Infor XA Configuration Guide for Infor OS MT CE using SiW AnyWhere

XA 9.2 and 10.0
Infor OS MT Cloud Edition 2023.xx

Publication Information

Release: Infor XA 9.2 and 10.0

Publication date: June 20, 2023

Contents

About this guide

This document describes the integration of XA On-premise with Infor Operating Service Multi-Tenant Cloud Edition (referred as Infor OS MT CE) using SiW AnyWhere. 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 MT CE.

Required knowledge

To integrate XA and Infor OS MT CE, you must understand the concepts behind System Manager, System i Workspace AnyWhere and Infor OS MT CE.

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

Contacting Infor

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

If we update this document after the product release, we will post the new version on the Infor Support Portal. To access documentation, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

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

Chapter 1 Introduction

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

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

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. 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.

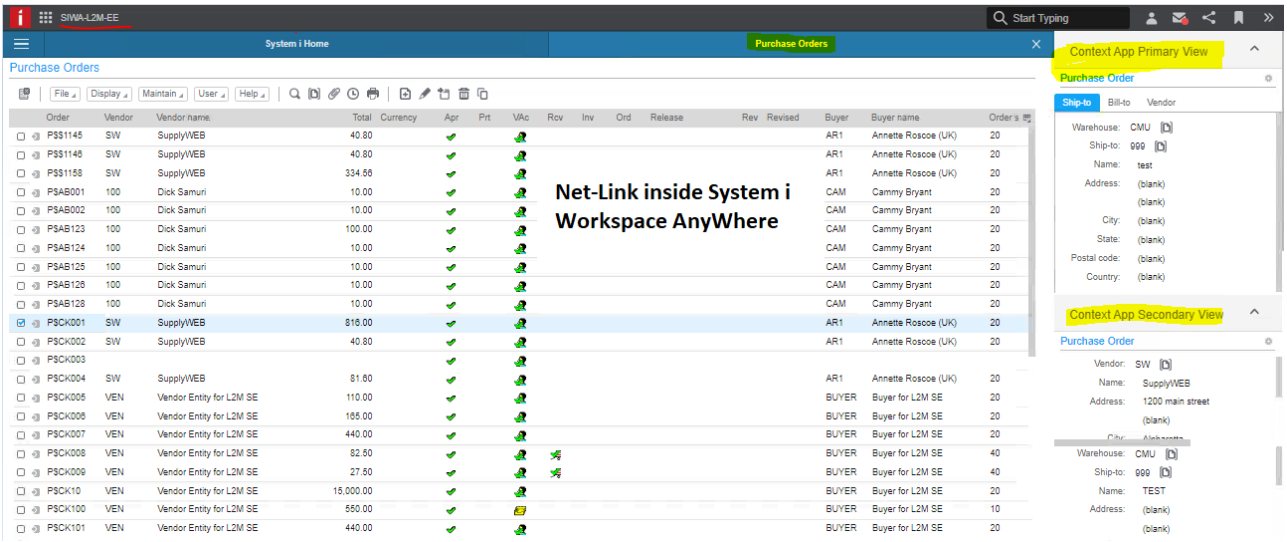
This guide describes the process to configure the components, to run XA within the Infor OS common user interface.

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) MT CE

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


SIWA-L2M-EE
Start Typing
System i Home
Purchase Orders
Purchase Orders
File
Display
Maintain
User
Help
Net-Link inside System i
Workspace AnyWhere
Context App Primary View
Purchase Order
Ship-to
Bill-to
Vendor
Warehouse: CMU
Ship-to: 999
Name: test
Address: (blank)
(blank)
City: (blank)
State: (blank)
Postal code: (blank)
Country: (blank)
Context App Secondary View
Purchase Order
Vendor: SW
Name: SupplyWEB
Address: 1200 main street
(blank)
Warehouse: CMU
Ship-to: 999
Name: TEST
Address: (blank)
(blank)

Chapter 2 Requirements

This chapter describes the requirements for configuring Infor XA within Infor OS MT CE using SiW Anywhere.

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 MT CE.

- Infor Development Framework for Infor XA 06.03 (IDF R9) and any additional IDF licensed applications like IDF Power-Link with Integrator and Net-Link.
- Infor XA IDF 9.2.2 client software build must be 02.09.02.02.30 or later.
- Infor XA IDF 9.2.2 server PTFs is PCM SH16055 (XA 9.2.2 with PTF level 025000).
- Infor XA IDF 10.0 client software build must be 03.10.00.01.03 or later
- Infor XA IDF 10.0 server PTFs is PCM SH16231 (XA 10.0 with PTF level 00100).
- IBMi standard software set option 5770SS1: Option 8 – AFP Compatibility Fonts (required for TIFF image support).
- IBMi standard software set option 5770TS1 on 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 (143 minimum)

  These PTFs are required to correctly generate self-signed certificates within the IBM HTTP Server as additional software for System i Workspace with IBMi deployment:
- OS400 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

IBMi accounts required

These user account(s) must be created, if not already present on your IBMi server. If the accounts already exist, then ensure that their security configuration is as specified:

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

Infor System i Workspace AnyWhere Requirements

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

Hardware requirements

Note: System i Workspace must NOT be installed on any server machines acting as a Domain Controller, DNS Server, WINS Server, Mail Server or any other mission critical machine.

Microsoft Windows deployment

These are the hardware requirements for the deployment of System i Workspace onto your Microsoft Windows Server:

Note: Please see https://docs.microsoft.com/en-us/windows-server/get-started/system-requirements for the core hardware requirements for Microsoft Windows Server.

The sizing figures below were produced from observations of a standard Infor System i Workspace AnyWhere deployment, with two versions of Infor System21 Screen Design Template and Help files installed. This requires an initial product footprint of 2GB of memory on top of the 2GB required by Microsoft Windows Server (with Desktop Experience enabled) and approximately 2GB of disk space (including JDK).

We observed that each unique user session consumed approximately 50Mb of memory, and each 5250 AnyWhere session consumed an approximate additional 5Mb of memory. Therefore, a minimum of 6GB of memory is recommended for a 5-user deployment for evaluation.

These sizing figures are provided as estimates to help establish base requirements for your Infor System i Workspace AnyWhere deployment. Before committing to a deployment, we strongly recommend you discuss sizing of your server hardware with your Infor representative so they can provide more accurate figures for the requirements within your enterprise with respect to the users, sessions and features you wish to utilize within Infor System i Workspace AnyWhere.

Component	Minimum Requirement
CPU	Table text

Component	Minimum Requirement
CPU	64-bit, 2 Cores for evaluation purposes only 64-bit, 4 Cores (15-50 users) 64-bit, 8 Cores (50+ users) System i Workspace uses a 64bit Java JVM so memory should not be a limitation. Some tuning of Java memory configuration may be required along with Tomcat thread configuration when supporting more than 250 users.
RAM	6 GB for evaluation purposes only 8 GB (15-50 users) 12 GB (50+ users)
Hard disk	100 GB
LAN	Gigabit Ethernet (Windows server should be located on the same LAN as your IBMi to keep network latency to a minimum)

IBMi deployment

These are the hardware requirements for the deployment of Infor System i Workspace AnyWhere onto your IBMi Server:

Component	Minimum Requirement
Processor	Minimum of 1000 CPW per partition.
Disk Space	Minimum of 5 GB of available disk space.

System i Workspace clients

Component	Minimum Requirement
CPU	CPU power is an important performance factor because System i Workspace is a rich and complex GUI browser application. We recommend that you use a CPU with an individual core speed of 2.0 GHz or faster.
RAM	Consult your web browser documentation for its memory requirements. To achieve optimal performance, usually 4 GB or more of internal memory is required, and at least 1 GB free after all other applications are loaded.
Hard disk	Consult your web browser documentation for its memory requirements. If you are planning to install the System i Emulator, then at least 2 GB of free hard disk space is required.
Video	Video adapter supporting a minimum resolution of 1440x900.

Note: The hardware requirements depend on many different factors and combinations which impact the performance of System i Workspace clients. Consideration must be given to the number, and type, of applications in use, the anti-virus software installed, browser plug-ins and importantly, the number of concurrent System i Workspace sessions that each user has open at any one time.

Software requirements

This section describes the software requirements for Infor System i Workspace AnyWhere including Operating System requirements, for the deployment configurations covered in this document.

Operating systems

Platform	Supported Versions
Client PC	• Microsoft Windows 8.1 (32bit or 64bit) • Microsoft Windows 10 (64bit) • Apple Mac OS (Big Sur or later)
System i Workspace Server	• Microsoft Windows Server 2019 Standard (or above) • Microsoft Windows Server 2016 Standard (or above) **Caution:** In this guide, when we refer to the term "Windows Server", it is this Operating System software version that is being referenced.
IBMi	OS400 V7R3 or V7R4

Software

Platform	Software Requirements
Client PC	• Microsoft Edge, Google Chrome, Mozilla Firefox or Apple Safari with latest updates applied • An installation of Acrobat Reader DC, or any alternative PDF viewer, that supports integration with your web browser All of these if the System i Emulator is going to be used: • Microsoft .NET Framework 4.8 • System i Emulator Update Manager (delivered within the System i Workspace ISO image)
Microsoft Windows Server	Amazon Corretto 11 JDK (x64) **Note:** At the time of writing the exact version of Corretto 11 was 11.0.5.10.1

Supported browser clients

System i Workspace supports these browsers on Microsoft Windows:

- Microsoft Edge (Chromium version)
- Google Chrome (version 80 or later)

System i Workspace supports these browsers on Apple Mac OS:

- Google Chrome (version 80 or later)
- Apple Safari (version 14 or later)

Removal of Internet Explorer Support

As of July 29, 2015, Microsoft ended support for Internet Explorer® (IE) browser IE11 (except for security patches) and recently announced the retirement of the product as of June 15, 2022. Please see the Microsoft Lifecycle Policy for more information.
Following Microsoft's announcement, Infor no longer supports IE with Infor System i Workspace AnyWhere from FP14.
While Microsoft recommends IE Mode within Microsoft Edge® as the default browser for all users moving forward with legacy software, Infor doesn't support System i Workspace and its associated applications running under IE Mode in Microsoft Edge and concentrate on non-proprietary industry standard browser technologies.
A project has been underway at Infor for several years to remove the dependency on Microsoft IE and ActiveX® technologies. That work was completed with the release of Feature Pack (FP)12 for System i Workspace AnyWhere in July 2021. FP12 delivered a complete HTML replacement for the System i Emulator Designer application to work alongside the 5250 AnyWhere Emulator. As a result, both are now independent of the Microsoft IE and ActiveX technologies. Future Development efforts arededicated to HTML-based versions of the applications.

Removal of the System i Emulator and Update Manager

As part of the removal of support for Internet Explorer, the remaining certified web browsers supported by Infor System i Workspace AnyWhere do not support Microsoft ActiveX®-based plugins, therefore, both the System i Emulator, and its Update Manager, have now been removed and isno longer be supported with Infor System i Workspace AnyWhere.

After upgrading to FP14, we recommend that customers who have existing deployments of the Infor System i Workspace AnyWhere version of the System i Emulator should uninstall it from their client PCs. if they are not utilizing it for any older versions of Infor System i Workspace (such as System i Workspace v2015)

The Infor System i Workspace AnyWhere documentation has been updated to reflect these changes, including the removal of the System i Workspace AnyWhere – Emulator Extensions Guide, which has been replaced by the new System i Workspace AnyWhere - 5250 AnyWhere Emulator Extensions Guide.

Caution: Support for any of the web-based products that run inside the System i Workspace framework (such as Infor IDF/Net-Link, WebTop, etc.) you should consult that product's Installation/Administration Guides for details of which browsers are supported and/or any configuration requirements

Refer the Client Settings chapter **in *System i Workspace AnyWhere Installation and Administration Guide*** for specific configuration that may be required for the client browsers.

Security and account requirements

IBMi accounts required

These user accounts must be created if not already present on your IBMi server. If the accounts already exist, then ensure that their security configuration is as specified:

User	Requirement
Security Officer User with sufficient authorities to install System i Workspace (the install will default to **QSECOFR**)	This user must have a profile with ***ALLOBJ** and ***SECADM** special authorities to be able to install System i Workspace.
Database User to access System Manager, WFi files (the install will default to **JDBC_AMV3**) depending on the version of System Manager you selected. The installer will create an account if it doesn't already exist and configure the account as per the requirements.	This user must have a Group Profile of **AULUSER**, Supplemental Groups of **AULSECOFR**, **AULEXTOWN**, **AULAMDBUSR** and **AULDBUSER** and the Password expiration interval (**PWDEXPITV**) set to ***NOMAX**. It is also recommended that this user is set to ***SIGNOFF** for security reasons. This user should also have a library list setup either by defining the job description or using an initial program, which should include the System Manager libraries as part of their initial library list.

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

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

SSL/TLS encryption

Microsoft Windows deployment

System i Workspace uses SSL/TLS encryption for all communication over HTTP between the Client and Server. The System i Workspace installer allows you to choose either a **Self-Signed Certificate**, which is created by the installer automatically, or, if performing a Microsoft Windows deployment, use one that has been purchased or generated from a **Certificate Authority** (such as Comodo, Symantec or from one of the many other providers).

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

• A Keystore file that contains your purchased SSL Certificate and a **full** Certificate Authority Chain

• The password to this Keystore file

• The Alias Name for this Certificate within the Keystore file

Please see section **Secure Sockets Layer (SSL)** in **Security** Chapter for further details regarding how to obtain these items **before** you begin installation of Infor System i Workspace AnyWhere

IBMi deployment

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

See IBMi deployment section of the Pre-requisite installations chapter for more information on configuring SSL before installing Infor System i Workspace AnyWhere

Infor Operating Service Requirements

You are expected to have latest version or minimum version of Infor OS MT CE tenant provisioned with all required applications and Authorizations.

Client prerequisites

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

Supported browsers

Infor OS recommends that users use these browsers:

- Chrome for Windows and Mac OS
- Safari 11.x and 12.x for Mac OS only
- Safari 9
- Microsoft Edge
- Microsoft Edge Chromium

Screen resolution

The Infor Ming.le shell supports responsive design and adjusts to fit the content on different devices depending on these resolution widths:

- Desktop – 1280px and up
- Recommended desktop resolution: 1280 x 1024
- Tablet - between 768px and 1279px
- Mobile - between 320px and 767px

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 Infor Support Portal (search with the guide title in the System i Common Components section).

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

Installing System i Workspace AnyWhere

Microsoft Windows deployment

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

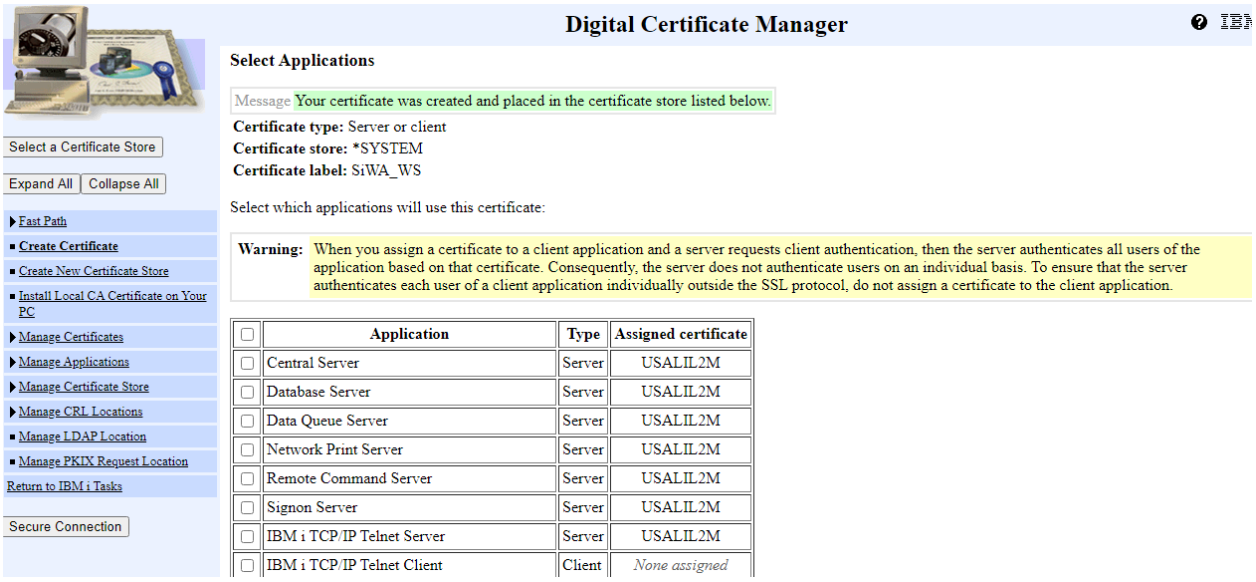
Note: If you want to install and run multiple instances of SiW AnyWhere Tomcat in a single Windows server using unique ports for each individual installation, please follow the required additional settings mentioned in ***Appendix F*** in this guide.

IBMi deployment

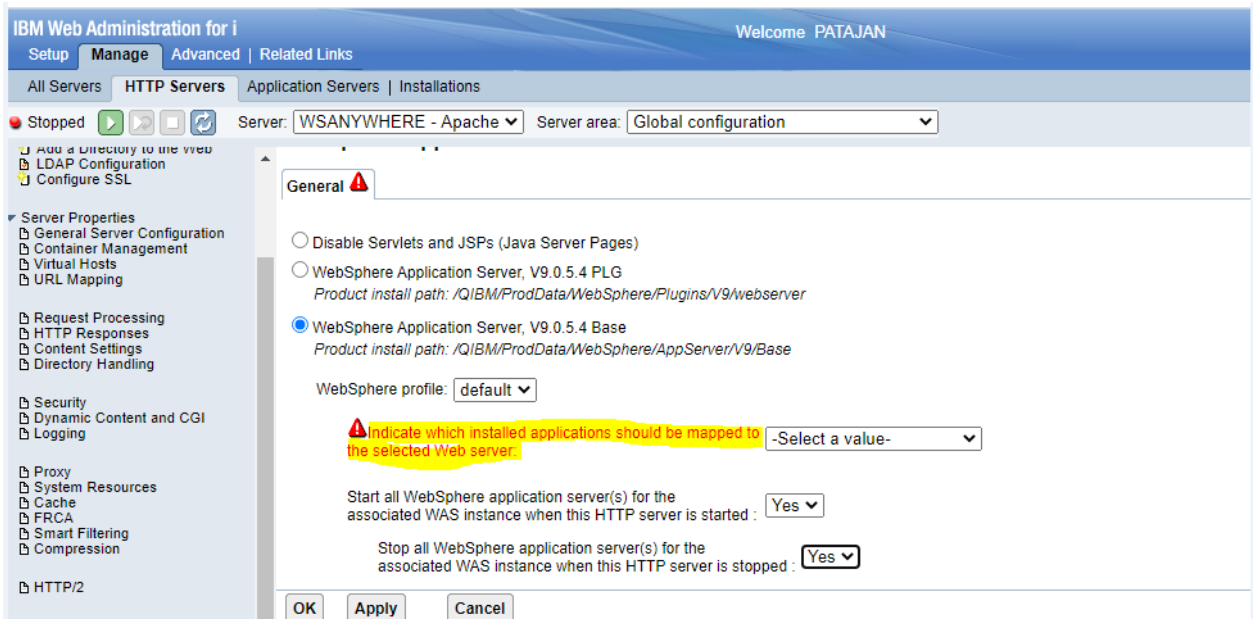
For installation and configuration of SiW AnyWhere to run on WebSphere Application Server, refer ***Infor System i Workspace AnyWhere Installation and Administration Guide*** and follow all the steps related to "**IBMi deployment**" section.

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 canuse 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 G*** 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 Operating Service Tenant

It is recommended to use XA with System i Workspace using Infor OS MT CE. You can use XA with System i Workspace but without Infor OS. You can omit the Infor OS 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, 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 the Infor Support Portal.

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 urls 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 H Validate IBMi Server and DB details in SiWA installation"* in this guide.

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

Note: If an Internal Server Error messages is displayed on screen when above url is hit, then follow "*Appendix C Internal Server Error Resolution"* 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 :

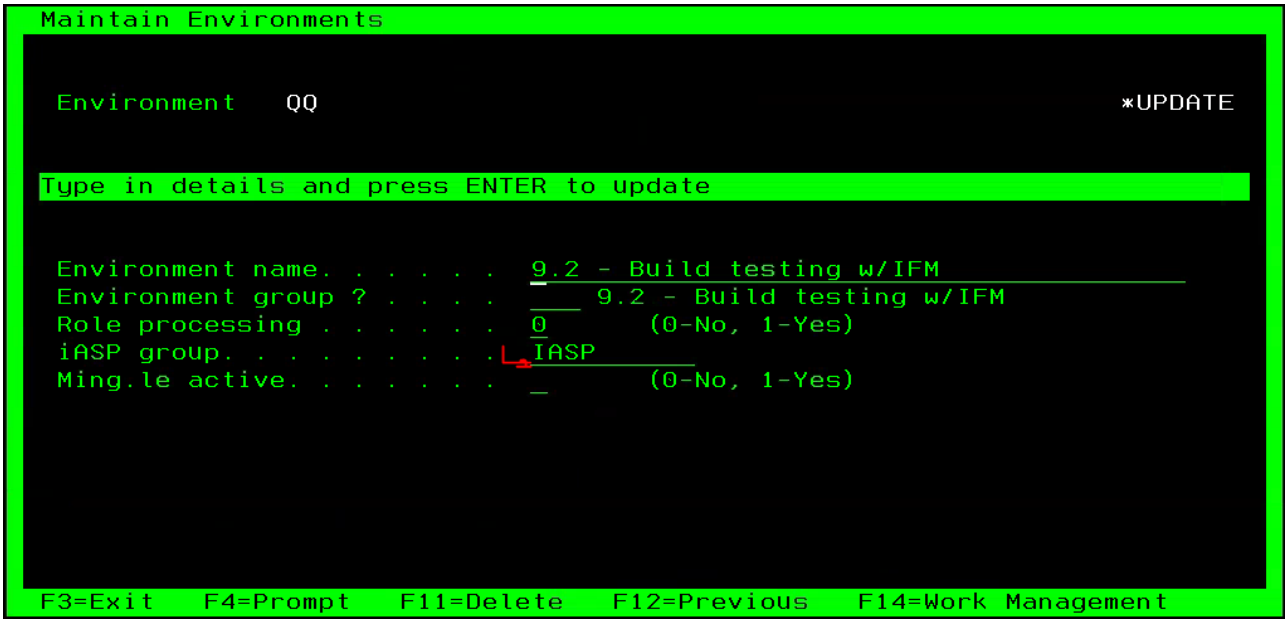
1 Specify STRM400 on the AS400 screen to start the System Manager.

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

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

Refer "***Net-Link WAR file deployment***", "***WAR file generation***", "***Tomcat (version 7.0 +) section*** **in "*WAR file deployment***" and "***Workspace Net-Link URL configuration***" sections in the ***Infor XA Setup Guide for Secure Net-Link*** *Guide* to set up a secured Net-Link in System i Workspace AnyWhere.

IBMi deployment

The “**Infor XA Setup Guide for Secure Net-Link**” document describes the process to set up a secure Net-Link and configuring SSL for a IBMi deployment(WebSphere).

Refer “***Net-Link WAR file deployment***”, “***WAR file generation***”, “***WebSphere (version 9.x) section* in “*WAR file deployment***”, “***Configure SSL***” and “***Workspace Net-Link URL configuration***” sections in the ***Infor XA Setup Guide for Secure Net-Link*** Guide to set up a secured Net-Link in System i Workspace AnyWhere.

Client Settings

This section explains about the client settings that needs to be configured on each client PC that accesses the System i Workspace AnyWhere. Follow the procedure described in the 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. Currently, the Tenant is used, which is associated with each Infor OS 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 latest.

Exporting metadata from IDF to Workspace

After installations, 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:

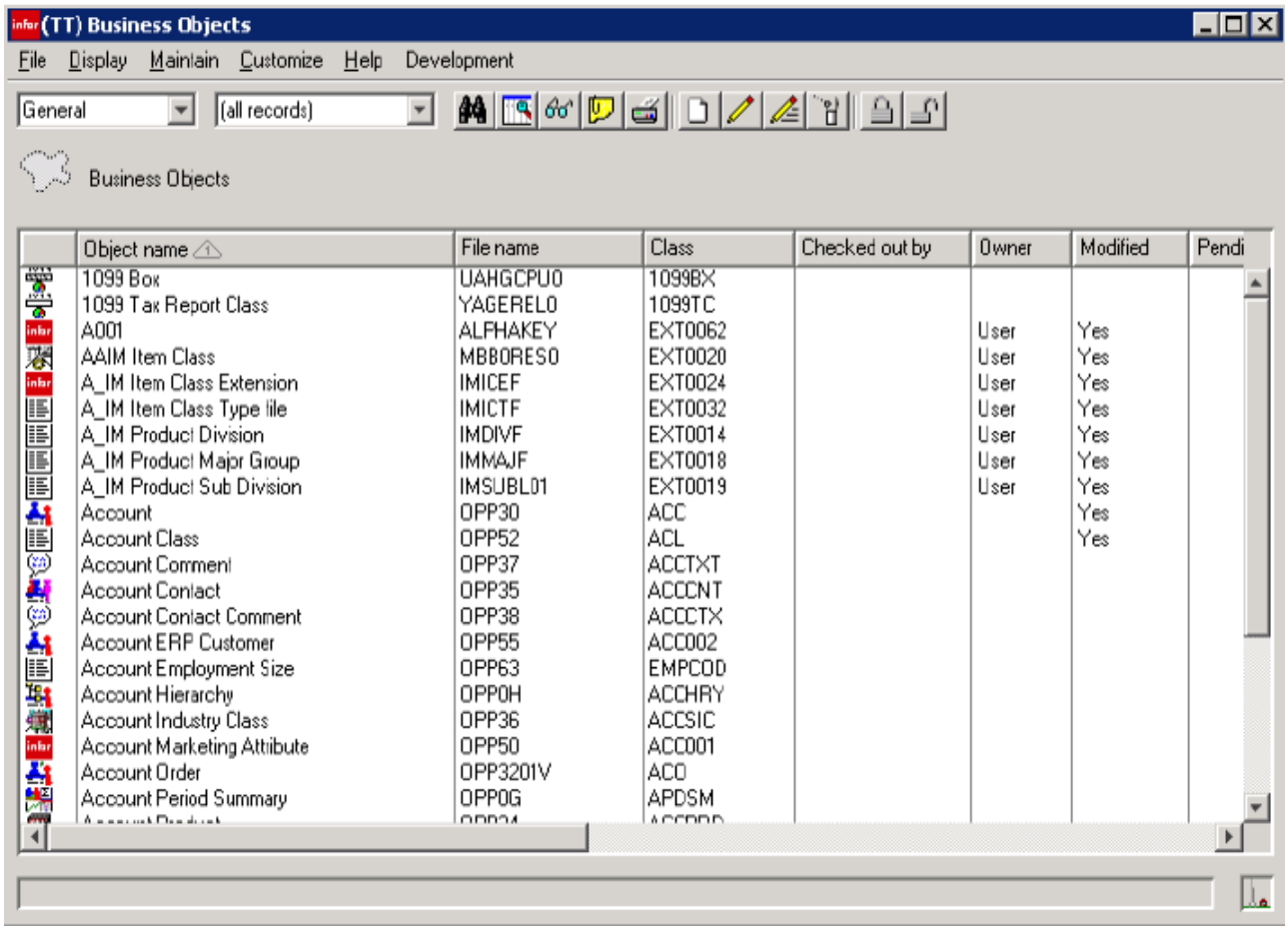
- Business Objects object on the Integrator card
- User Profiles object on the Integrator card
- User Profiles object on the Environment card.

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 Power-Link.

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



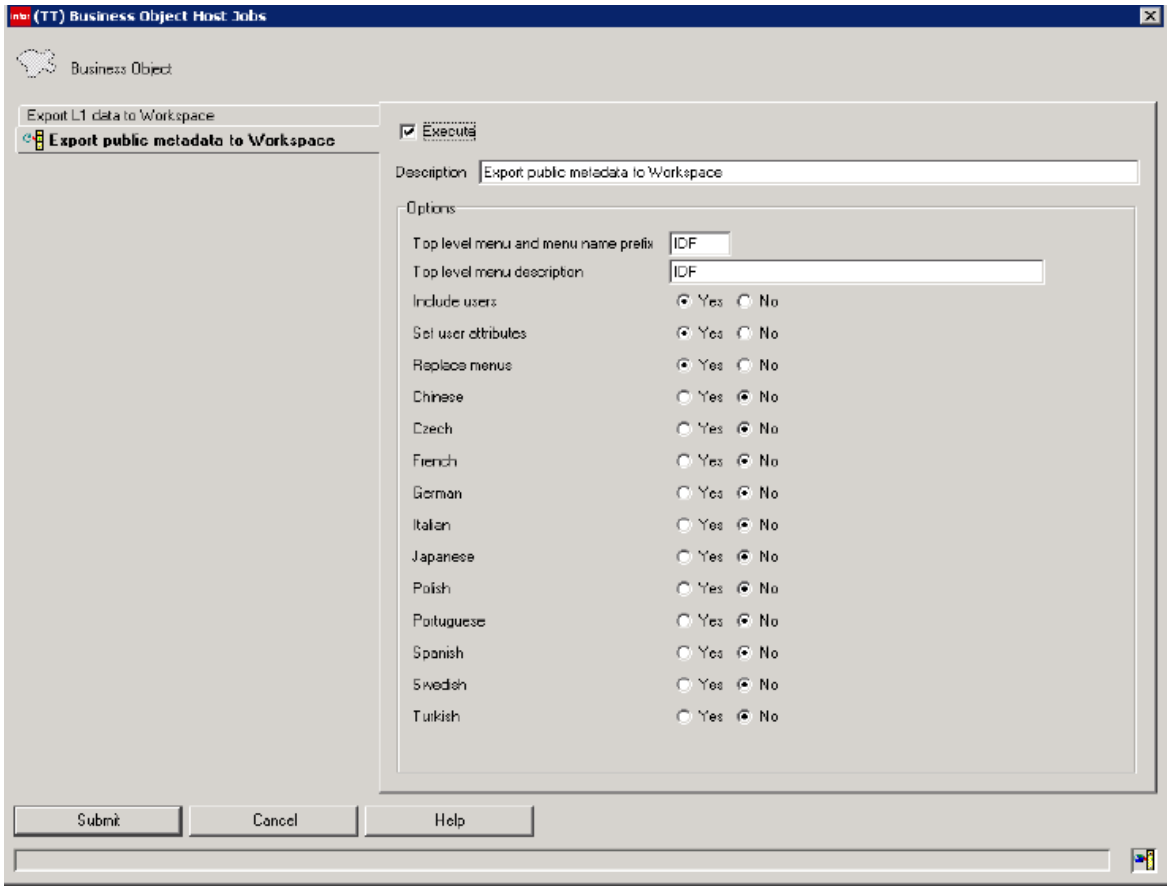
1 Select **File** > **Host** Jobs**.**

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**.**

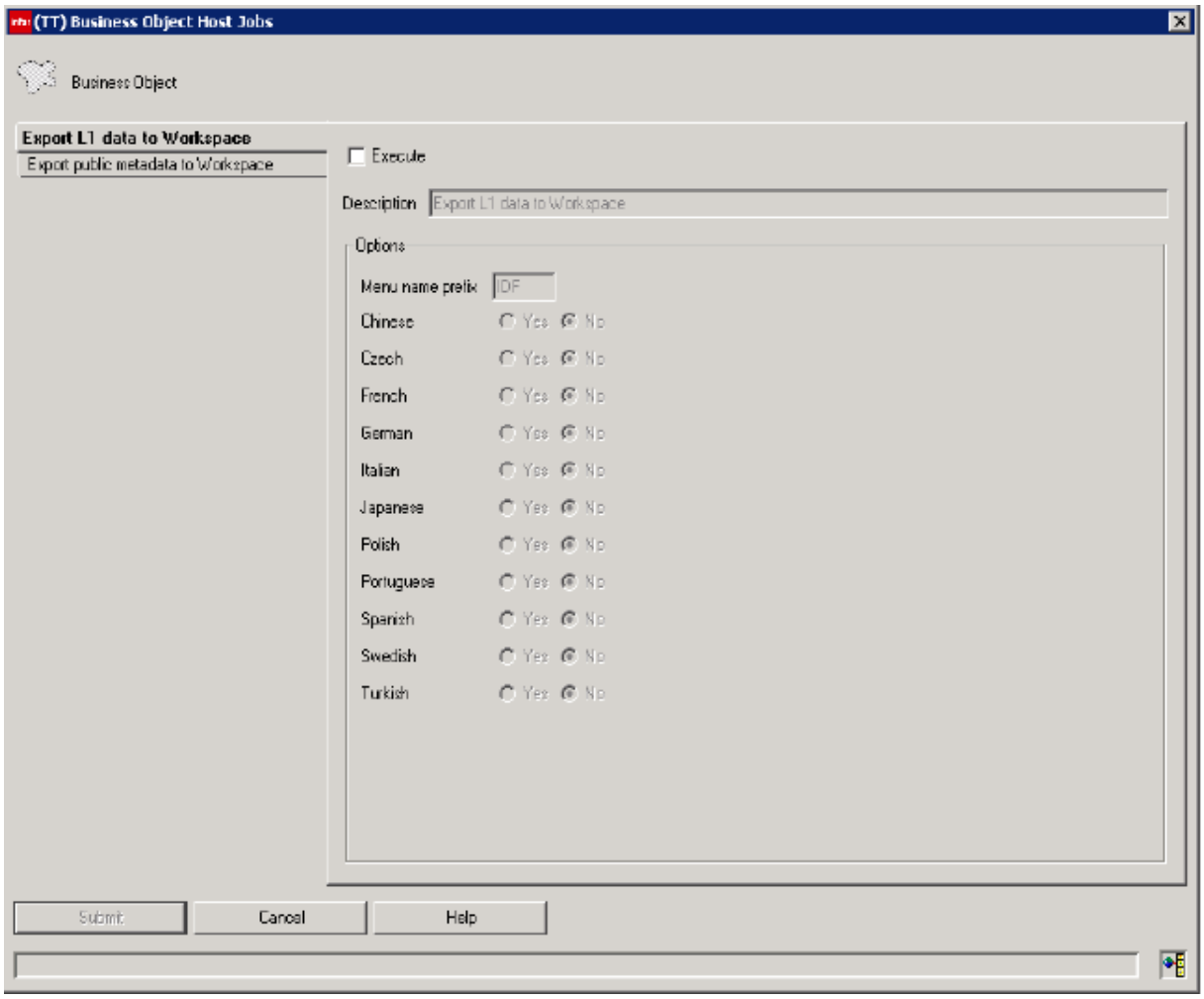
2 Navigate to the **Business Objects** object on the Integrator card.

