primary, Secondary Context Widgets

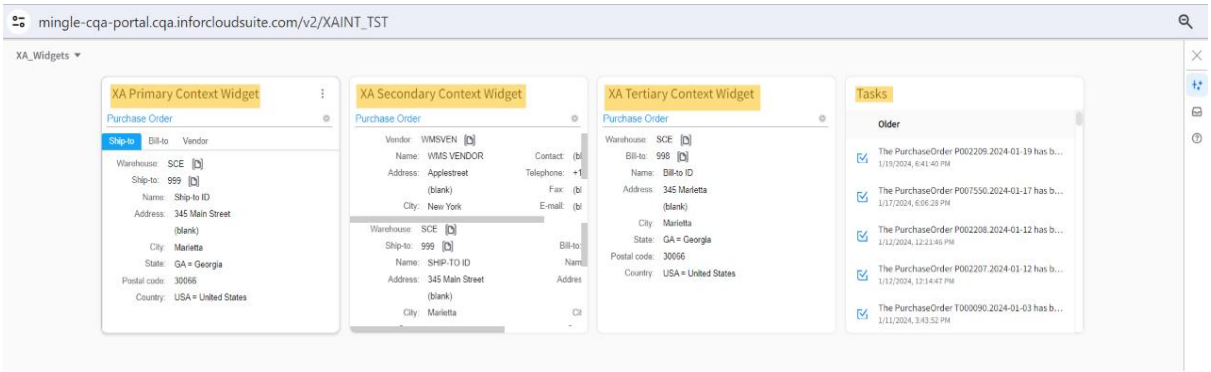


Pop-Out Insight Group with Widgets

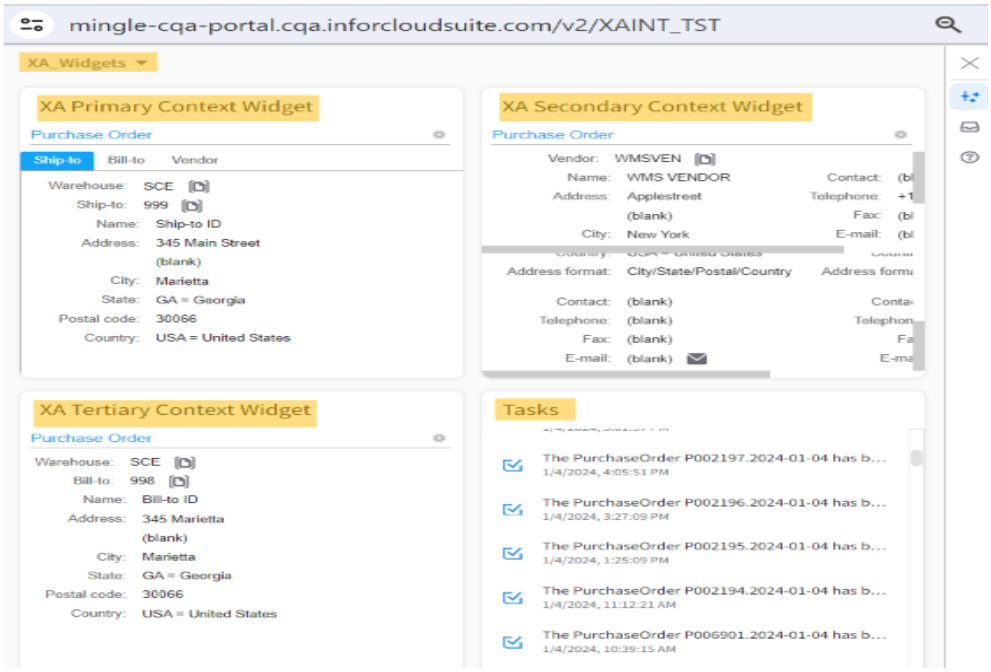
By using the Pop-Out feature we can view the Insight Group having Primary, Secondary, Tertiary Context Widgets and other widgets in Separate window.

Click-On Pop-Out at bottom right side of the screen.





This Pop-out window can be resized as per need.

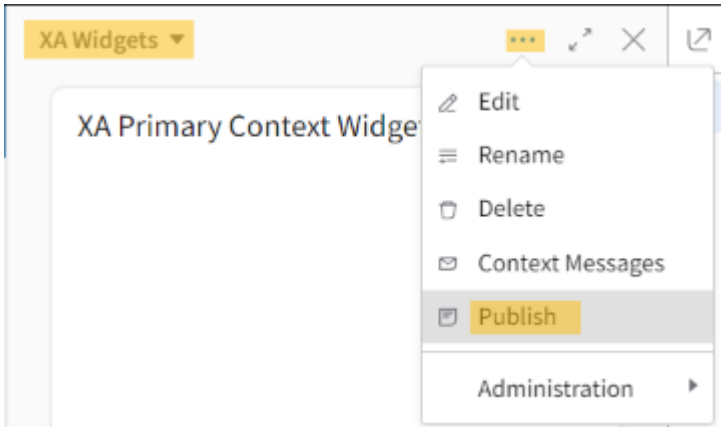


Publishing and Edit Permissions on Insight Group

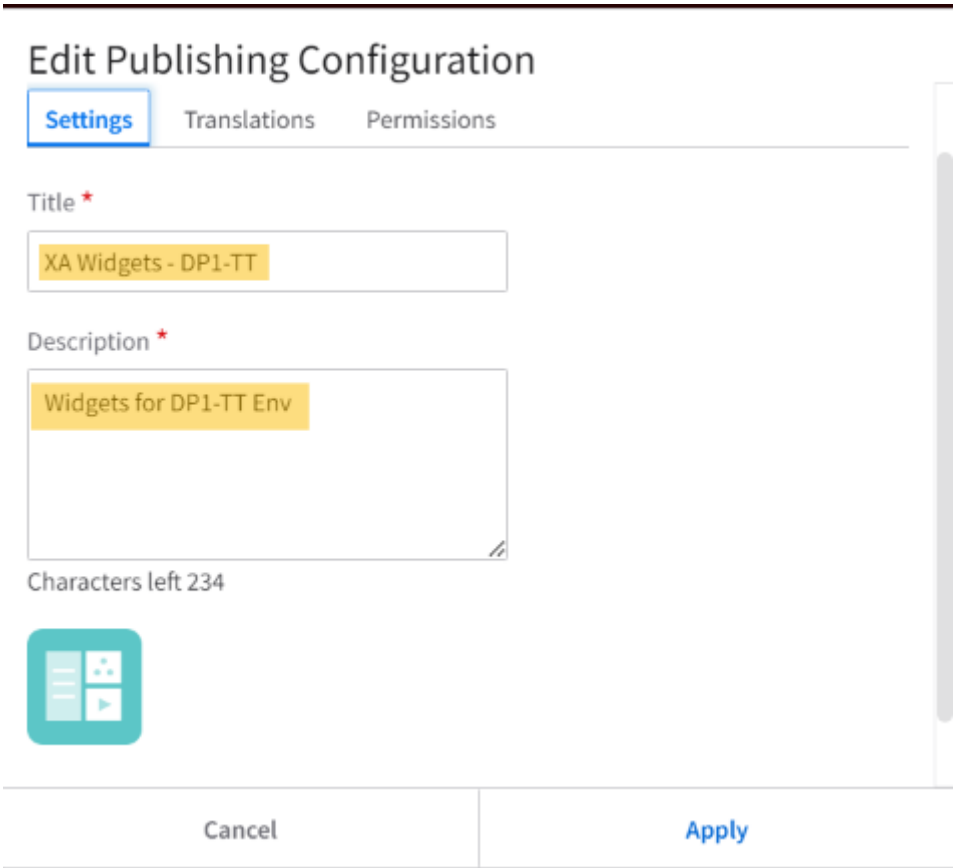
The Insight Groups created can be published by the creator having "**Portal – ContentAdministrator**" or "**MingleAdministrator**" role to other users on same Infor OS Portal tenant. Insight Groups that can be reused by different users on same tenant can be published to avoid duplication.

As mentioned above, the Insight Groups created with context widgets can be published to different users on the same tenant and can be used with the same XA application.

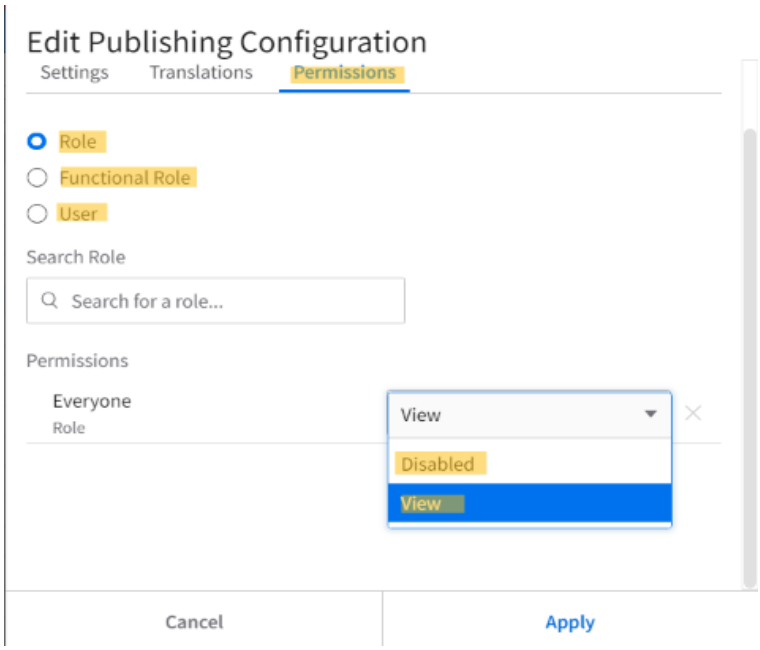
Go to XA Widgets Insight Group Ellipse (…) and Click-On **Publish**:



Under **Settings** section, we can change the **Title**, **Description**, and **Icon** as per business need.

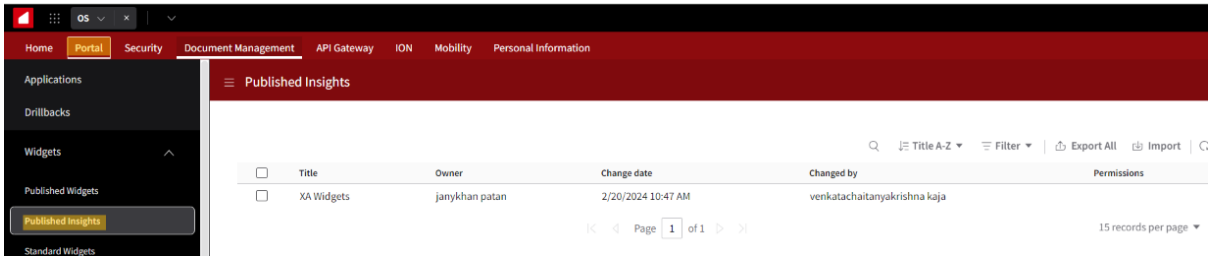


Under **Permissions** section, we can limit the access or disable the Insight Group to users by selecting Roles or User etc.

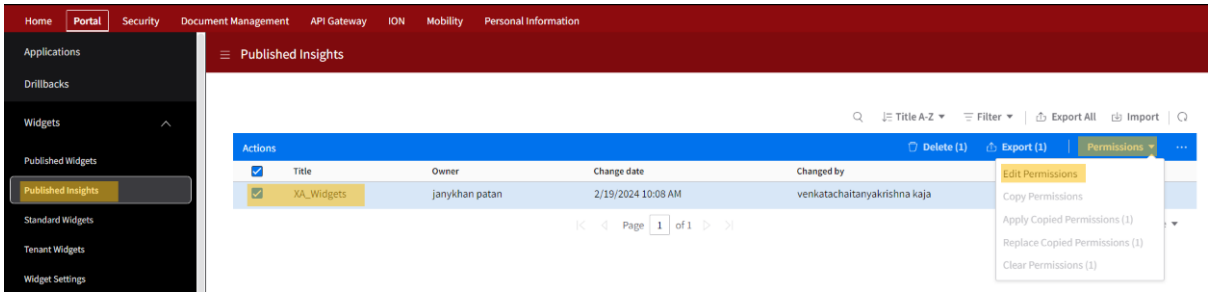


Click-On **Apply** to save changes.

Navigate to Portal and Click-On “**Published Insights”** to Check this Insight Group in List of Published Insights.



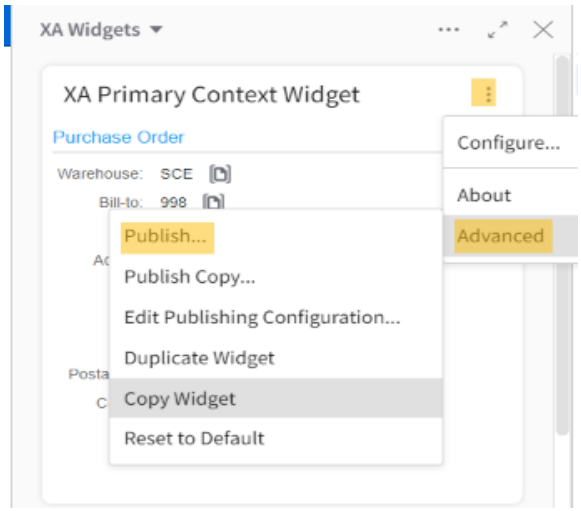
Select the Insight Group and Click-On “**Edit Permissions”**, this is same as above where we setup Permissions to limit the access.



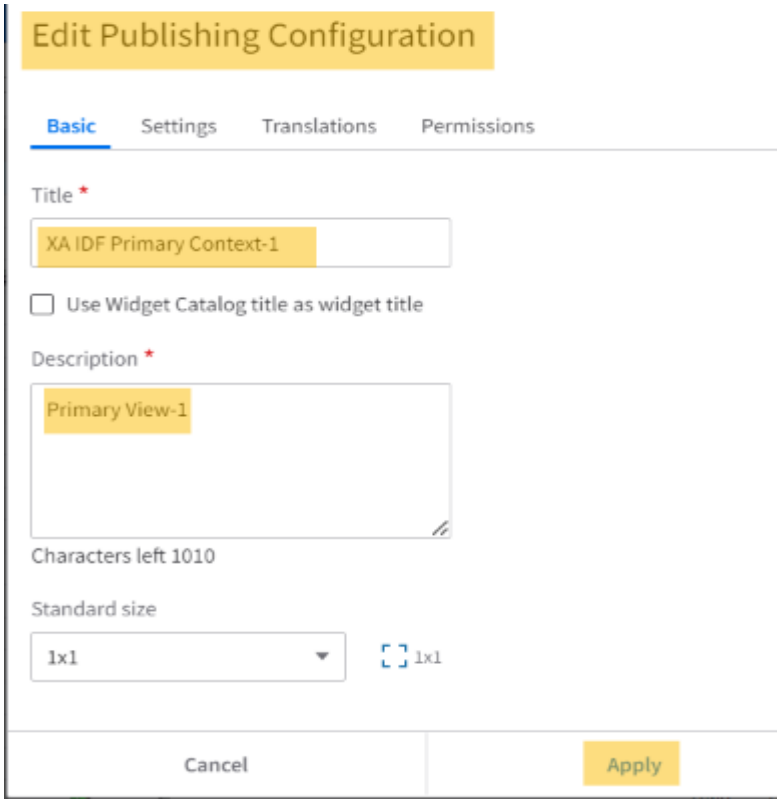
Publishing XA Context Widgets

XA IDF Context widgets added and customized in Insight Groups can also be published to other users on same Infor OS Portal tenant.

Go to XA Context Widget and Select **Advanced** and Click-On **Publish**...

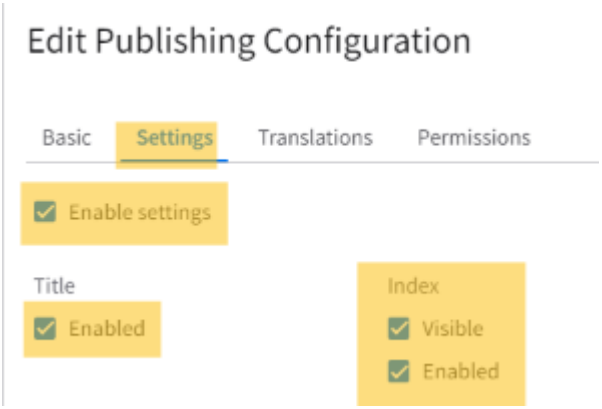


On "**Edit Publishing Configuration**" window, change **Title**, **Description**, **Standard size** according to your business need and Click-On Apply. Enabling "**Use Widget Catalog title as widget title**" check-box will show default "XA IDF Context" as title for this published widget.

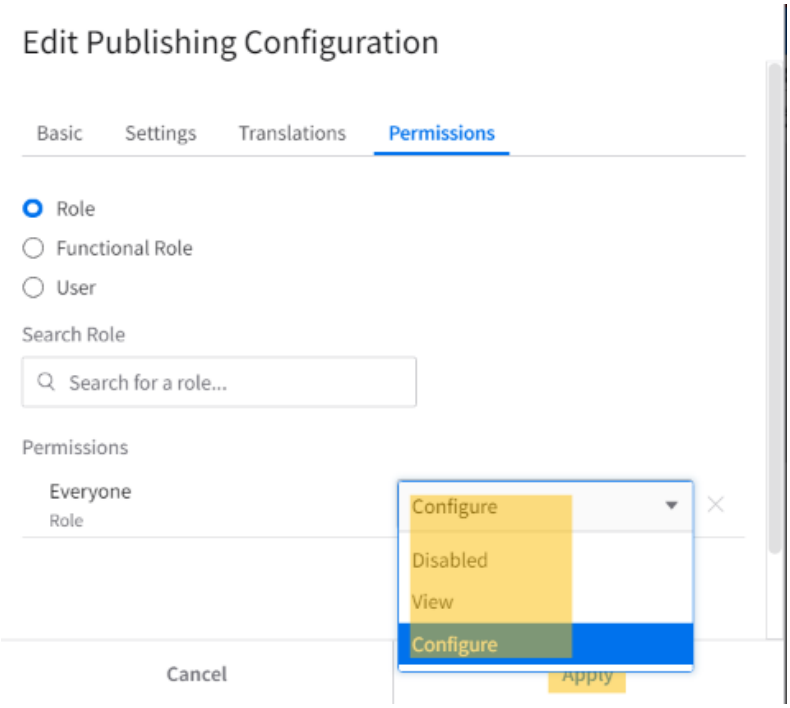


Go to **Settings** –> Click-On “**Enable Settings**” check-box to enable **Title** and **Index** settings.

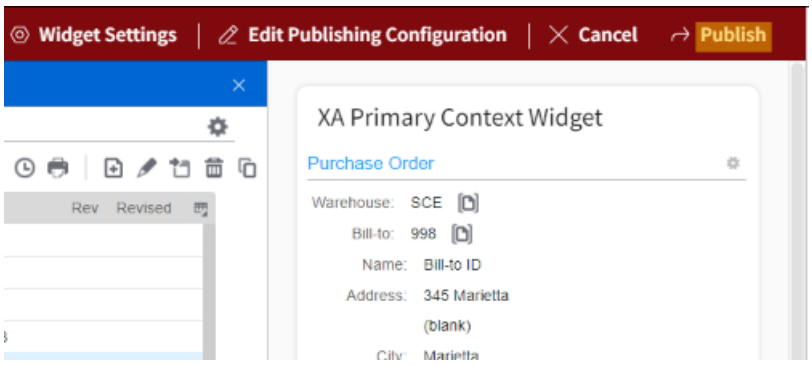
Enabling these settings will allow other users to view these details in the published widget.



Go to **Permissions** section and modify the Permissions to allow access to limited users or roles if needed. Default will allow all users to use this widget when published.

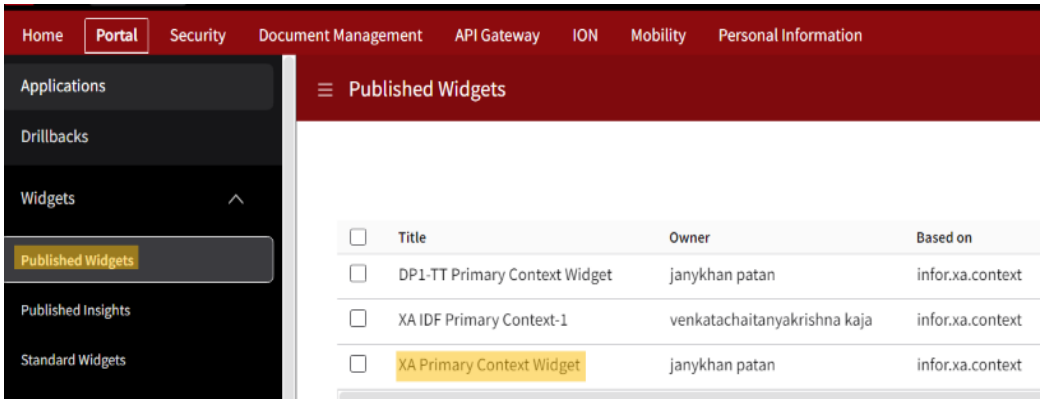


Click-On **Apply** and then **Publish**.