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

Updating Workspace Application Manager in SIW

After the completion of Export metadata, the users must update the Workspace Application manager to update the definitions in SiW.

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

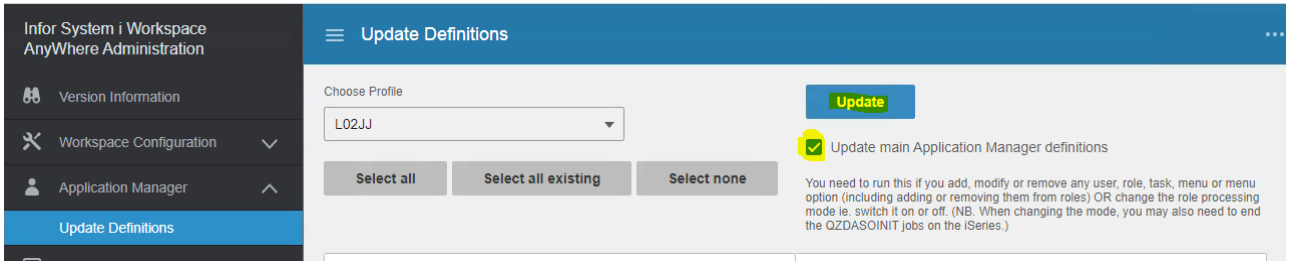
1 Open the utility by specifying this URL for SiW Anywhere:

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.

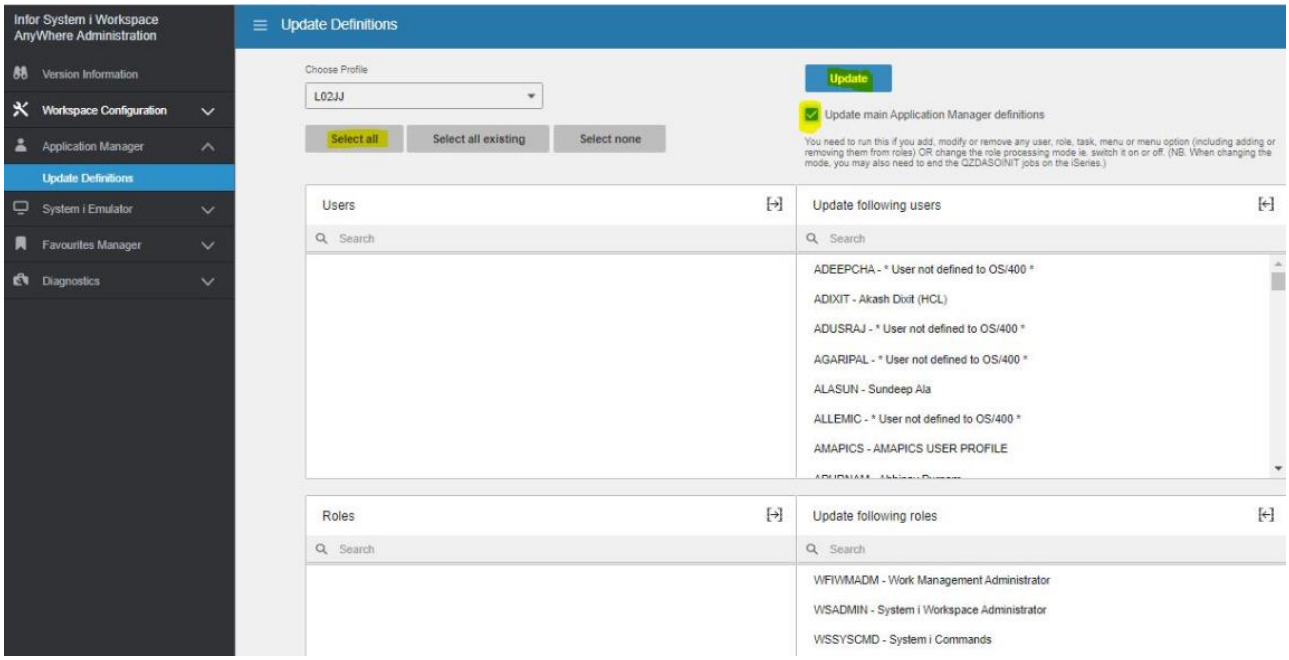
4 If you are performing this process for the first time after environment setup or after metadata export, then select **Update main Application Manager definitions** and click **Update**.



1 Click **Select all** to select all users/roles or select a specific user.

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

3 Select **Update**.



Note: Refer the" Application/*System Manager Synchronisation* " section in the Chapter "*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

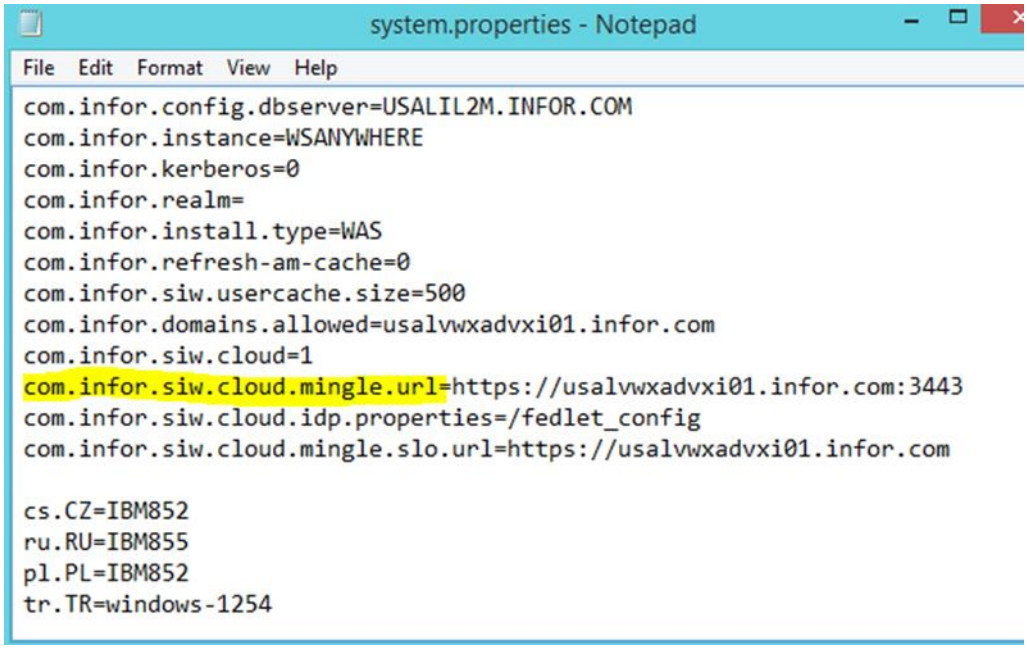
1 Locate the System i Workspace **system.properties** file (as documented in the System i Workspace AnyWhere Installation Guide).

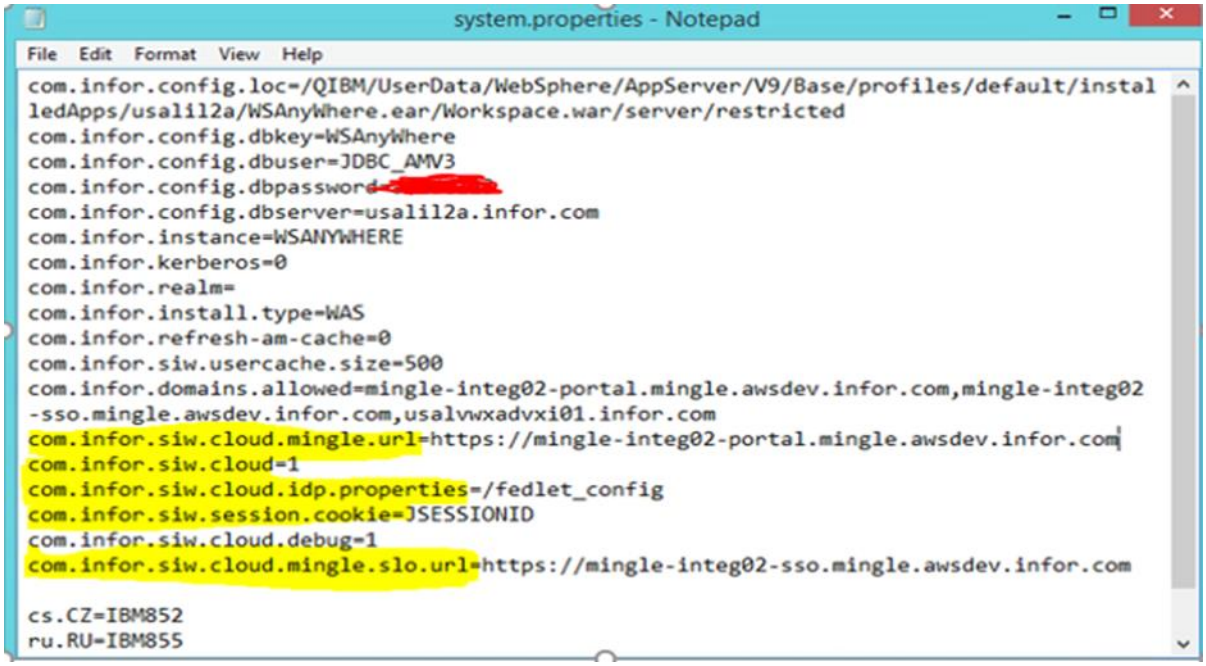
2 Add this property to enable System i Workspace AnyWhere to be launched from Infor OS:

Property	Description
com.infor.siw.cloud.mingle.url	The URL, minus any context path, of the Infor OS 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. For example: https://mingle.your-enterprise.com

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

Note: If the Infor OS uses port as well in URL while launching, then you must add the port number also in the previous example:
https://mingle.your-enterprise.com:XXX





Configuring Single Log Out

Note: If using SiWA FP 14 or above below settings are discontinued hence not be available for customers.

The Single Log Out (SLO) behavior is set via the System i Workspace AnyWhere Administration UI (admin.html), **Workspace Configuration > Profiles**, using the **Single Log Out Behavior** field found in the section **InforOS Platform Integration Settings**:

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

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 MT CE**. To get around this issue we must enable the Same Site Cookie flag which alters how the browse treats these cookies.

Windows SiWA Deployment:

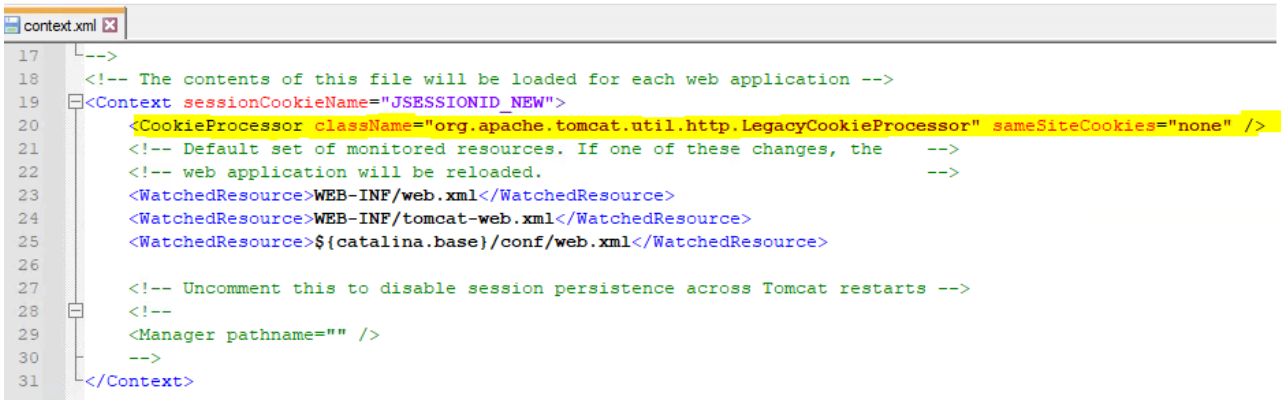
1 Edit file ***conext.xml*** which can be located in the ***tomcat\conf*** folder:

(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

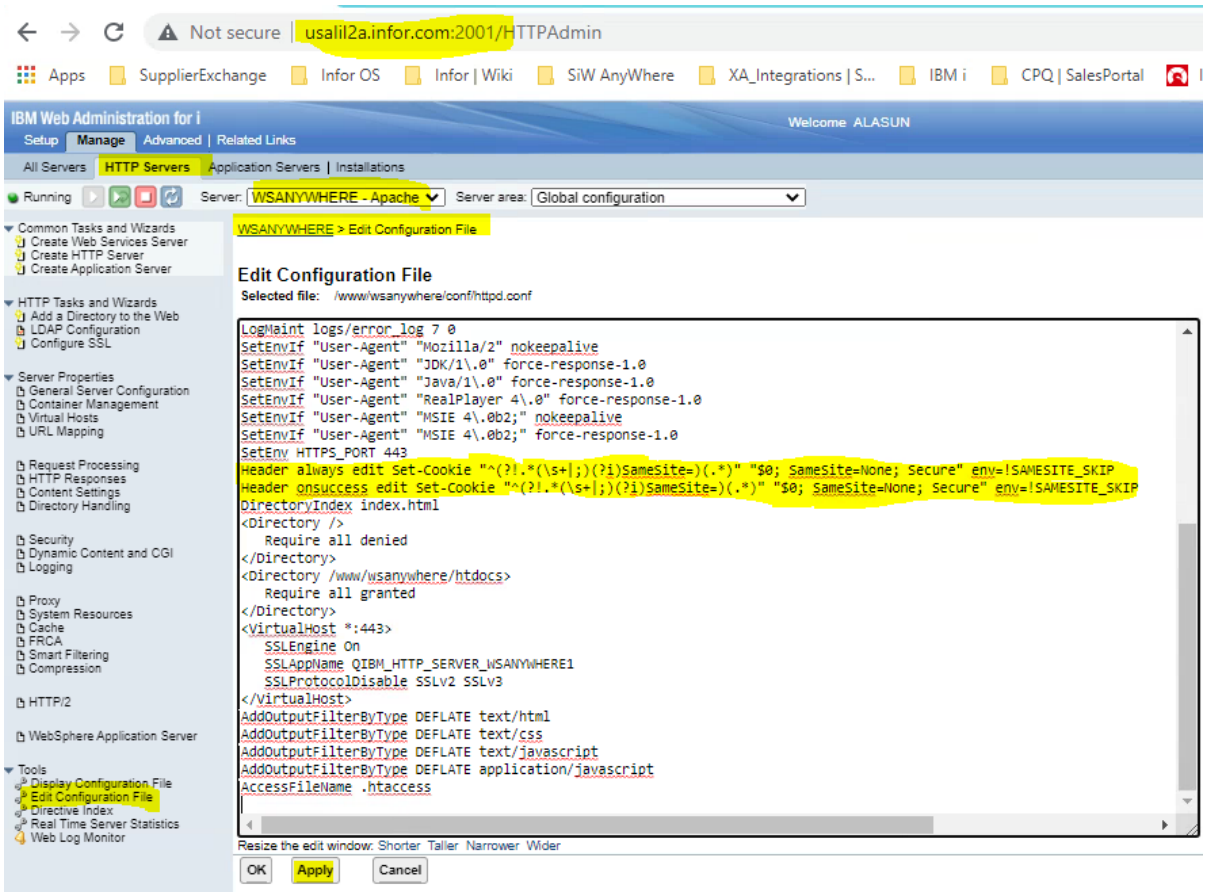
(for example: http://usalil2a.infor.com:2001/HTTPAdmin)

2 Navigate to your SiWAnyWhere installed HTTP Instance and select Edit Configuration File

3 Add the following lines as shown below:

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



4 Click on **Apply** and then click **OK**.

5 Restart the HTTP Instance and its associated Application instances. (for example: HTTP instance ***WSSANYWHERE*** and its associated Application instances ***default/server1*** and ***default/WSAnyWhere***)

Note:

Same Site Cookie configuration need to be implemented in Net-Link related HTTP instance Configuration File as well along with SiWAnyWhere HTTP instance, if both are running on different ports on WebSphere.

As an alternate below changes can also be implemented to handle this issue.

Follow the "***Appendix D Configuring SiWA IBMI WAS with single port***" from ***Infor XA Infor XA Setup Guide for Secure Net-Link*** guide to run both SiWA and Net-Link applications from same port and Same Site Cookie configuration done on SiWA HTTP instance will be enough to handle this.

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 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 "***System i Workspace additional configuration****"* in the ***System i Workspace AnyWhere Installation & Administration Guide***.

Chapter 7 Configuring XA in Infor OS MT CE

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

As mentioned in "**Post installation**" chapter, 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 application. For example, you can have an XA test environment and an XA production environment, each with their own Application tab.

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

You can use the Infor OS environment to access the IDF views and screens. Users can access the Net-Link 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 Ming.le uses Infor ION terminology. If you have installed Infor ION and configured ION to work with XA, use the same values that you used in that installation. If you are configuring Infor Ming.le but have not yet implemented Infor ION, note the values that you use and then use these same values when you install Infor ION.

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

- **Tenant**

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

  The accounting entity is the lowest level for financial reporting. In an XA implementation, a Financial Divisions, Companies, Sites, and Warehouses are Accounting entities. Accounting Entities are defined as 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 by using Admin Settings option in Ming.le.

After configuring XA in Ming.le, 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 MT CE

To configure for Infor OS MT CE (Cloud Edition):

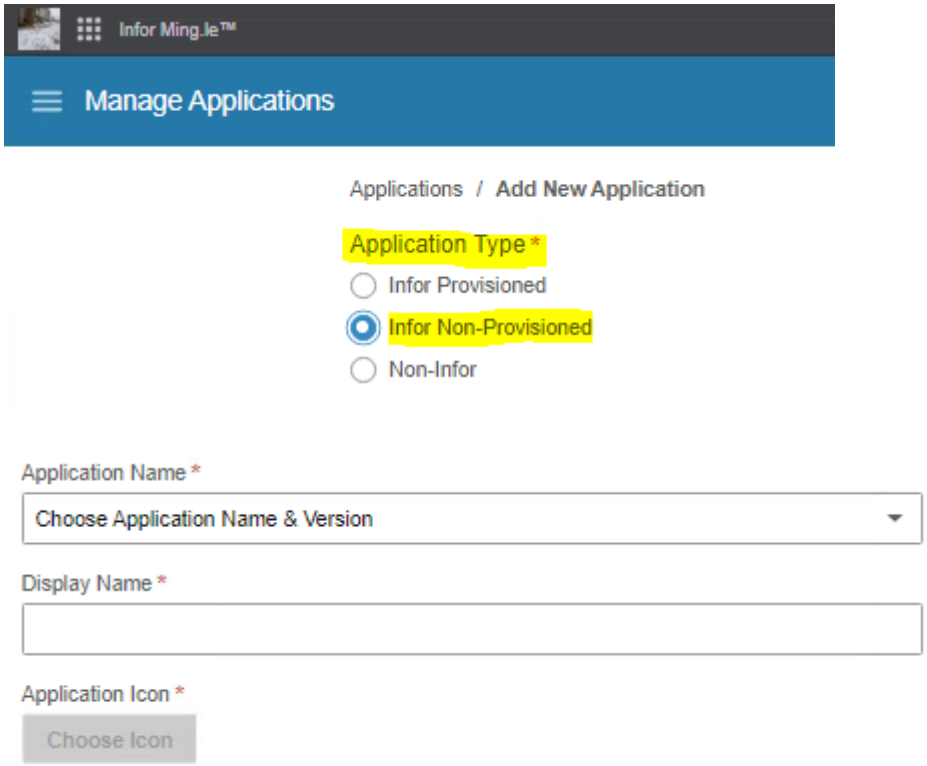
1 Login to Infor OS MT CE using the account setup for IFS administration.

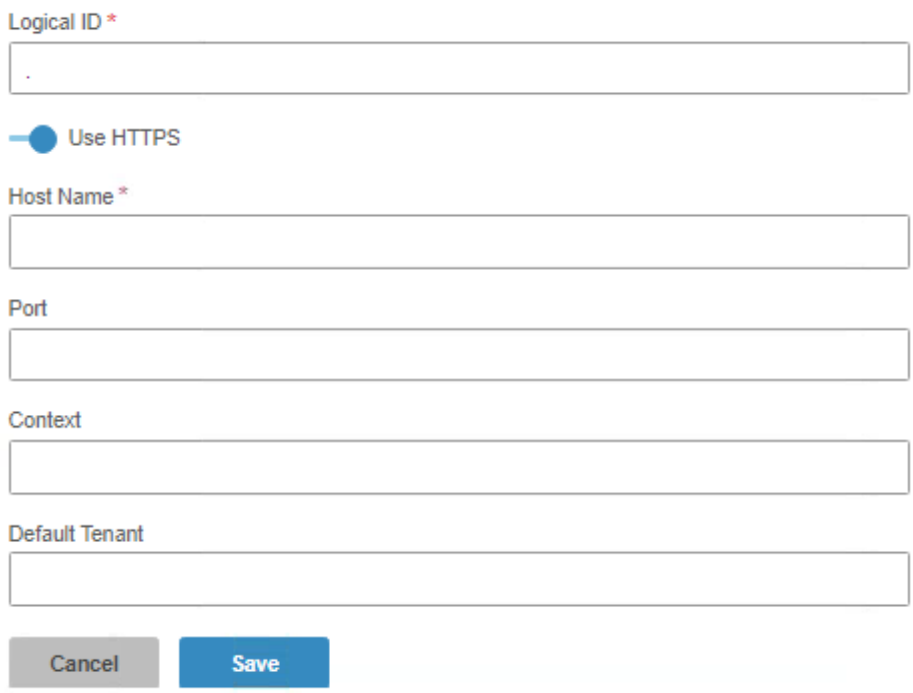
2 Click the **User** option located in the top-right hand corner and then select **Admin Settings**.

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

4 Select the Application type as **Infor Non-provisioned** and Application Name for an example as **ERP Discrete iEnterprise (XA) – 9.2**

5 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 XA 10** 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**.
Host Name	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**.
Default Tenant	Specify the profile name defined within System i Workspace. It is recommended that this is set to the XA Profile ID, which is case sensitive.

1 Click **Save** and Click **OK**.

2 Select the **Permissions** tab.

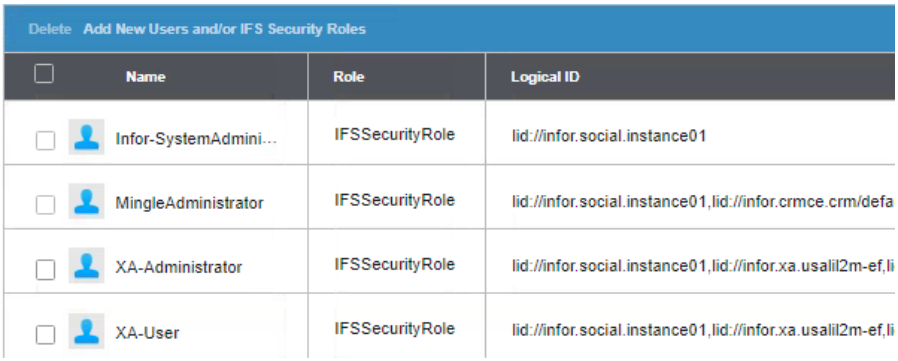
Click **Add New Users and/or IFS Security Roles**.

3 Otherwise, refer "***Create a new application security role***" in this Chapter. Search and select the role created.

4 Click **Done**.

5 Click **Save**.

6 Click **OK**.

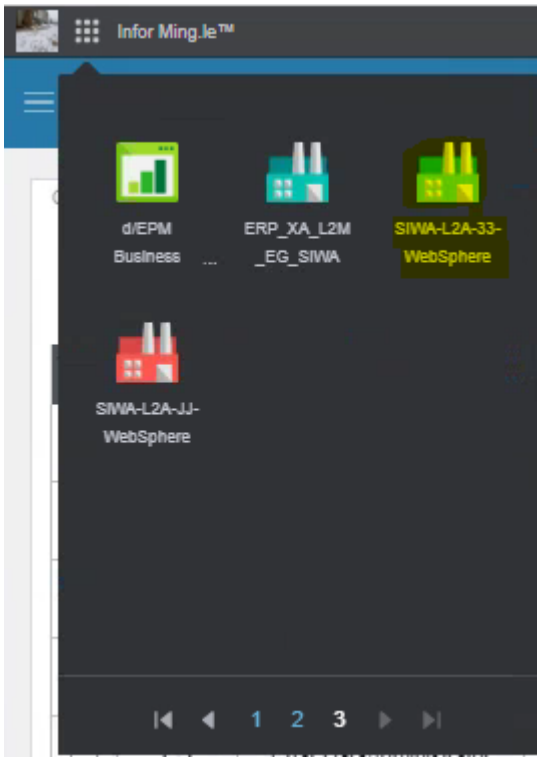


7 Click **Cancel** to **exit**.

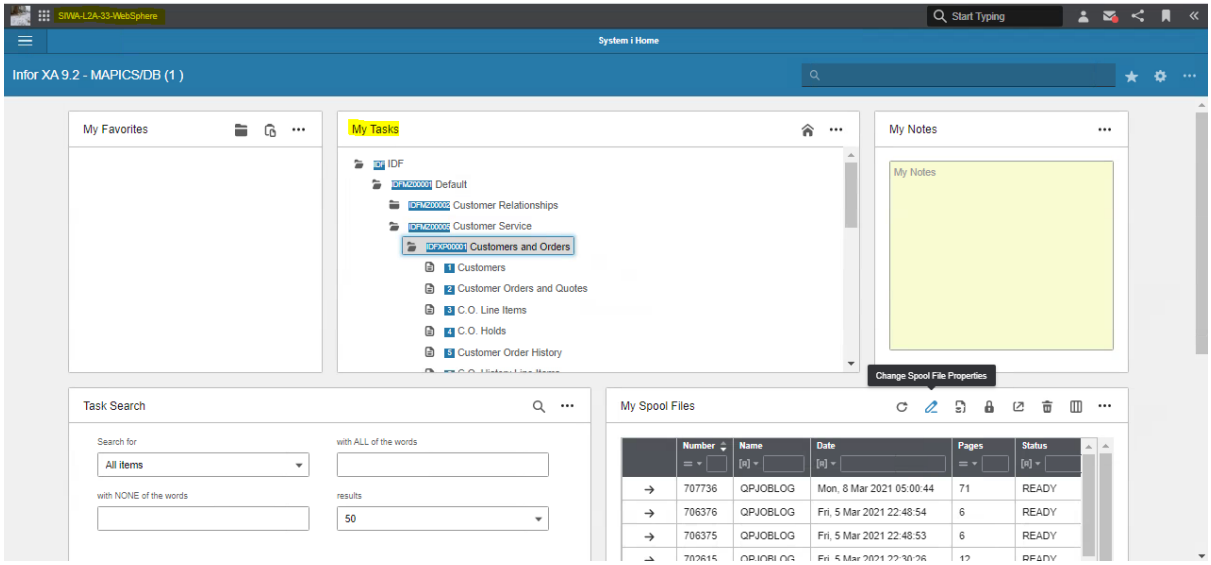
For enabling Manage Context/Utility App, refer **Chapter 9** ***Drillback Configuration*** in this guide. For adding the tab on screen, add the group/users to permissions in Admin settings of Manage Context/Utility Apps.

Launch XA in Infor OS MT CE

1 Go to "App Menu" and click the configured XA application icon.



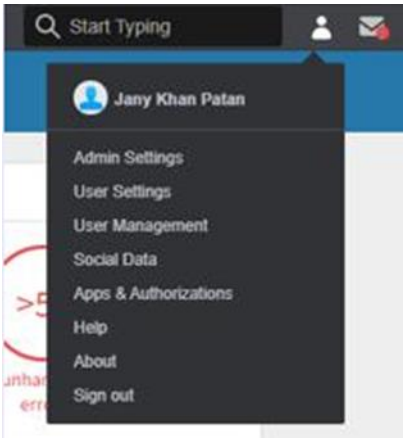
2 XA application is launched with menu and other details to access.



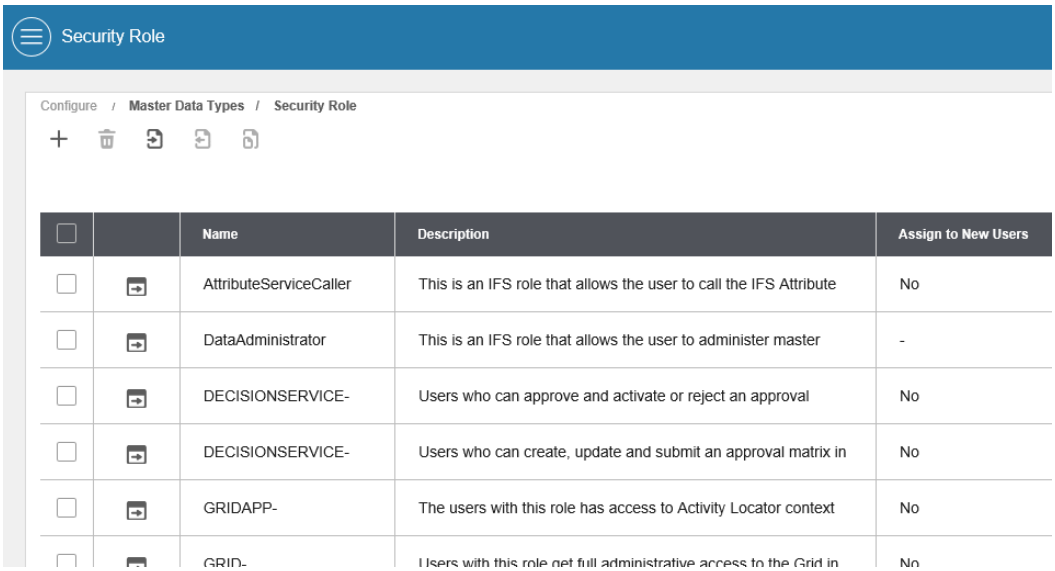
Create a new application security role

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

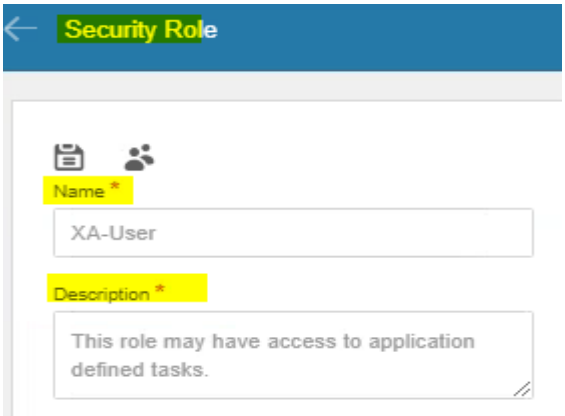
2 Click the **User** option in the top-right corner and select **User Management**.



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



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



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

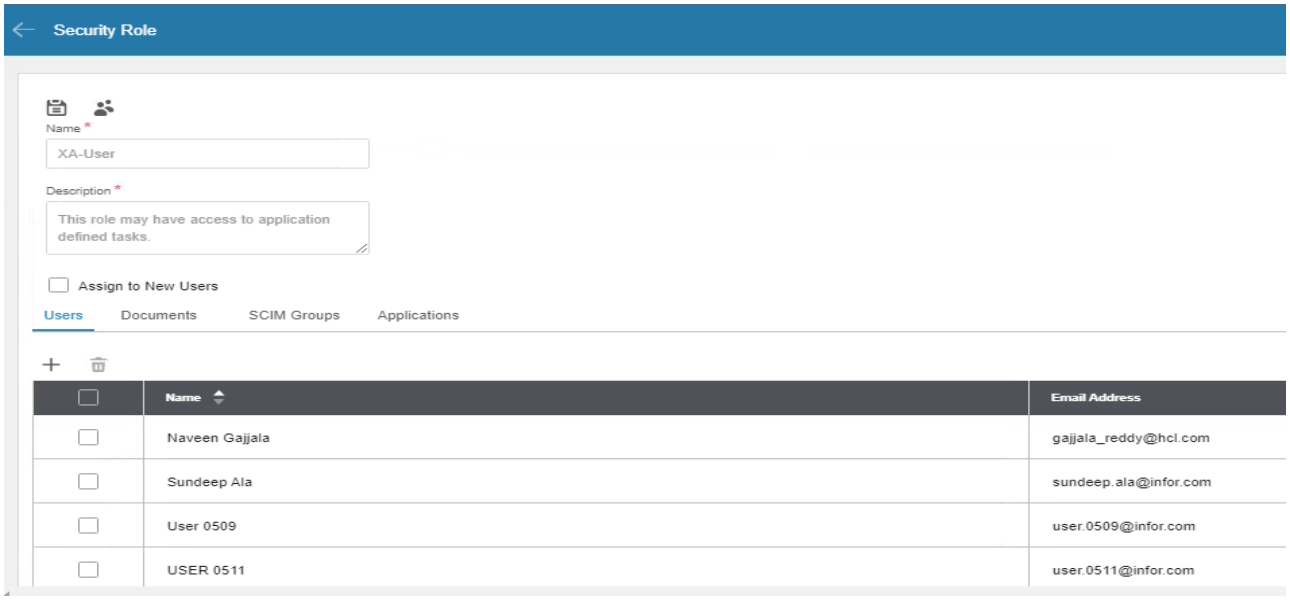
6 Check the **Assign to New Users** field so that, in future, any new users that you add to Infor OS can automatically get access to this new Security Role.

7 Click the **+** option to add users to the Security Role. If you have not yet added any users, then refer Chapter 11 - *Adding users* for adding users into Infor OS.

8 Specify the username you want to add to the Security Role in the Search for Users prompt 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.

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 On-Premise, with Infor OS MT CE.

Note: SiWA should be running on FP 13 (minimum) and latest Infor OS for SSO with Infor OS MT CE 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 MT CE** using ***SAML SSO.***

b System i Workspace AnyWhere with Windows deployment (Tomcat) on **Infor OS MT CE** 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.3
- Infor XA IDF 9.2.2 client software build must be 02.09.02.02.30 or later.