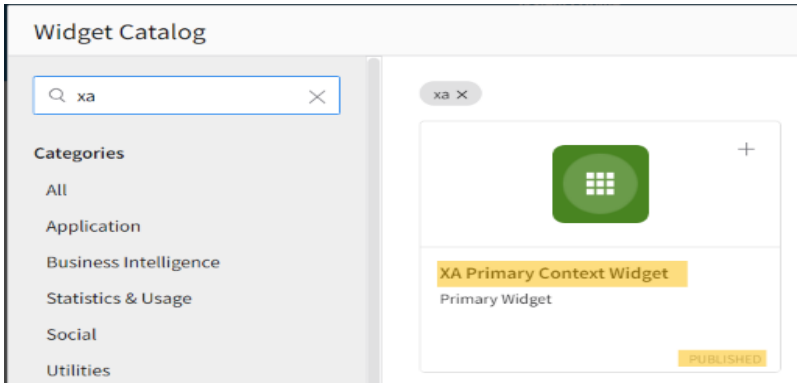


Widget is successfully published.

Verify Published Widget in **Portal** -> **Published Widgets**.



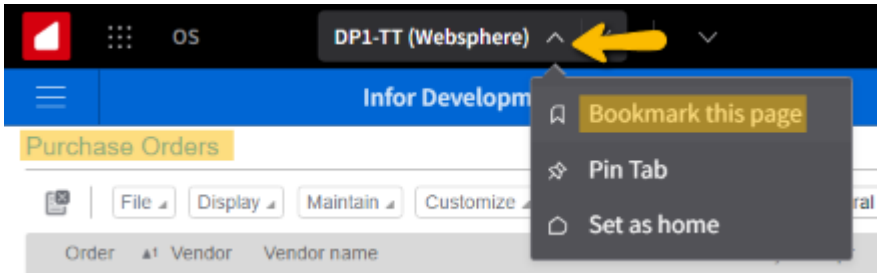
This published widget is now available in **Widget Catalog** to add in Insight Groups for other users.



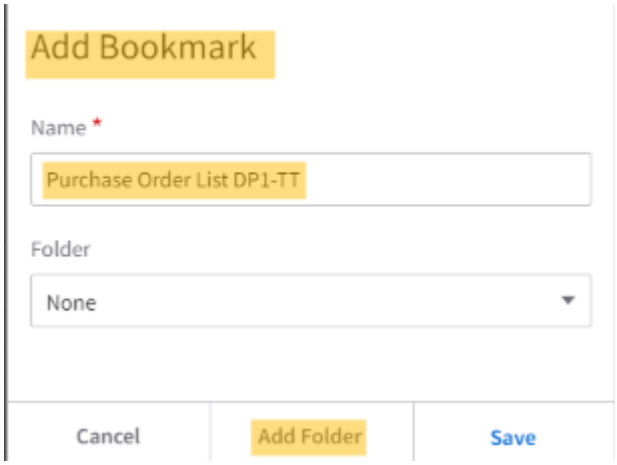
Configure and use Bookmarks

Bookmarks are deep links within your application to access whenever needed. Important and mostly reusable pages or links or objects can be bookmarked. This will save time when user want to go back to those links or pages quickly.

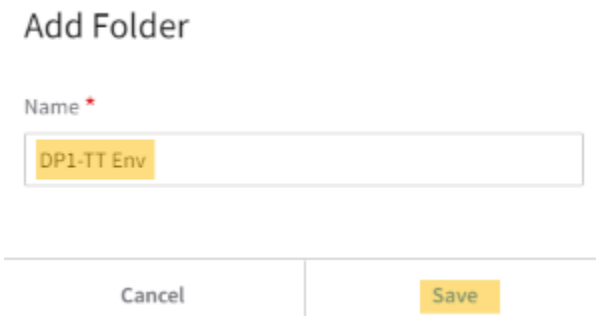
Launch required XA Environment open some Business Object and Click-On “Bookmark this page” to Configure required object Ex: Configured Purchase Order List as Bookmark for quick access.



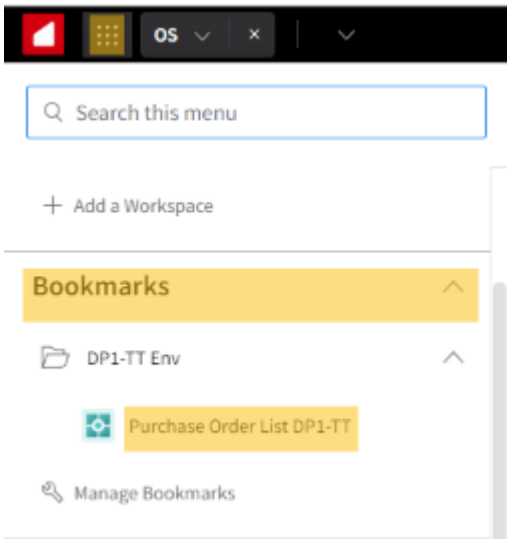
Provide “**Name**” for easy identification of the Bookmark Link and Click-On “**Add Folder”**.

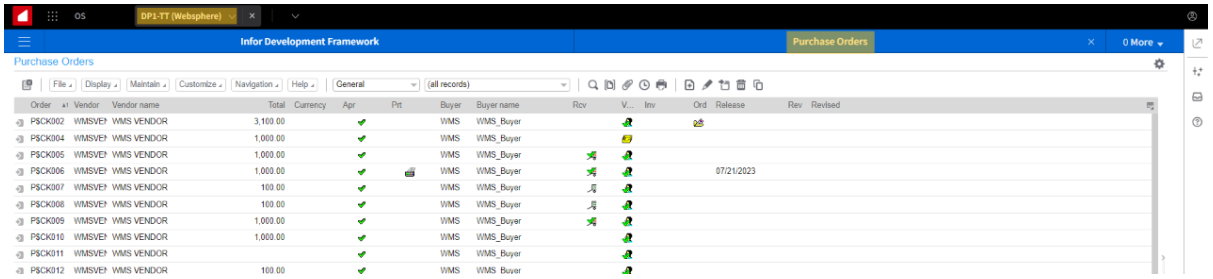


Provide Folder Name and Click-On Save. We can create separate folder per Application to easy understanding.



Goto **Navigation Menu** -> **Bookmarks**-> Open required Folder and Select the required Bookmark to Launch.

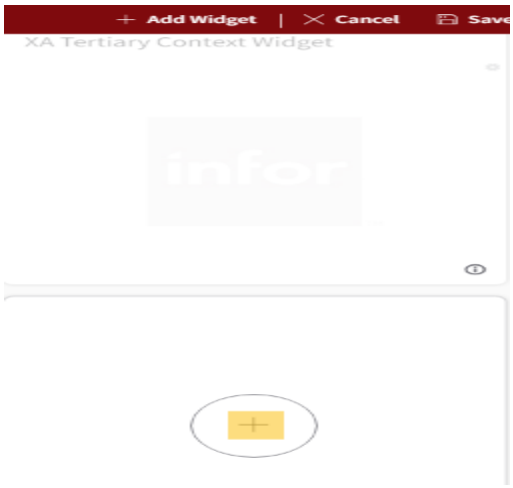




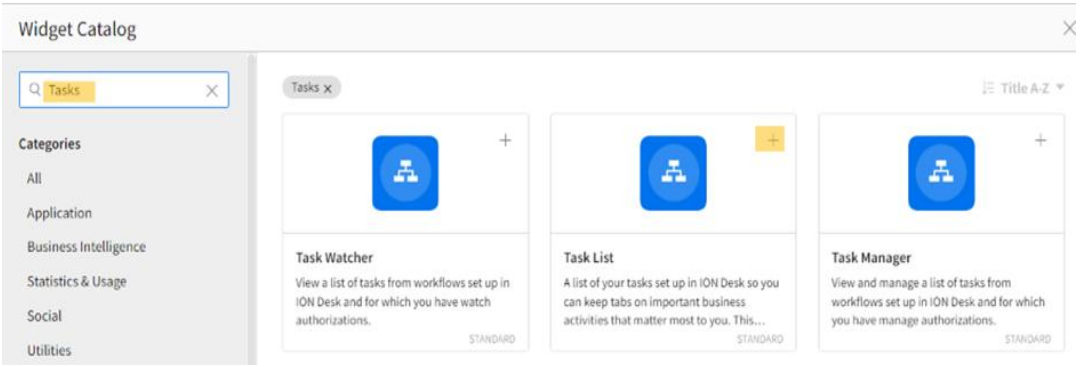
Configuring Tasks and Context Viewer Widgets in Insight Group

Tasks is the envelope icon in the Smart Panel. You can see and manage business messages such as tasks and notifications. These messages can be created from various sources integrated with Infor OS Portal.

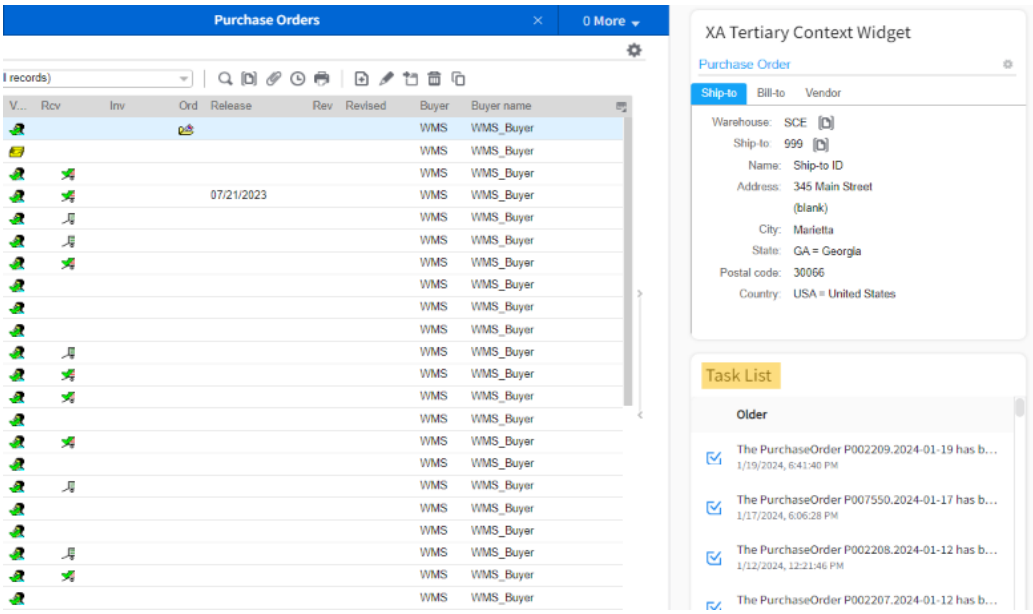
1. Go to Insight Group and Click-On **"+ Add Widget**" to add new widgets from Widget Catalog.



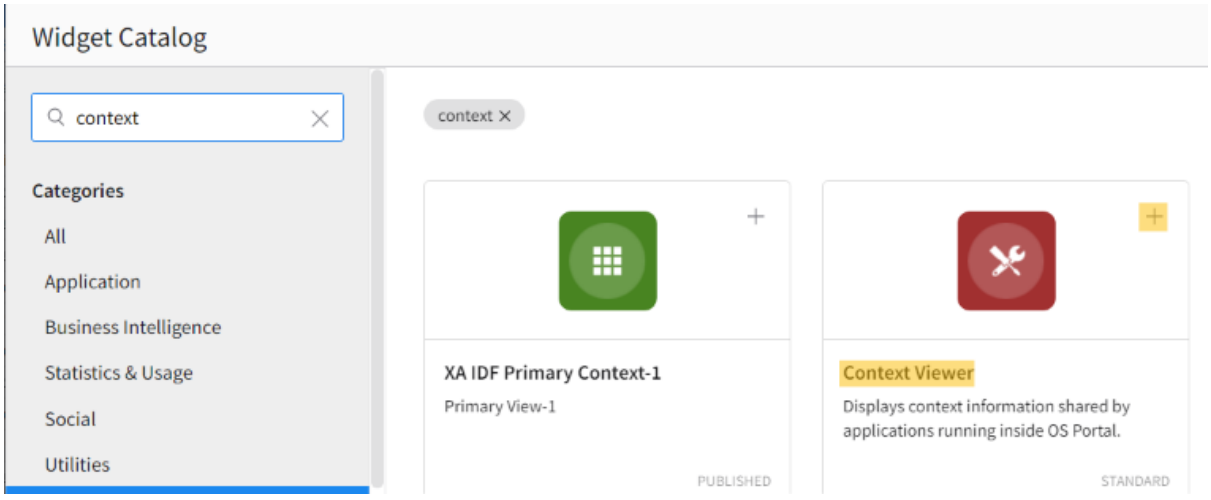
Browse through the **Widget catalog** and search for Task Widget then Click "**+**".



Click-On Save and Now Task List widget is added in Insight Group.



Similarly follow same for Context Viewer widget as well.



Configuring Drillbacks in Portal

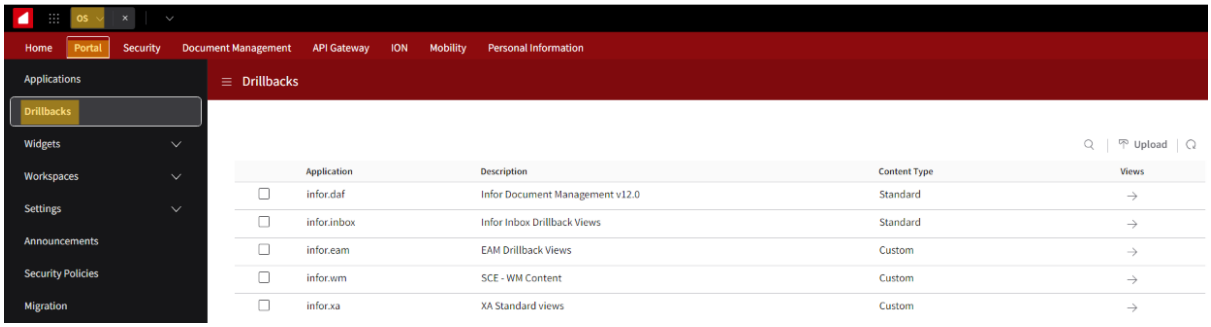
Drillback is an action in Infor OS Portal, which can be thought of as a link or a jump from one application to another.

Typically, a drillback links summary information in one application to more detailed information in another application.

To configure Drillbacks in Infor OS Portal, you must import the XA_Standard_Views.xml drillback definition file. Navigate to the **infor\vlib\Mingle** folder in the client IFS directory, which is the location of the XA sample solution files used for integrations through Infor OS/ION and save the **XA_Standard_Views.xml** file.

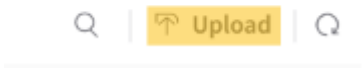
Login to OS Portal as the administrator.

Go to Portal tab and Click-On **Drillbacks** you require an Admin profile to manage drill-backs.



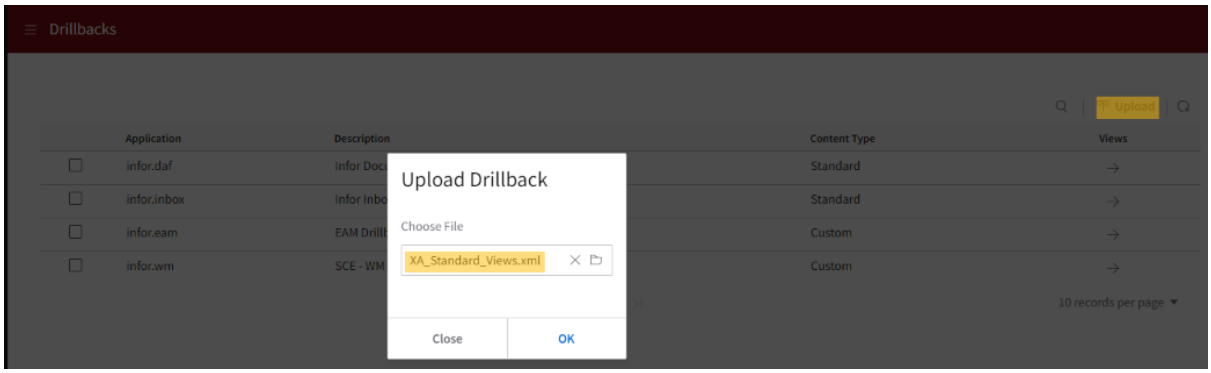
When the **Portal** loads, Click **Drillbacks**. A list of drill-back definition files that are uploaded is displayed. If the list already contains the XA Standard views (as displayed), remove the existing definitions, by clicking **Delete**.

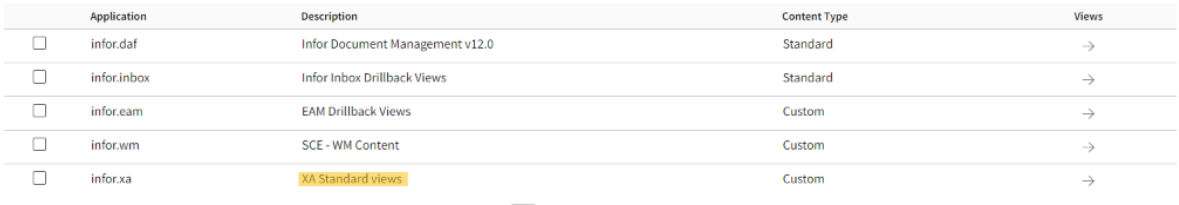
Click **Yes**.



Click on **Upload** and Choose File to select the Drillback definition file as specified earlier.

Click **OK**.





These Drillback definition files are used in Infor OS Portal to generate the drill-back links for ION tasks/alerts.

Drill-backs are supported from InforBusinessContext messages which are shared in SocialSpace or subscribed by other Infor OS Portal applications. Each InforBusinessContext message supported by XA IDF includes a drill-back URL the receiving product can use to drill back into XA. These drillbacks 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, 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.

ERP XA supports 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

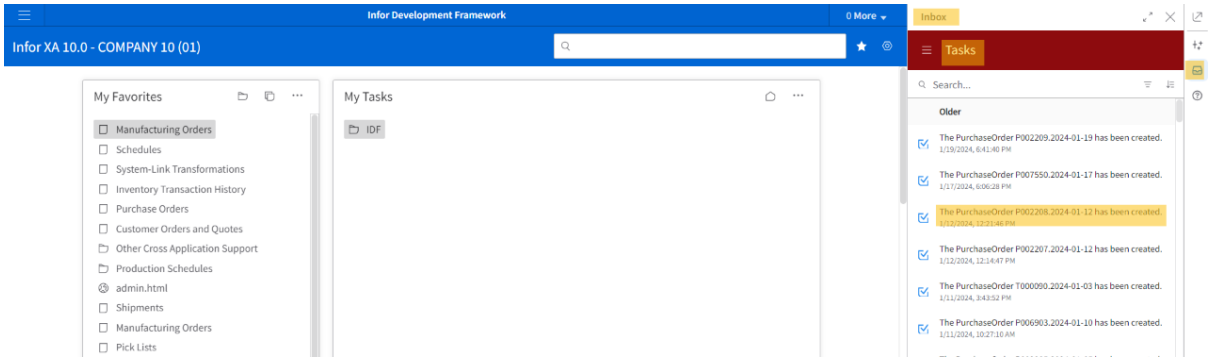
BOD	Infor XA Object
Contract	Customer Quote Customer Contract Quote
CustomerPartyMaster	Customer
FinancialCalendar	Financial Division
FinancialPartyMaster	Entity Financial Division Vendor Customer Company Account
ItemMaster	Item Revision Item Warehouse Item
Invoice	Financial Transaction Customer Invoice
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

BOD	Infor XA Object
ShipFromPartyMaster	Entity Financial Division Vendor Customer Company Account
ShipToPartyMaster	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
SupplierShipmentSchedule	Purchase Order Purchase Order History
TradingPartner	Entity Financial Division Vendor Customer Company Account
ChartofAccounts	Chart of Accounts Segments
CodeDefination	Account Segment Account Segment Value
FinancialCalendar	Financial Calendar
SourceSystemJournalEntry	Financial Journal Entry
AccountingChart	Chart of Accounts Chart of Accounts History
AccountingBookDefinition AccountingEntity	Ledger Book

Using Drillbacks from Tasks in Inbox

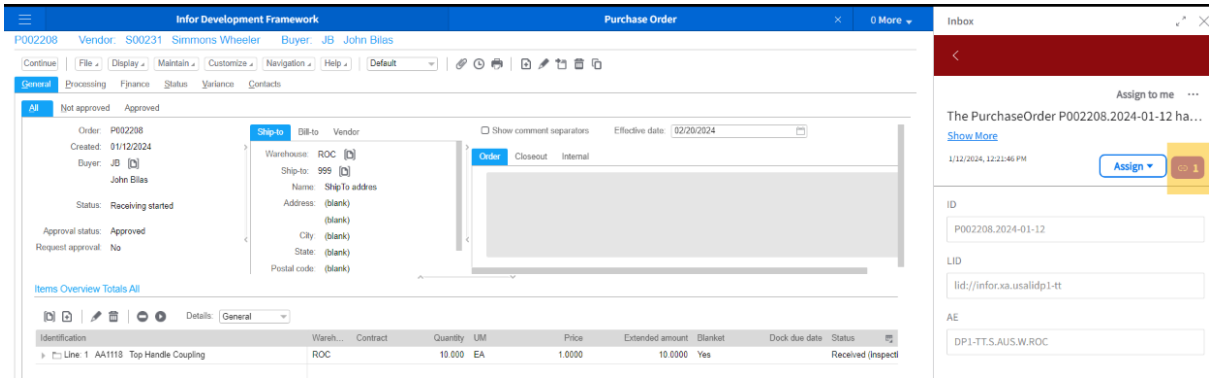
To use the drillback functionality, completing section “Configuring Drillbacks in Portal” in this Chapter is the pre-requisite.