- Infor XA IDF 9.2.2 server PTFs is PCM SH16055 (XA 9.2.2 with PTF level 025000).
- Infor XA IDF 10.0 client software build must be 03.10.00.01.03 or later
- Infor XA IDF 10.0 server PTFs is PCM SH16231 (XA 10.0 with PTF level 00100).
- System i Workspace AnyWhere (with latest Feature/Fix Packs applied – at least FP13)
- Infor OS MT CE

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 a Infor OS MT CE (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 MT CE

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 and are currently integrated with PingFederate using the SAML/WS-FED and OPENID protocols, are required to transition from PingFederate to InforSTS.

Note: PingFederate in Infor OS MT will be deprecated at the end of **Oct 2023.**

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

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 (*KB 1963350*).

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

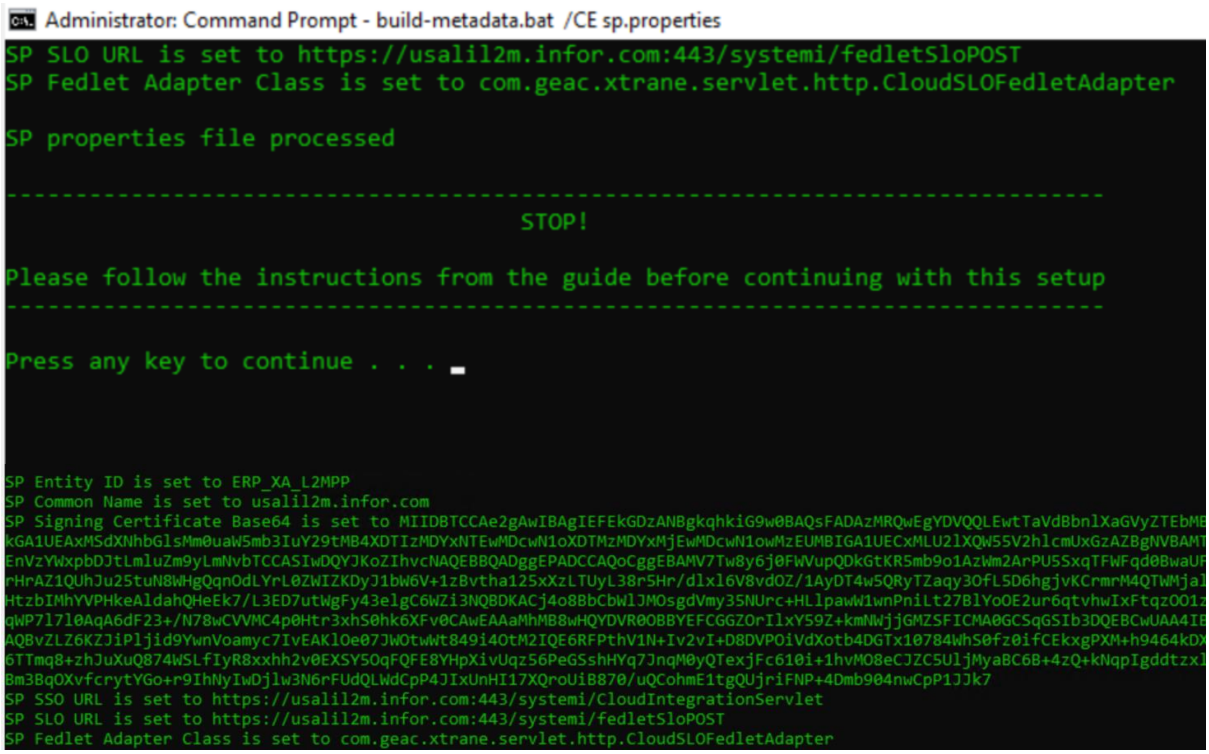
Creating the identity provider and fedlet metadata

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

build-metadata.bat /CE sp.properties

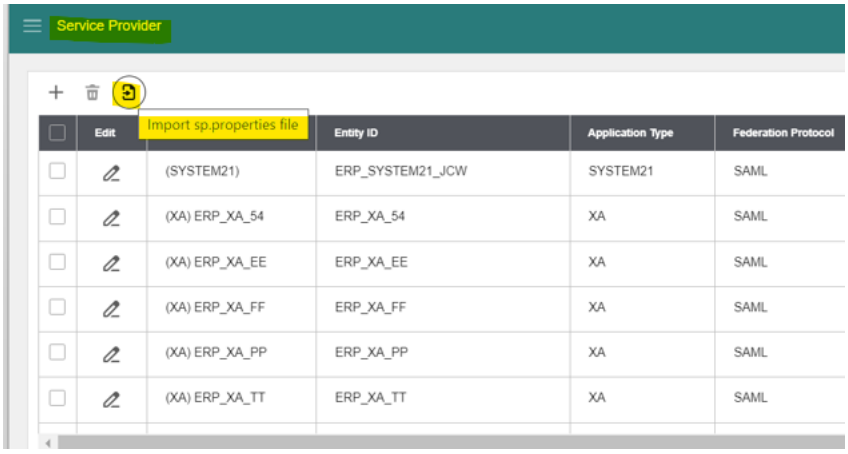
2 This creates a populated set of Fedlet Metadata in the folder ***fedlet_config*** at the end of the process.

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

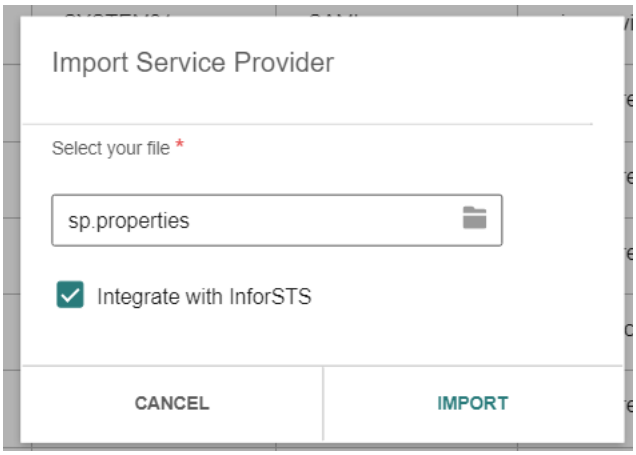


a. Log into InforOS using the account setup for IFS administration authority.

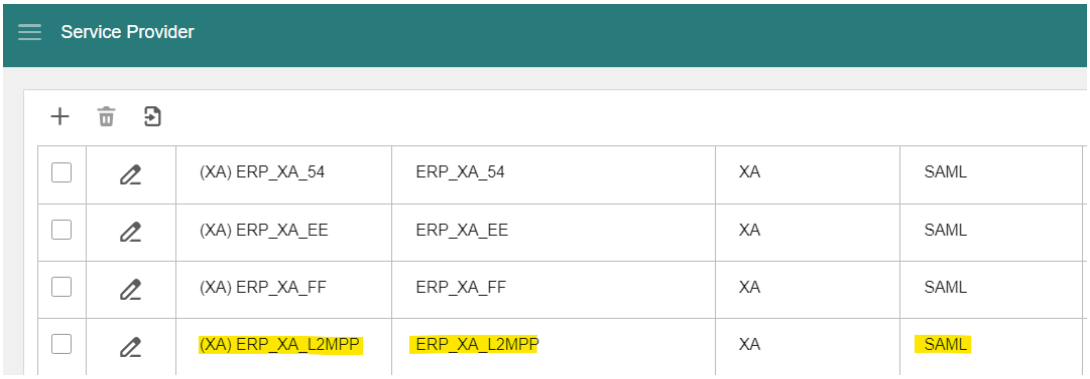
b. Click on the **User Icon** and then select ***User Management > Security Administration > Service Provider,*** click on ***Import Icon*** as shown below.



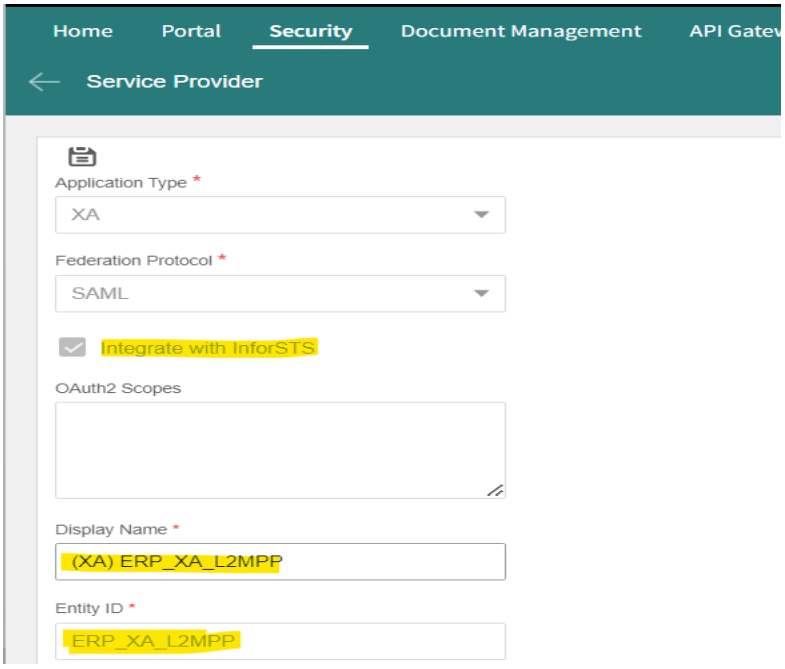
c. Select the file ***sp.properties*** from the populated folder ***fedlet_config,*** check the "***Integrate with InforSTS***" check box and Click ***Import.***

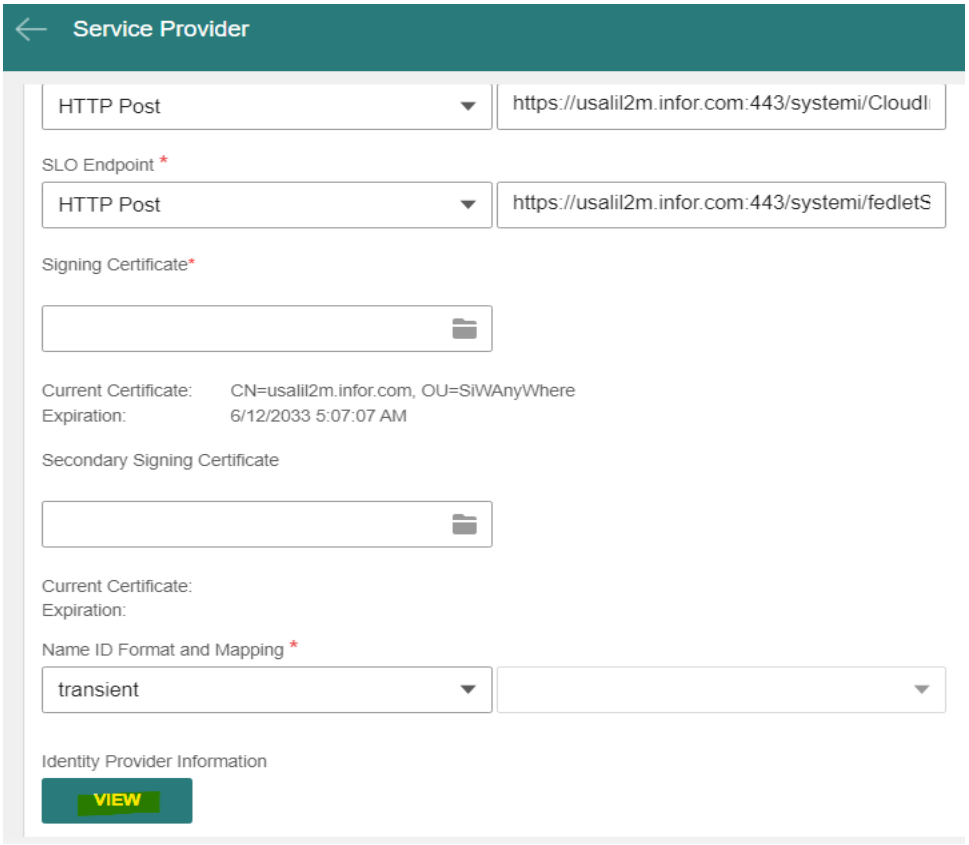


d. SP Entry is added successfully. Click on Edit, shown as below.

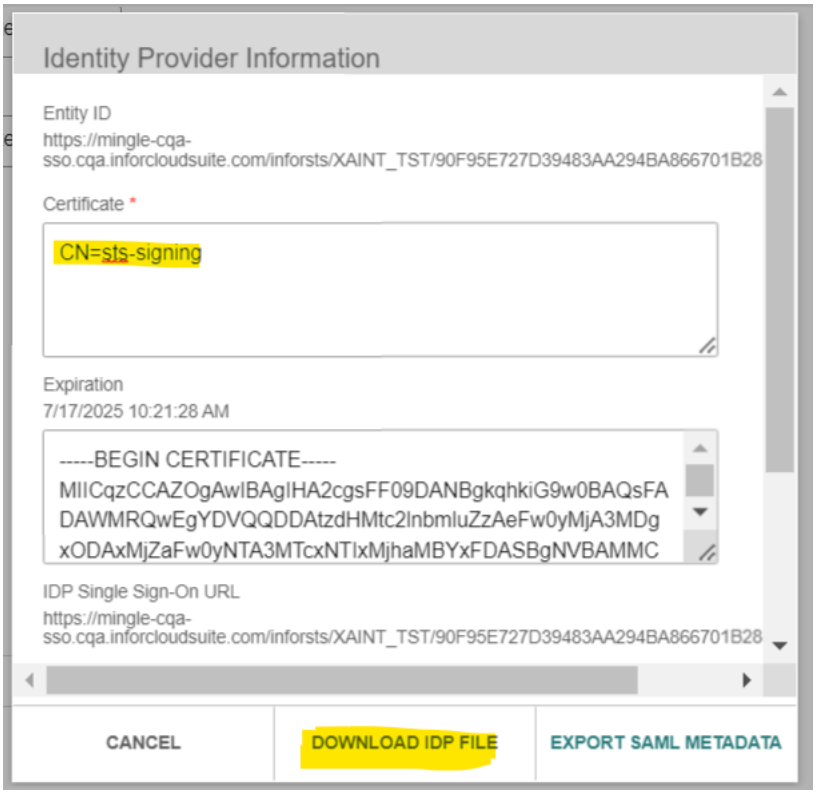


e. Scroll to the bottom and click on VIEW.



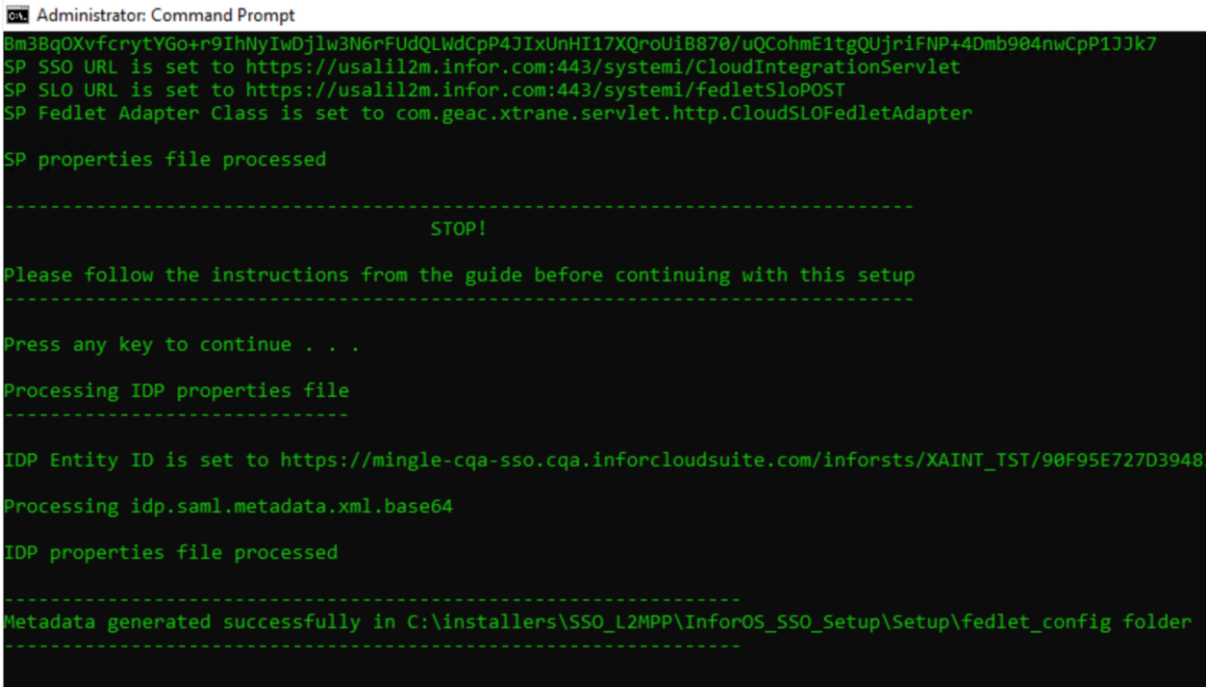


f. The Identity provider information pop-up is displayed with the details. Click the **Download IDP File** option as displayed.



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

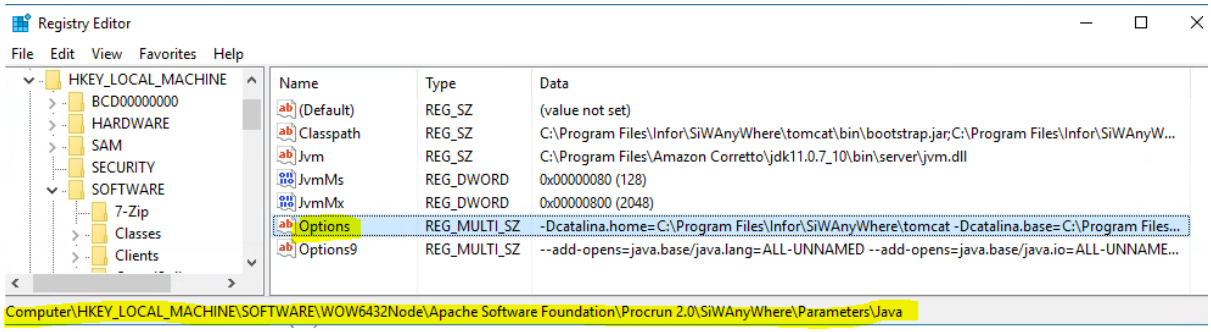
- An additional Java runtime property is required for the Web Server to identify the location of the SAML2 metadata folder created during the previous steps, For example,

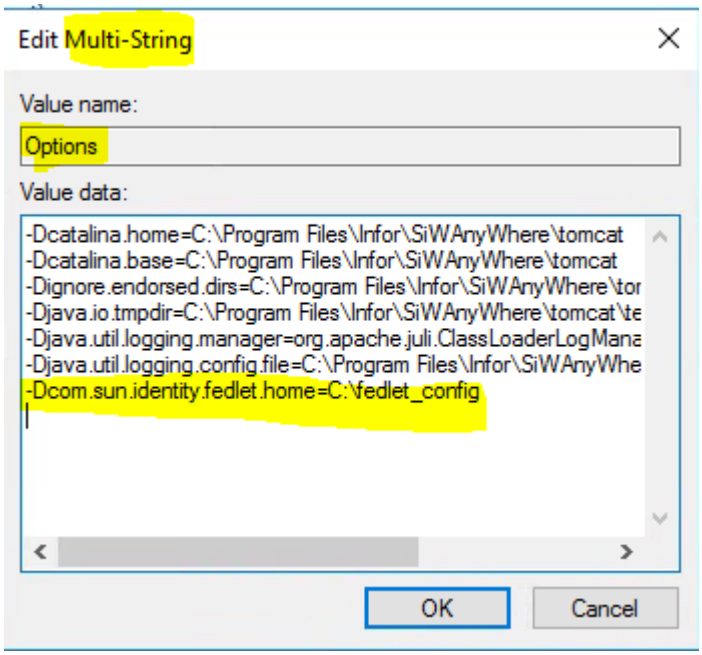
-Dcom.sun.identity.fedlet.home=<Path to SAML2 metadata folder>

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



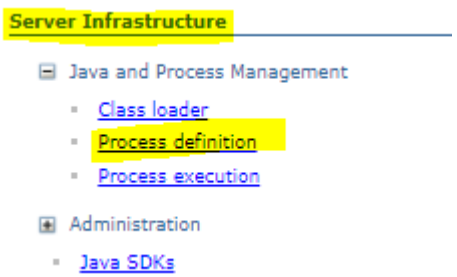


IBMi Deployment

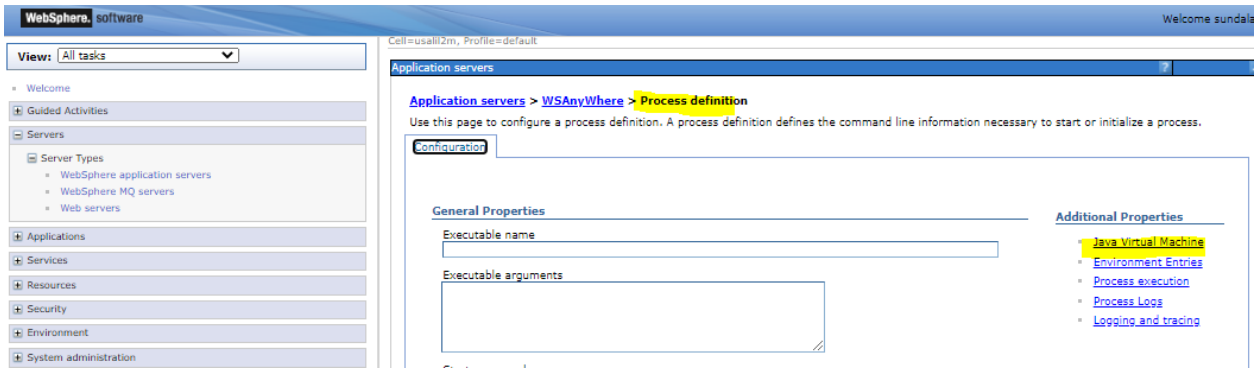
1 Use the IBM WebSphere Administrative Console to make configuration changes. From the menus on the left-hand side, select ***Servers -> Server Types -> WebSphere Application Servers.***

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.

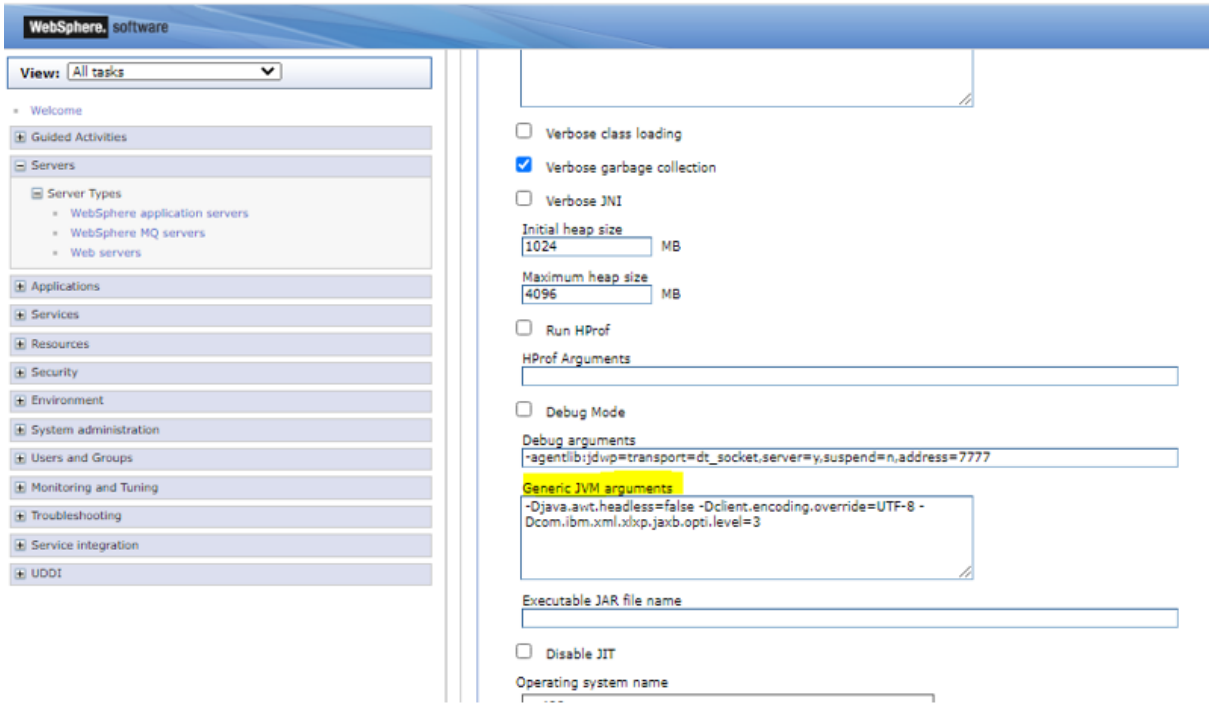
3 Select **Process definition.**



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



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



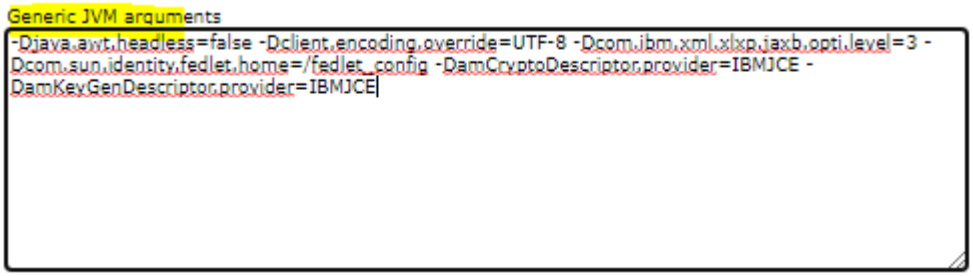
6 At the end of the existing arguments, type a space followed by the setting pointing to the path to your fedlet_config folder.

-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

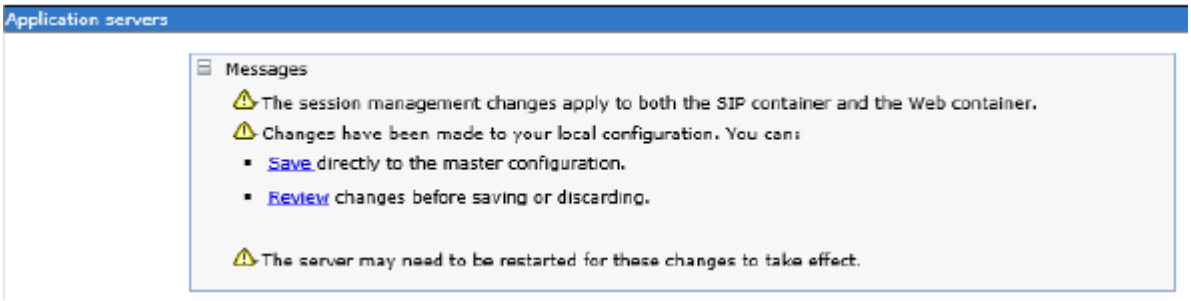


8 Click Apply and then, click Save.

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 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 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 MT CE. 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 MT CE. 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.

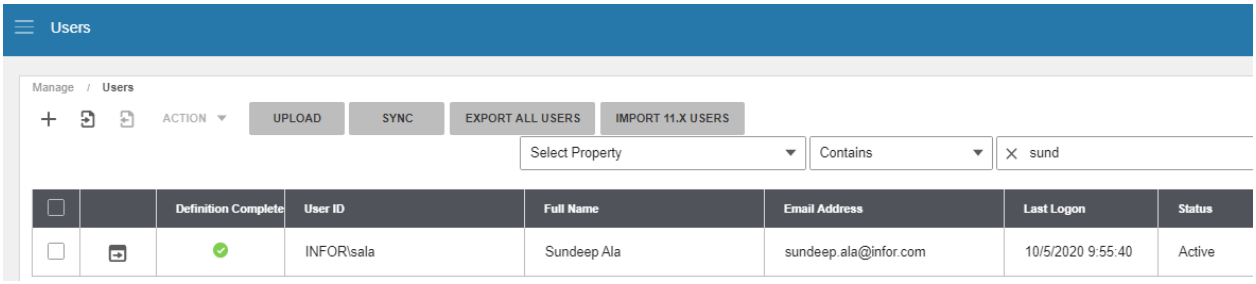
Caution: End of the SAML SSO implementation for InforOS CE MT.

Configuring XA User IDs in Infor OS MT CE for SSO Support

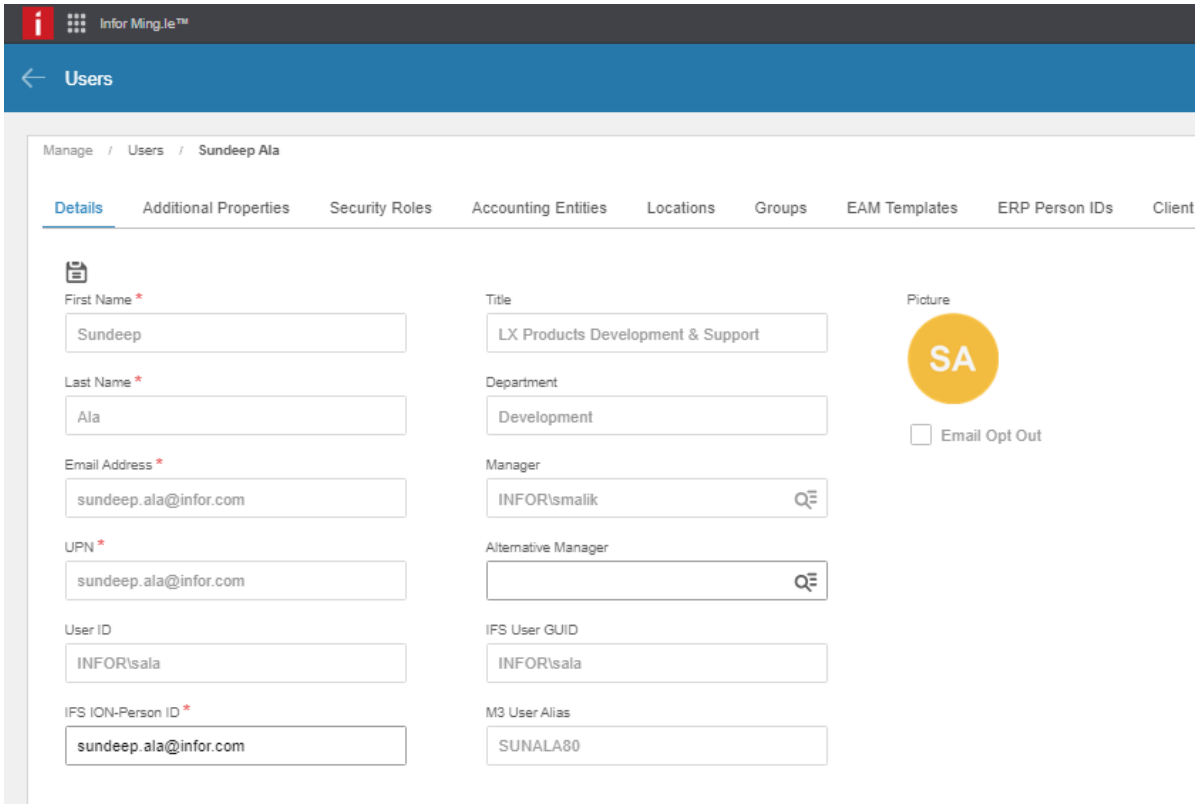
Caution: This step is not required if you are using automated user-provisioning functionality mentioned in Chapter 9 User Provisioning Implementation.

Each user that needs access to System i Workspace AnyWhere must be configured to add a mapping from the Infor OS platform to their ERP User (i.e. their IBMi user account). This is done via the User Management interface. This setup same for both Infor OS On-premise and Cloud.

1 Log into Infor OS and select **User Management** from the User menu.

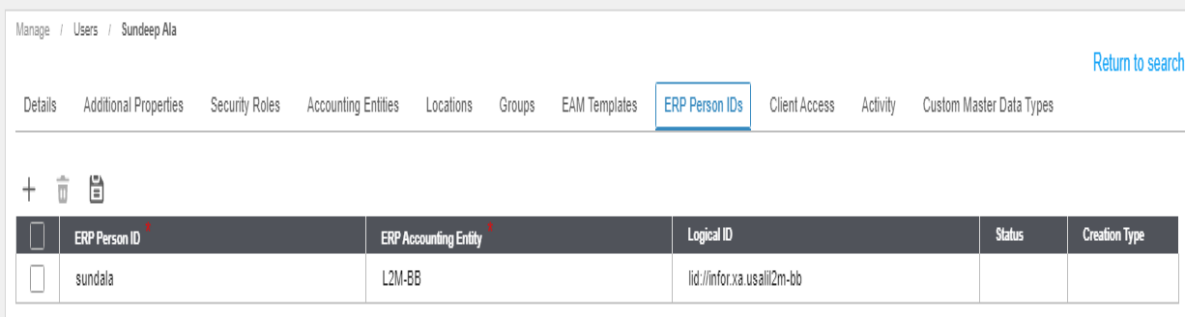


2 Use the table navigation or search to locate each user profile that needs changing. Click the drilldown option next to the username in the grid to display their properties.



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 sundeep.ala@infor.com logs in to Infor OS and accesses the Infor IBMi based application that runs inside System i Workspace AnyWhere, the IBMi profile ID of SUNDALA 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 MT CE.

Infor OS MT CE should on 2021-07 or later to 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 02.09.02.02.33 and XA 10 client should be on 03.10.00.01.06

SH69855 and SH71181 PTFs should be applied on 9.2.2.

SH69855 and SH71633 PTFs should be applied on 10.

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 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 MT CE via SSO.