Goto **Inbox** in Smart Panel in the right corner **-> Tasks** to display the list of ION Workflow tasks created and select the required task.



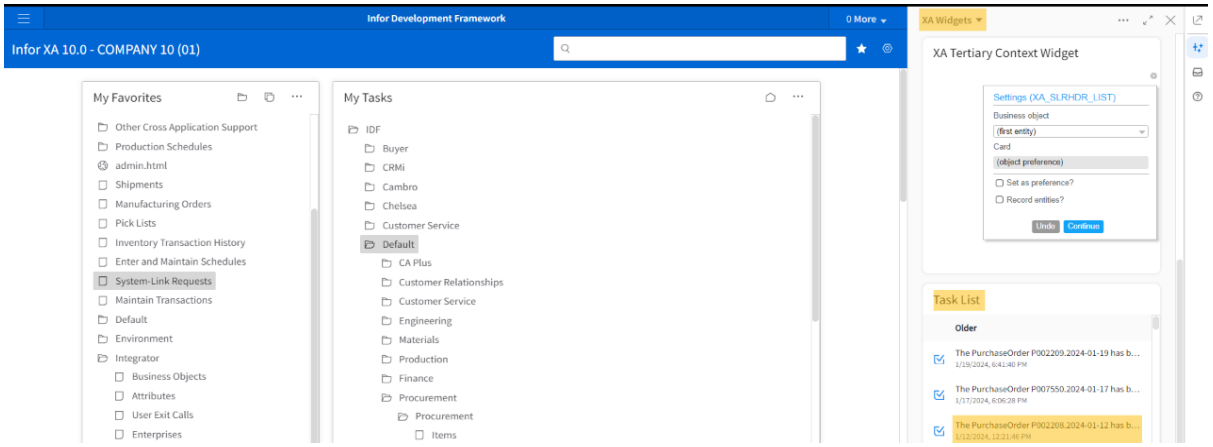
Click-On drillback link as highlighted in the below screenshot.

The page is redirected to the specific XA object (Purchase order in this example) as displayed.

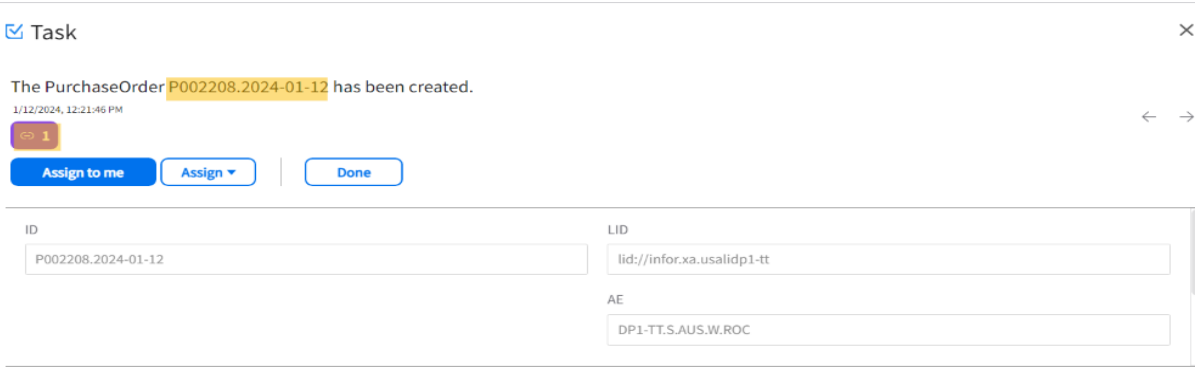


Using Drillbacks from Tasks List in Insight Group

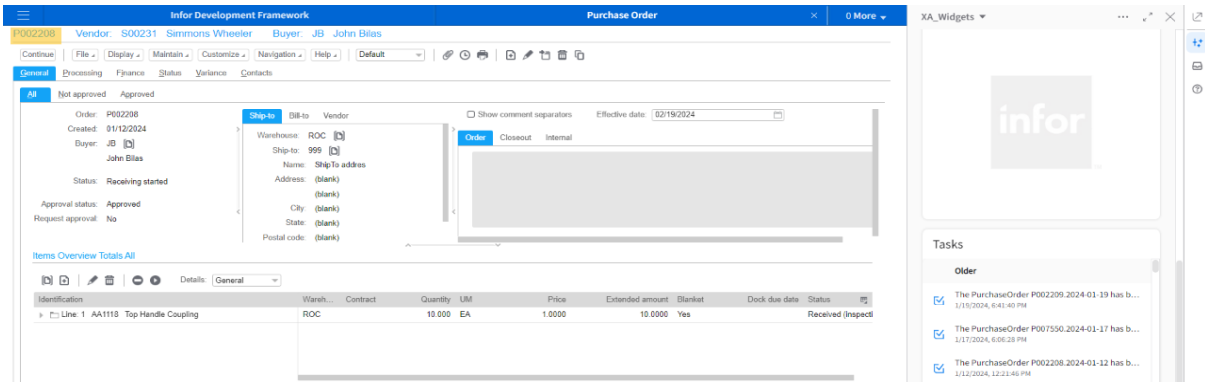
Goto XA Widgets Insight Group and Select “**Tasks List**” Widget to view the message.



Click-On Message. The Task details screen is displayed. Click-On the **Drillback** link and it will



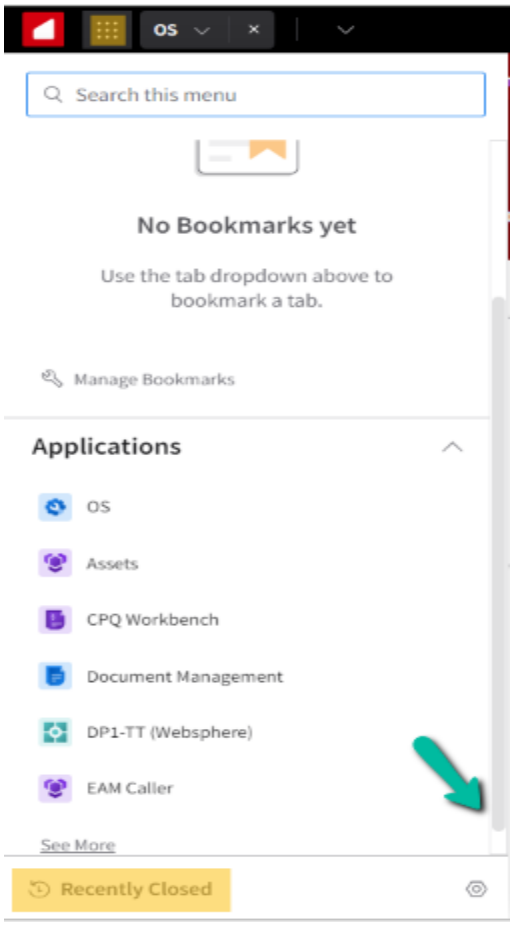
redirect to Purchase Order details in the XA.



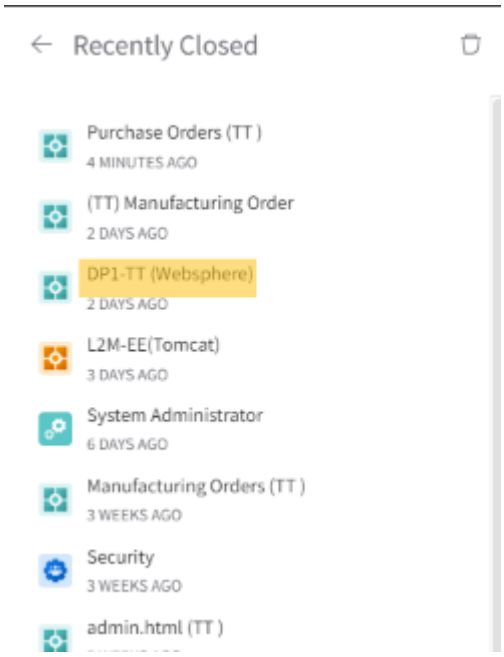
Using Recently Closed

We can view and reuse all the recently closed applications and restore closed tabs in the Portal by using this feature.

1. Goto **Navigation Menu**-> Scroll Down to bottom and Click-On “**Recently Closed”.**

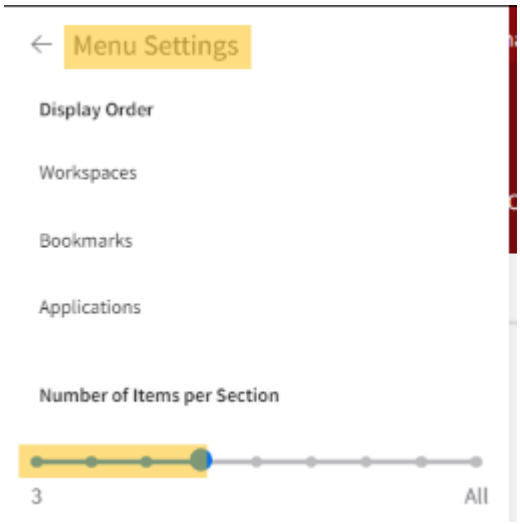


2.Click on tab to reopen it.



Able to see and access or open the recently closed applications again.

We can configure the Number of Applications allowed to be shown in recently closed by Clicking on **Menu settings** and configure according to our requirement.

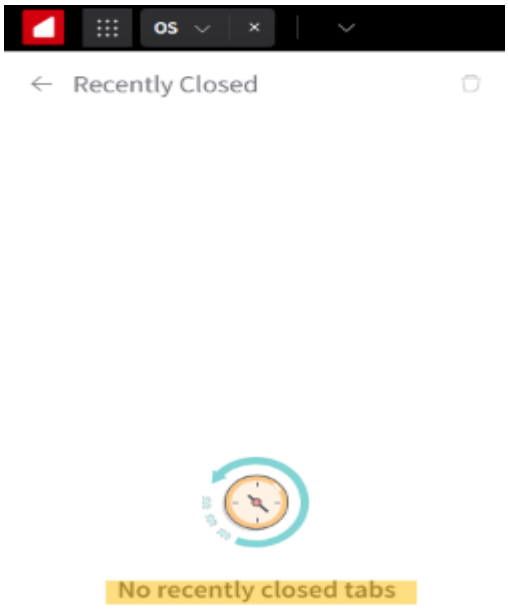


Clearing Recently Closed tabs

You can clear all recently closed tabs.

Click-On “**Delete Icon**” on Recently Closed. A confirmation message is displayed.

Click “**Confirm**” Delete


OS
Recently Closed
No recently closed tabs

Chapter 11 Infor Business Context (IBC) messages

Overview

The Infor Business context message is a Infor OS Portal standard message that broadcasts the current status of an application. The message consists of the identity of the application and the view that is being displayed, and a list of “entities”.

All Infor applications running inside Infor OS Portal sends these messages. In IDF, the entities correspond to the business objects that are currently being displayed.

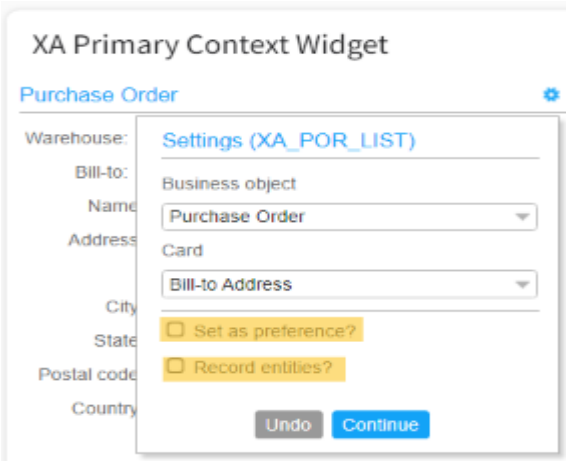
In list view, the IDF always sends a message when the selection changes. The message contains an entity for each selected row.

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.

XA Context Widget can be added to any XA application page in Infor OS Portal. These XA Context Widgets display data that is appropriate for the message.

The IDF context application listens for Infor Business Context messages and when the XA Context Widget receives a message and recognizes the first entity, the XA Context Widget 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 XA Context Widget displays the object using that card preference.

To add Widgets in Insight Group inside XA application refer to Chapter 10 Using Infor OS Portal.



Set as preference:

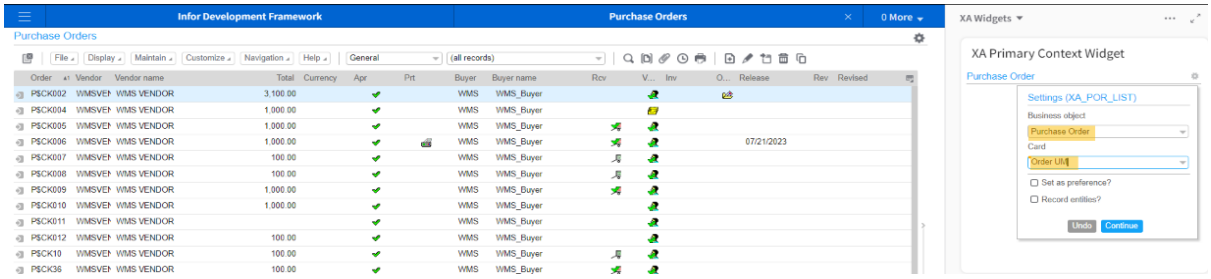
When you select a Business object and/or Card in the XA Context Widget preferences, they are for the lifetime of the current session - i.e. when you log out and back in, then they will revert to the defaults. However, if you select the "Set as preference" option, then the setting is persisted and re-used for new sessions. The settings are for the current view only - so the card used on the list of buyers can be different to that of the buyer detail.

Record entities:

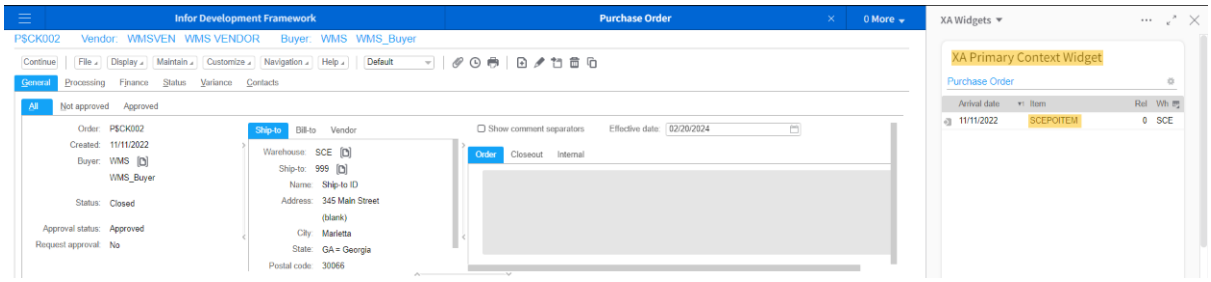
The Record Entities option is there to record the list of entity types (i.e. business objects) that are being sent to the context app. This is of little importance for the local application as they are known. Where this becomes important is when the XA Context Widget is being shown next to an alternative application - then IDF won't know which entity types will be included in the IBC message(s), so this option will record them.

Configuring Business Object and Card in XA Context Widget

You can select the settings option and select the **Business object** and **Card** from dropdown. In this example, **Purchase** Order and **Order UM** are selected, respectively.



Purchase Order Line item is displayed when you open the purchase order as displayed in the screenshot.

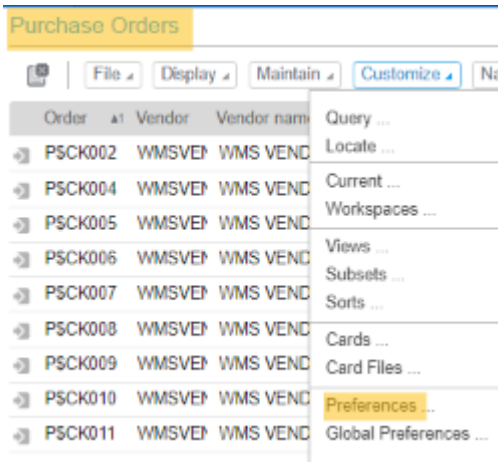


Configuring Preference definition in XA Business Object.

Preferences for the XA Context Widgets for any business object are defined in SiWA.

From the Main browser, double-click the Business Object to display the XA Context Widgets.

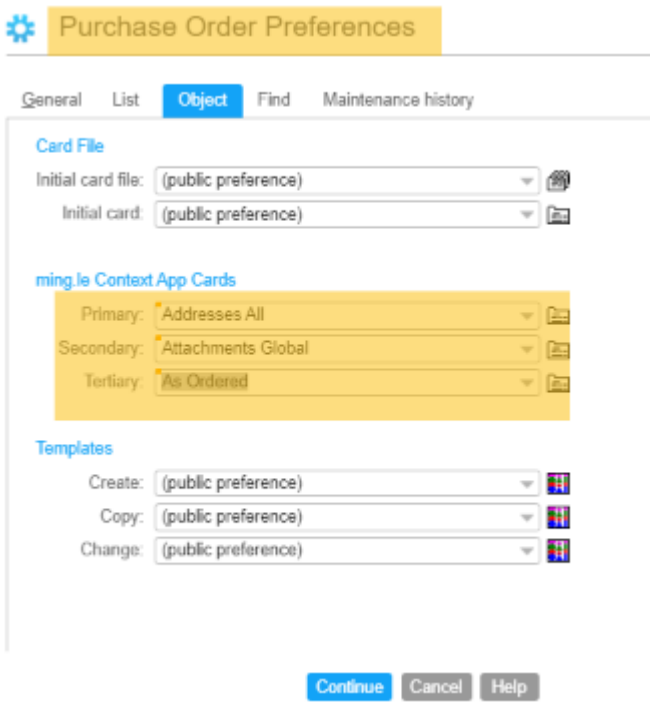
Select **Customize > Preferences**.



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

Select the **Object** tab.

Select the **ming.le Context App Cards** tab.



Specify the preferences for the XA Primary, Secondary, Tertiary Context Widgets.

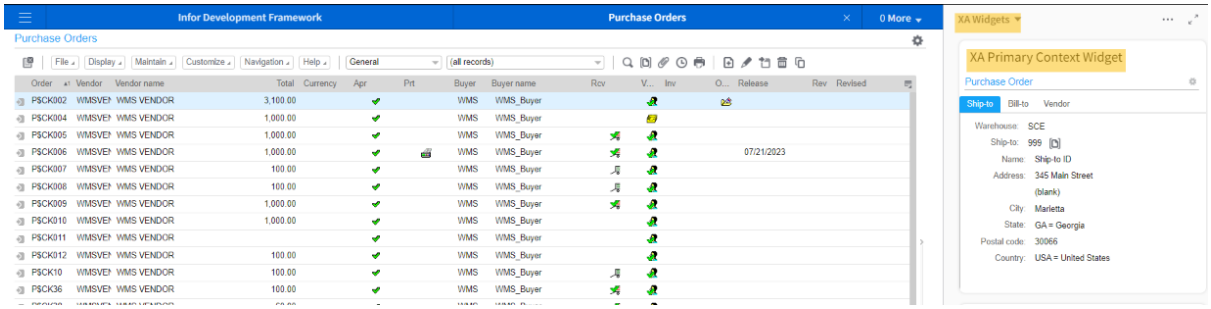
The XA Primary Context Widget content area is where the cards that are to be used by the IDF context application are defined. You can use any cards, but most cards are designed to be used in a full screen and may result in unwanted scrollbars when presented in the limited space available to the context application. It is recommended that you define specific cards using the customization features of SiWA specifically for the XA Context Widgets. See the context help of SiWA for guidance about how the customization facilities are used. Similarly, setup XA Secondary, Tertiary Context Widget according to your requirement.

Refer to Export Metadata from XA section **in *Infor System Manager Quick Installation guide for Infor XA***, after setting up Preferences in SiWA, to reflect the changes made in SiWA export Private metadata.

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

Launch XA in Infor OS Portal, to display the XA Primary Context Widget with Addresses All.

Select a purchase order in the XA Primary Context Widget View to display the Purchase orders Addresses All.