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

Limitations

Current implementation has below limitations or considerations:

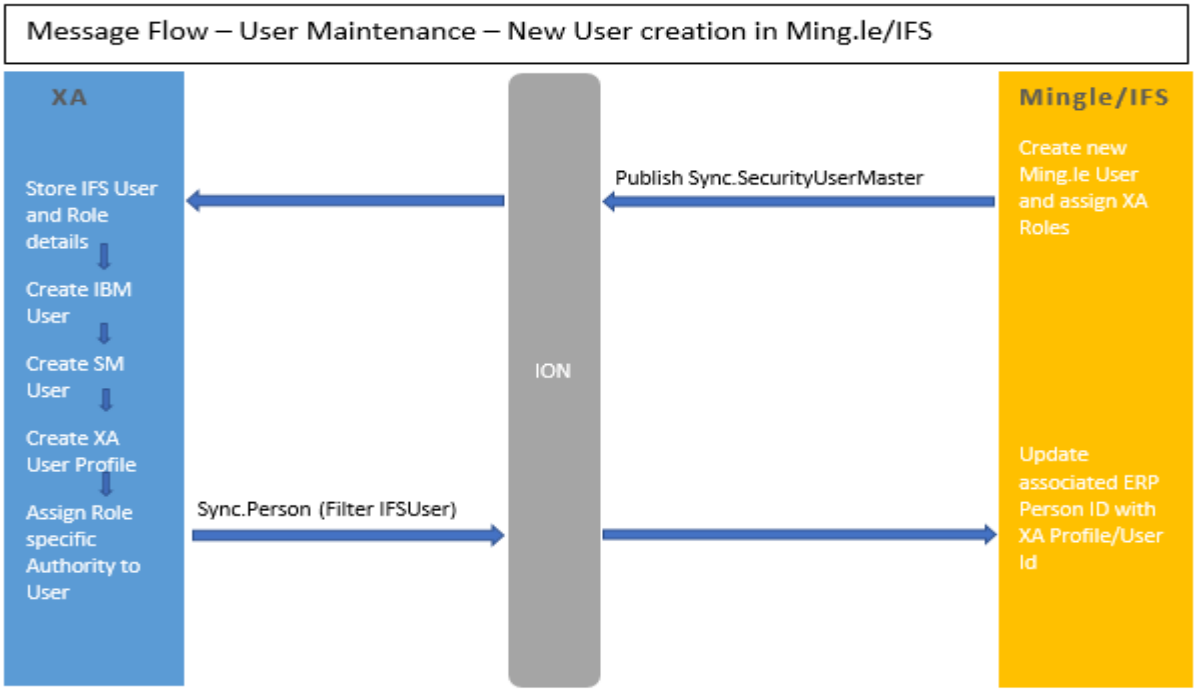
- XA environment is a one to one relationship to tenant on Infor OS.
- This solution is best suited or intended for customers with freshly installed XA and Infor OS MT applications and no existing users in both the applications.
- Creation of new users in XA does not trigger user creation in IFS. XA 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 MT with SSO) the admin need 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

1 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.

2 ION routes the Sync.SecurityUserMaster to the XA environment associated with the OS CE Tenant as per active ION Document flows.

3 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.

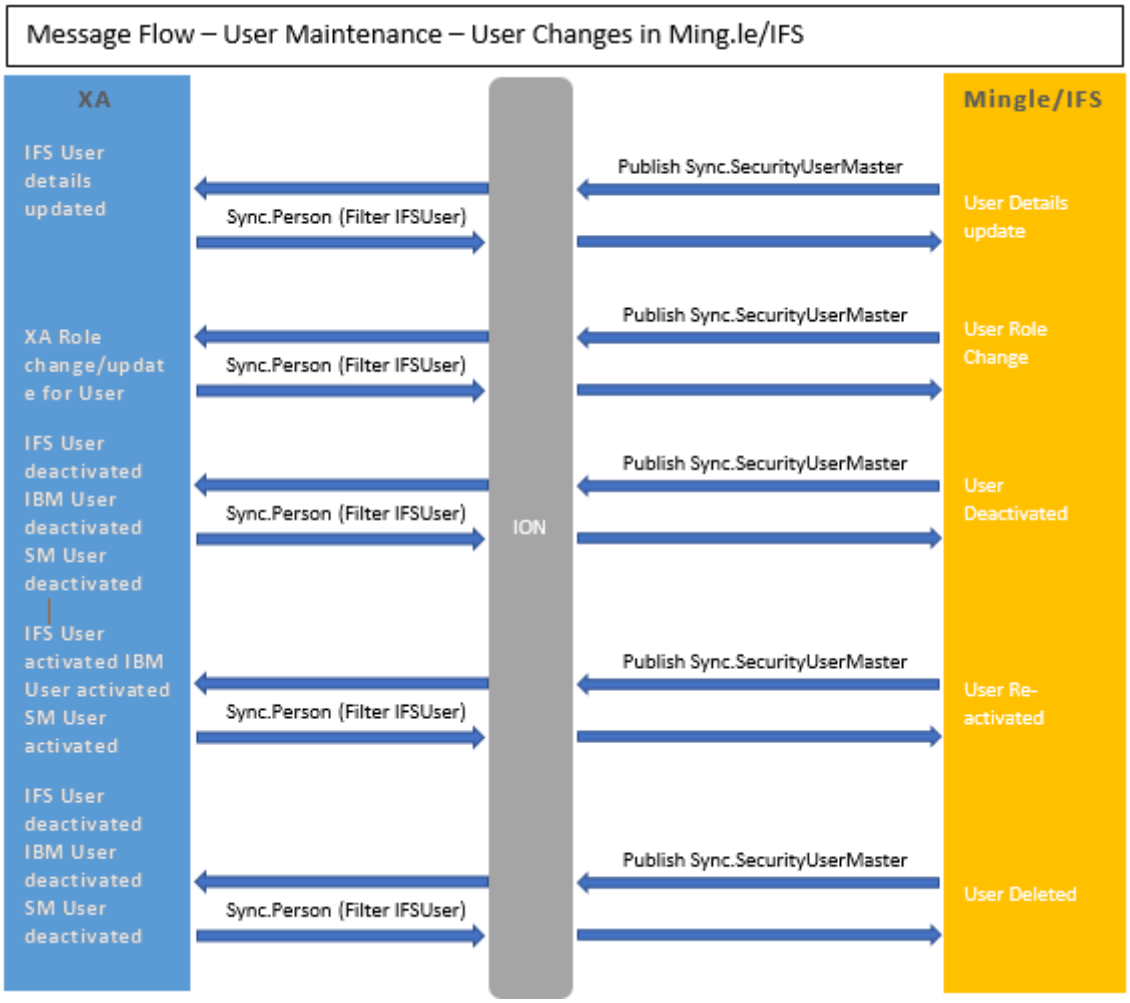
4 IBMi user is created automatically same as SM user. Same user is added into Cross Application Support -> XA User profiles in the current XA environment.

5 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.

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

User Changes in IFS



7 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.

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

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

10 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.

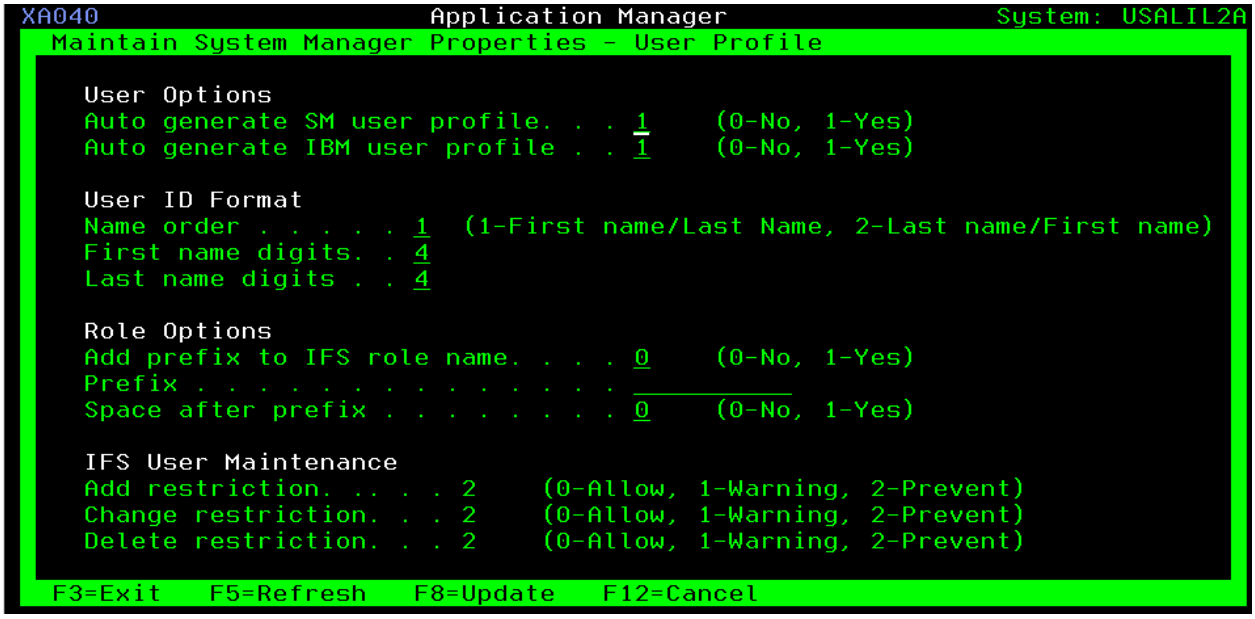
System i Manager Setup

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.

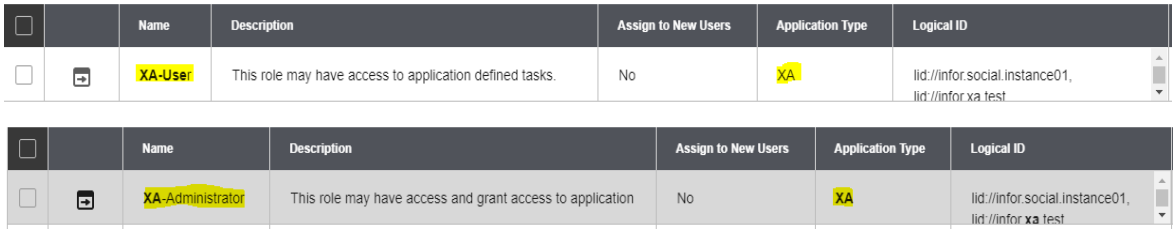
IFS user maintenance

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 MT CE should be running on 2021-07 (minimum) to 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 explain 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

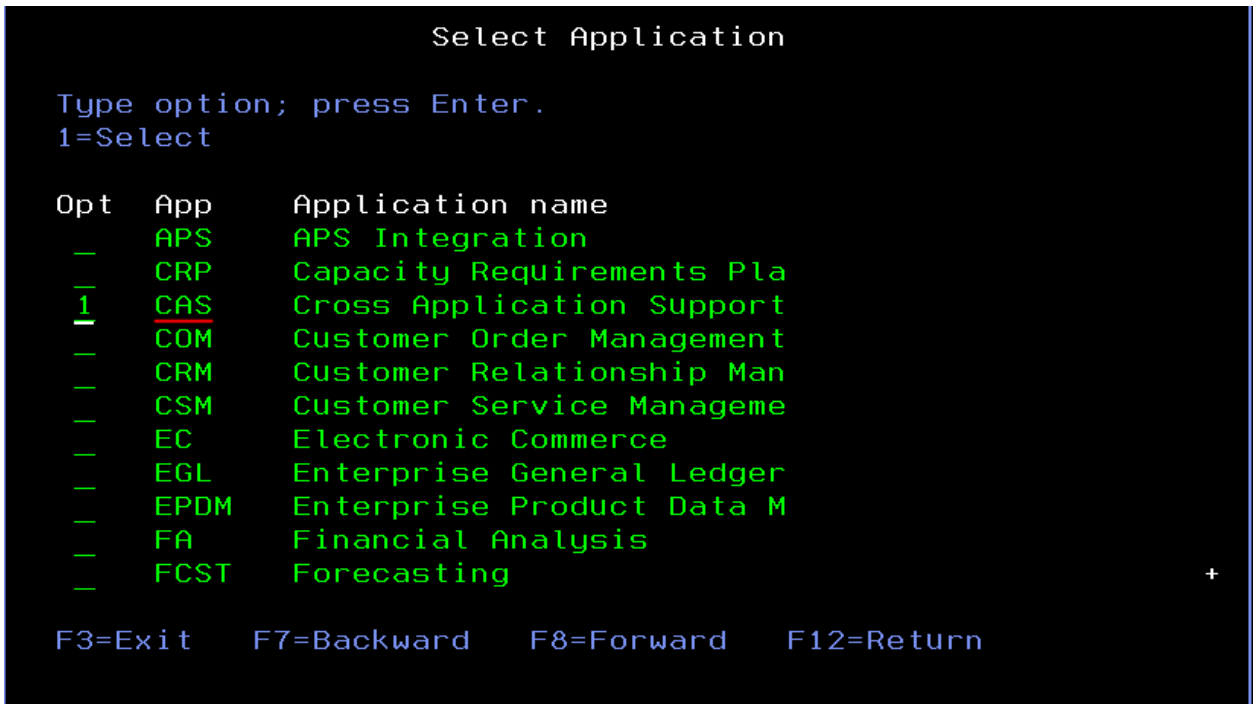
In XA Environment -> Application Settings -> Business Information Services -> Organization Node value need to be setup with proper value to reflect XA environment detail. This Organization Node value is sent as Accounting Entity value in Sync.Person BOD from XA to IFS and updated.

XA-User and XA-Administrator Role Setup

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

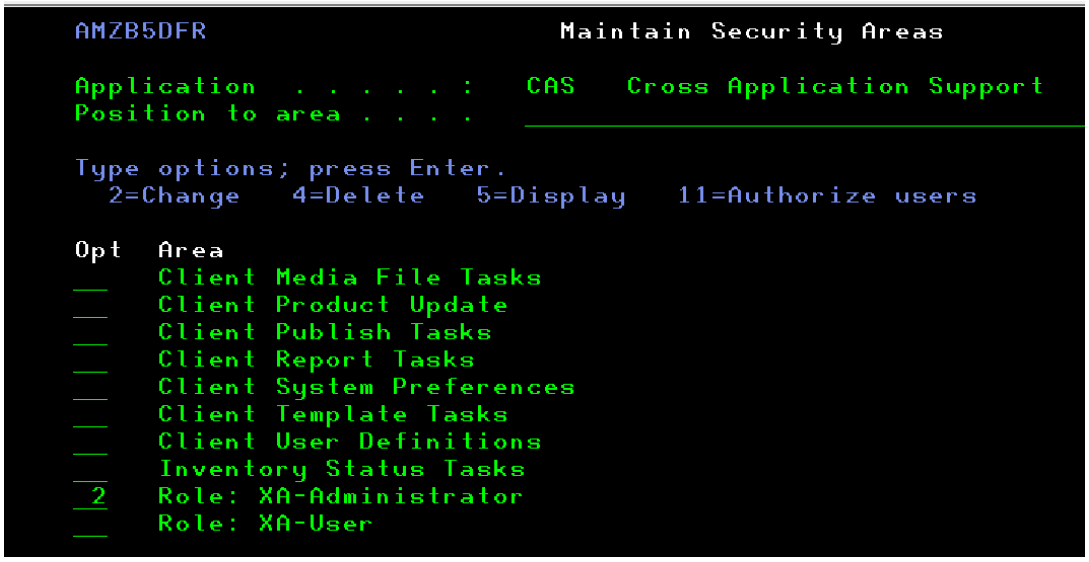
2 Take option “1” and press ENTER to access Area and task authorizations.

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

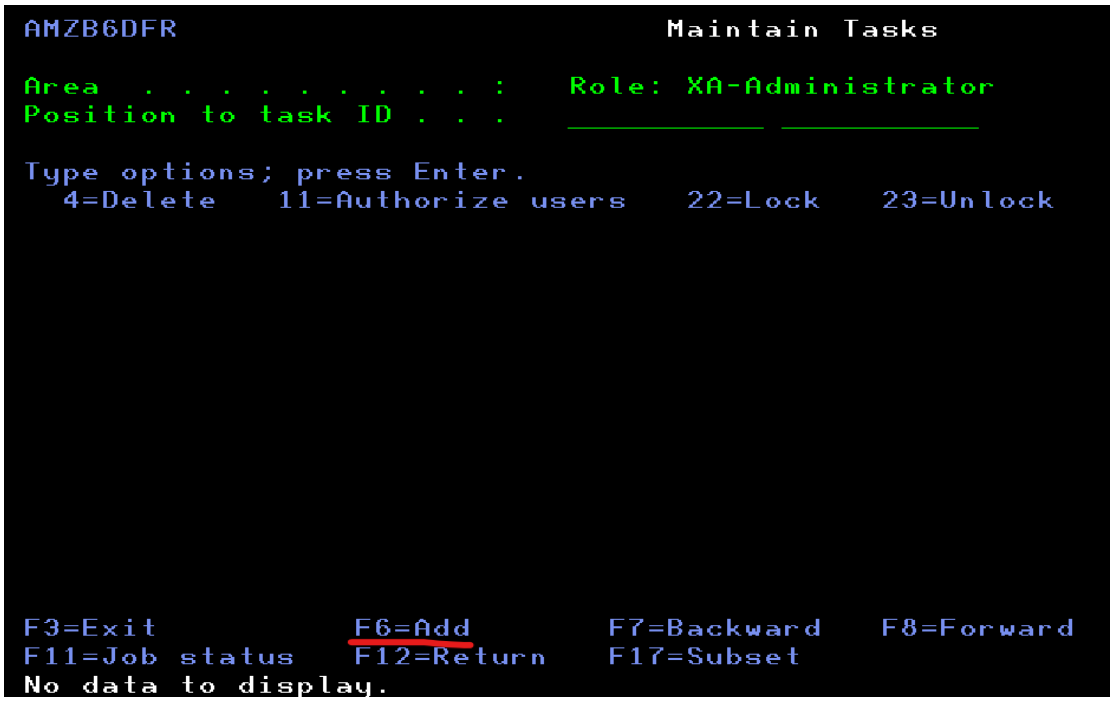


2 At Maintain Security Areas screen, navigate to ***Role: XA-Administrator*** and ***Role: XA-User***

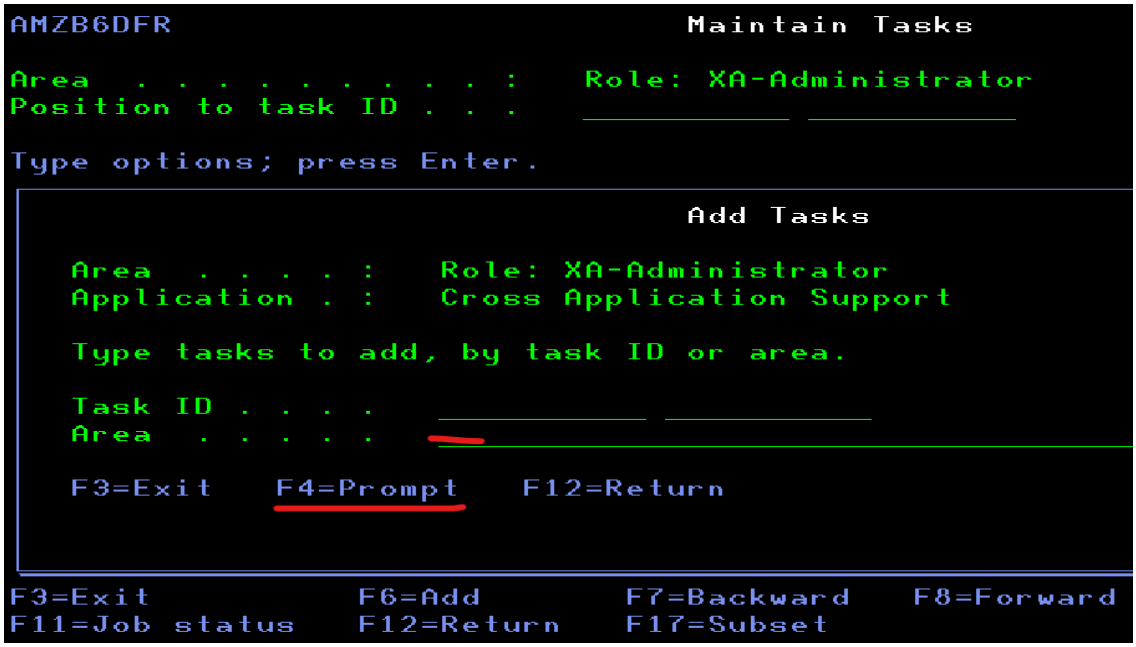
3 Take option “2’ and press ENTER to perform changes on Role: XA-Administrator security area.



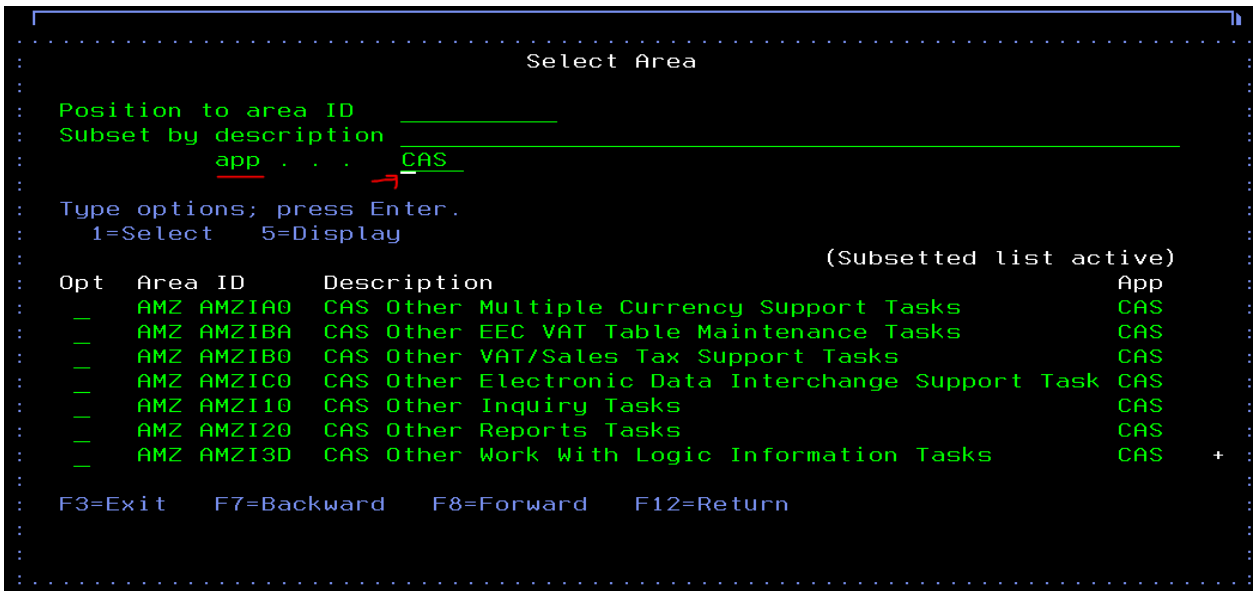
4 In Maintain Tasks screen, take “F6” to add new tasks, shown as below.



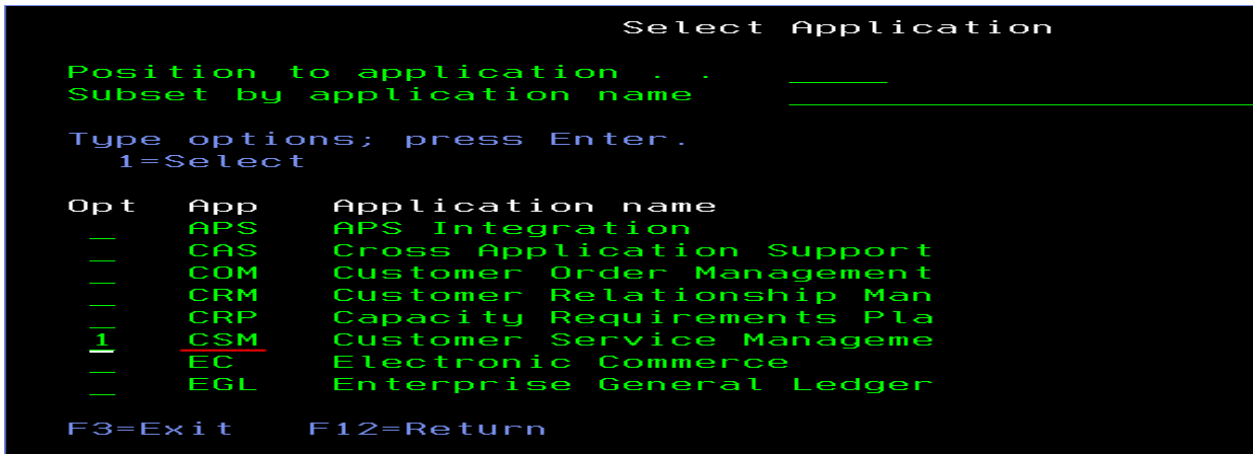
5 At Add Tasks screen, move cursor to Area and then take “F4” to Prompt the available options, shown as below.

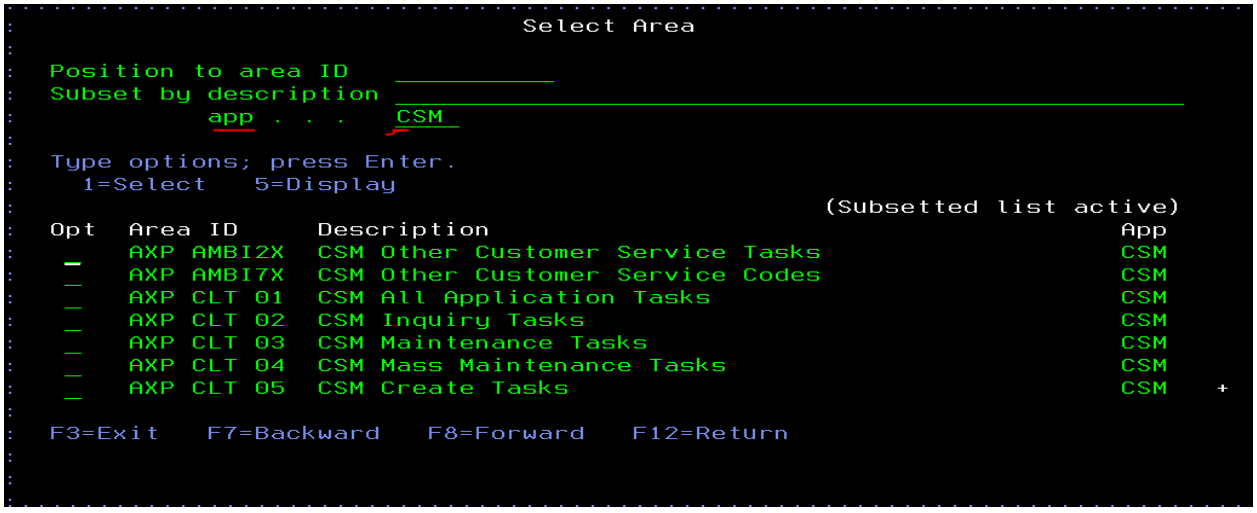


6 The below Select Areas screen shows the list of CAS application areas. If you want to get the other application areas, place cursor at app and take “F4”, shown as below.

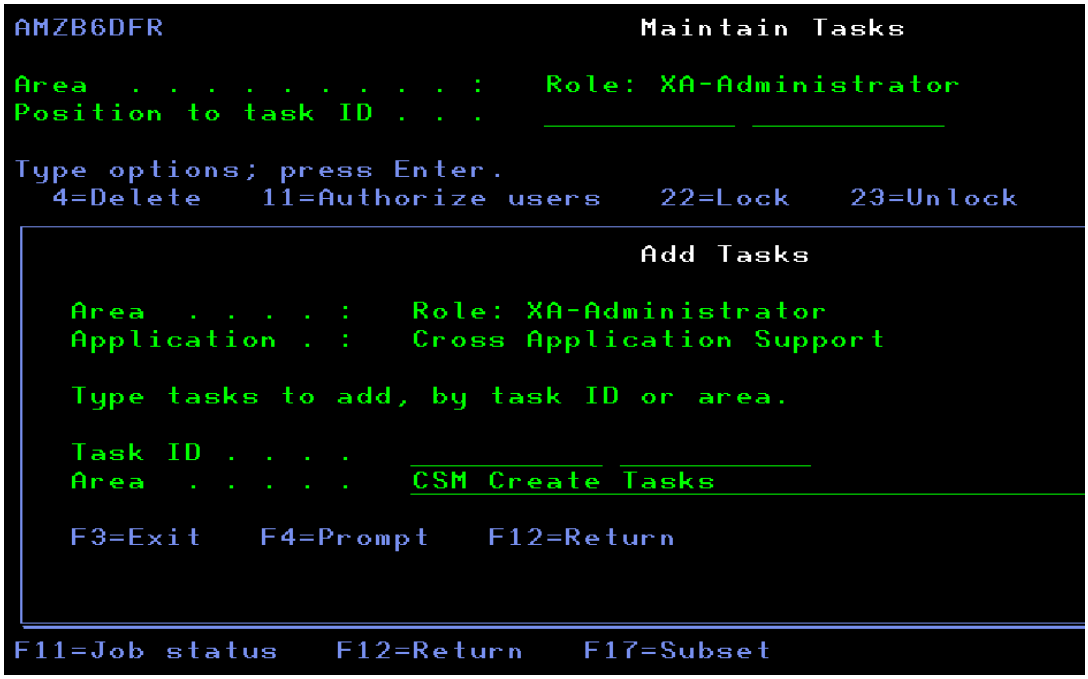


7 For an example: Here we are selecting the ***CSM*** application by taking option “1” and press ENTER, shown as below.





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.

```
AMZB6DFR                            Maintain Tasks

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

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

Opt  Task ID                        Type       App        Locked
__   CAXHDR      ATTACH             SEC        CAS           Y
     Maintain Master Calendar Attachments
__   CAXHDR      CHANGE             SEC        CAS           Y
     Change Master Calendars
__   CAXHDR      COPY               SEC        CAS           Y
     Copy Master Calendars
__   CAXHDR      CREATE             SEC        CAS           Y
     Create Master Calendars
__   CAXHDR      DELETE             SEC        CAS           Y
     Delete Master Calendars


F3=Exit          F6=Add       F7=Backward   F8=Forward
F11=Job status   F12=Return   F17=Subset
```

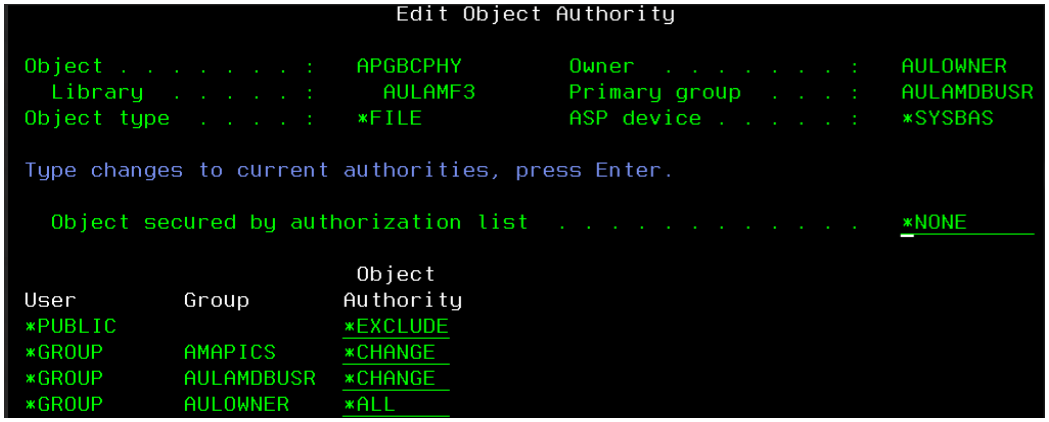
Follow same process to add tasks into ***Role: XA-User.***

```
AMZB6DFR                            Maintain Tasks

Area  . . . . . . . . . . :   Role: XA-User
Position to task ID . . .     __________ __________

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

Opt  Task ID                        Type       App        Locked
__   AM6M1009                       SEL        PUR           N
     Purchase Order Closeout Selection
__   AM6M1012                       MNT        PUR           N
     Create Shipping Schedule
__   AM6M3001                       INQ        PUR           N
     Purchase Orders
__   AM6M4002                       RPT        PUR           N
     Requisition Analysis
__   AM6M4007                       RPT        PUR           N
     Purchase Order Closeout Audit


F3=Exit          F6=Add       F7=Backward   F8=Forward
F11=Job status   F12=Return   F17=Subset
```

Changes to APGBCPHY and APGBC01P objects

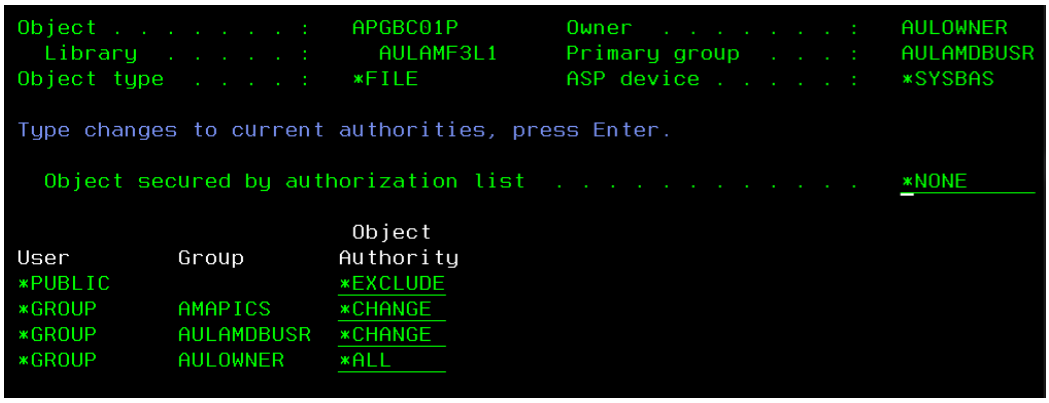
Login to XA and run command *EDTOBJAUT AULAMF3/APGBCPHY *FILE*

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



Similarly run *EDTOBJAUT AULAMF3L1/APGBC01P *FILE.*

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



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

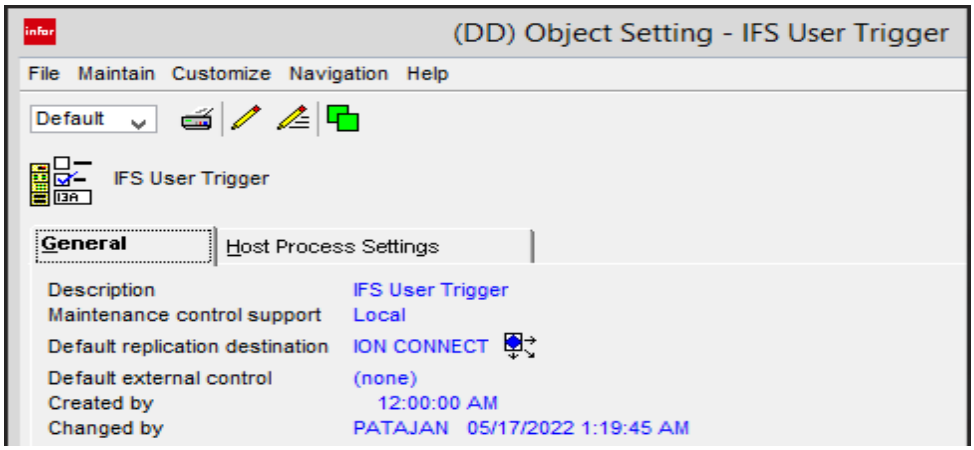
Sync Person (XA User)

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.