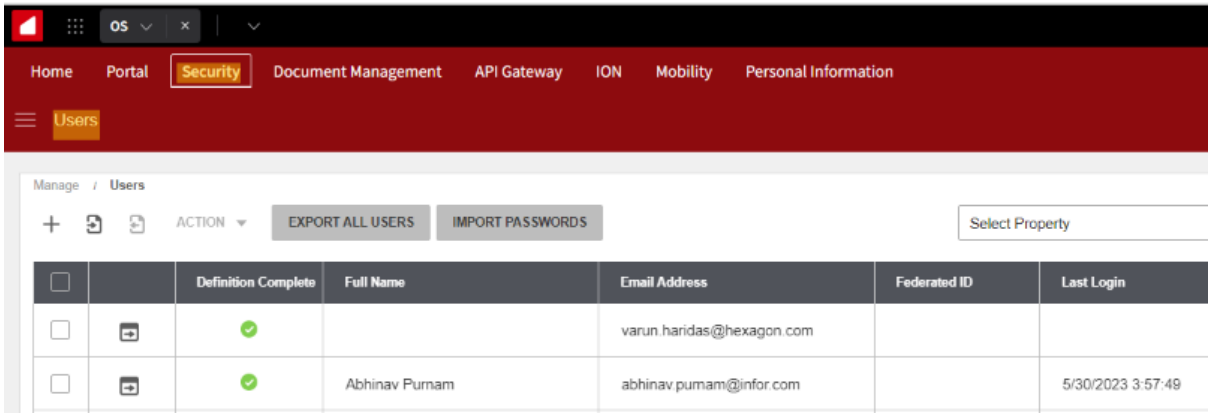
Chapter 12 User maintenance

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

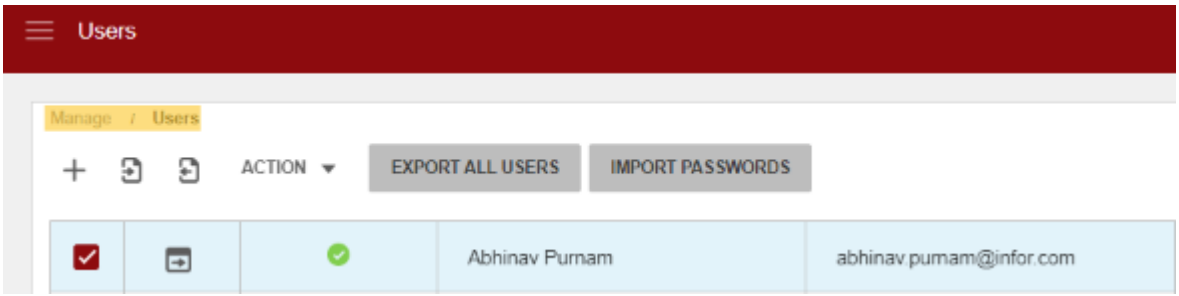
Adding users

Log into Infor OS Portal using the account that your setup for IFS administration

Click the **Security** option located in the top-left hand corner from OS and then select **Users**

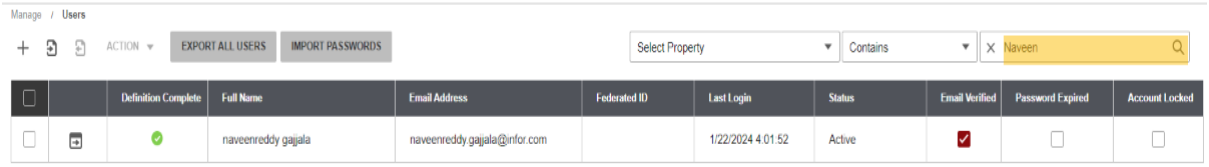


Select **Users** on the menu to the left**.**



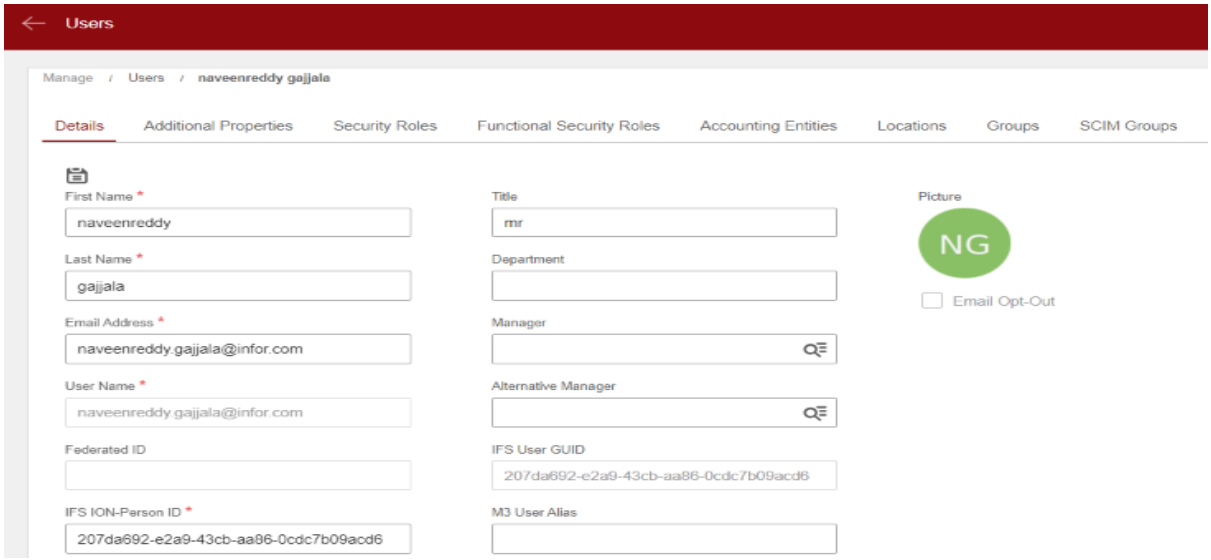
Select **Users** on the menu to the left**.**

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

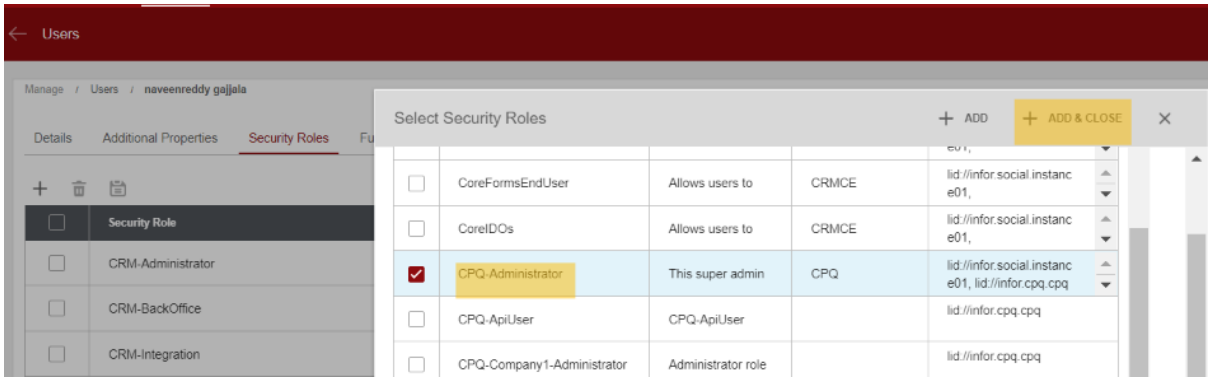


Enter a name in the search box and click **Load**.

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



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



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

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

Chapter 13 Net-Link WAR file redeployment

This section explains the procedure to re-deploy Net-Link WAR file on Tomcat and WebSphere. This action is needed when there are major changes or fixes in XA client build.

If you are using **Reverse Proxy configuration in IBM i HTTP Server to access default Net-Link,** then this action is not need, since you are using default Net-Link and not the WAR file deployed on WebSphere.

WAR file re-deployment

Refer to *Chapter 5 WAR file Re-deployment* in "***Infor IDF Setup Guide for Secure Net-Link***" guide, which describes process to re-deploy Net-Link WAR file on Tomcat and WebSphere.

Appendix A Publishing 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.

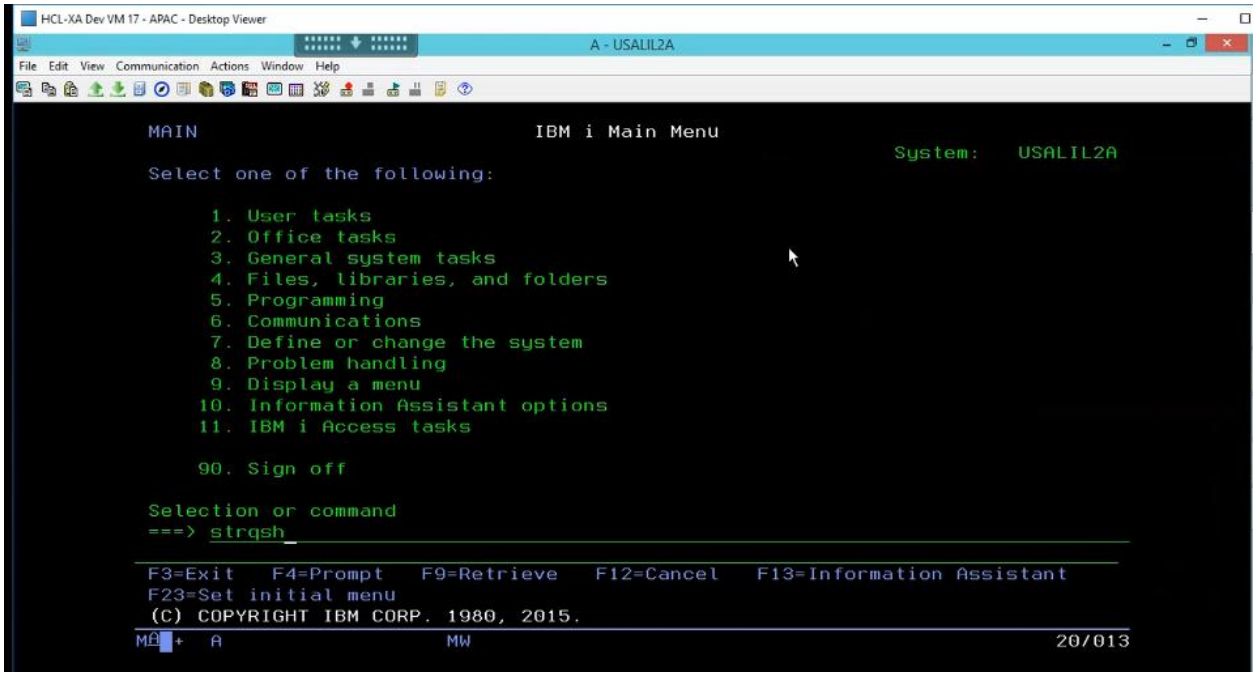
If the root Organization Node accounting entity is changed in BIS, you must clear PUB* files and re- publish all accounting entities.

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 publishes 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 QSH session in iseries.



2 Run these commands:

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

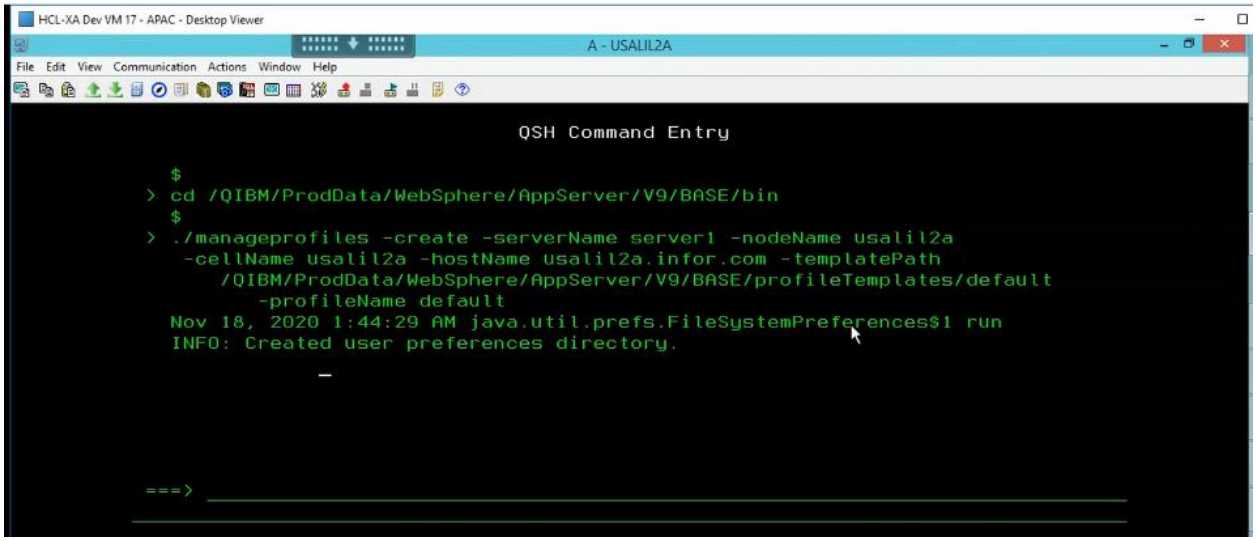
$ ./manageprofiles –create -serverName server1 -nodeName <hostname> -cellName <hostname> -hostName <hostname.domain.com> -templatePath /QIBM/ProdData/WebSphere/AppServer/V9/BASE/profileTemplates/default -profileName default

...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



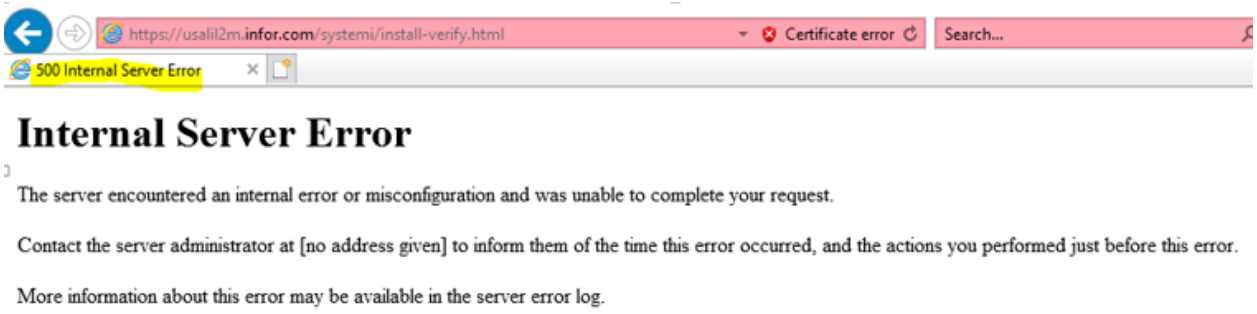
Note: In some severs the folder "**BASE**" is "**Base**". Check the folder structure before running the command.

3 Once done, you can go back to **WebSphere HTTP admin -> HTTP servers -> WebSphere applications server**. Now, the default profile is listed in the dropdown.

Note: If you still face issue 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.



Follow these steps to get the issue resolved:

- 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
- STOP the HTTP server and Application servers related to SiWAnyWhere
- 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\
- 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

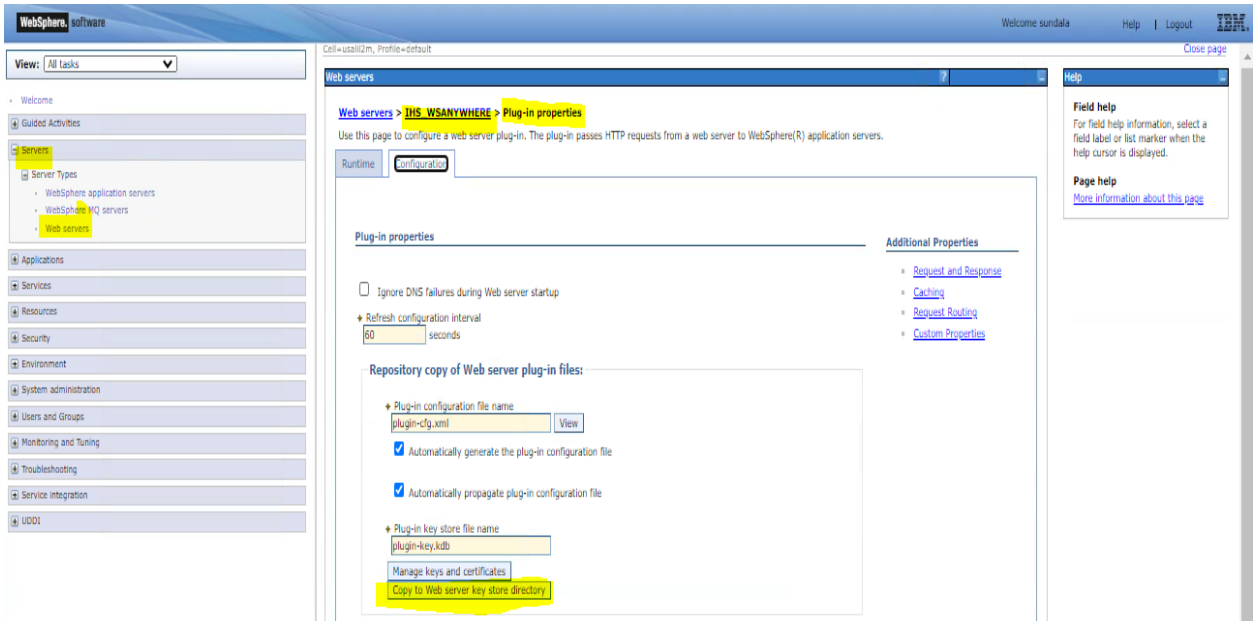
  TO

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

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

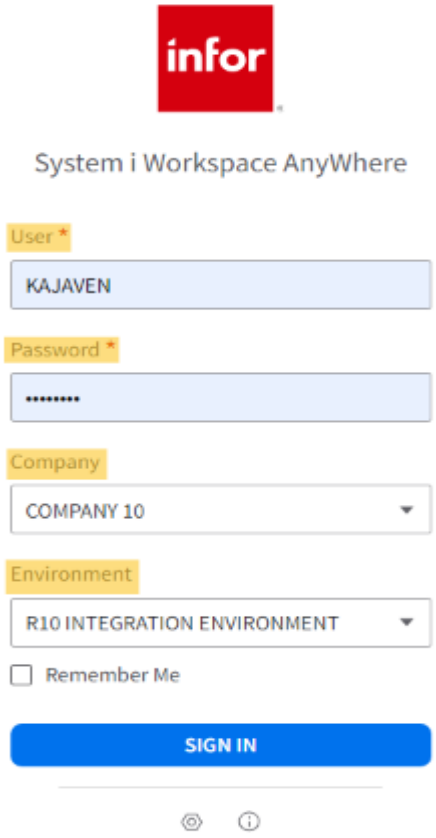
- START the HTTP server and Application servers related to SiWAnyWhere.
- Once done, launch https://usalil2m.infor.com/systemi/install-verify.html

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.

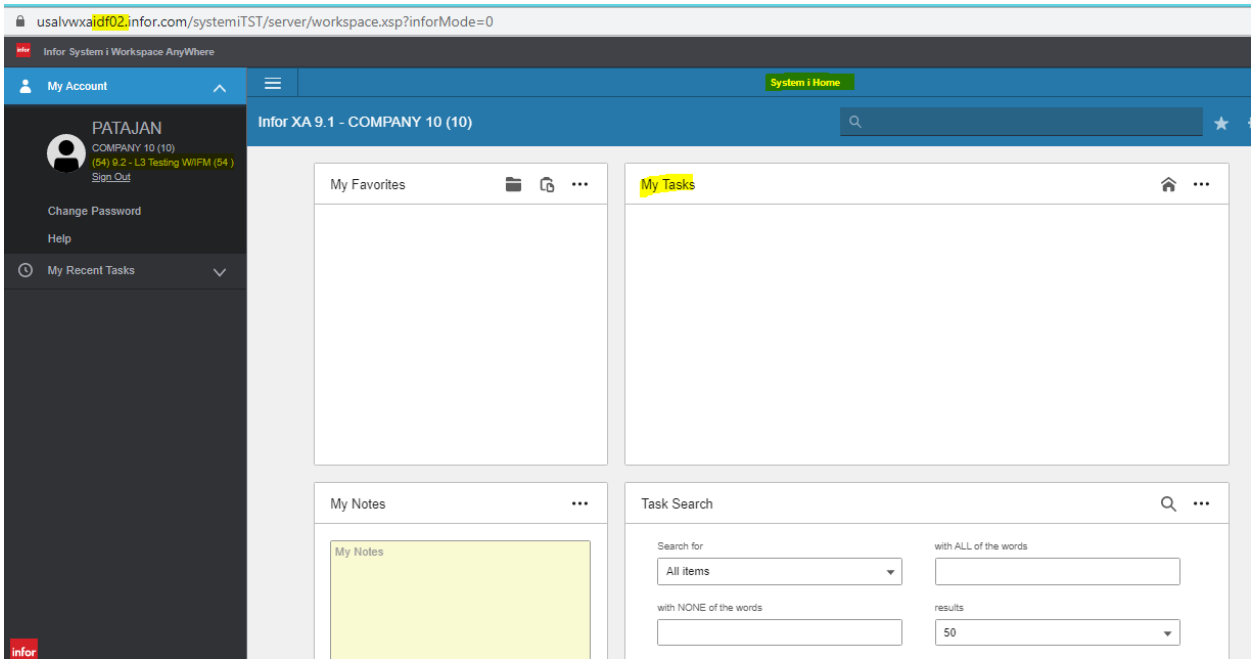


Appendix D Troubleshooting

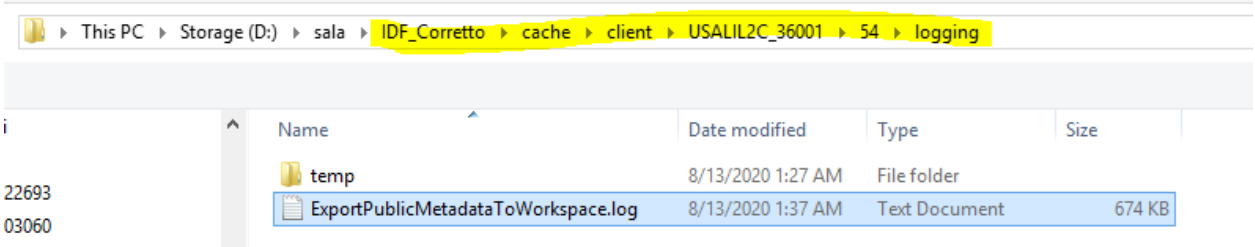
1. If a user is trying to login to Infor OS Portal for the first time using Infor credentials and observed that user is unable to login to the Infor OS successfully, then you must make sure whether the user profile is configured in Infor OS Portal application or not. If not, user can request the Project Manager or XA Integration team for user provision in Infor OS with the user's Infor mail ID and need to specify whether user needs access on Infor OS Development or Infor OS Portal QA environment.
2. If a user log into Infor OS Portal successfully but gets prompt again for credentials while launching the SiWA applications, then user can enter the respective IBM i user ID and credentials. (For example, in this screen, login prompt screen is displayed for USALIDP1 IBM i machine).