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 Drillback Configuration

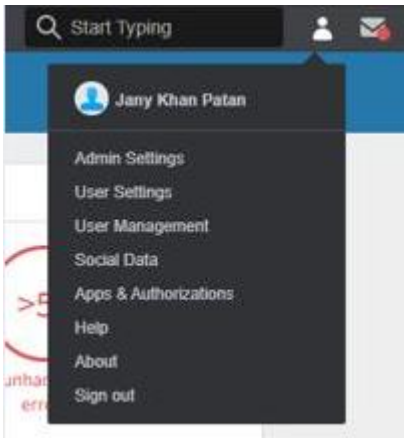
Drillback configuration requires the deployment of a configuration file within Infor Ming.le and Infor ION. This file is supplied by XA for drillback support.

Configuring Ming.le Drillbacks

To configure drillbacks in Infor Ming.le, you must import the XA_Standard_Views.xml Drillback Definition File. Navigate to the **infor\vlib\Ming.le** folder in the client IFS directory, which is the location of the XA sample solution files used for integrations through Infor OS and save the **XA_Standard_Views.xml** file.

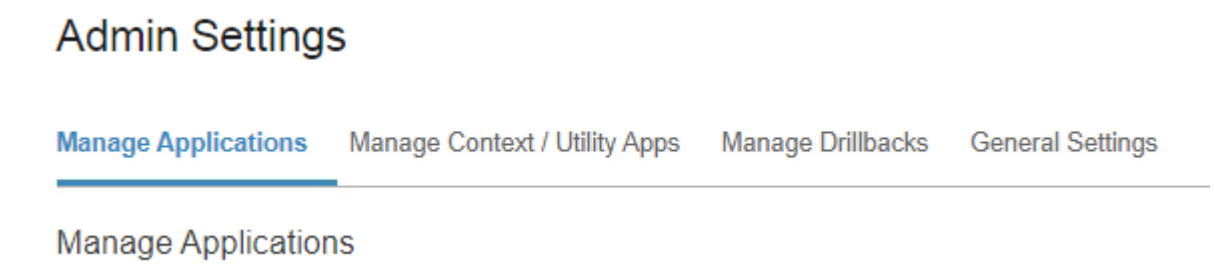
1 Log on to Infor OS as the administrator.

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



2 When the **Admin Settings** loads, click **Manage 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**.

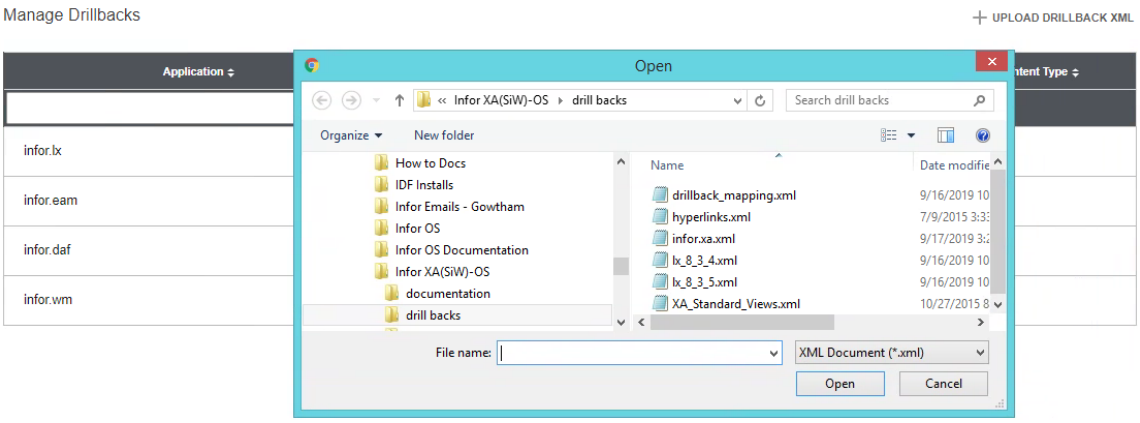
3 Click **Yes**.



4 Click **UPLOAD DRILLBACK XML** and browse to select the Drillback Definition file as specified earlier.

5 Click **Open**.

6 Click **OK**.



Manage Drillbacks

UPLOAD DRILLBACK XML

Application	Description	Content Type
infor.lx	LXStandardView_8.3.4.003	Standard
infor.eam	EAM Drillback Views	Custom
infor.daf	Infor Document Management v12.0	Standard
infor.wm	SCE - WM Content	Custom
infor.xa	XA Standard views	Custom

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

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

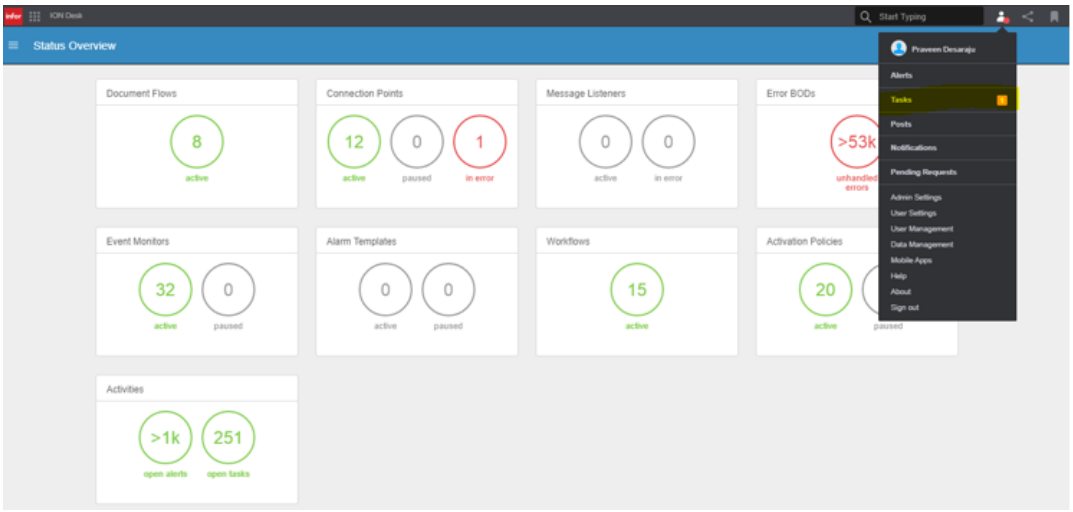
BOD	Infor XA Object
Location	Company Site Financial Division Warehouse
Opportunity	Opportunity
PayableTransaction	Financial Transaction Vendor Invoice
PayFromPartyMaster	Entity Financial Division Vendor Customer Company Account
Person	Buyer Sales Representative
ProductionOrder	Manufacturing Order
PurchaseOrder	Purchase Order Purchase Order History
Quote	CustomerQuote Quote
RemitToPartyMaster	Entity
Requisition	Purchase Request
SalesOrder	Customer Order or Quote Customer Order History
ShipFromPartyMaster	Entity 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

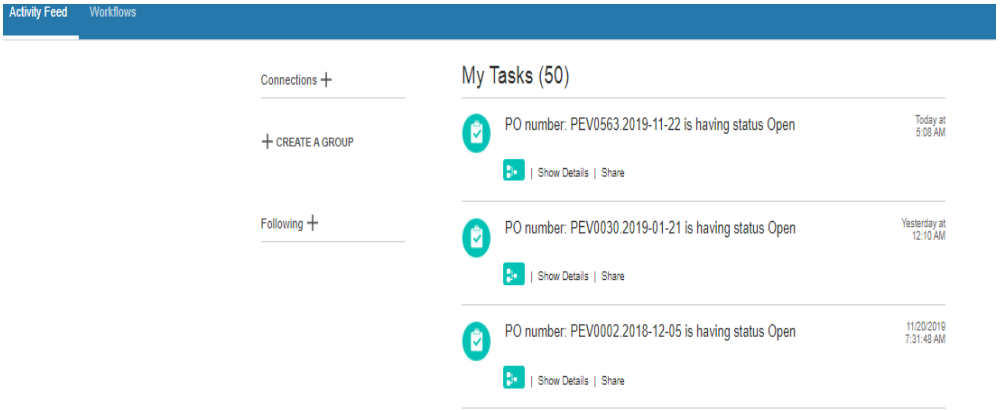
BOD	Infor XA Object
SupplierShipmentSchedule	Purchase Order Purchase Order History
TradingPartner	Entity Financial Division Vendor Customer Company Account

Using Drillbacks in Ming.le and Context/Utility App

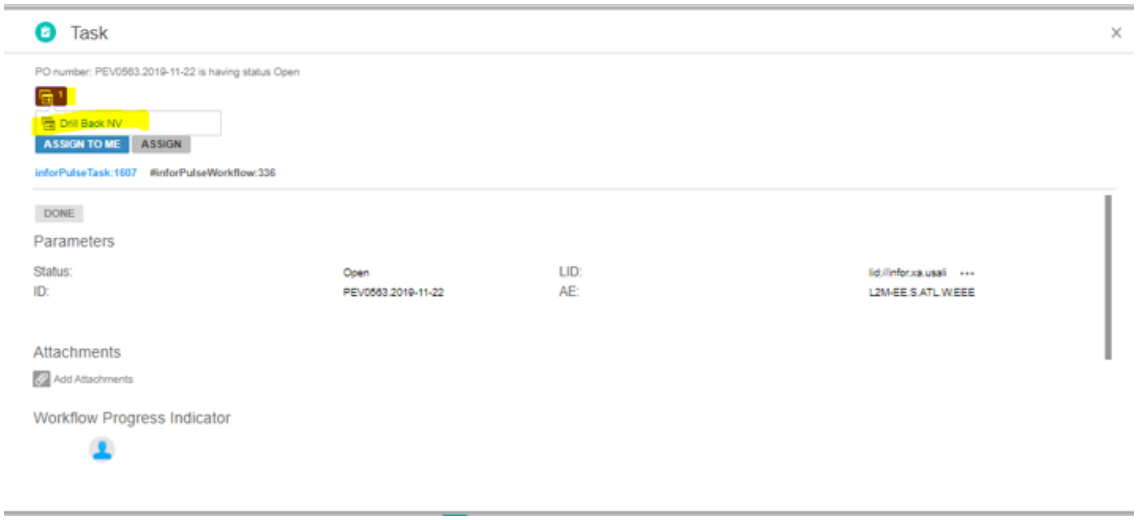
To use the drillback functionality in Ming.le and Tasks Context/Utility Apps, configuring drillbacks and enabling Tasks Context/Utility app for that XA environment in Ming.le is a pre-requisite.

1 Select **My Tasks > Activity Feed** to display the list of tasks created for you in Infor Ming.le.

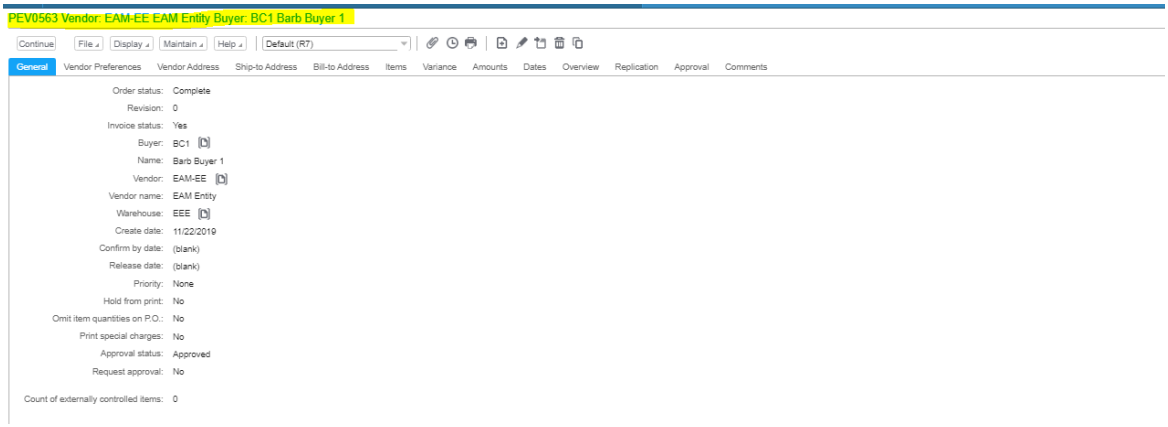




2 Click **Show Details** to open and select the Drillback link as highlighted in this screenshot.



3 Click the **Drillback** link. The page is redirected to the specific XA object (Purchase order in this example) as displayed.



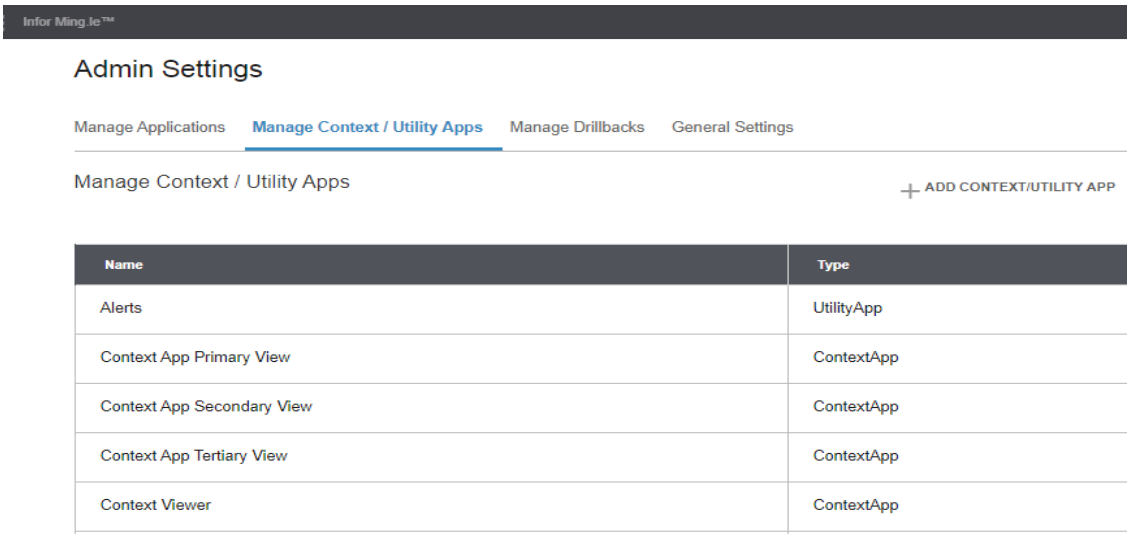
Configuring the IDF Context Application

You can configure IDF Context application in Ming.le and the application is displayed on the right.

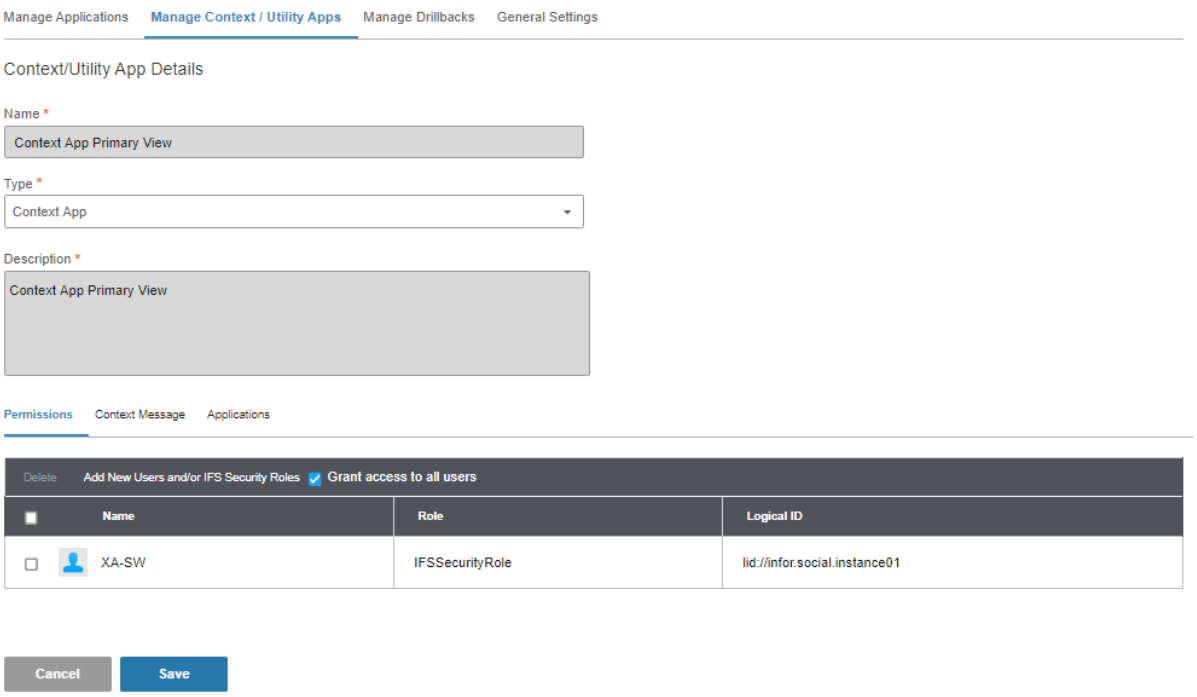
Note: To use the IDF Context App, System i Workspace must be at PTF level 16 or later.

Enabling IDF Context Applications

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

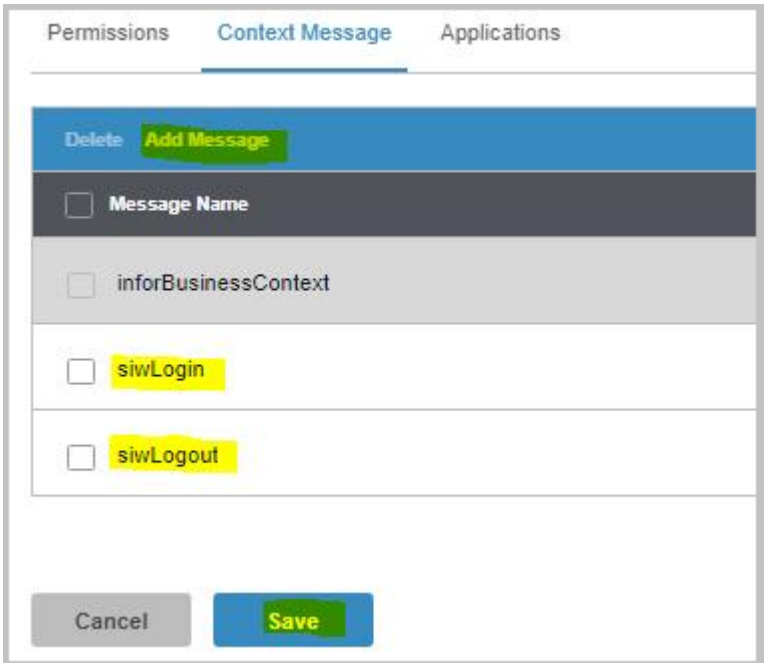


2 Click **Context App Primary View** to display the details.

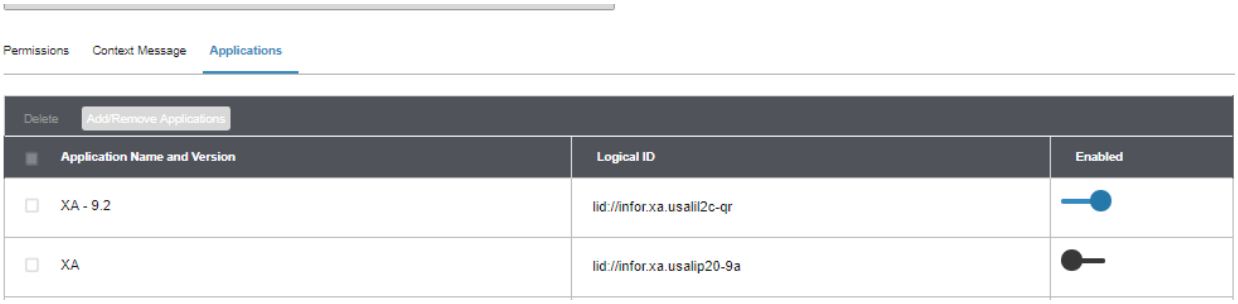


3 In Permissions section add the security role created for XA using “Add New Users and/or IFS Security Roles”. All the users under this security roles can view this Context App while accessing XA.

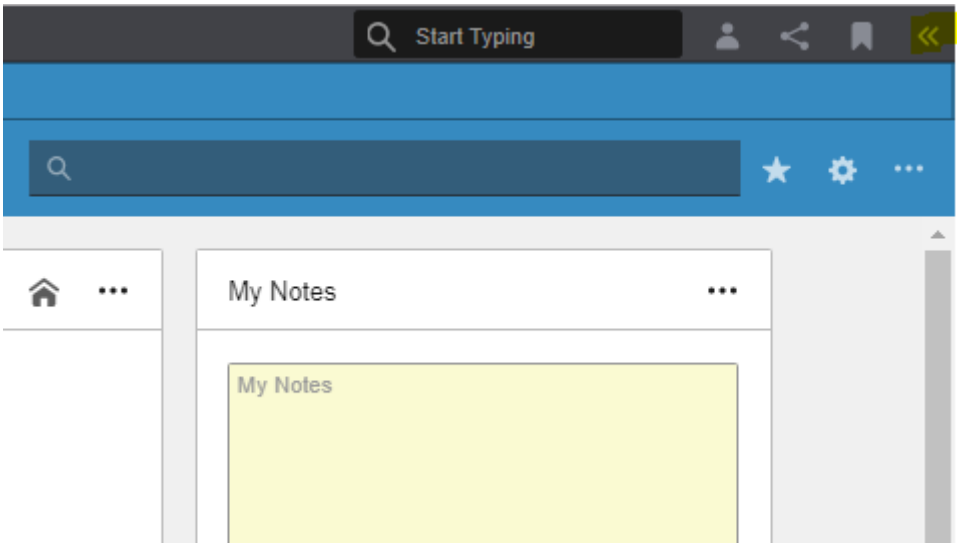
4 Go to Context Message section and add these messages as displayed. Refer KB 2046253 for more details.



5 Go to **Applications** section and enable the toggle for required XA application.

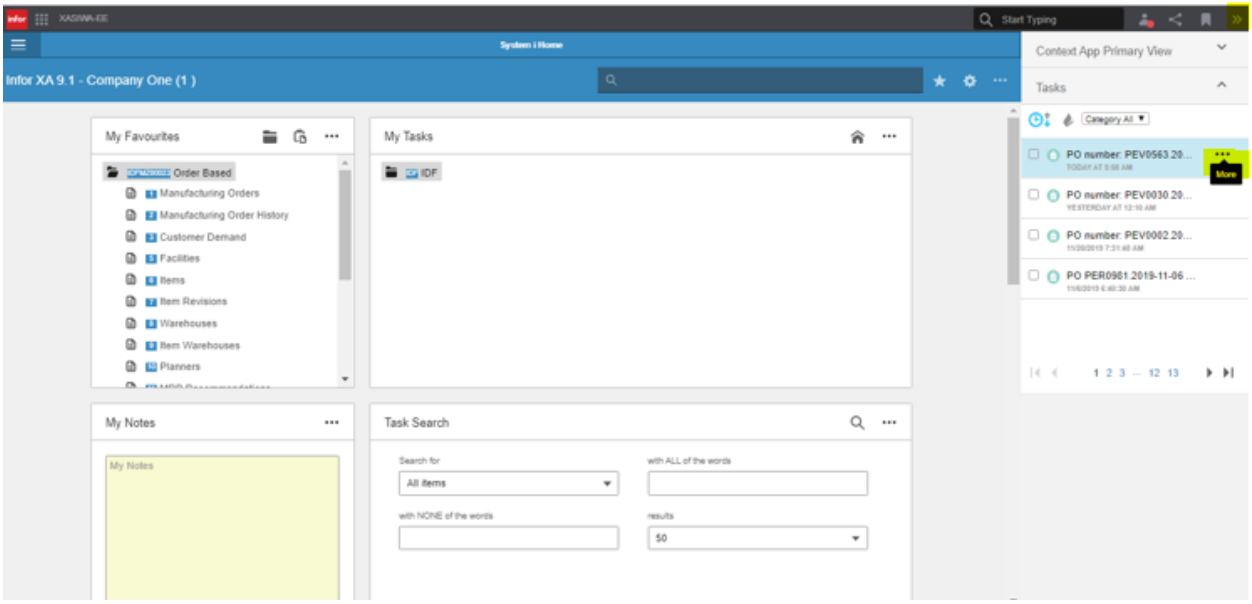


6 Now launch XA and click the double arrow option on top right corner to launch context apps.



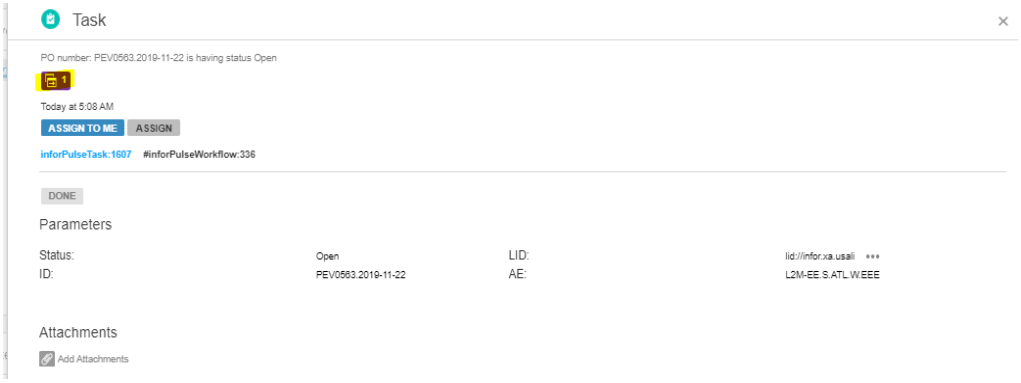
Drillbacks in Task Context/Utility App

Tasks Utility App enabled in Manage Context / Utility App enables users to view the Tasks in the right-side corner of SiW Anywhere System I Home screen. A list of tasks available for current user on the right is displayed.

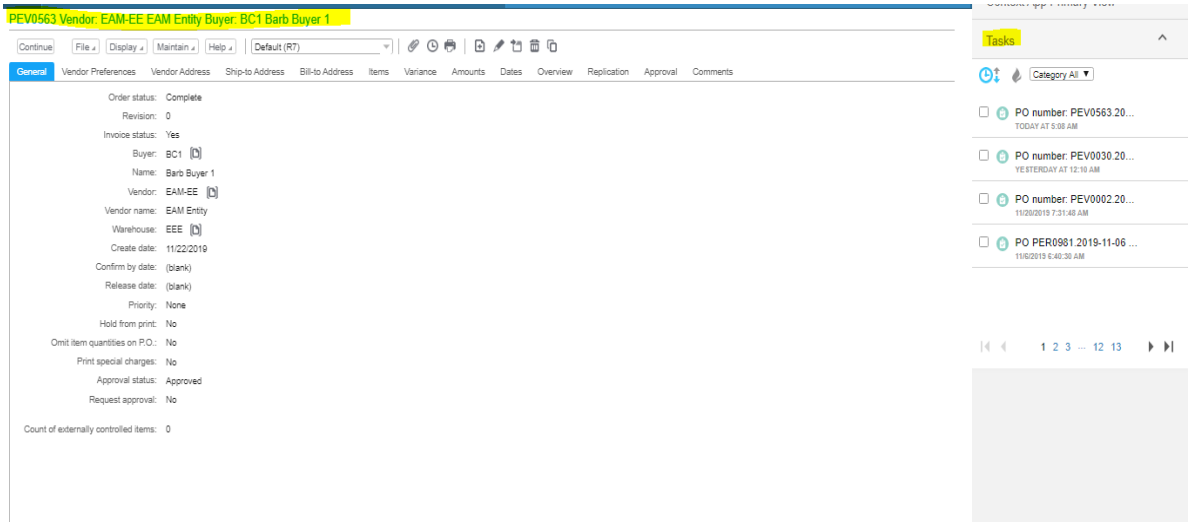


1 Click **More > View Details**. The Task details screen is displayed.

2 Click Drillback.



3 Click **Drillback** to launch and redirect to PO details in XA.


PEV0563 Vendor: EAM-EE EAM Entity Buyer: BC1 Barb Buyer 1
Continue
File
Display
Maintain
Help
Default (R7)
General
Vendor Preferences
Vendor Address
Ship-to Address
Bill-to Address
Items
Variance
Amounts
Dates
Overview
Replication
Approval
Comments
Order status: Complete
Revision: 0
Invoice status: Yes
Buyer: BC1
Name: Barb Buyer 1
Vendor: EAM-EE
Vendor name: EAM Entity
Warehouse: EEE
Create date: 11/22/2019
Confirm by date: (blank)
Release date: (blank)
Priority: None
Hold from print: No
Omit item quantities on P.O.: No
Print special charges: No
Approval status: Approved
Request approval: No
Count of externally controlled items: 0
Tasks
Category All
PO number: PEV0563.20...
TODAY AT 5:08 AM
PO number: PEV0030.20...
YESTERDAY AT 12:10 AM
PO number: PEV0002.20...
11/20/2019 7:31:48 AM
PO PER0981.2019-11-06 ...
11/6/2019 6:40:30 AM
1 2 3 ... 12 13

Chapter 11 Infor Business Context IBC

Overview

The Infor Business context message is a Ming.le 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”.

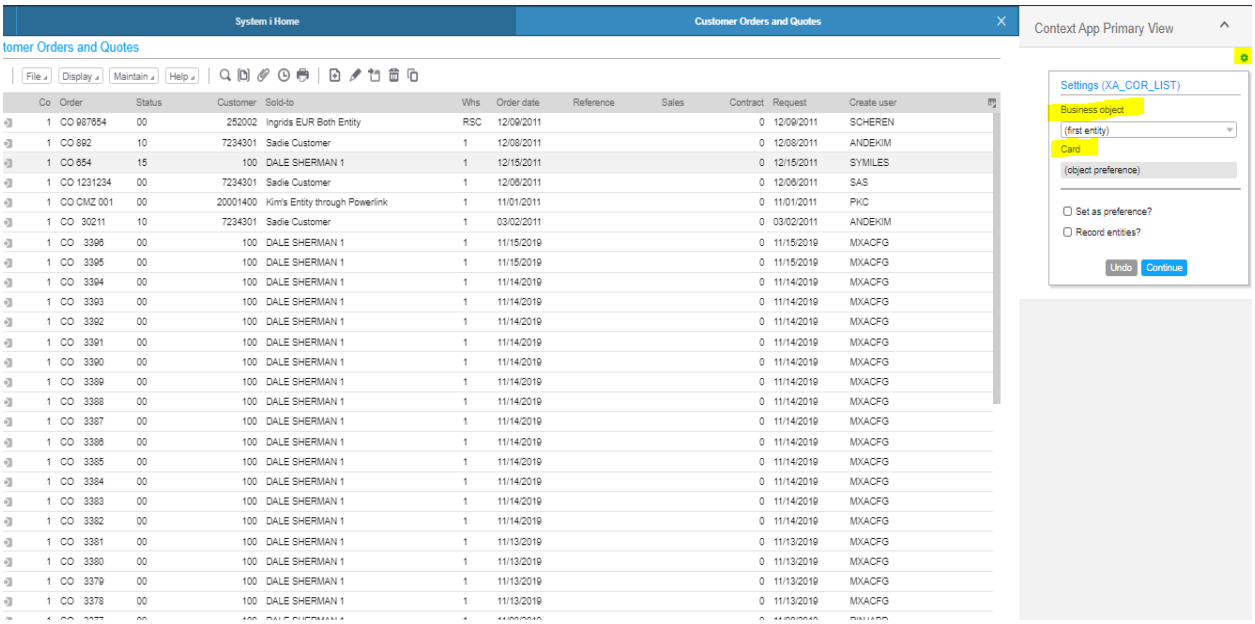
All Infor applications running inside Infor Ming.le send these messages. In IDF, the entities correspond to the business objects that are currently being displayed.

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

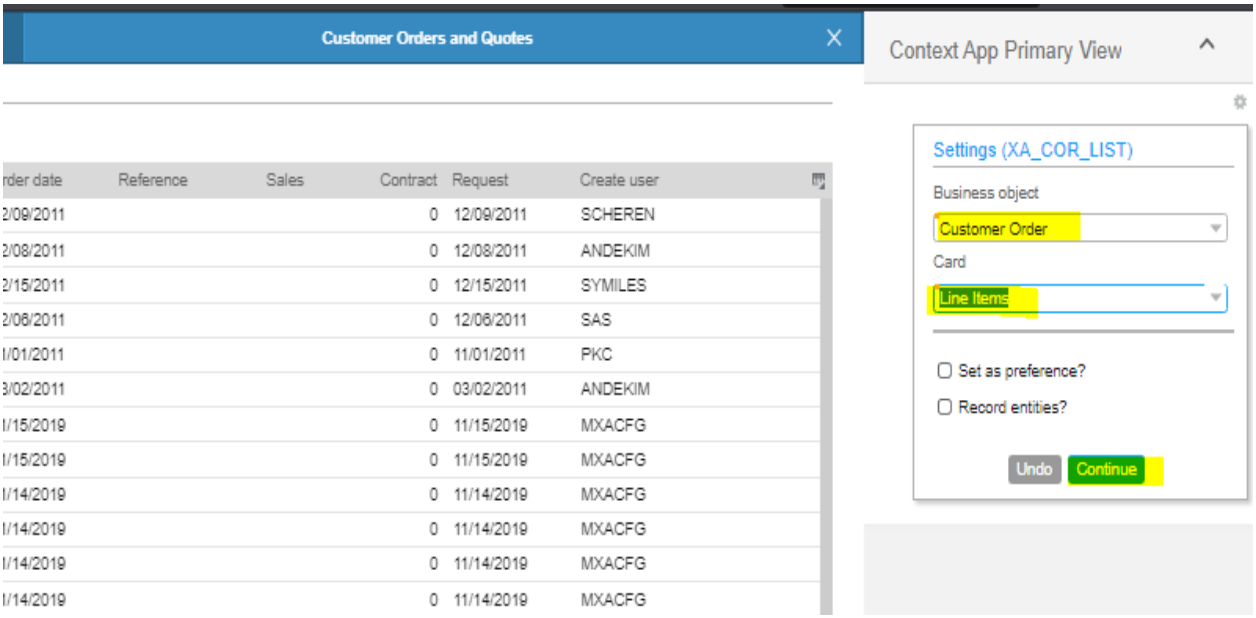
In object view, the IDF sends a message containing the displayed object and any many-to-one related objects. When the user selects a row from a list card, the currently selected object is added to the message.