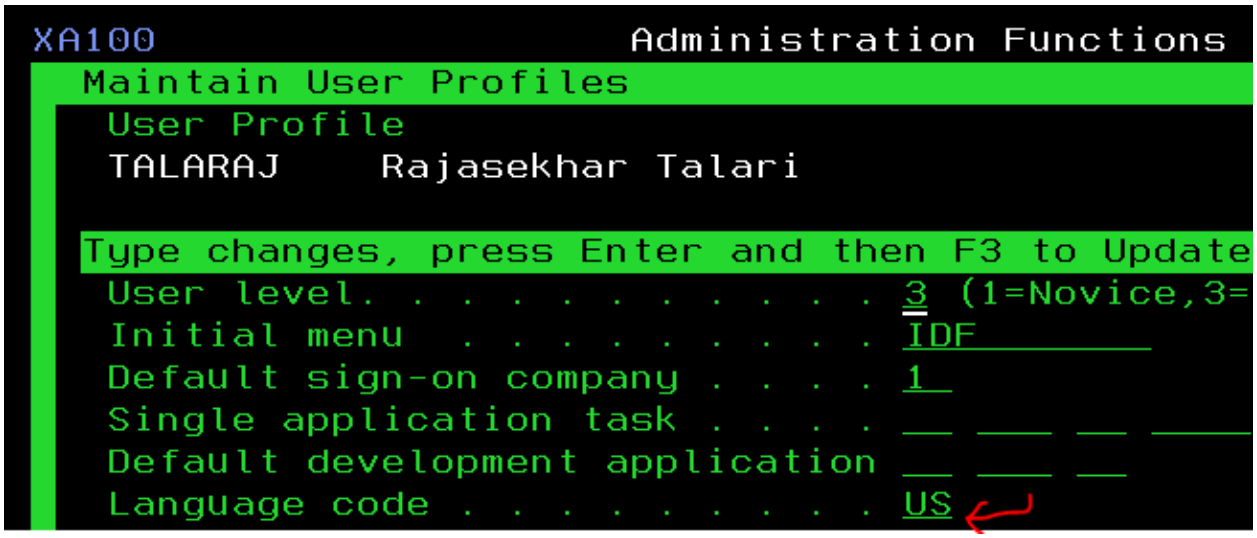
1 Even after successfully SIWA environment setup, if the environment is launching with no IDF tasks in home page.



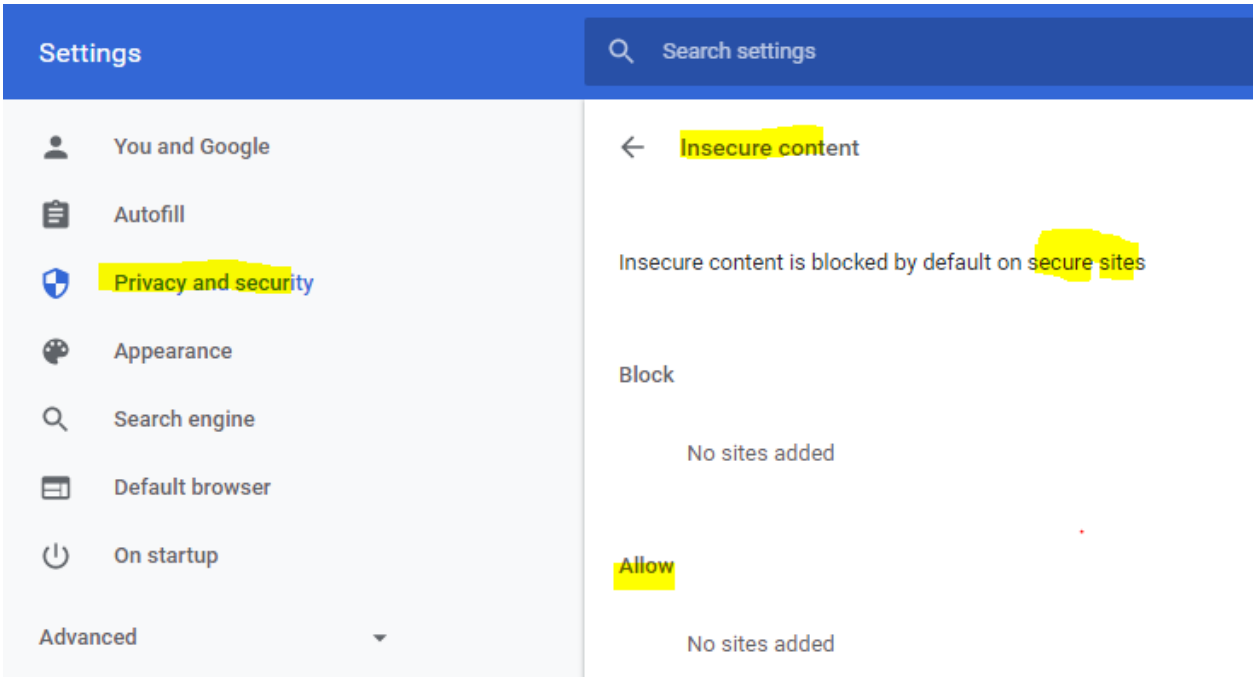
- Then you need to check whether exporting is done successfully or not in the ExportPublicMetadataToWorkspace.log at the local IDF logging folder (similar to going to Power- Link -> help -> About -> Ctrl + D -> Ctrl + L and going to logging folder).



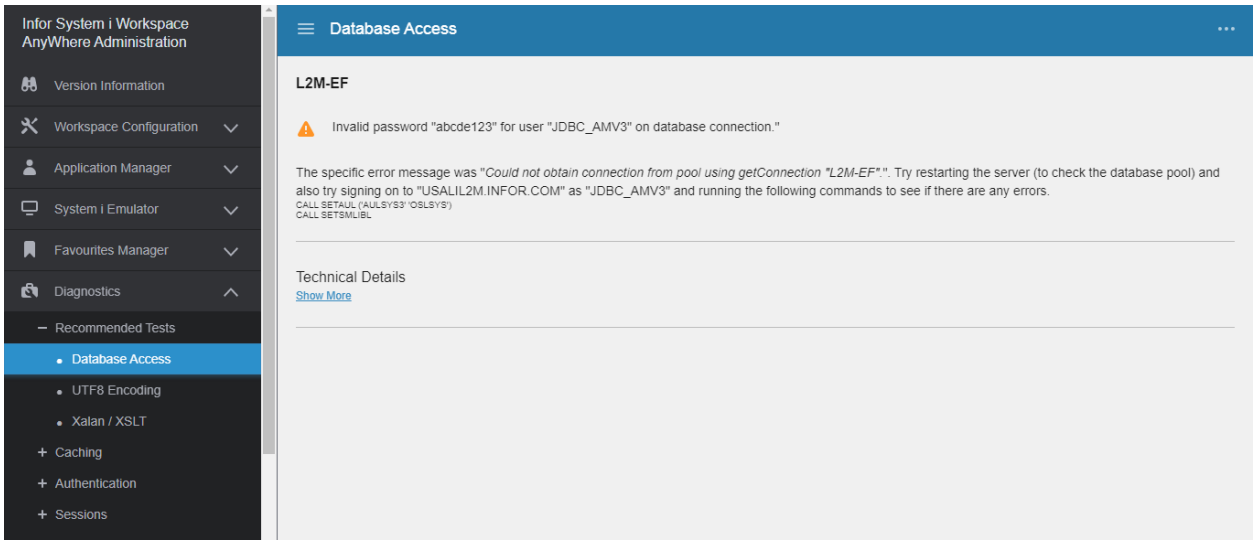
- If you find any errors, those need to be resolved and re-run export metadata again and make sure you are not encountered with any errors.
- If you encounter with “Language Code is not defined” error, you need to cross check and update language code in SIM console.



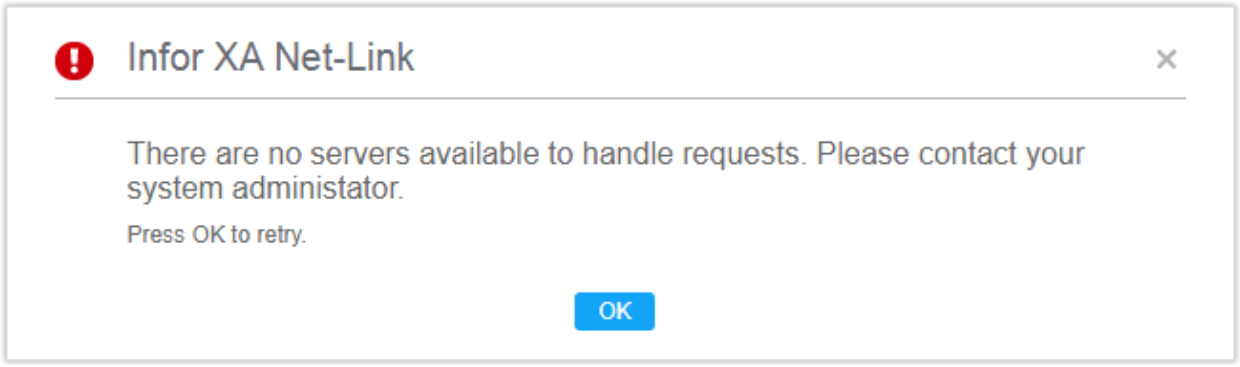
2 When you try to open any business object from IDF using SIWA, if it displays a blank page, you need to add the SIWA URL to the insecure content and try to relaunch the application.

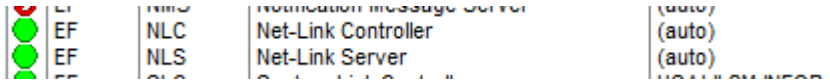


Restart the server SIWA application installed server if this issue appears and recheck the Database access under diagnosis in SIWA admin page.



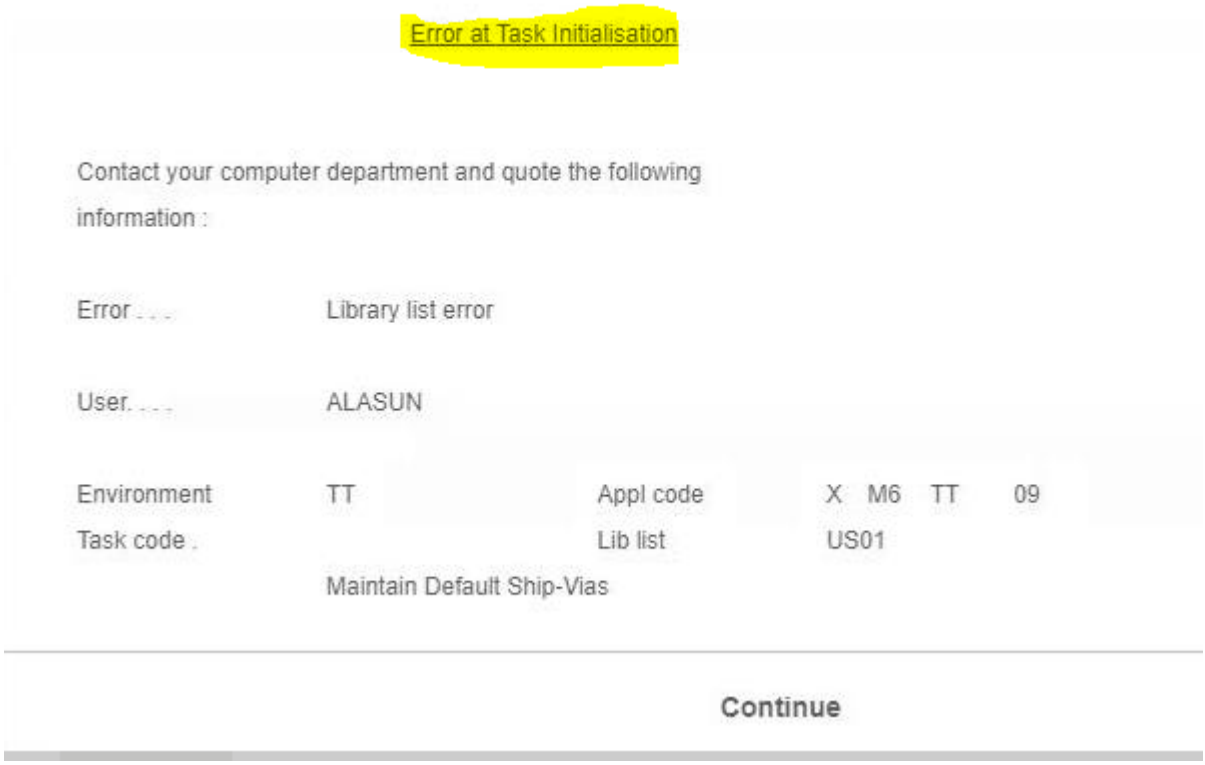
3 If you receive this request, cross check the NLS and NLC processes are in active state or not, if not start the processes.

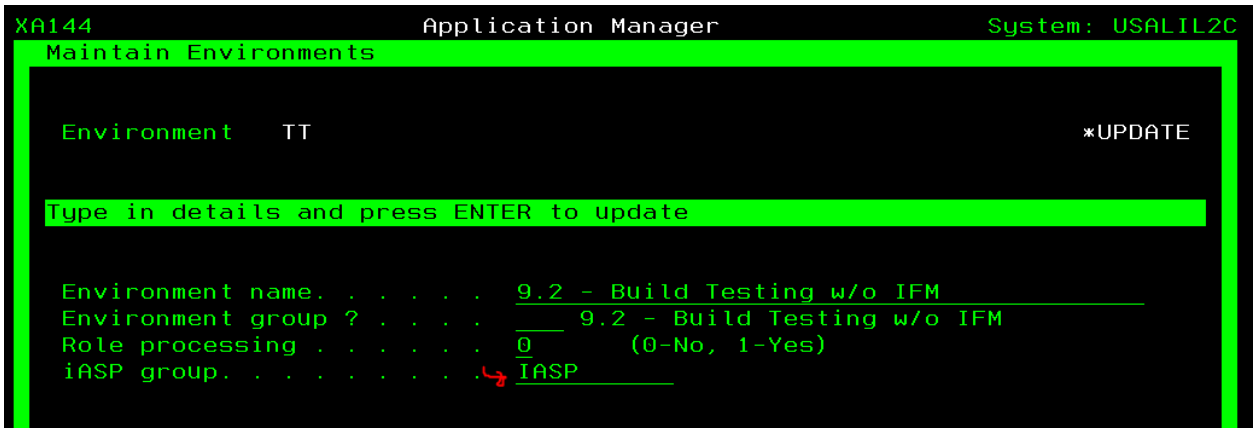




4 If you face issue, as displayed, when launching L1 tasks, check the whether the environment is pointing to correct iASP group or not by navigating to this path in System Manager Console.

STRM400 → **Application Manager → Maintain Environments**

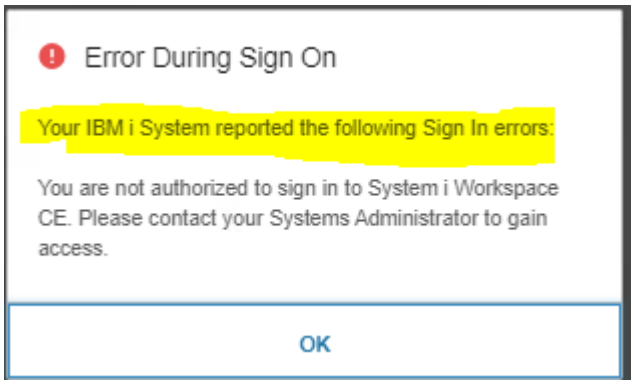




5 Due to maintenance activities in weekends and holidays, SiW and Net-Link related Http and Application servers in “IBMi Web Administration Console” goes down similar to XA servers in Link Manager. You need to check and start them if you face any issues while launching SiWA application.

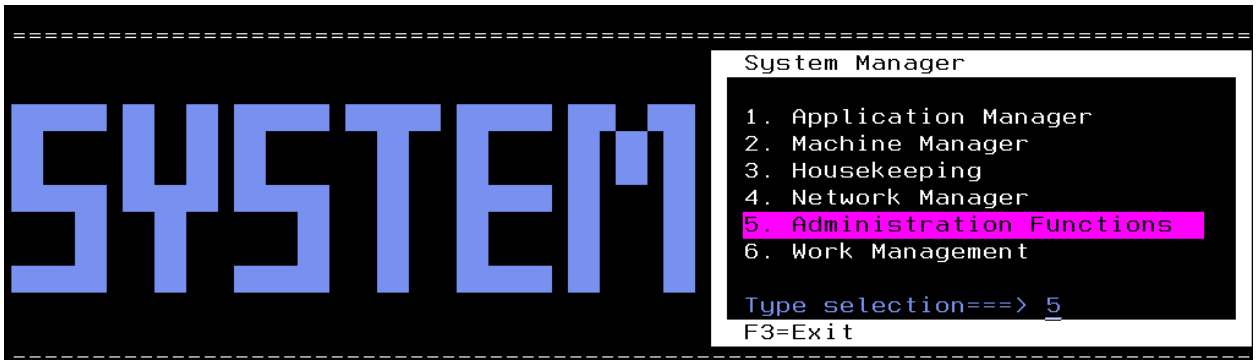
6 To Secure the Net-Link and launch the SiWA application in Infor OS Portal, the Globals for the XA server must be on 9.2. If the globals is on 9.1, user cannot download Net-Link.war file and fails to secure the Net-Link on SiWA. It is not recommended to run SiWA on Infor OS Portal without securing Net-Link.

7 If the client system is getting blocked at System Manager (SIM) or if you are facing below error while accessing SIWA environments with or without SSO, you have to add the IPv4 address of the client system in the allowed clients at SIM.

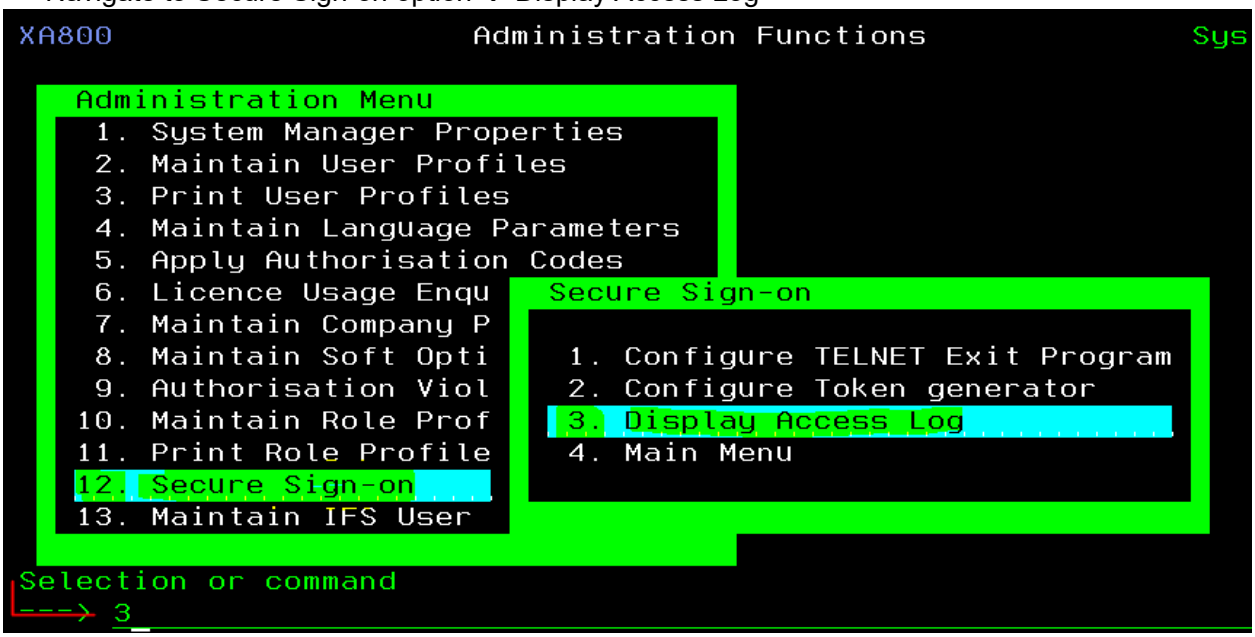


Note: Follow *KB2321732* before updating client IP address in SIM.

- Navigate to STRM400 → Administration Functions



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

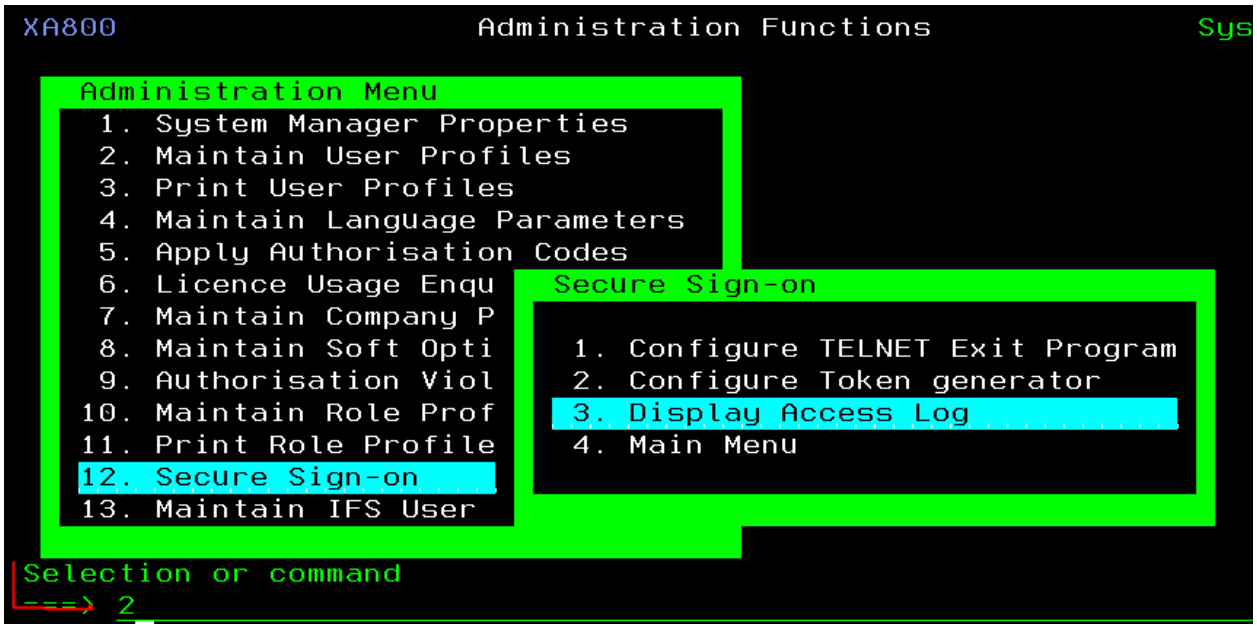


- Identify and copy the client IPv4 address with result as blocked, as displayed.

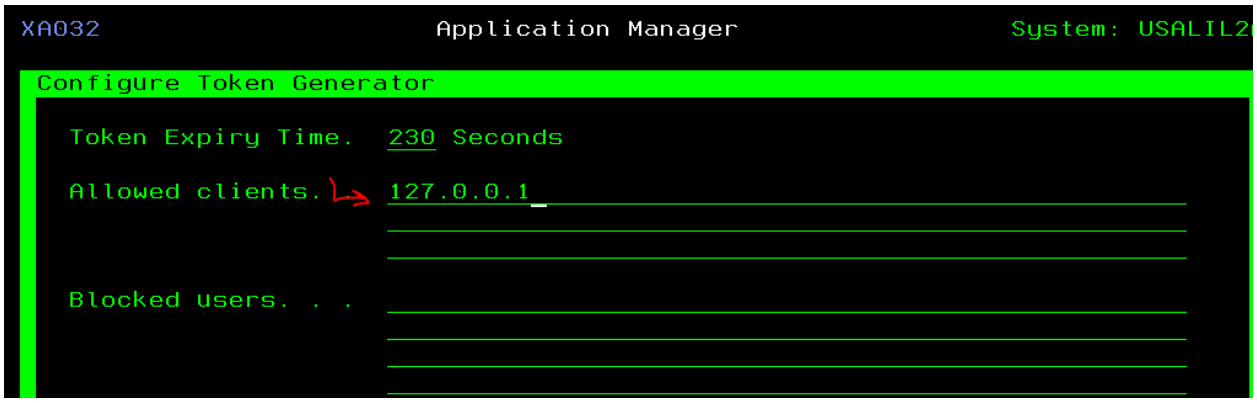
For example: 127.0.0.1

- Take F3 to exit.

Navigate to Secure Sign-on option → Configure Token generator.



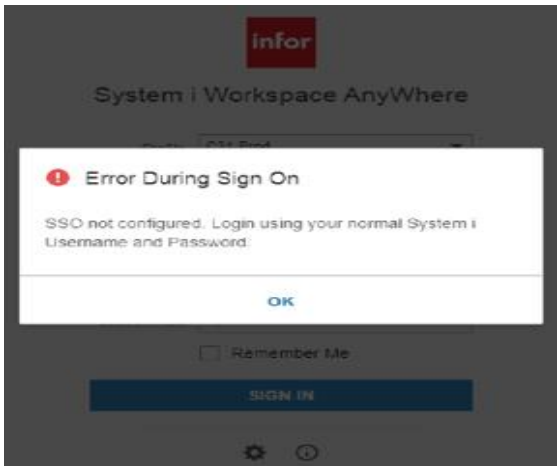
- Update the Client IPv4 address at Allowed clients, as displayed.

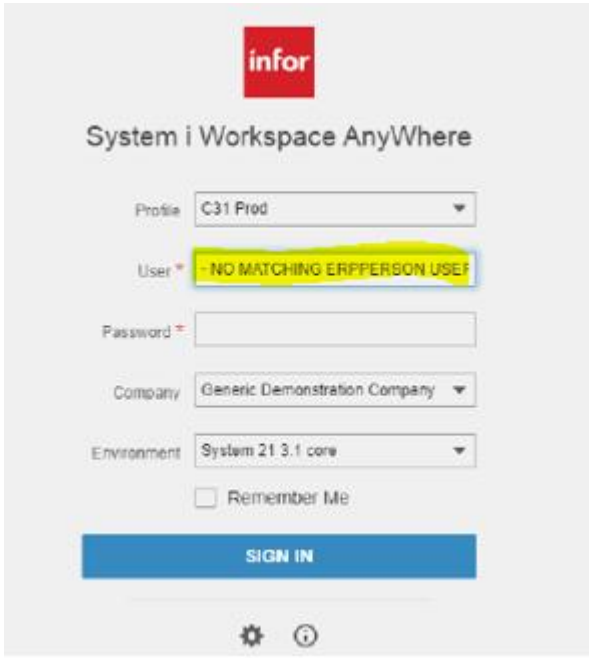


Press F8 to Update.

Press F3 to Exit.

8 If, on launching the XA application from Infor OS Portal, you see either a blank screen or one, or both, of these screens.

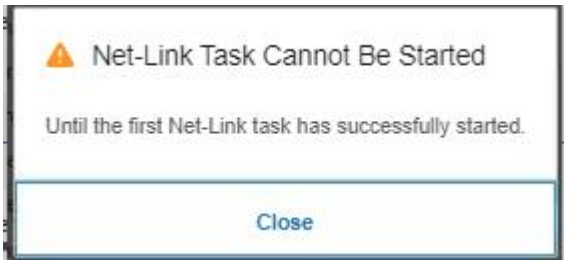




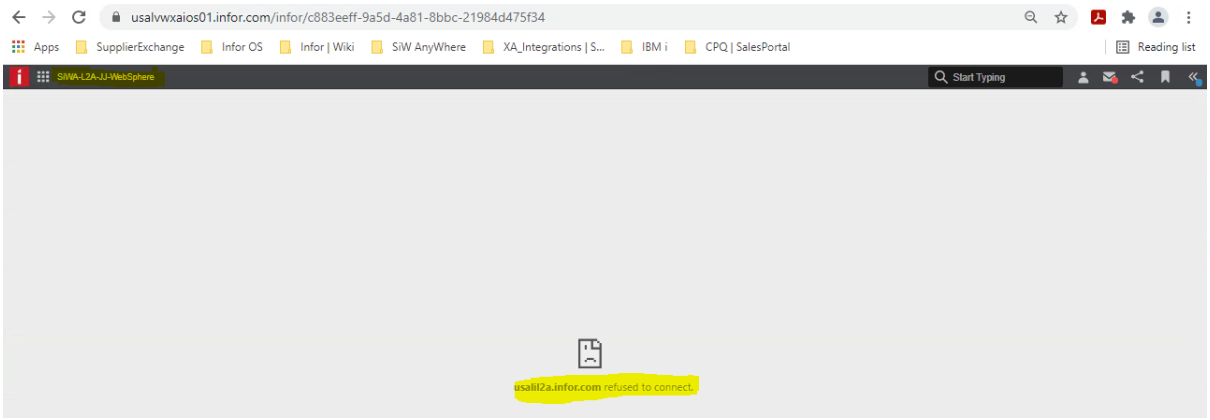
Then Single Sign-On (SSO) is not correctly configured in Infor OS Portal, System Manager, System i Workspace AnyWhere, or all three. Check the SSO setup once again.

Note: It is expected that you have already tested System i Workspace AnyWhere as a stand-alone application, from a client PC, and resolved any issues with that setup before enabling any of the SSO features.

9 If the message below 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 Portal.

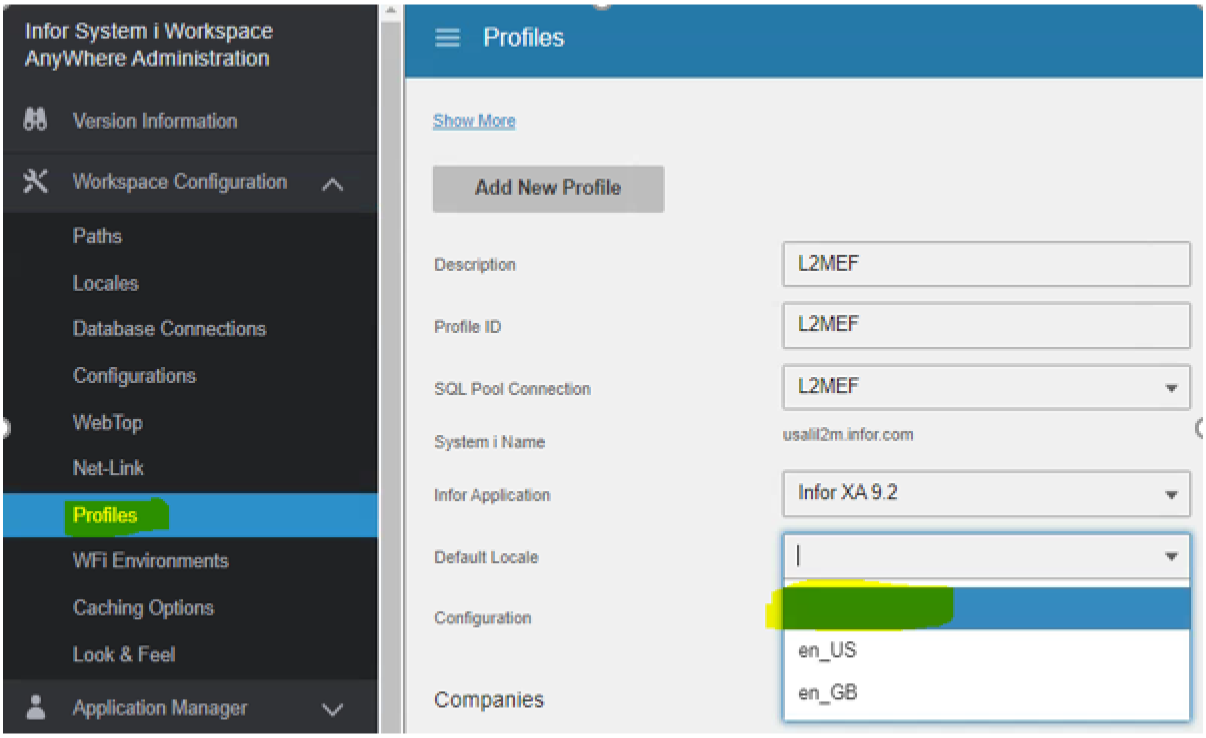


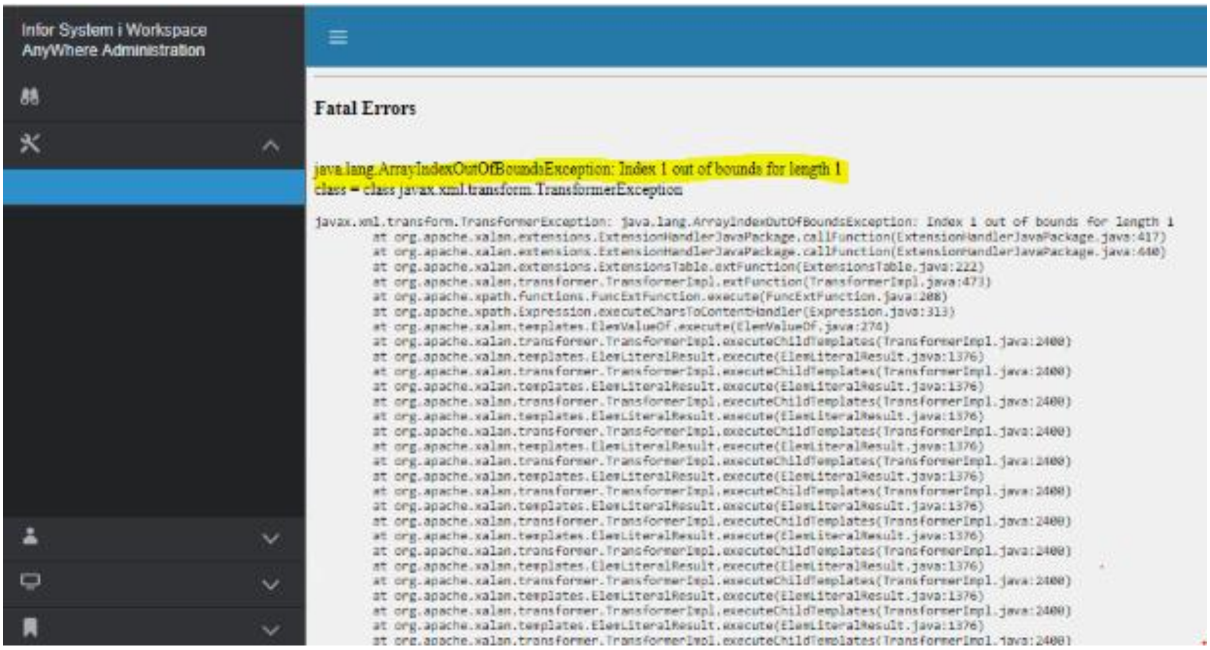
10 If you encounter an error “abc.infor.com refused to connect”, shown as below, where abc is SiWA installed server hostname.



Check if cross-domain cookies configuration is done as mentioned in “**Allow cross-domain cookies”** section in **“Chapter 6 Additional configuring in SiW”**.

11 In SiWA Admin page, under Profiles, if you have selected empty value for default locale and saved it. Then we might receive “java.lang.ArrayIndexOutOfBoundException”, shown as below.

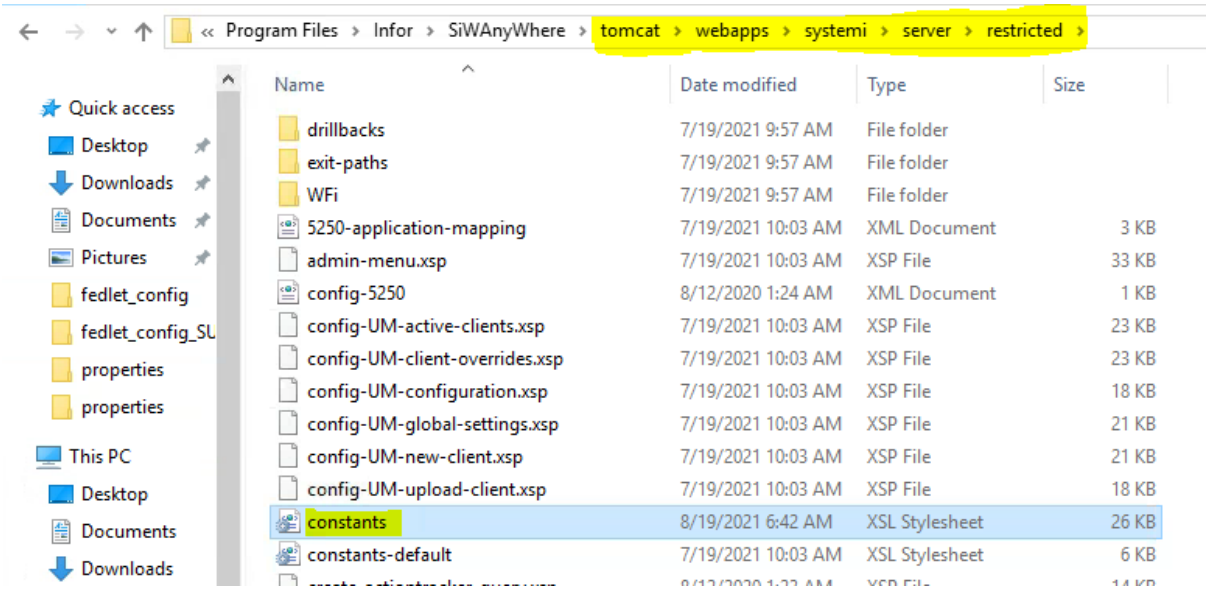




To resolve the issue, please follow the below steps:

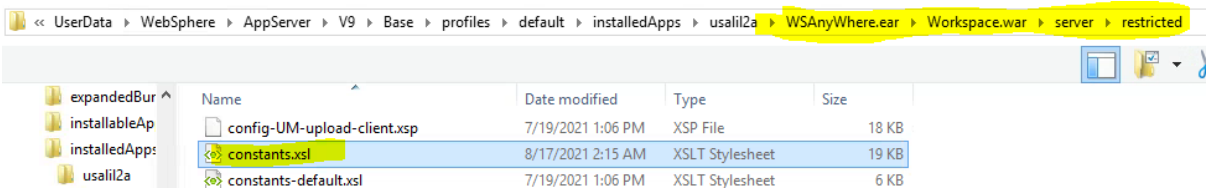
- Navigate and open the *“constants.xsl”* file, shown as below:

  For SIWA Tomcat, it is located in *restricted* folder under: tomcat\webapps\systemi\server\restricted



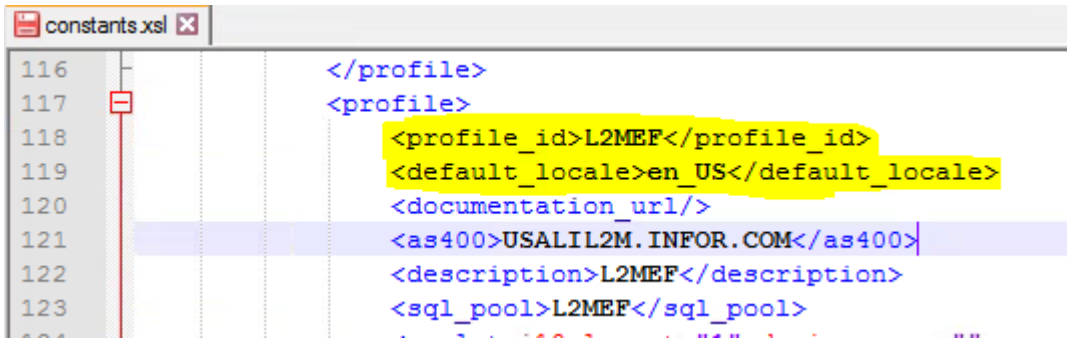
For SIWA WebSpere, it is located in *restricted* folder under:

\QIBM\UserData\WebSphere\AppServer\V9\Base\profiles\<ProfileName\installedApps\<NodeName>\WSAnyWhere.ear\Workspace.war\server\restricted