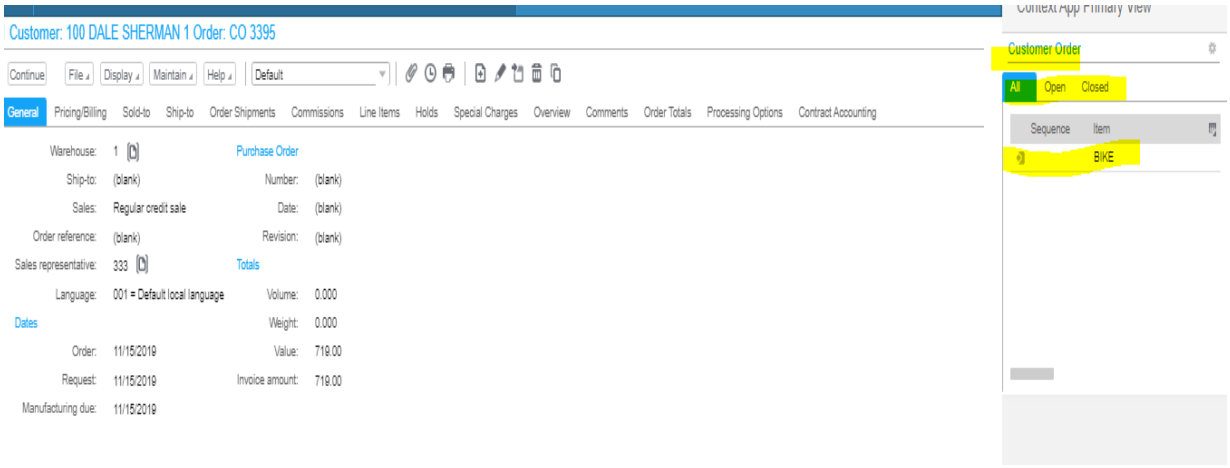
Context applications or web parts can be added to any application page in Infor Ming.le. These context applications display data that is appropriate for the message.

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



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



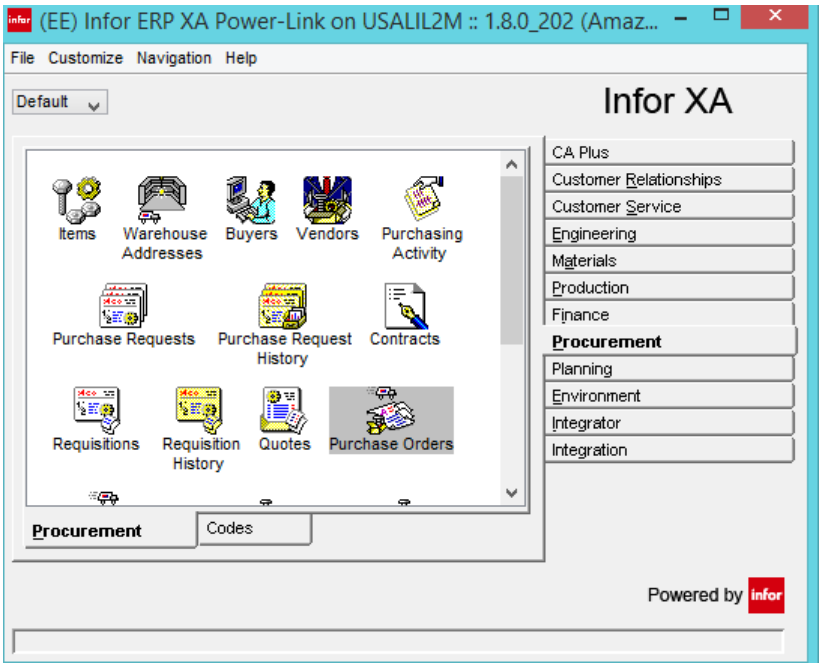


Line items are displayed when you open the customer order as displayed in the screenshot.

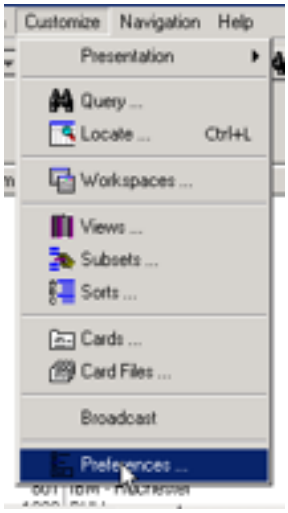
Preference definition

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

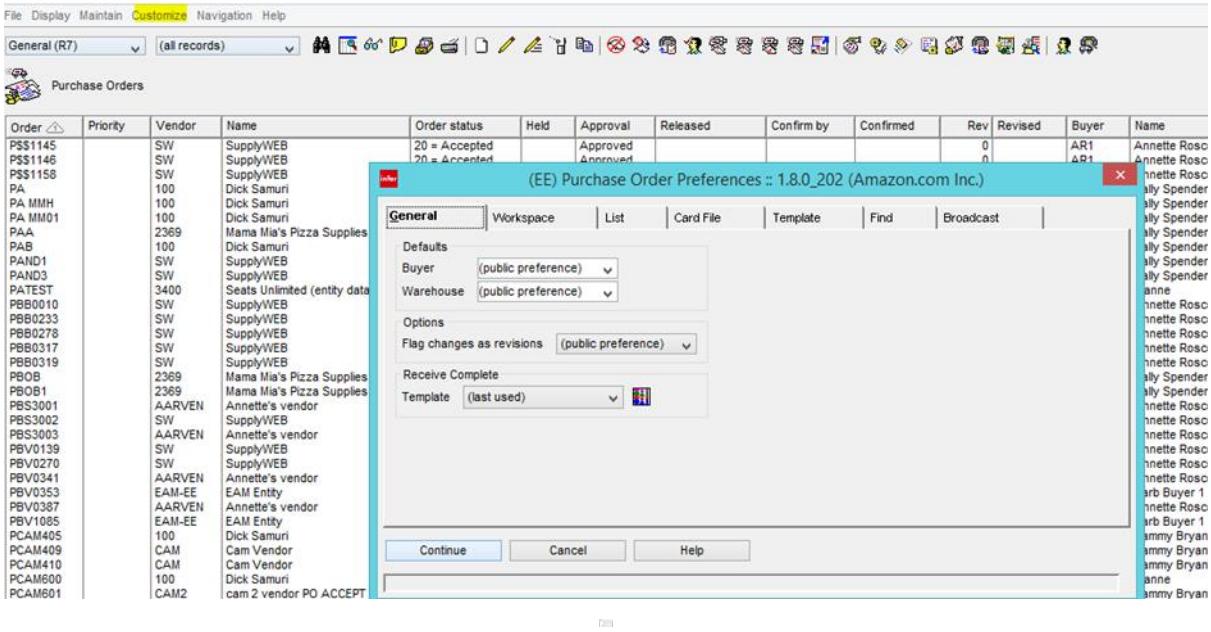
1 From the Main browser, double-click the Business Object to display the context application.



2 Select **Customize > Preferences**.



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



3 Select the **Card File** tab.

4 Select the **Net-Link** tab.

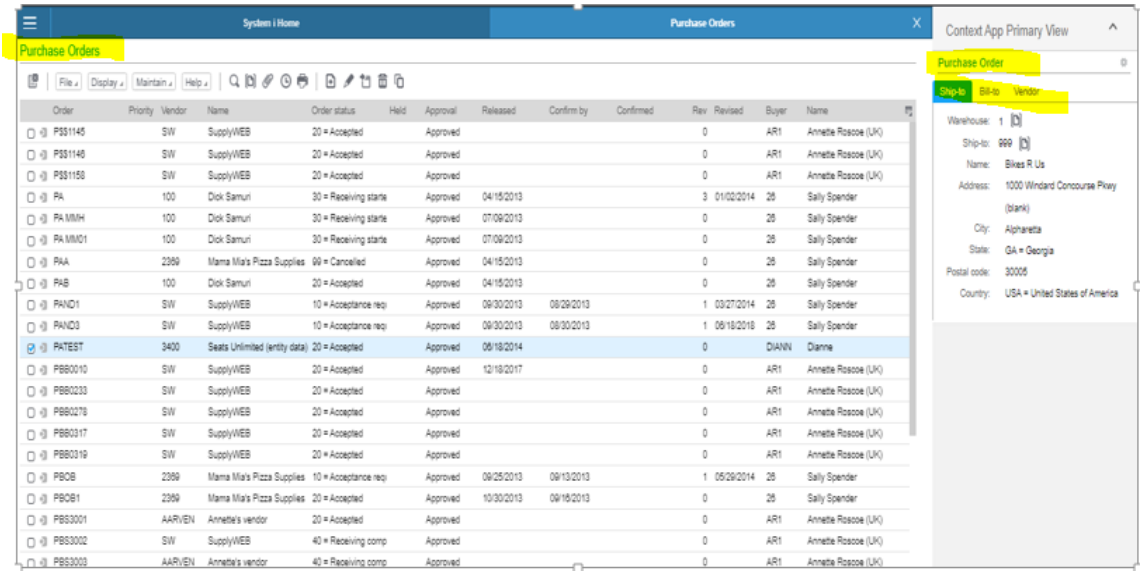
5 Specify the preferences for the context application.

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

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

7 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***.

8 Launch XA in Infor OS, to display the Context App Primary View with Addresses.



9 Select a purchase order in the Context App Primary View to display the Purchase orders Addresses.

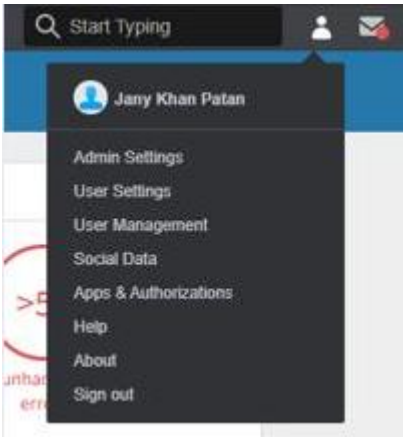
Chapter 12 User maintenance

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

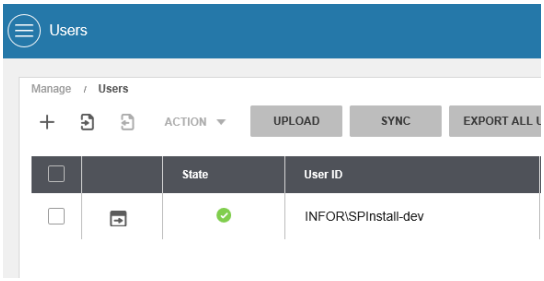
Adding users

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

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

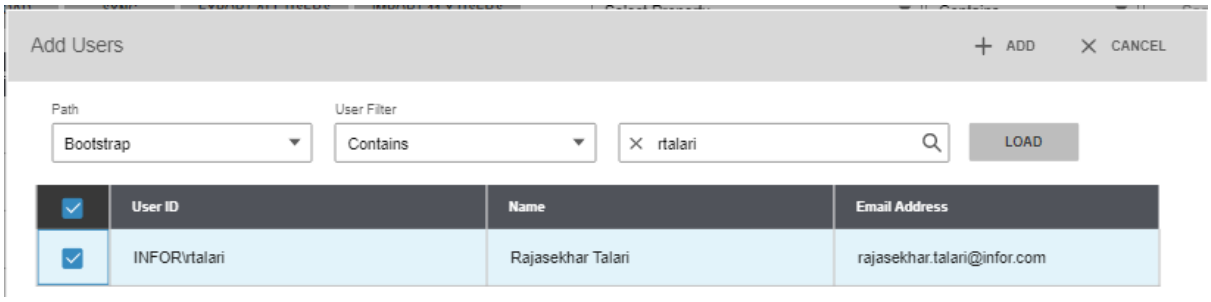


3 Select **Users** on the menu to the left**.**

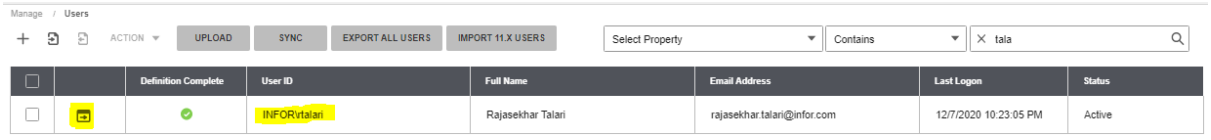


4 Click the **+** option to add a new user.

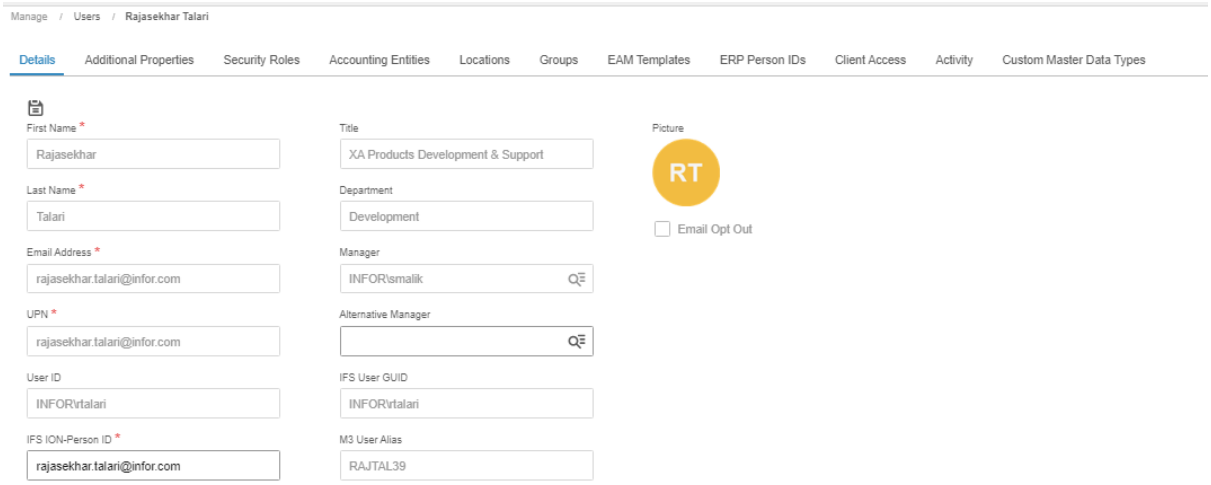
5 Enter a name in the search box and click **Load**.



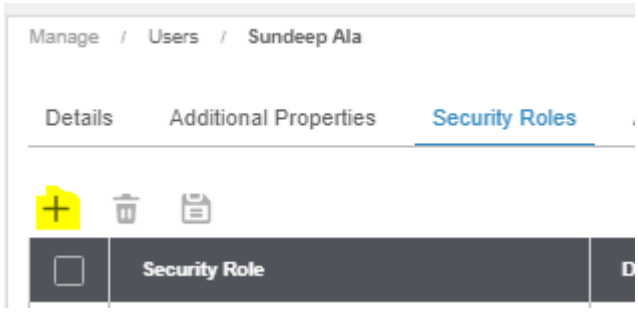
6 Select the user from the list and click **Add**.

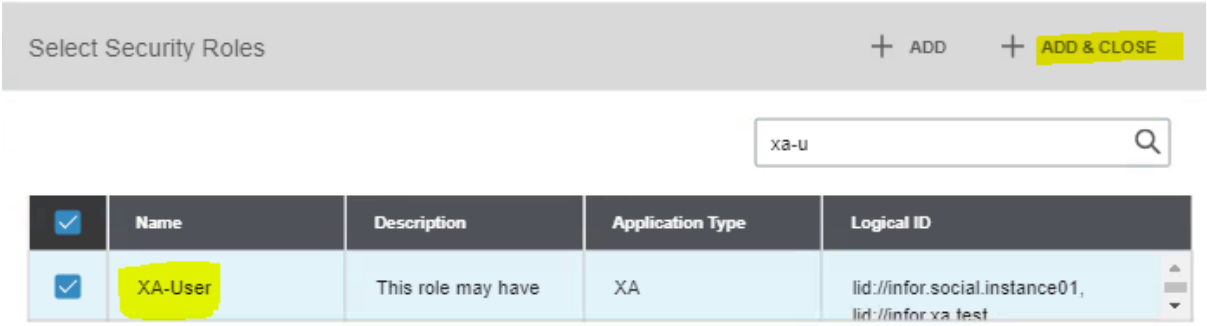


7 Verify the user information and update as per the business requirement.



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





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

Chapter 13 Net-Link WAR file redeployment

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

System i Workspace AnyWhere with Windows deployment

Refer "***WAR file Generation***" and "***Tomcat (version 7.0 +)***" sections in "***Appendix C WAR file redeployment"*** from the "***Infor XA Setup Guide for Secure Net-Link***" document, which describes about the Net-Link WAR file redeployment with SiW AnyWhere using Windows deployment.

System i Workspace AnyWhere with IBMi deployment

Refer "***W*AR file Generation**" and "**WebSphere (version 9.x*)***" sections in "**Appendix C WAR file redeployment*"*** from the "**Infor XA Setup Guide for Secure Net-Link**" document, which describes about the Net-Link WAR file redeployment with SiW AnyWhere using IBMi deployment.

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.

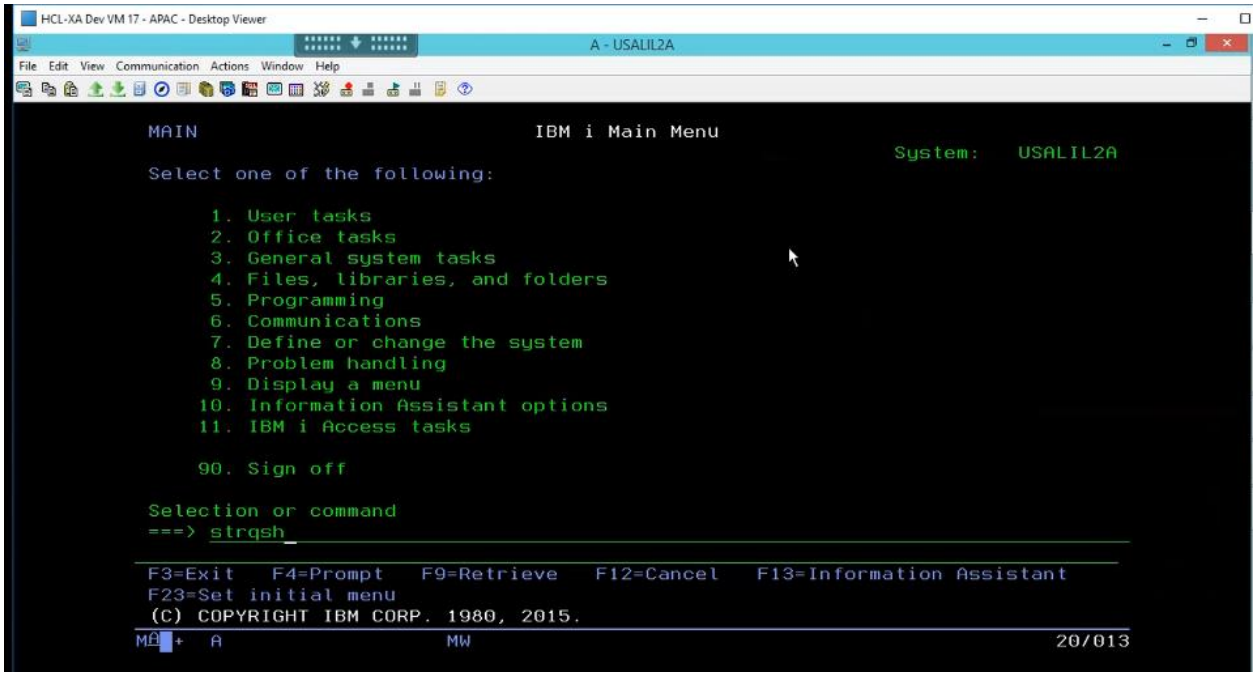
If the root Organization Node accounting entity is changed in BIS, you must clear PUB* files and re- publish all accounting entities.

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

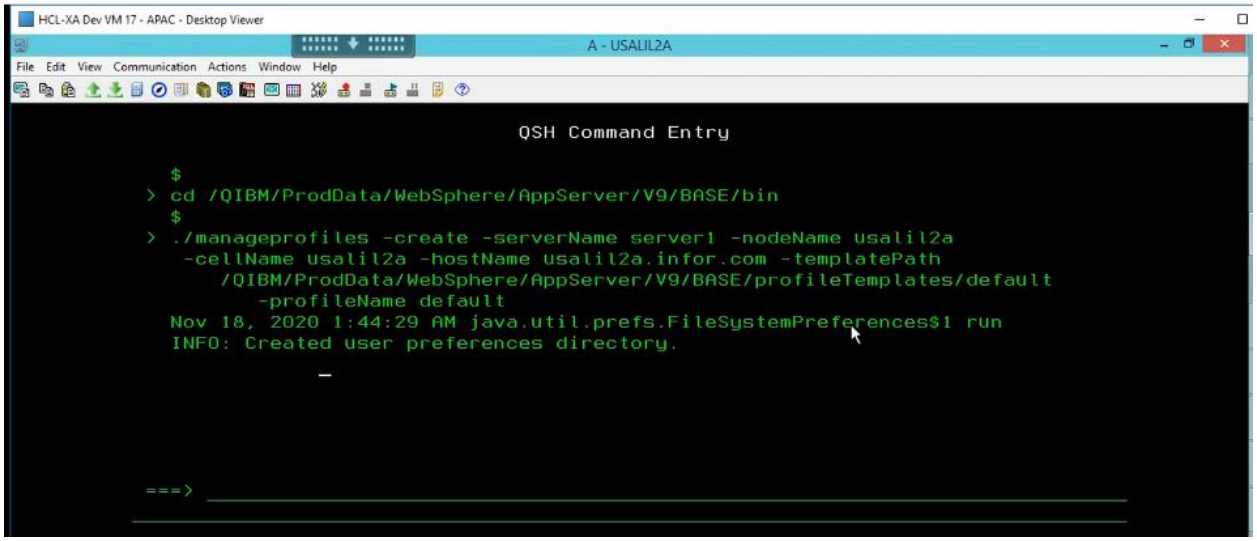
$ ./manageprofiles –create -serverName server1 -nodeName <hostname> -cellName <hostname> -hostName <hostname.domain.com> -templatePath /QIBM/ProdData/WebSphere/AppServer/V9/BASE/profileTemplates/default -profileName default

...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



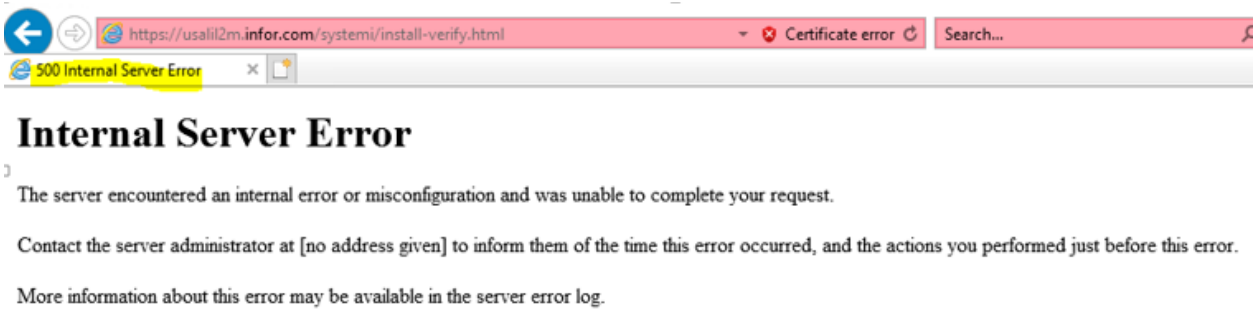
Note: In some severs the folder "**BASE**" is "**Base**". Check the folder structure before running the command.

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

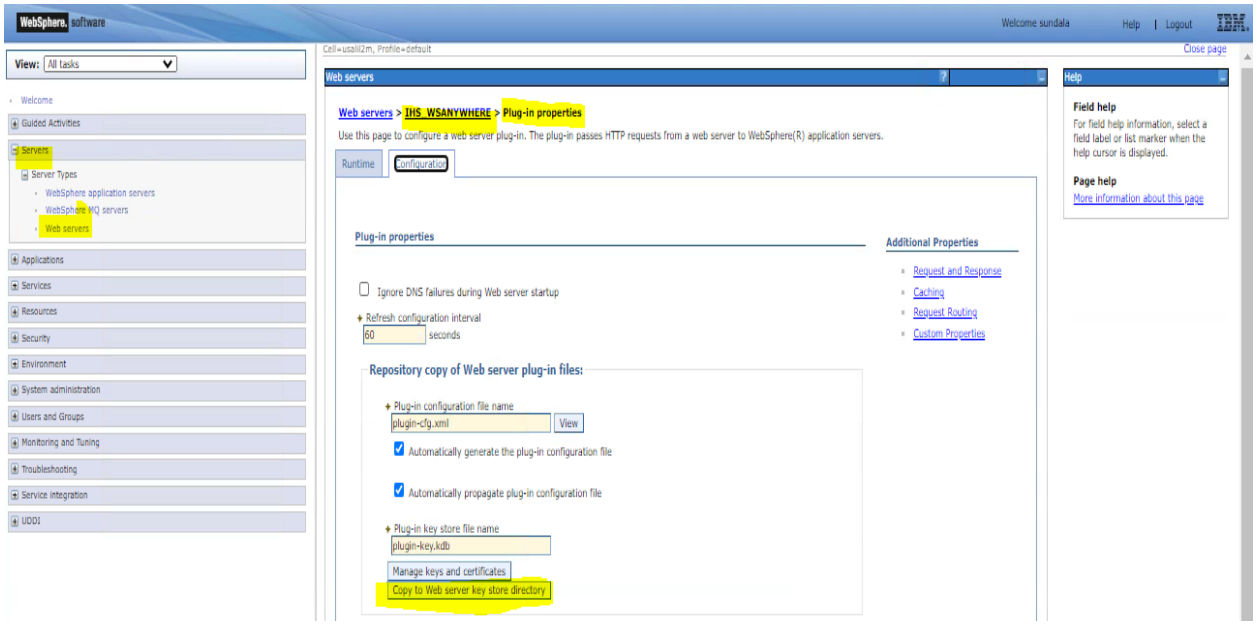
  TO

  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

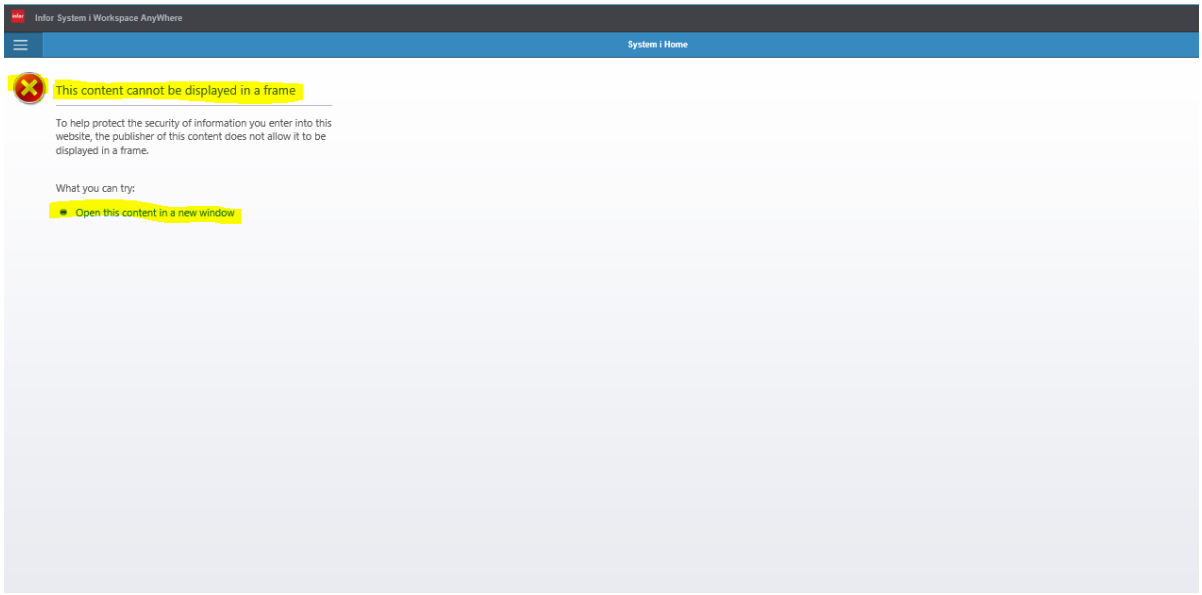
If you still receive an Internal Server Error, then navigate to the WebSphere Application Server > Launch Administrative Console > Servers > WebServers > IHS_WSANYWHERE > Additional properties > Plug-in properties and select Copy to WebSphere KeyStore Directory > Apply and click Save.



Appendix D Known Issues

In IE browser, standalone application (SiWAnywhere or SiW v2015) does not work after inserting Mingle link in properties file.

There are known issues when accessing SiW from IE browser after inserting “com.infor.siw.cloud.mingle.url” in properties file to access from Infor OS, in IE browser both standalone and from Infor OS this error message is displayed:



If you use IE11 (because of the HTTP allow-from headers you have to set for Infor OS compliance, which other browsers ignore), and configure SiW to run inside Infor OS, then you have to run it inside Infor OS.

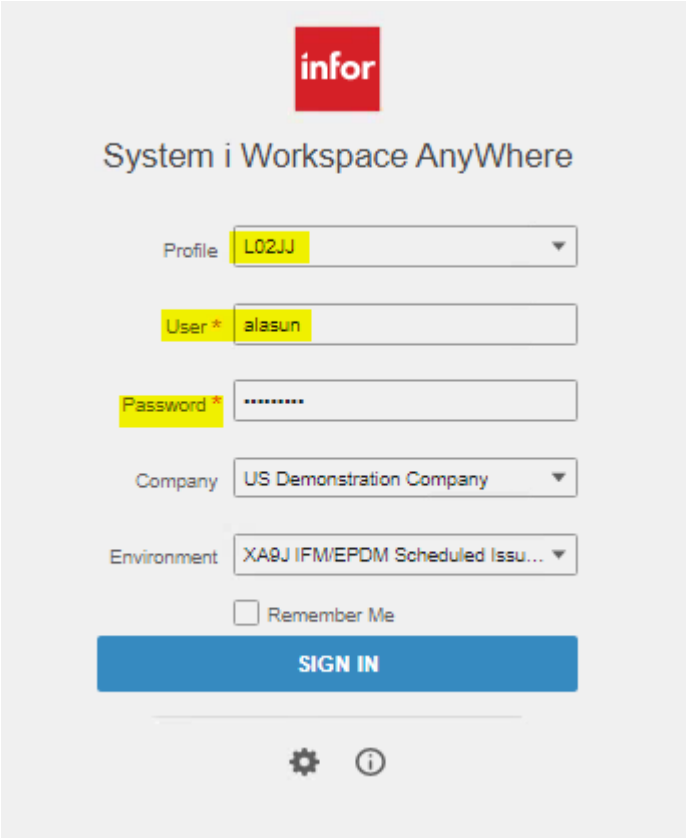
To run SiW or the related administration pages outside Infor OS, you can choose one of these options:

- Use a different browser from IE11 to access SiW.
- Add additional icons in Infor OS to explicitly call admin pages (which can be authorised to administrators).

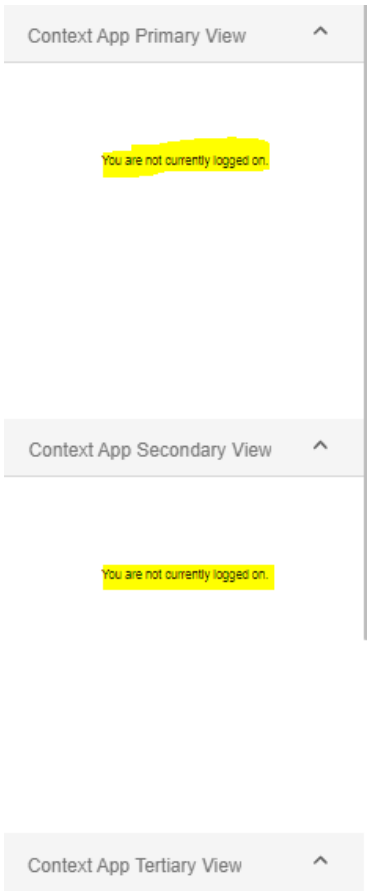
Appendix E Troubleshooting

1 If a user is trying to login to Infor OS 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 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 QA environment.

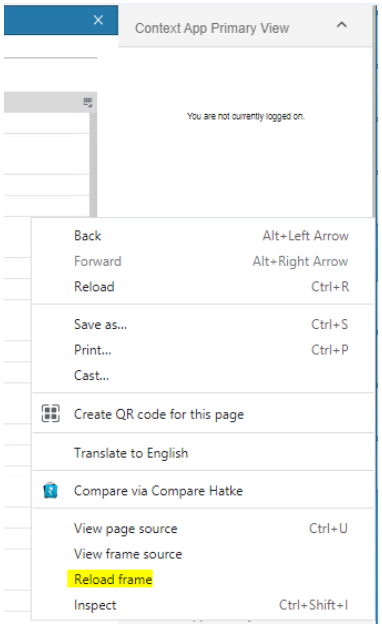
2 If a user log into Infor OS successfully, but gets prompt again for credentials while launching the SiWA applications, then user can enter the respective IBM i user ID and credentials. (For example, in this screen, login prompt screen is displayed for USALIL02 IBM i machine).