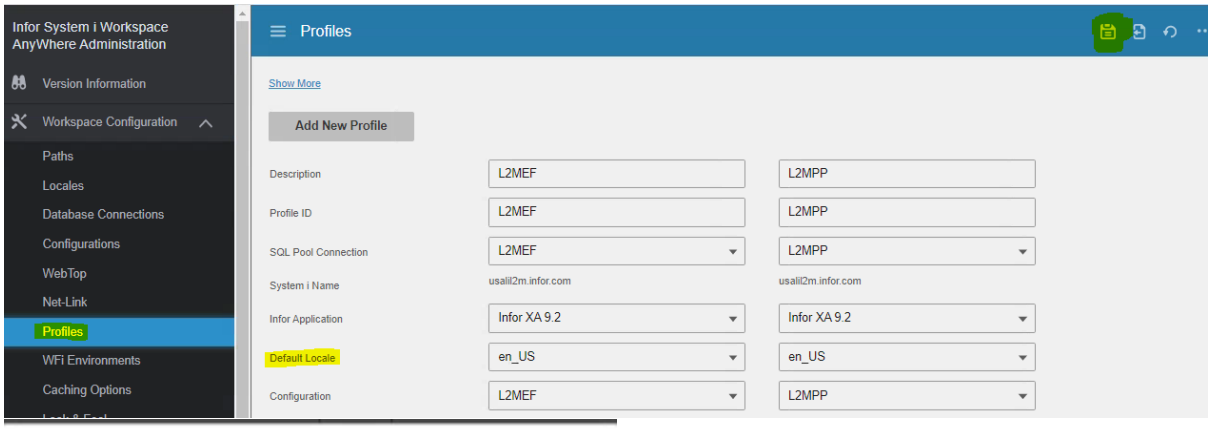


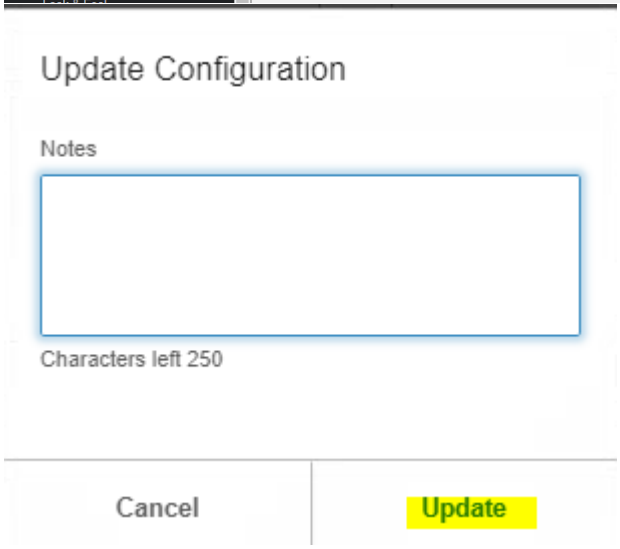
- Navigate to ***default_locale*** element for the respective ***profile*** and observe that value would be empty space, shown as below:

- Now, update the value of ***default_locale*** manually from the available locale information and save the file (for example: "***en_US***"), shown as below:



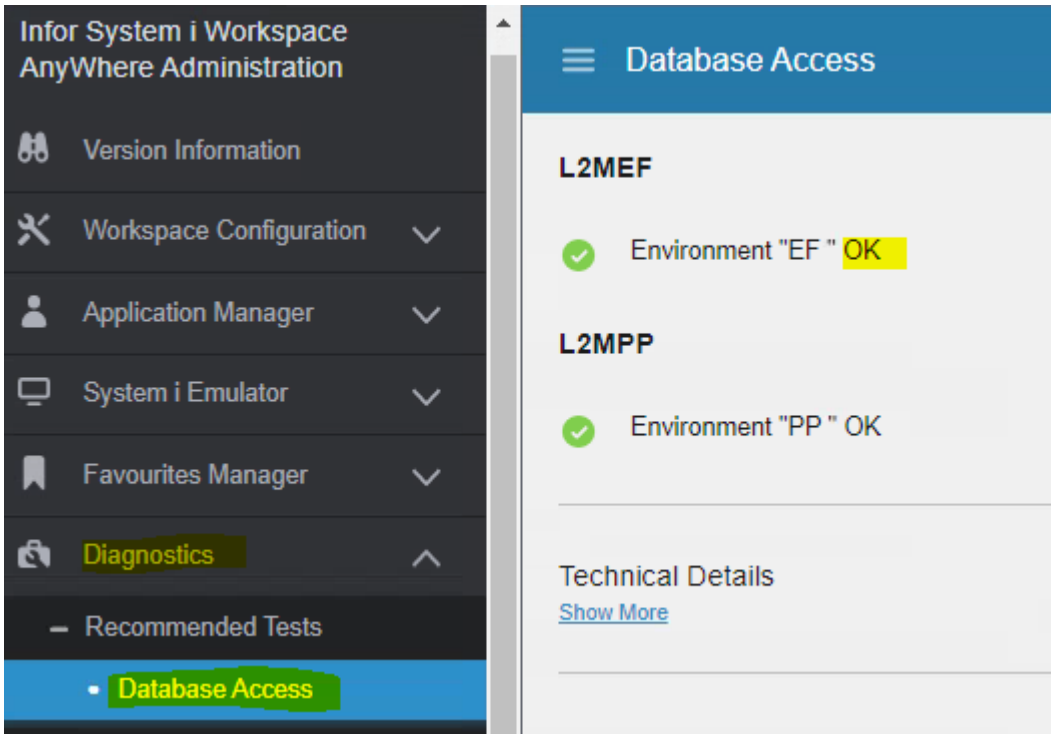
- In SIWA Admin page, navigate to Profiles and click on Save icon and then Update, shown as below.





Note: If required, refresh the SiWA Admin page URL.

- In SIWA Admin page, navigate to Diagnostics and click on Database Access and observe that the respective environment is OK, shown as below.



Enable debugging in System i Workspace AnyWhere

- Firstly, locate the System i Workspace AnyWhere system.properties file (as documented in the ***System i Workspace AnyWhere Installation & Administration Guide***). Add this property to enable SSO Debug mode inm System i Workspace AnyWhere:

Property	Description
com.infor.siw.cloud.debug	Set to 1 to enable SSO debugging specific features of System i Workspace Anywhere

- Secondly, locate the server\xsl folder within your web application deployment. 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'"/>.
- Save the file.
- Finally, locate the WEB-INF\classes folder within your web application deployment. Edit the log4j.xml file using a text editor and change <Root level="warn"> to <Root level="debug">.
- Save the file and restart System i Workspace AnyWhere to apply these changes.

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

The next time a user logs into System i Workspace AnyWhere, via InforOS, debugging information is written to the Standard Output log file of your web application/server.

Enable debugging of the identify provider

- To change the debugging level that is logged by the Identity Provider, locate the fedlet_config folder. If you have followed the instructions within this document, this folder must be located in the root directory of your System i Workspace AnyWhere server.
- Edit the FederationConfig.properties file contained within this folder using a text editor and locate this line: *com.iplanet.services.debug.level=error.*
- Change the *com.iplanet.services.debug.level* setting to one of off, error, warning or message.
- Save the file and restart System i Workspace AnyWhere to apply the change.

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

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

Additional Troubleshootings

For any additional troubleshooting steps, refer "***Troubleshooting Techniques***" Chapter in the ***System i Workspace AnyWhere Installation & Administration Guide***.

Appendix E Multiple SiW AnyWhere Tomcat Installations in a single Windows server

If you want to install and run multiple instances of SiW AnyWhere in a single Windows server using unique ports for each individual installation, please follow the below additional settings for each SiW AnyWhere installations:

1 Navigate to SiWA Installation folder

(for example ***/tomcat/conf/context.xml*** file.)

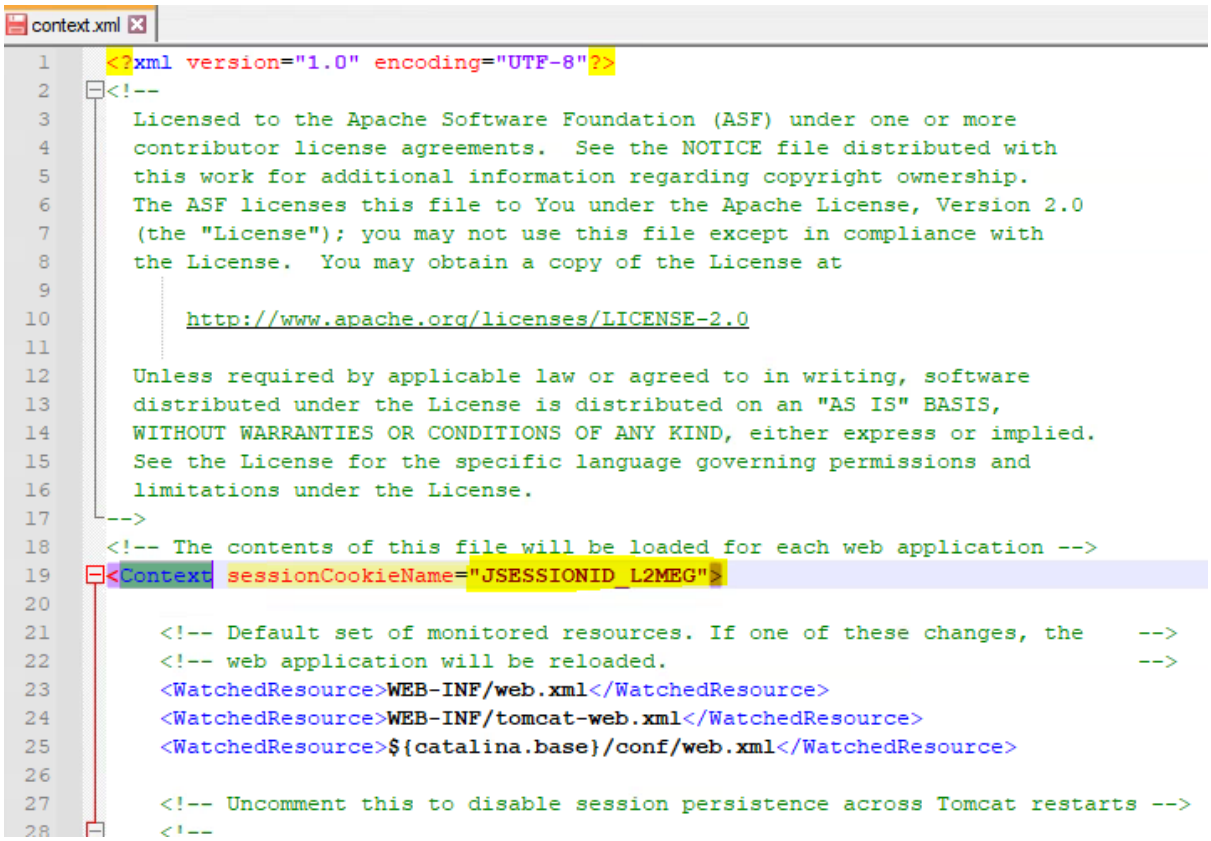
2 Edit the ***context.xml*** file and change the following line:

<Context>

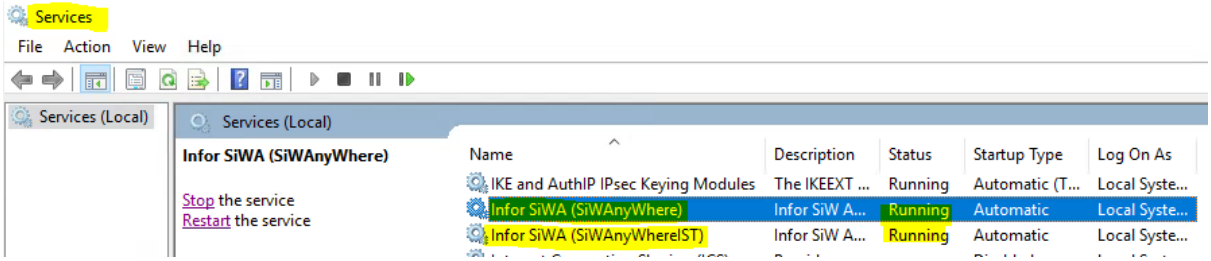
To

<Context sessionCookieName="JSESSIONID_{environmentID}">

where {**environmentID**} is the id of the environment.



1 Restart the SiW AnyWhere Windows server and make sure the status of SiW Anywhere services are ***running*** post server restart.



Appendix F Multiple SiW AnyWhere WebSphere Installations in a Single IBMi server

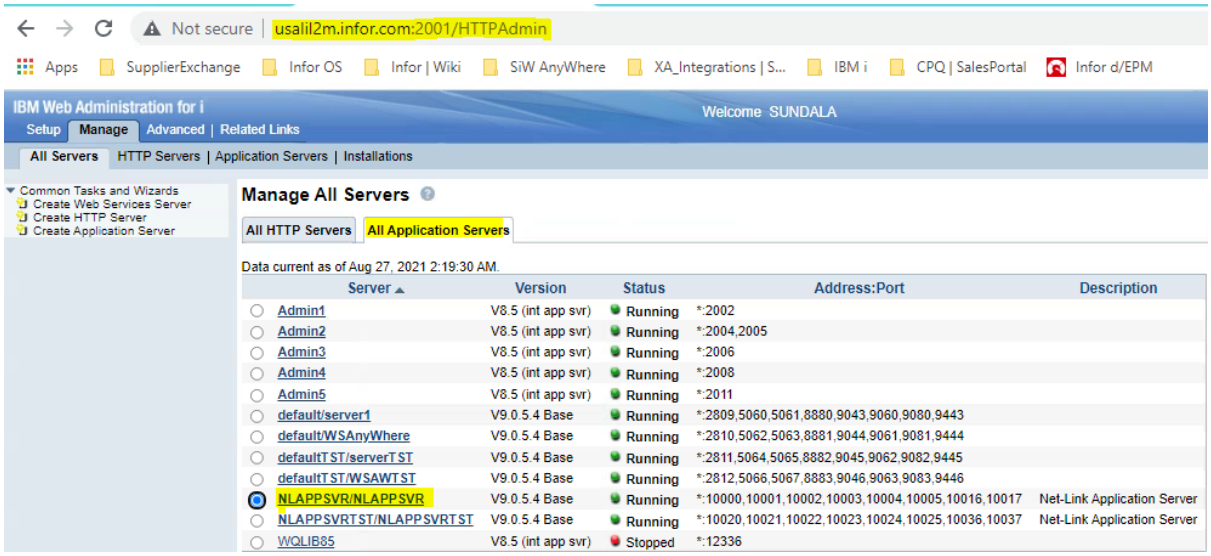
If you want to install and run multiple instances of SiW AnyWhere WebSphere in a single IBMi server using unique ports for each individual installation, please follow the below additional settings for each SiW AnyWhere installations:

1 Login to IBMi Web Administrator for i using the below URL, then navigate and select the Net-Link WebSphere Application server, which is used for Securing Net-Link, shown as below:

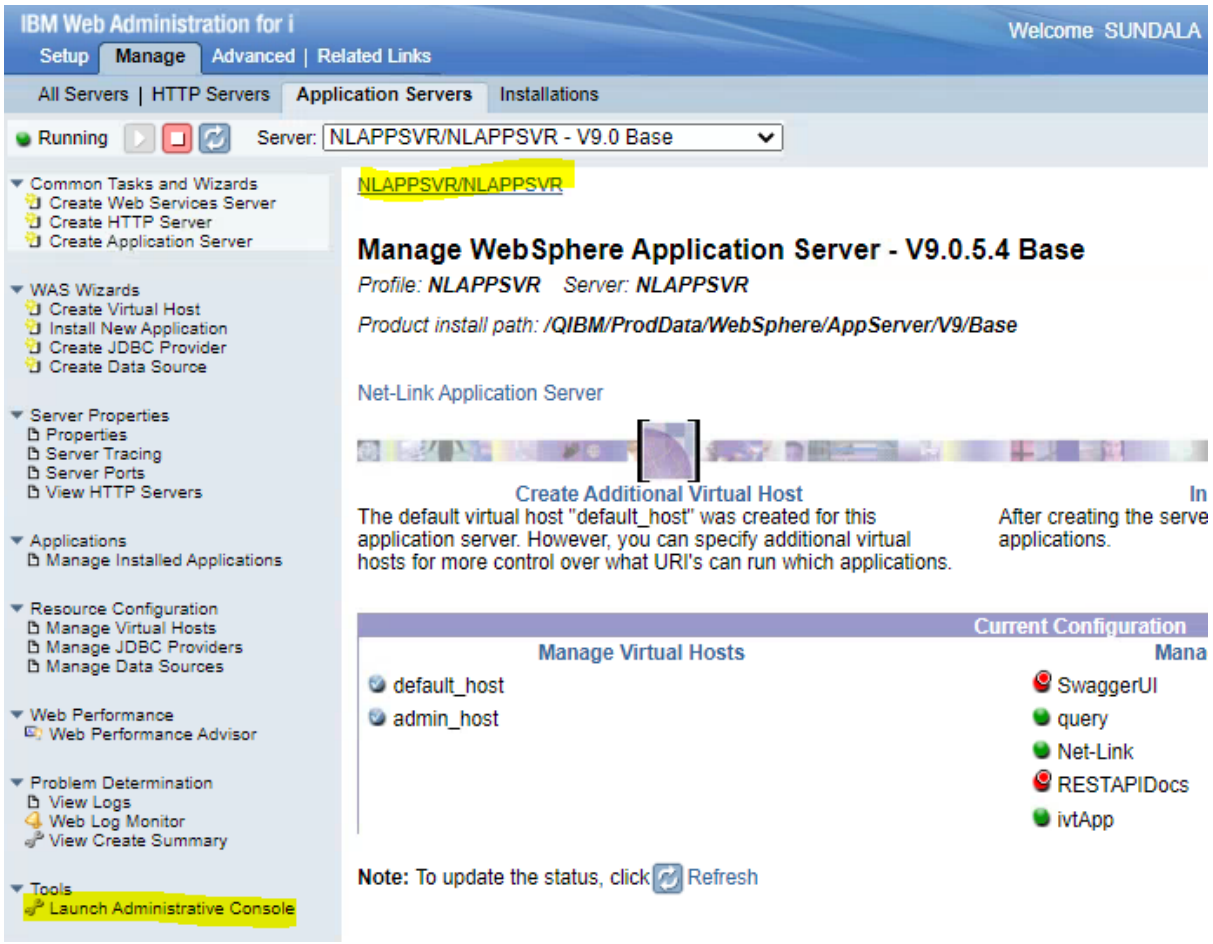
http://<hostname>:2001/HTTPAdmin

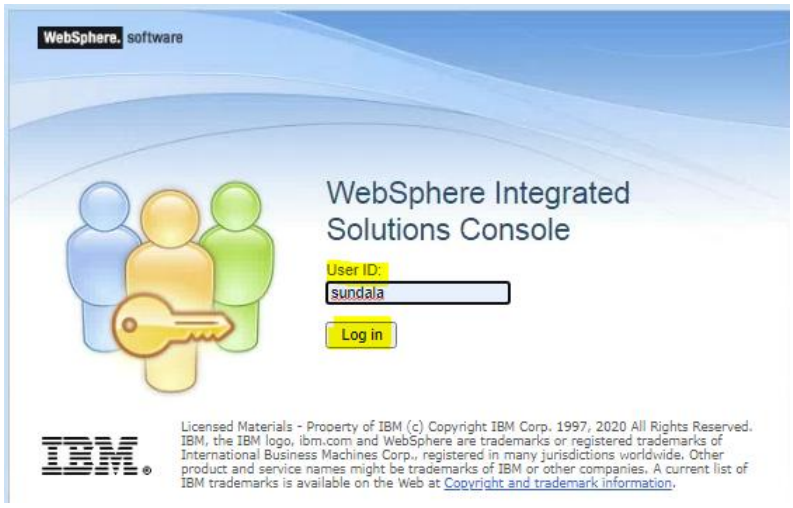
where <hostname> is FQDN of IBMi server

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

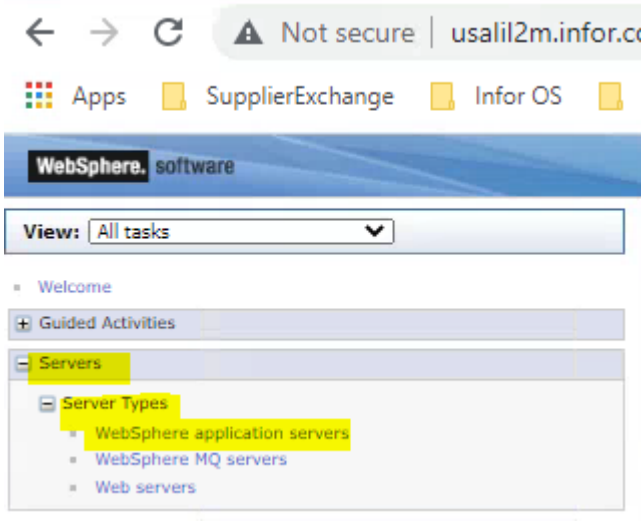


1 Launch the IBM WebSphere Administrative Console to make configuration changes, shown as below:



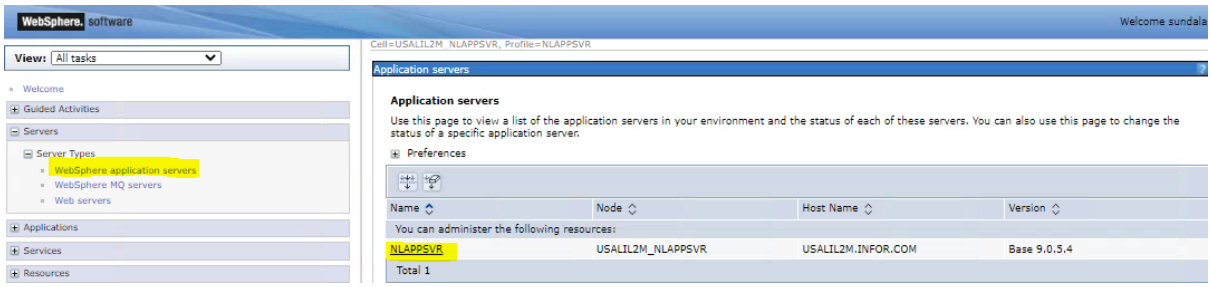


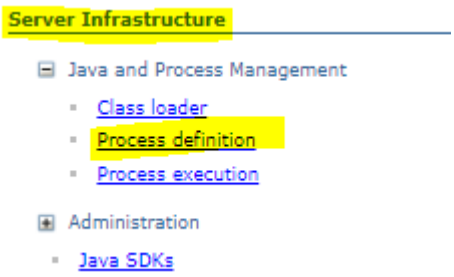
1 From the menus on the left-hand side, select **Servers** > **Server Types** > **WebSphere Application Servers**

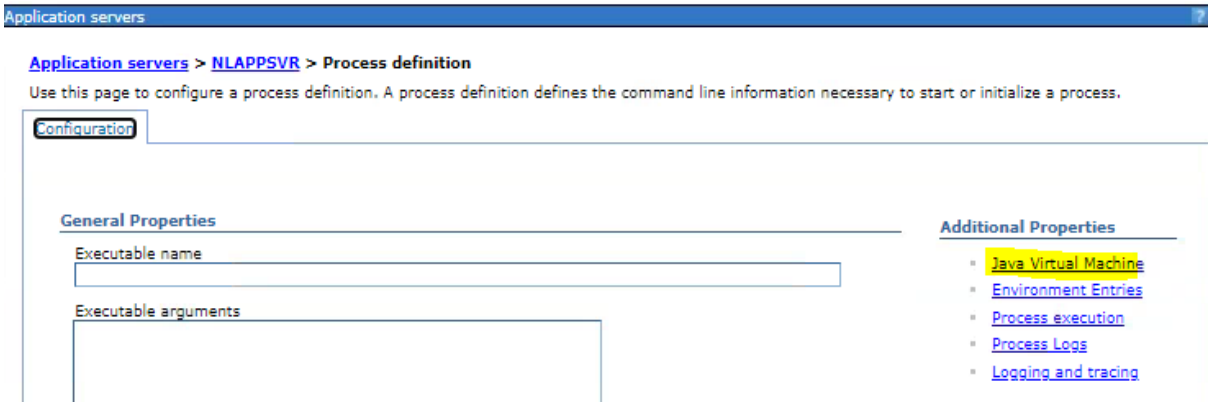


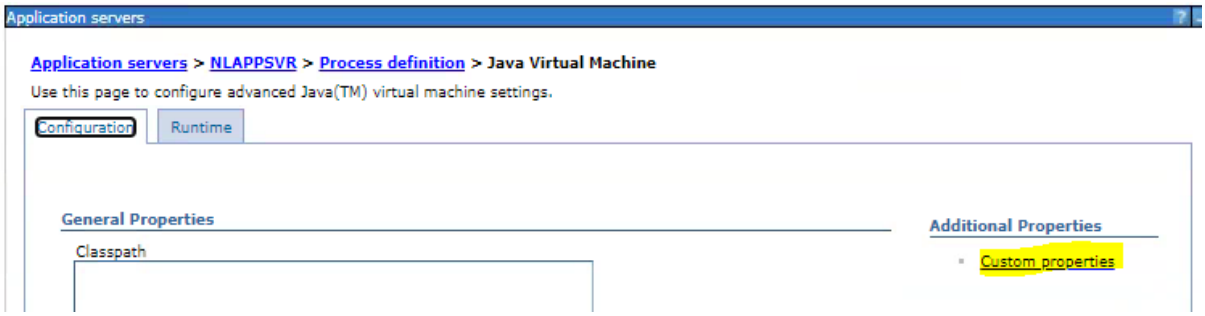
1 Click on the Net-Link configured WebSphere Application server and then navigate to

Server Infrastructure > Java and Process Management > Process Definition > Java Virtual Machine > Custom Properties

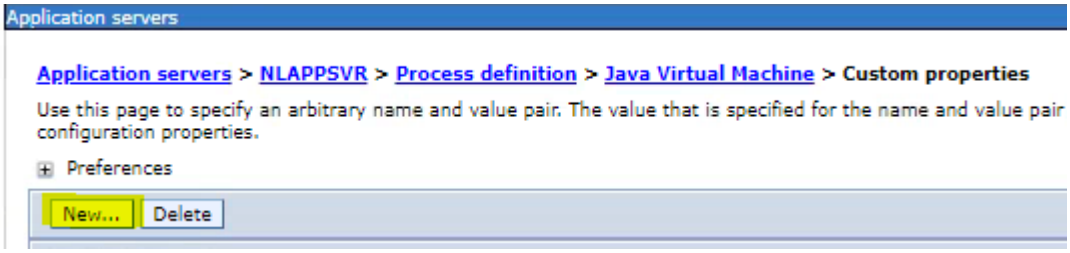




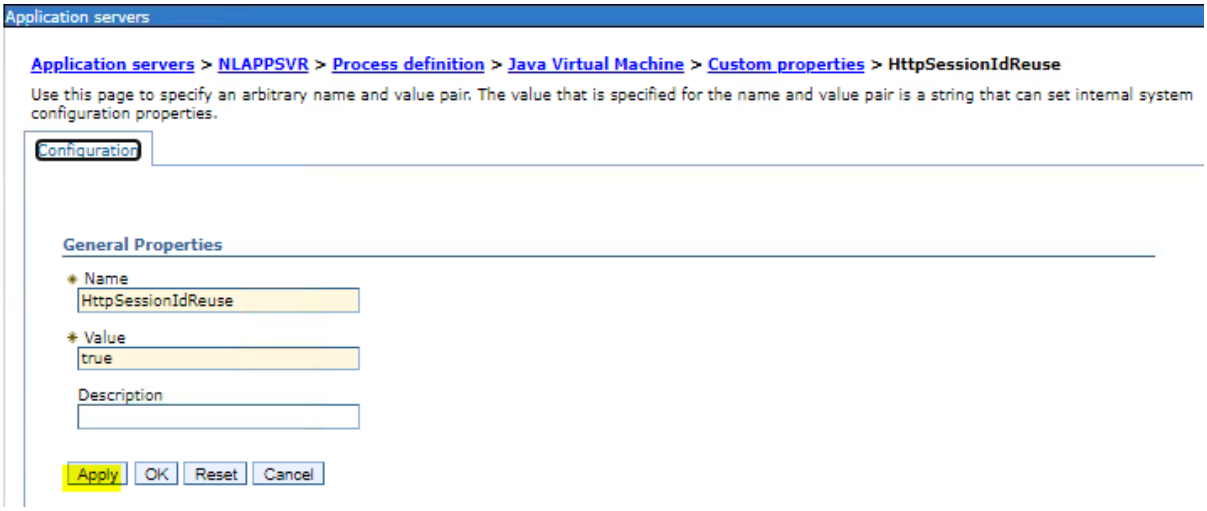




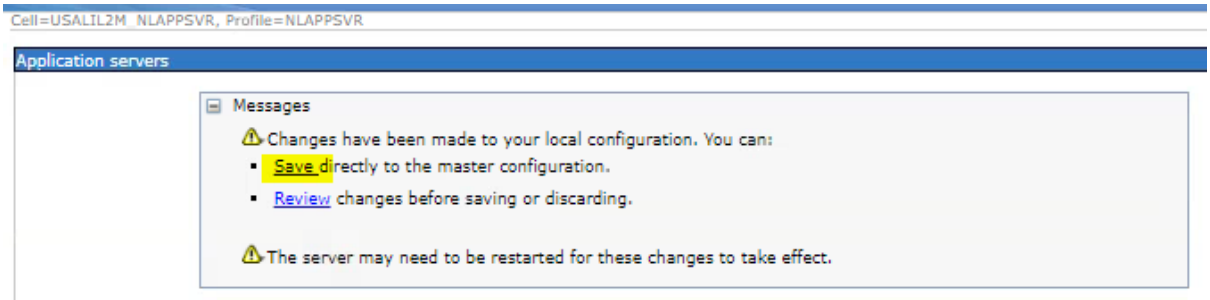
1) Click on **New** and add a new Custom Property for the JVM to reuse the sessionId, shown as below:

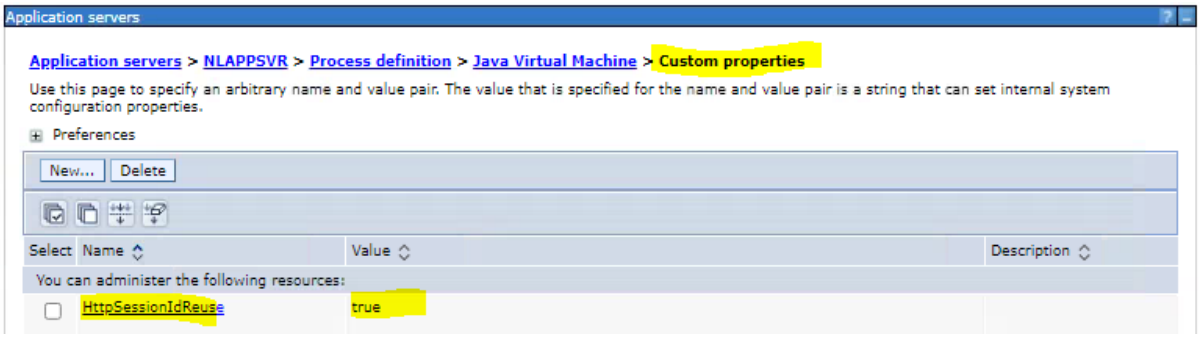


Use System Property Name: ***HttpSessionIdReuse*** and System Property Value: ***true***



2) Save your changes and restart the Application Server.



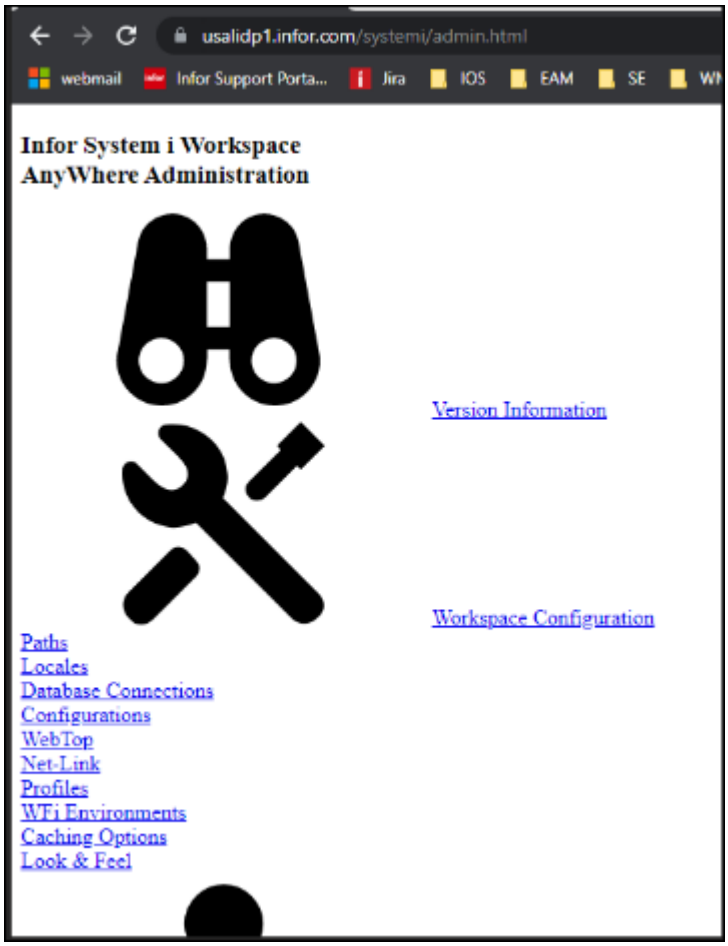


Note: SSO cannot be implemented for the second instance of SiWA, as we are using single WebSphere for 2 SiWA. This is a limitation.

Appendix G Validate IBMi Server and DB details in SiWA installation

SiWA Admin page not loading properly

After successful installation of SiWA instance if you observed below page while accessing admin.html page, then this suggests that there might be some issue IBMI server or DB credentials in the installation.



Note: This issue is observed in a scenario when you have deleted an existing SiWA installation on a WebSphere or Tomcat and gone for fresh SiWA installation, but with same instance/ User Key name.

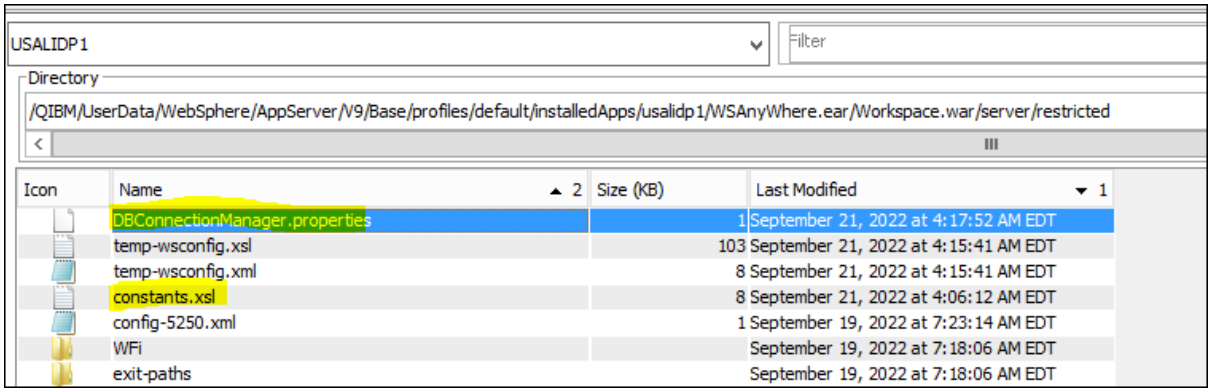
Though the previous SiWA installation is deleted on WebSphere or Tomcat, the previous installation data will be stored in IBMi server and same old configuration might be re-used in new installation due to using same User Key.

IBMi Deployment:

Go to below folder in IFS.

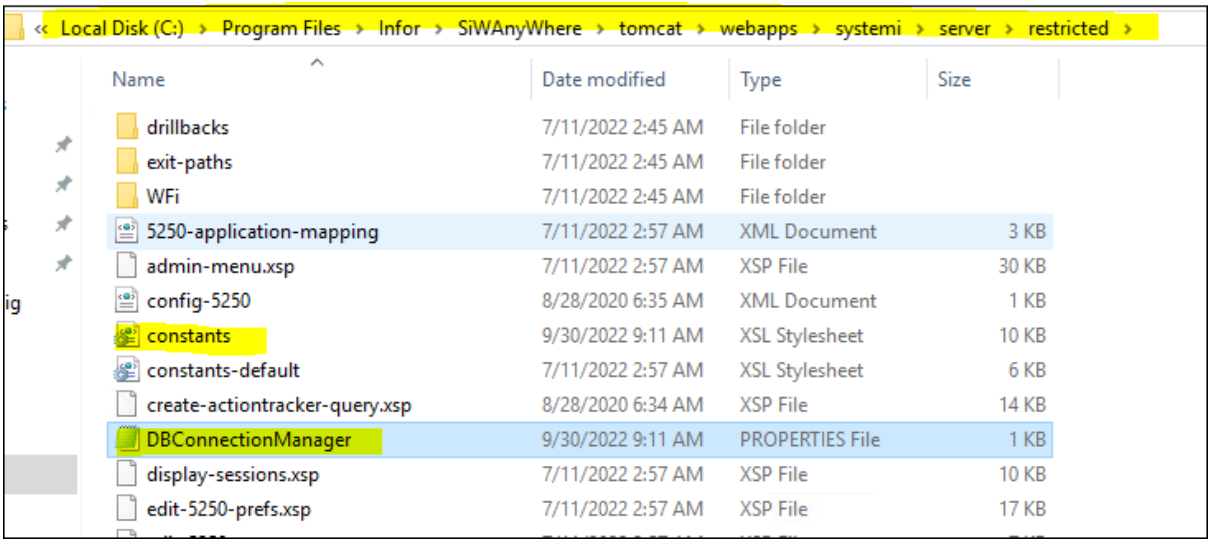
/QIBM/UserData/WebSphere/AppServer/V9/Base/profiles/<ProfileName>/installedApps/<NodeName>/WSAnyWhere.ear/Workspace.war/server/restricted

Open and validate details in DBConnectionManager.properties and constants.xsl files.



Windows Deployment:

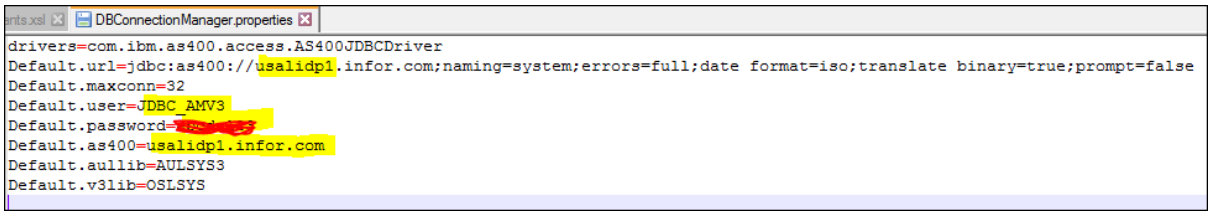
Go to SiWA Tomcat installation folder, tomcat -> webapps -> systemi -> server - > restricted folder.



For example validate below details in constants.xsl file:

Check as400, STATIC_URL with https, AURORA_URL with https, STATIC_LOCATION, JDBC_AMV3 password.

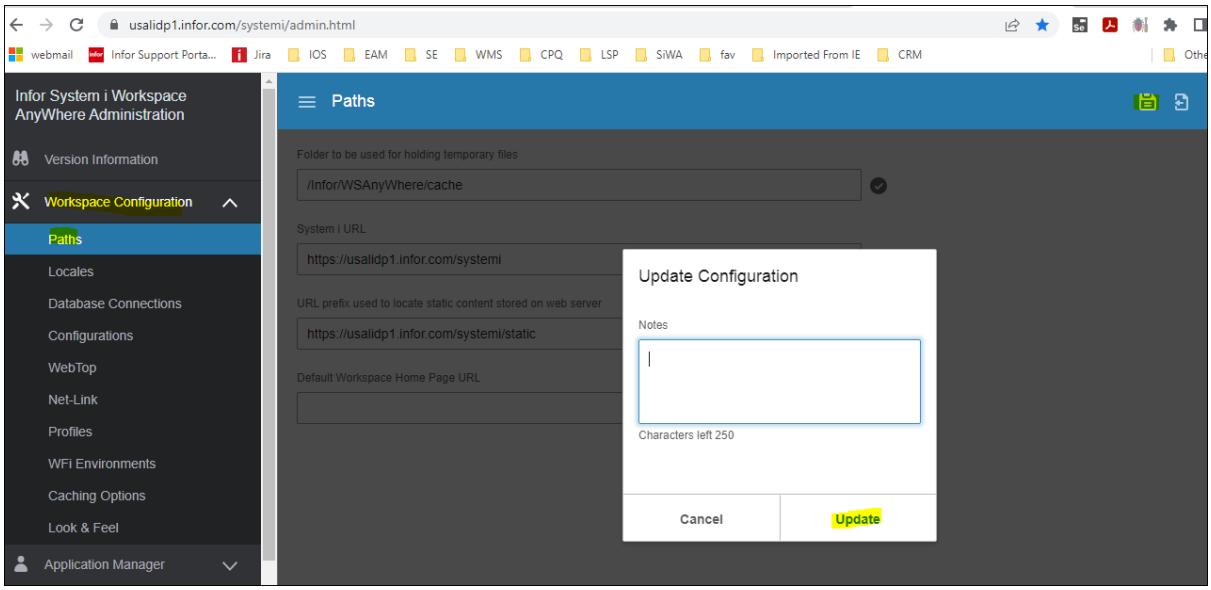
For example validate below details in DBConnectionManager.properties file.



Note: After changing these files and updating same in IFS folder, we should not restart the HTTP and Application servers or SiWA service. This is revert the changes in these files.

After changing these files, refresh the admin.html and install-verify.html.

Once SiWA admin launches fine, then go “Workspace Configuration” and click on save/Update Configuration.



Now we can go and restart HTTP and APP servers in WebSphere. Similarly, SiWA service for Tomcat.