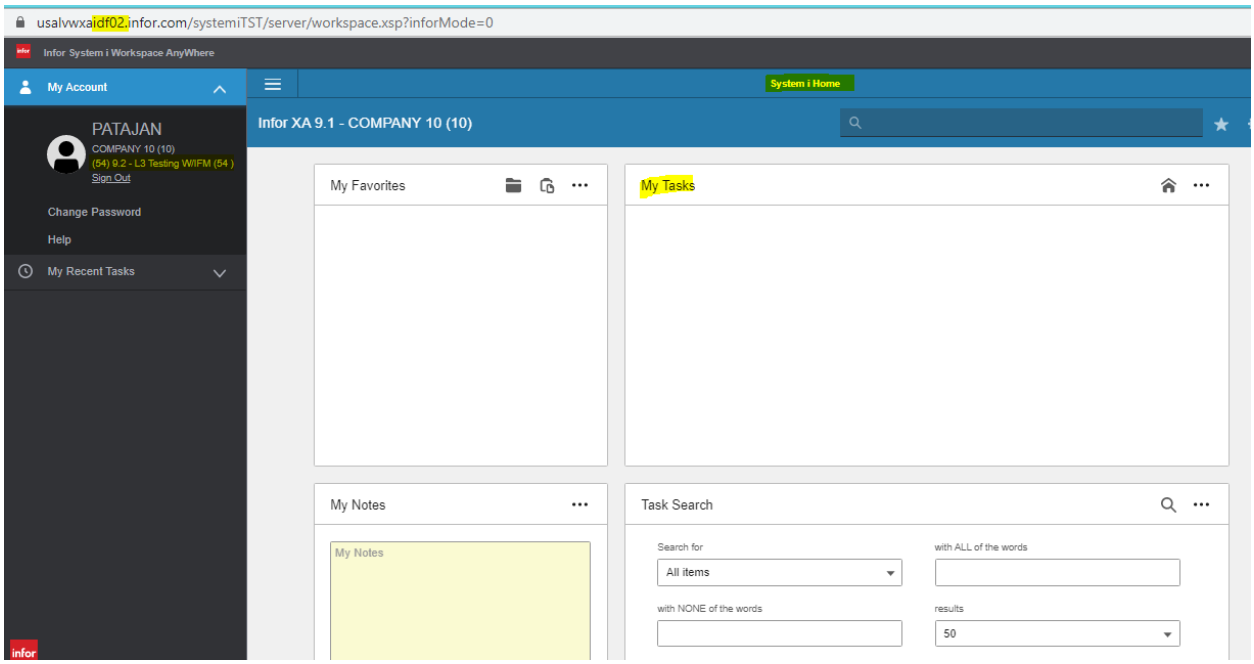
1 If user is able to login to Infor OS and SiWA applications, but facing issue at Context App Primary, Secondary & Tertiary Views with an error message *"You are not currently logged on"* displayed.



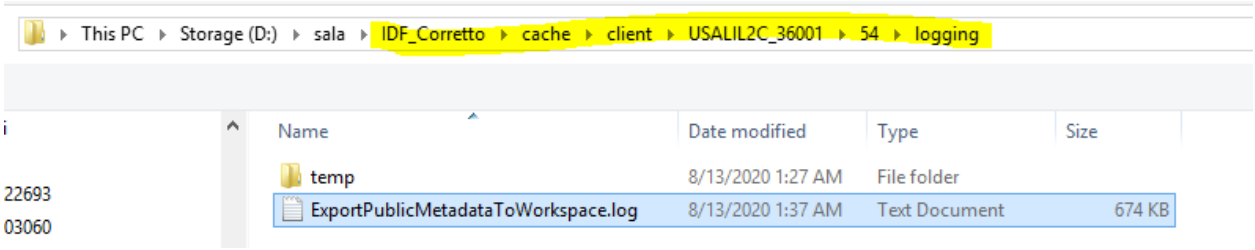
- Then as a workaround, right click the respective Context App view and click the *"Reload frame"*, as displayed.



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

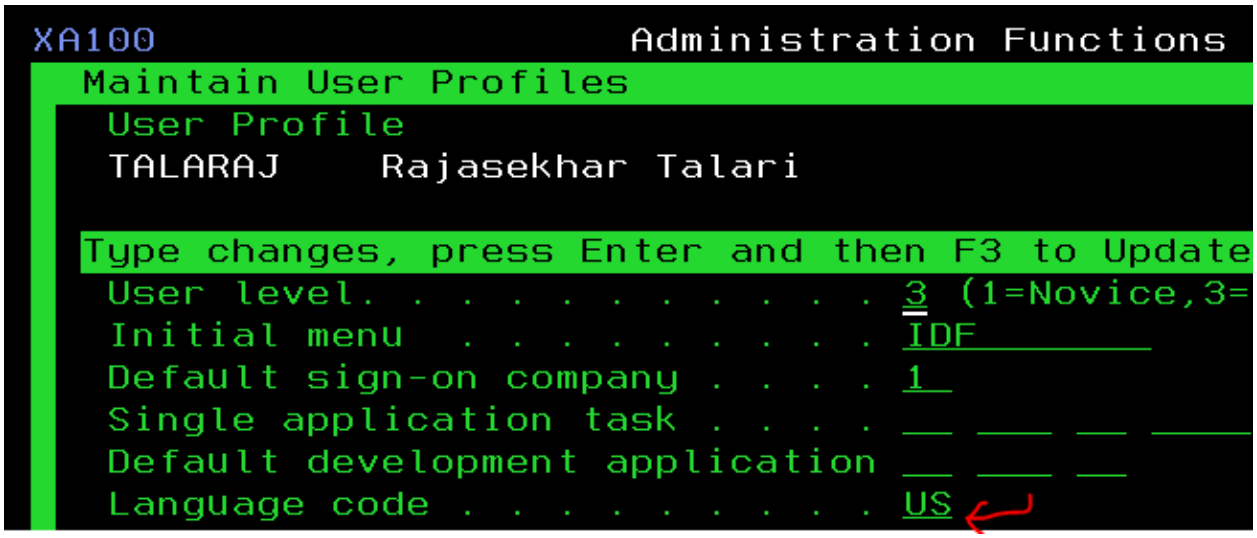


- Then you need to check whether exporting is done successfully or not in the ExportPublicMetadataToWorkspace.log at the local IDF logging folder (similar to going to Power- Link -> help -> About -> Ctrl + D -> Ctrl + L and going to logging folder).

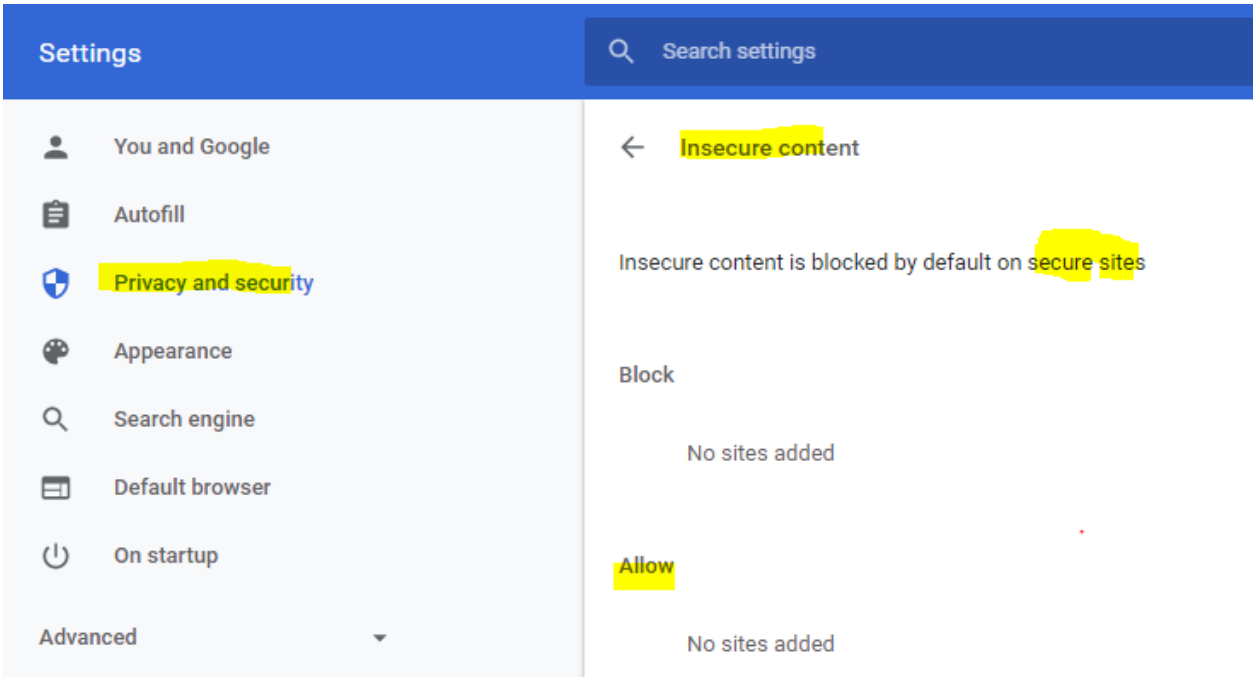


- If you find any errors, those need to be resolved and re-run export metadata again and make sure you are not encountered with any errors.

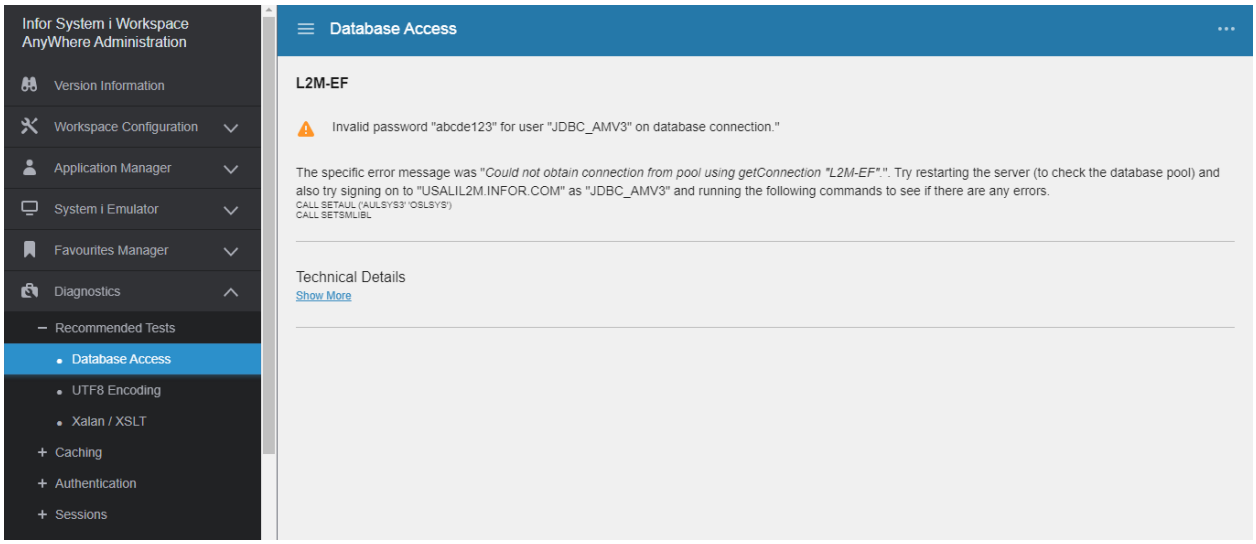
2 If you encounter with “Language Code is not defined” error, you need to cross check and update language code in SIM console.



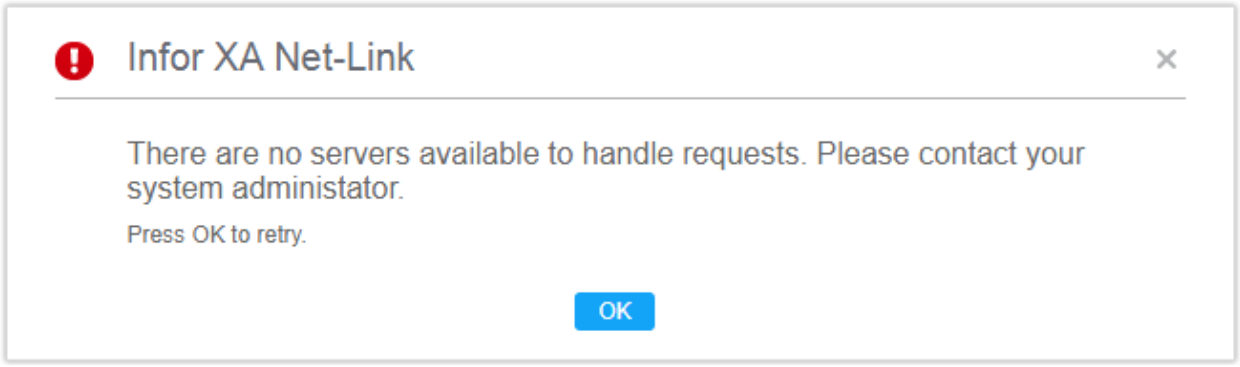
1 When you try to open any business object from IDF using SIWA, if it displays a blank page, you need to add the SIWA URL to the insecure content and try to relaunch the application.

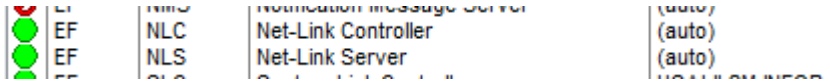


1 Restart the server SIWA application installed server if this issue appears and recheck the Database access under diagnosis in SIWA admin page.



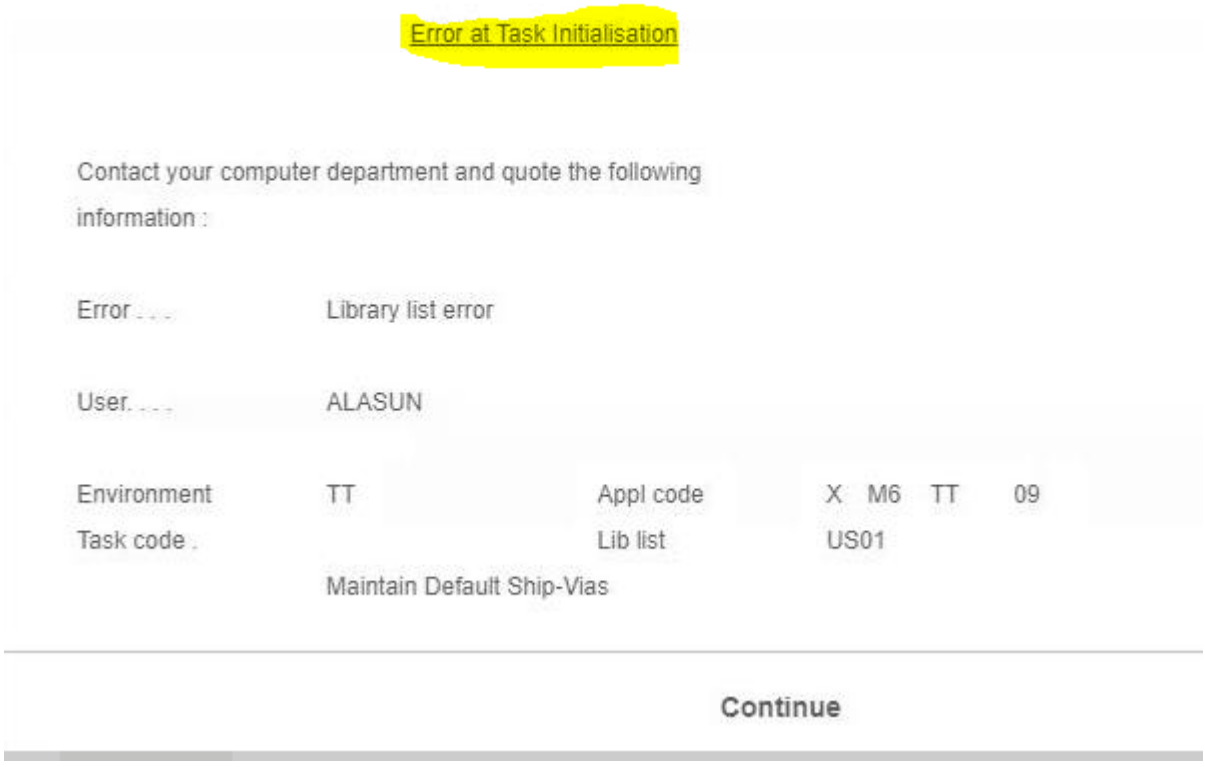
2 If you receive this request, cross check the NLS and NLC processes are in active state or not, if not start the processes.

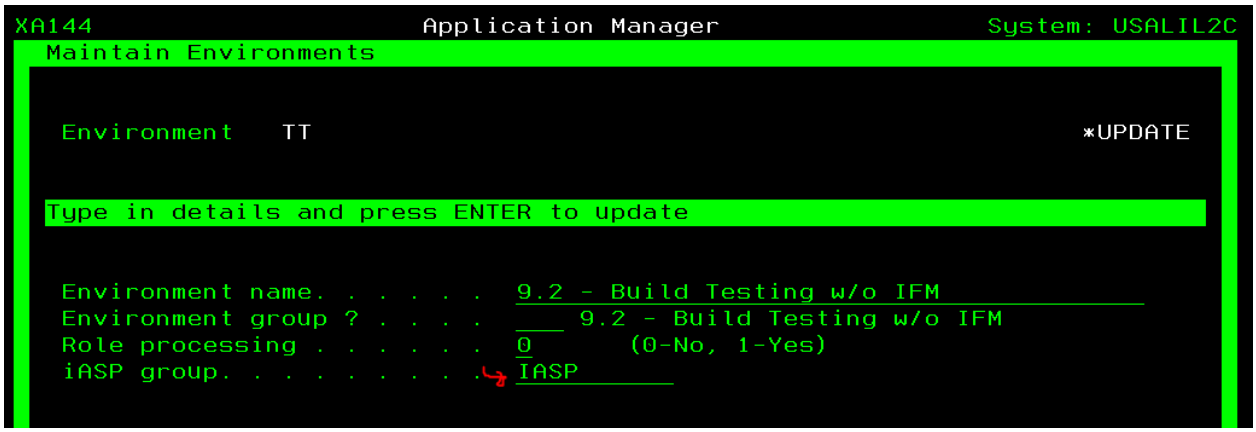




1 If you face issue, as displayed, when launching L1 tasks, check the whether the environment is pointing to correct iASP group or not by navigating to this path in System Manager Console.

STRM400 → **Application Manager → Maintain Environments**

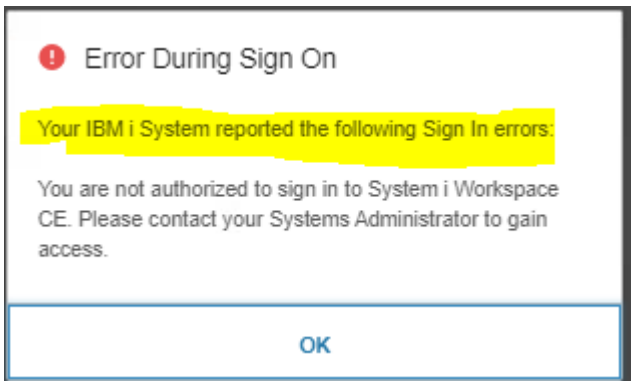




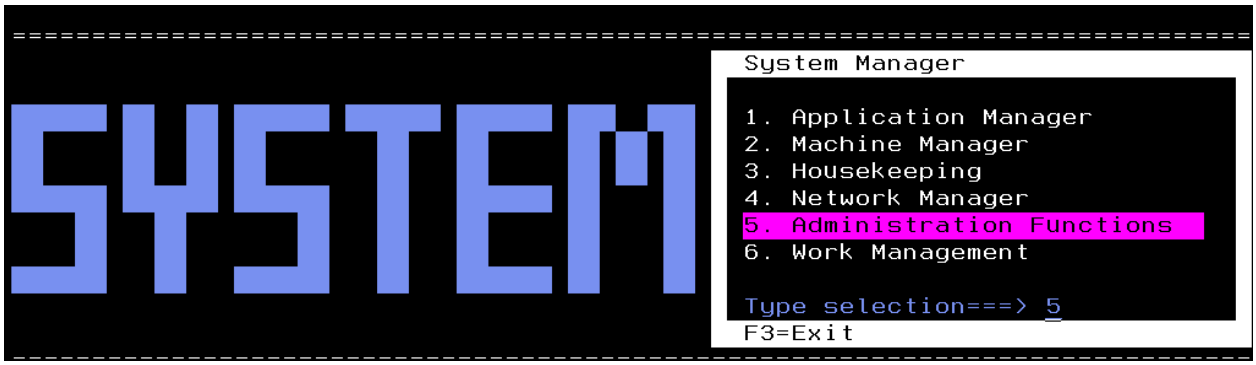
1 Due to maintenance activities in weekends and holidays, SiW and Net-Link related Http and Application servers in "*IBMi Web Administration Console*" goes down similar to XA servers in Link Manager. You need to check and start them if you face any issues while launching SiWA application.

2 To Secure the Net-Link and launch the SiWA application in Infor OS, 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 without securing Net-Link.

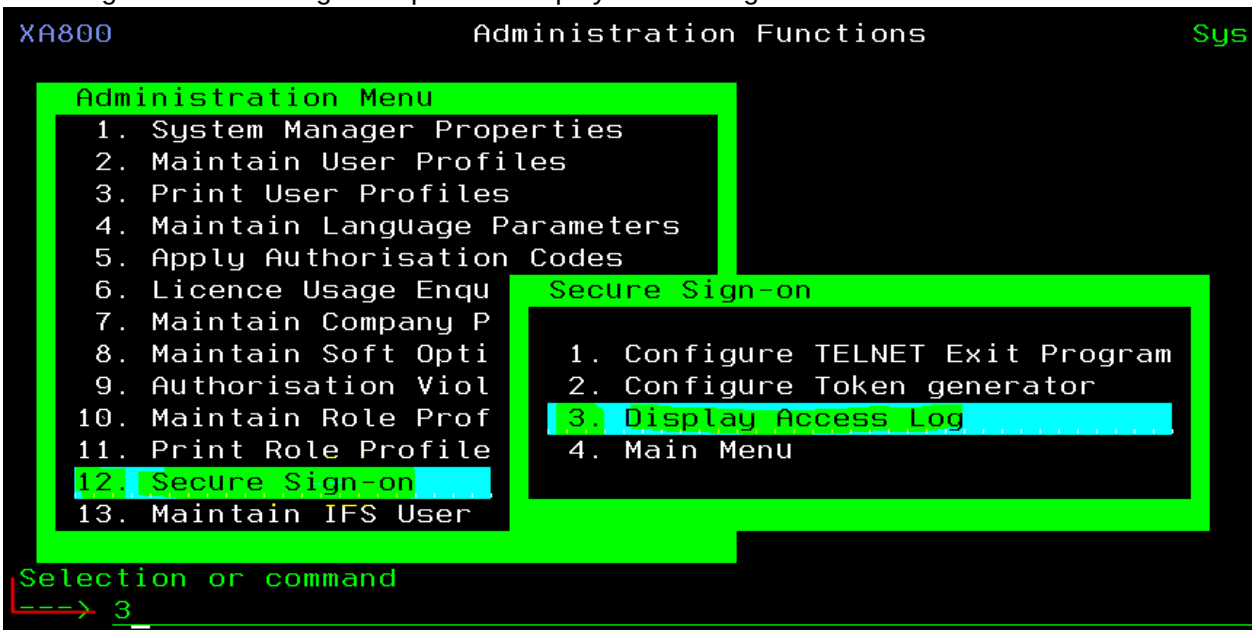
3 If the the client system is getting blocked at System Manager(SIM) or if you are facing below error while accessing SIWA environments with or without SSO, you have to add the IPv4 address of the client system in the allowed clients at SIM.



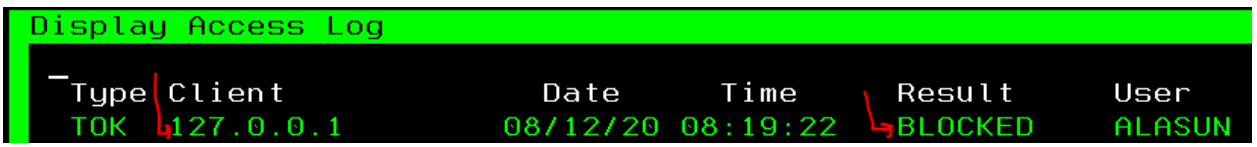
- Navigate to STRM400 → Administration Functions



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

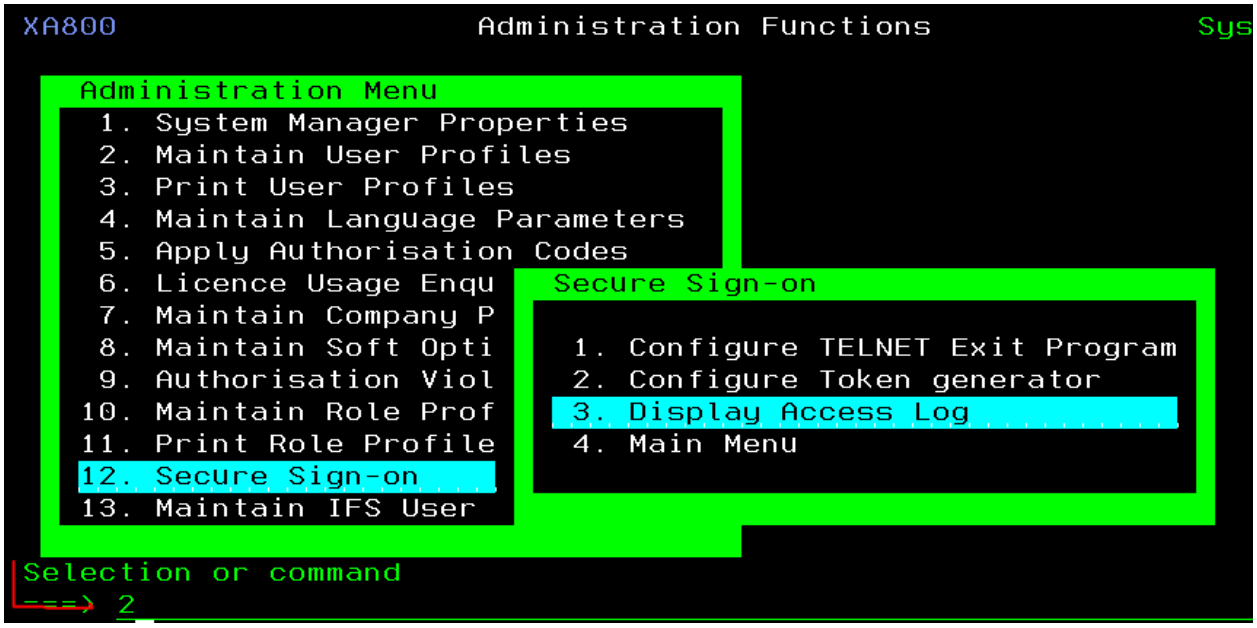


- Identify and copy the client IPv4 address with result as blocked, as displayed.
  For example: 127.0.0.1

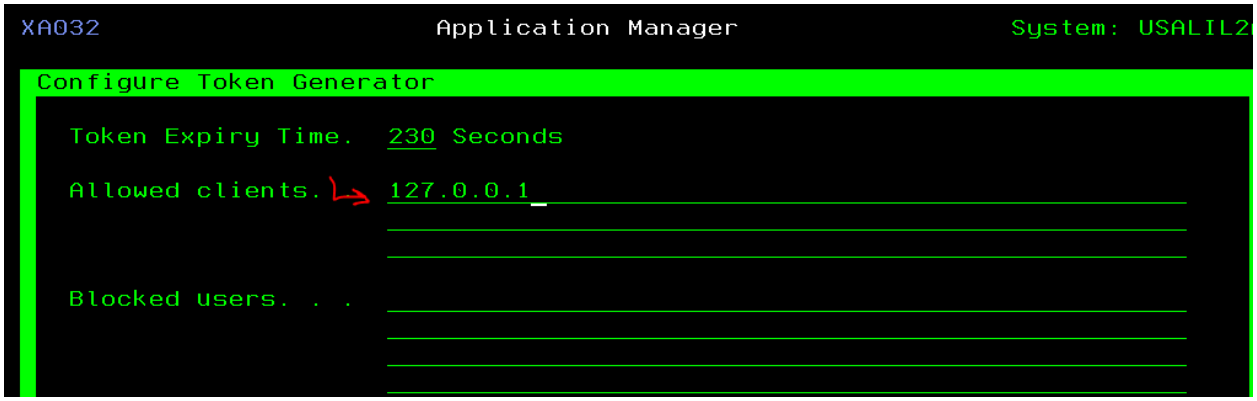


- Take F3 to exit.

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

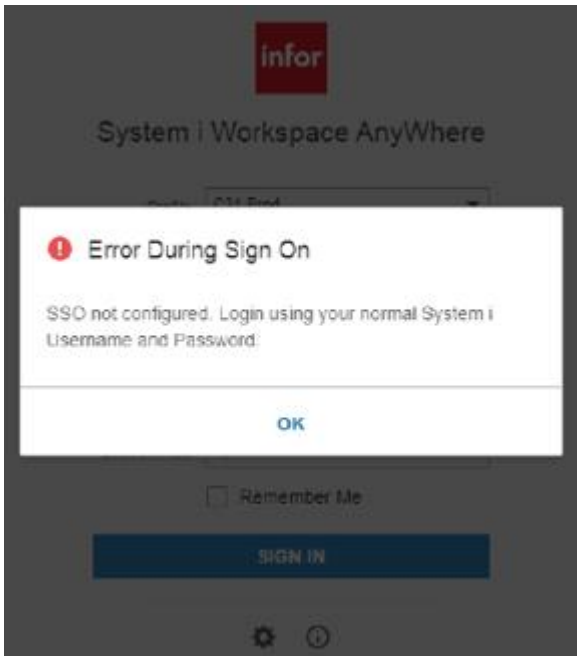


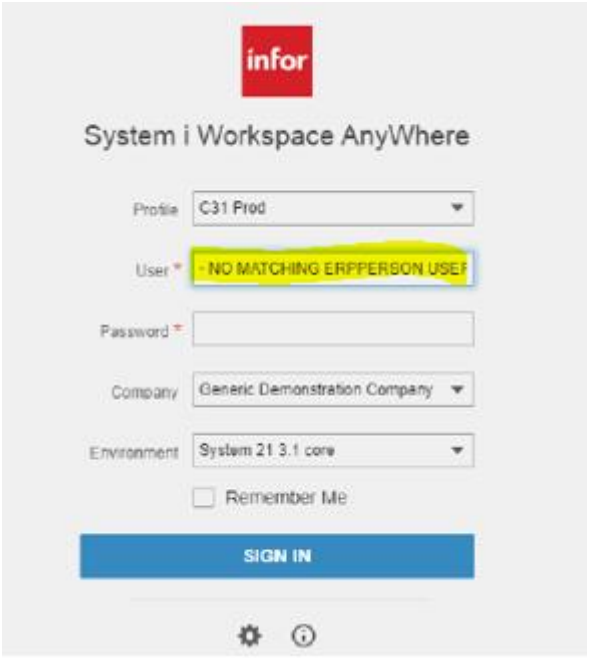
- Update the Client IPv4 address at Allowed clients, as displayed.



- Press F8 to Update.
- Press F3 to Exit.

1 If, on launching the XA application from InforOS, you see either a blank screen or one, or both, of these screens.

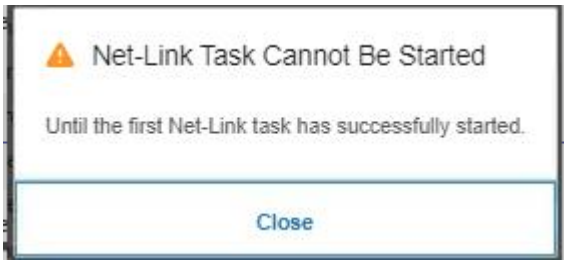




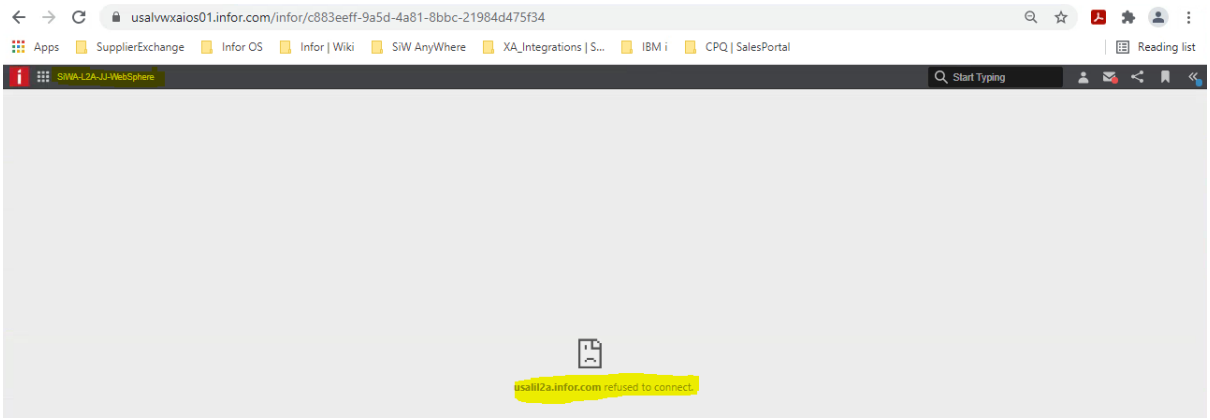
Then Single Sign-On (SSO) is not correctly configured in InforOS, System Manager, System i Workspace AnyWhere, or all three.

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.

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

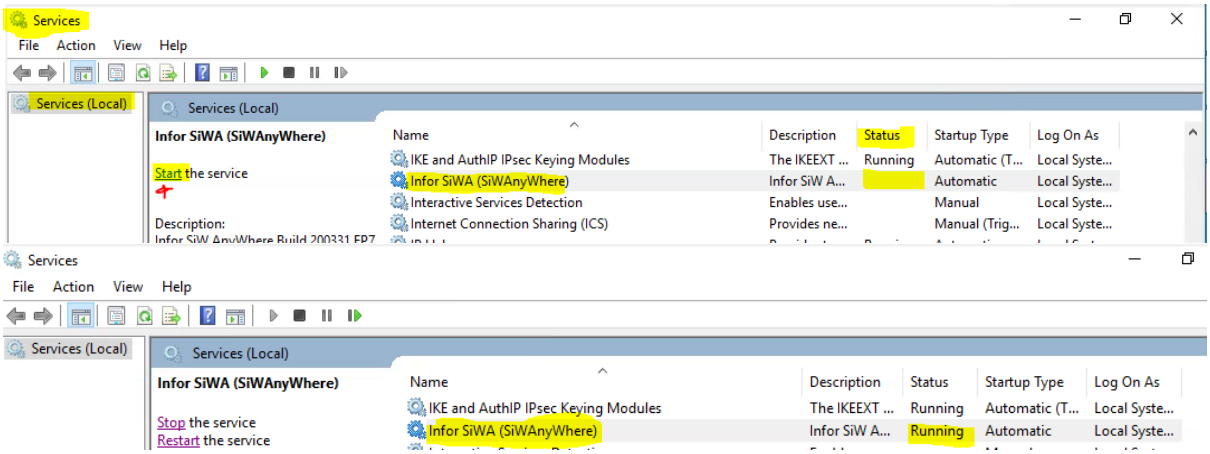


1 If you encounter with an error "***abc.infor.com refused to connect***", shown as below, where **abc** is SiWA installed server hostname.



For SiWA with Microsoft Windows deployment:

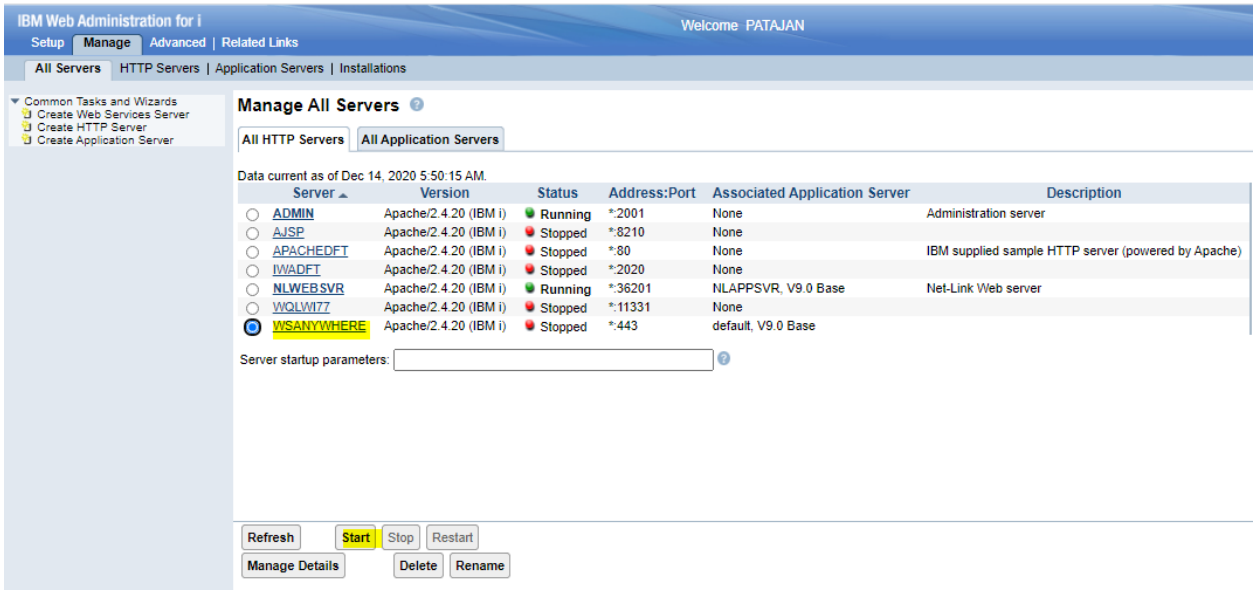
- Login to the SiWA installed server with an admin privileges, and from windows search open ***services***, check if the ***Infor SiWA (SiWAnyWhere)*** service is in Running status or not. If not, start the service by clicking on ***Start*** the service, shown as below.

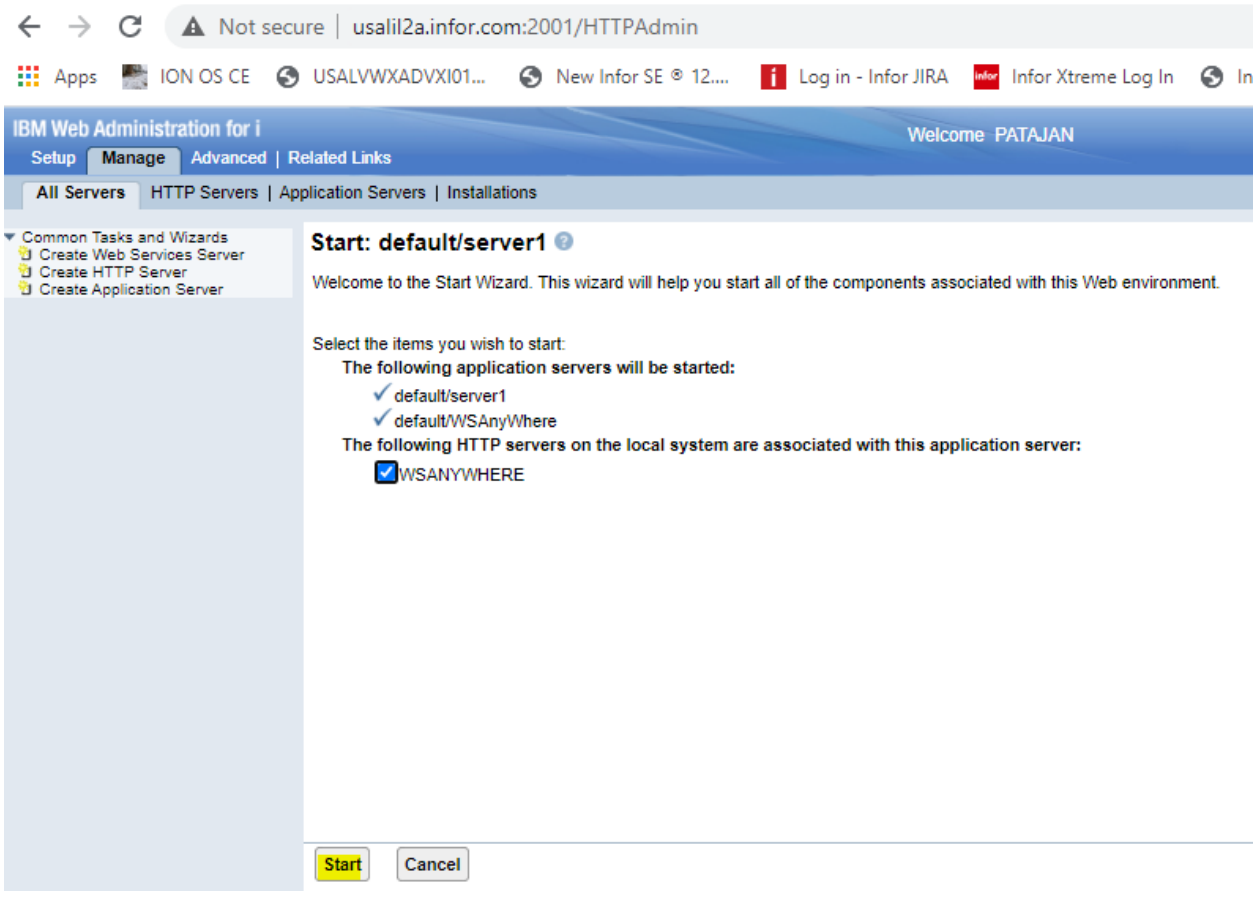


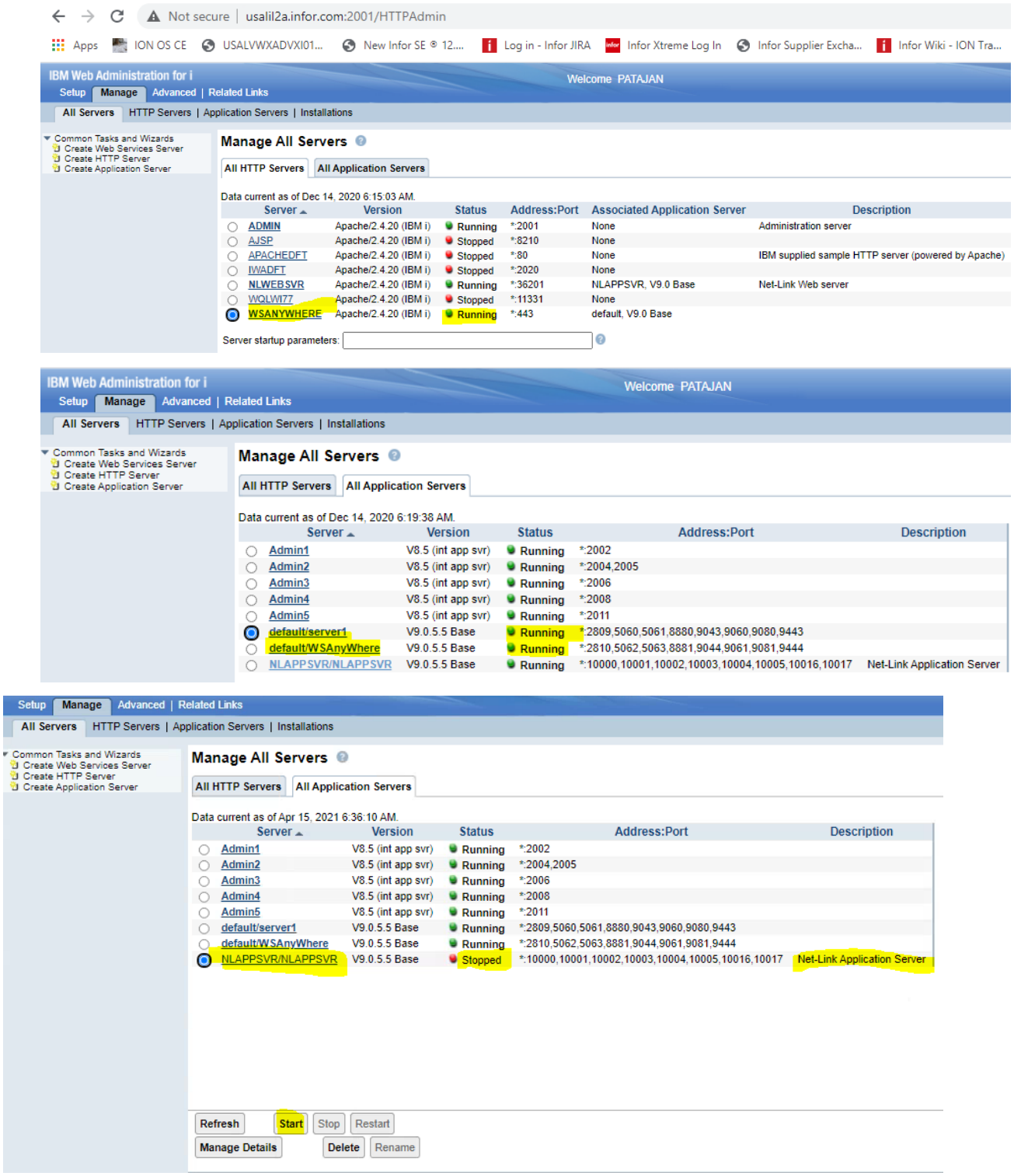
For SiWA with an IBMi deployment:

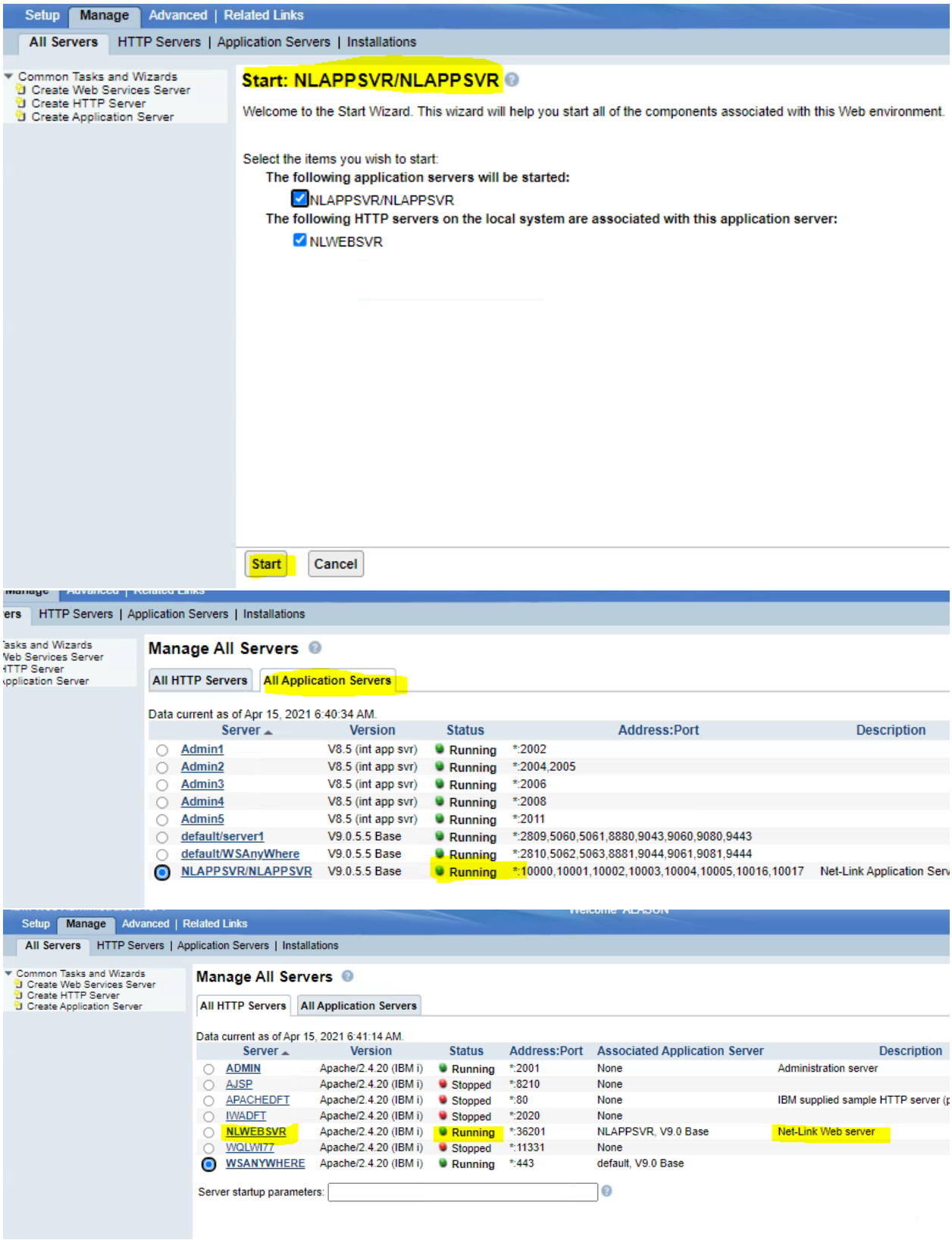
- Login to IBM Web Administration console and check if the HTTP & Application servers related to SiWA WebSphere and Net-Link are in ***Running*** status or not. If not, start both the SiWA WebSphere and Net-Link server instances, shown as below.

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

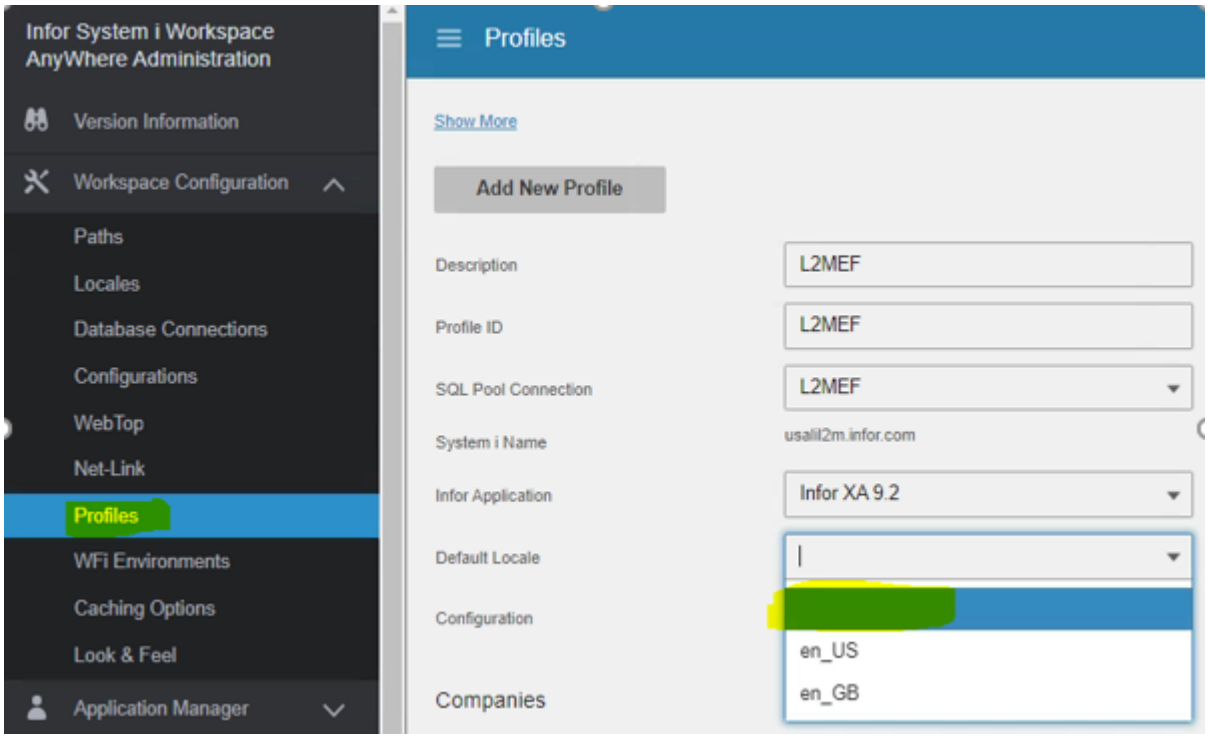


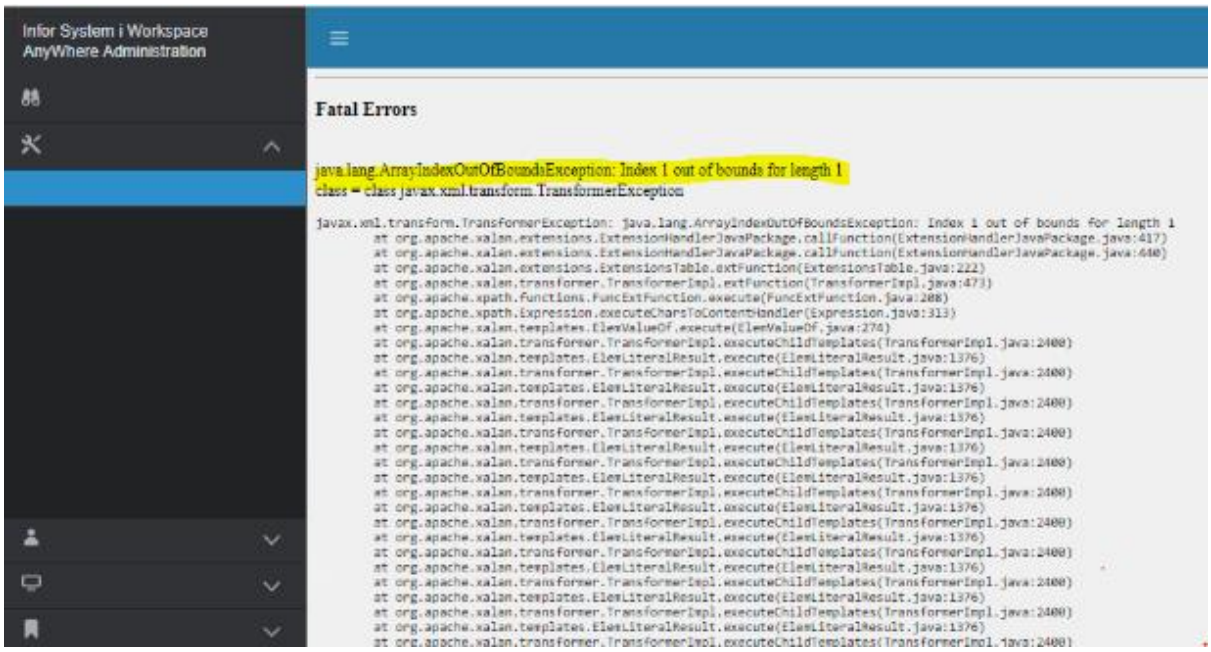



Not secure | usalil2a.infor.com:2001/HTTPAdmin
Apps
ION OS CE
USALVWXADVXI01...
New Infor SE ® 12....
Log in - Infor JIRA
Infor Xtreme Log In
Infor Supplier Excha...
Infor Wiki - ION Tra...
IBM Web Administration for i
Welcome PATAJAN
Setup
Manage
Advanced | Related Links
All Servers
HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Manage All Servers
All HTTP Servers
All Application Servers
Data current as of Dec 14, 2020 6:15:03 AM.
Server
Version
Status
Address:Port
Associated Application Server
Description
ADMIN Apache/2.4.20 (IBM i) Running *:2001 None Administration server
AJSP Apache/2.4.20 (IBM i) Stopped *:8210 None
APACHEDFT Apache/2.4.20 (IBM i) Stopped *:80 None IBM supplied sample HTTP server (powered by Apache)
IWADFT Apache/2.4.20 (IBM i) Stopped *:2020 None
NLWEBSVR Apache/2.4.20 (IBM i) Running *:36201 NLAPPSVR, V9.0 Base Net-Link Web server
WQLWI77 Apache/2.4.20 (IBM i) Stopped *:11331 None
WSANYWHERE Apache/2.4.20 (IBM i) Running *:443 default, V9.0 Base
Server startup parameters:
IBM Web Administration for i
Welcome PATAJAN
Setup
Manage
Advanced | Related Links
All Servers
HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Manage All Servers
All HTTP Servers
All Application Servers
Data current as of Dec 14, 2020 6:19:38 AM.
Server
Version
Status
Address:Port
Description
Admin1 V8.5 (int app svr) Running *:2002
Admin2 V8.5 (int app svr) Running *:2004,2005
Admin3 V8.5 (int app svr) Running *:2006
Admin4 V8.5 (int app svr) Running *:2008
Admin5 V8.5 (int app svr) Running *:2011
default/server1 V9.0.5.5 Base Running *:2809,5060,5061,8880,9043,9060,9080,9443
default/WSAnyWhere V9.0.5.5 Base Running *:2810,5062,5063,8881,9044,9061,9081,9444
NLAPPSVR/NLAPPSVR V9.0.5.5 Base Running *:10000,10001,10002,10003,10004,10005,10016,10017 Net-Link Application Server
Setup
Manage
Advanced | Related Links
All Servers
HTTP Servers | Application Servers | Installations
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
Manage All Servers
All HTTP Servers
All Application Servers
Data current as of Apr 15, 2021 6:36:10 AM.
Server
Version
Status
Address:Port
Description
Admin1 V8.5 (int app svr) Running *:2002
Admin2 V8.5 (int app svr) Running *:2004,2005
Admin3 V8.5 (int app svr) Running *:2006
Admin4 V8.5 (int app svr) Running *:2008
Admin5 V8.5 (int app svr) Running *:2011
default/server1 V9.0.5.5 Base Running *:2809,5060,5061,8880,9043,9060,9080,9443
default/WSAnyWhere V9.0.5.5 Base Running *:2810,5062,5063,8881,9044,9061,9081,9444
NLAPPSVR/NLAPPSVR V9.0.5.5 Base Stopped *:10000,10001,10002,10003,10004,10005,10016,10017 Net-Link Application Server
Refresh
Start
Stop
Restart
Manage Details
Delete
Rename



1 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.

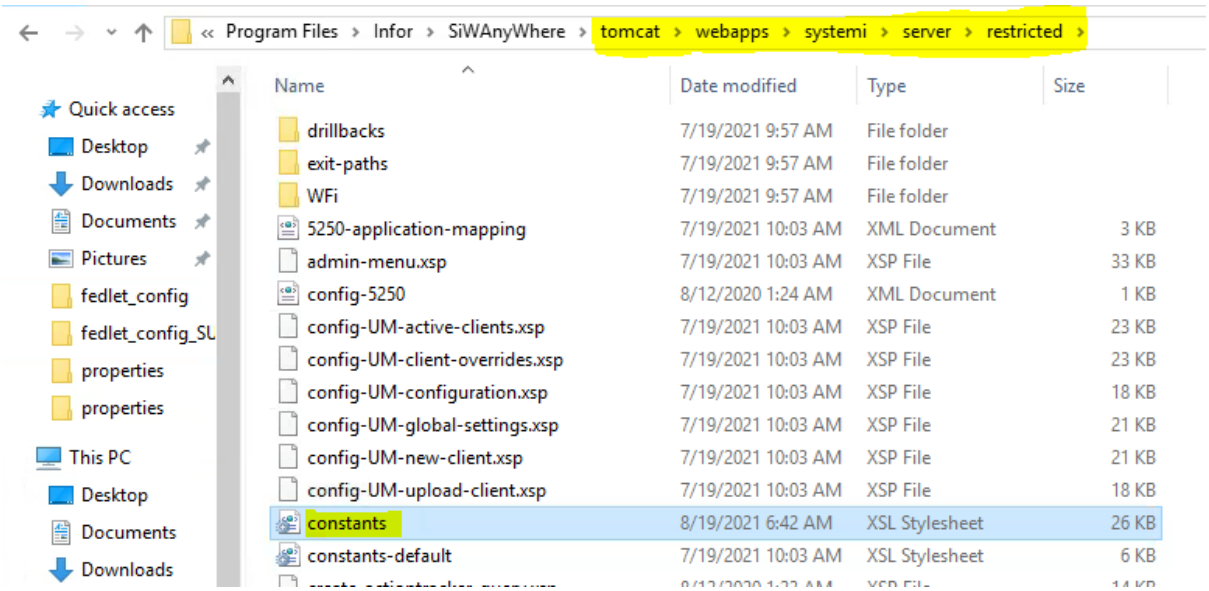




To resolve the issue, please follow the below steps:

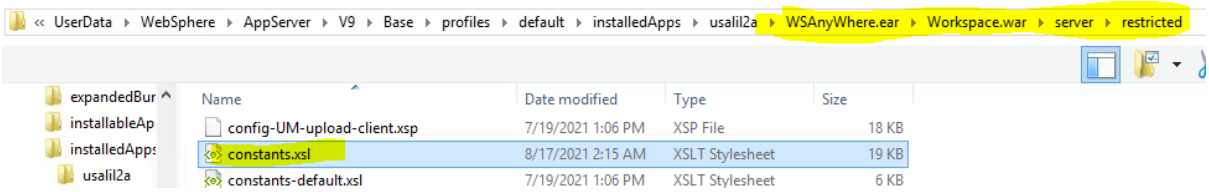
- Navigate and open the *"constants.xsl"* file, shown as below:

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



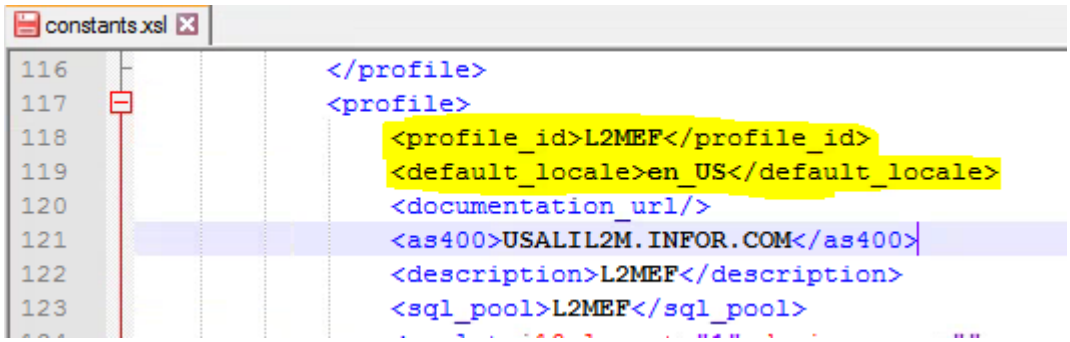
For SIWA WebSpere, it is located in *restricted* folder under:

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

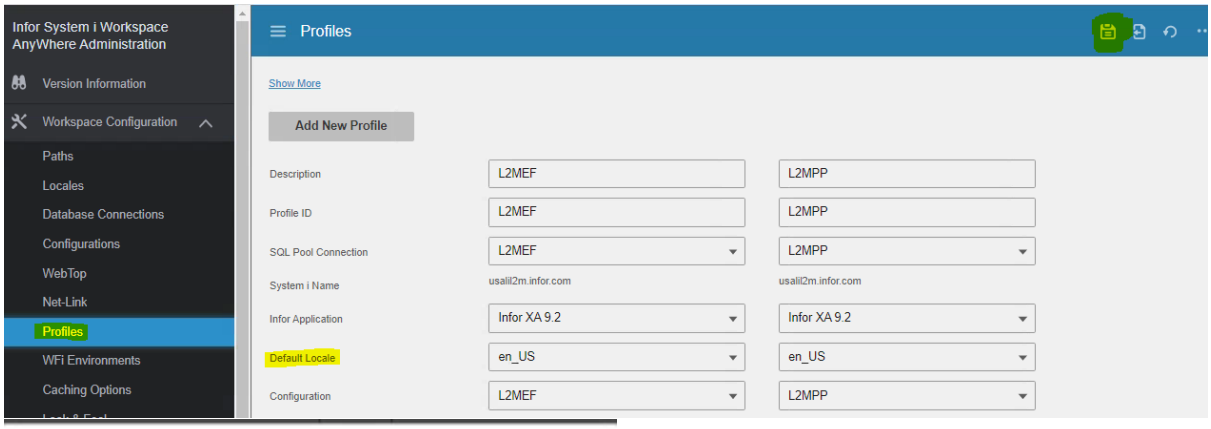


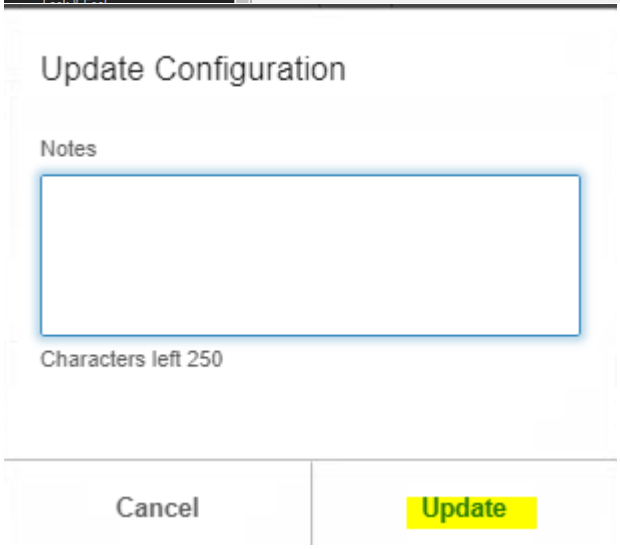
- Navigate to ***default_locale*** element for the respective ***profile*** and observe that value would be empty space, shown as below:

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



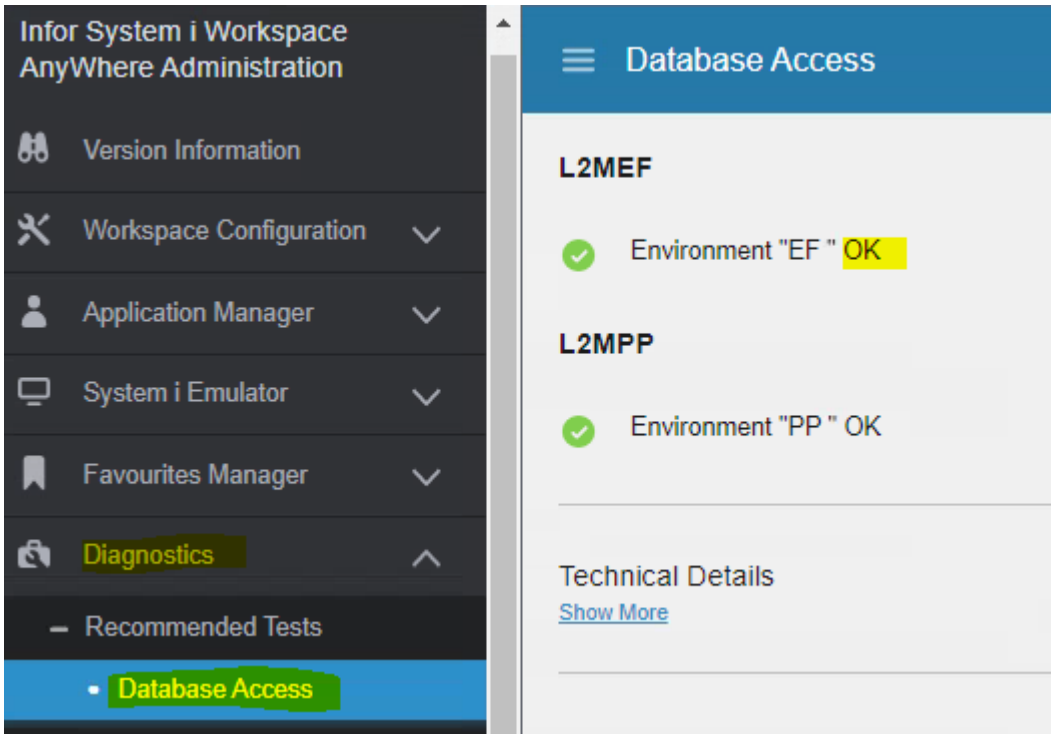
- In SIWA Admin page, navigate to Profiles and click on Save icon and then Update, shown as below.





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 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 F 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

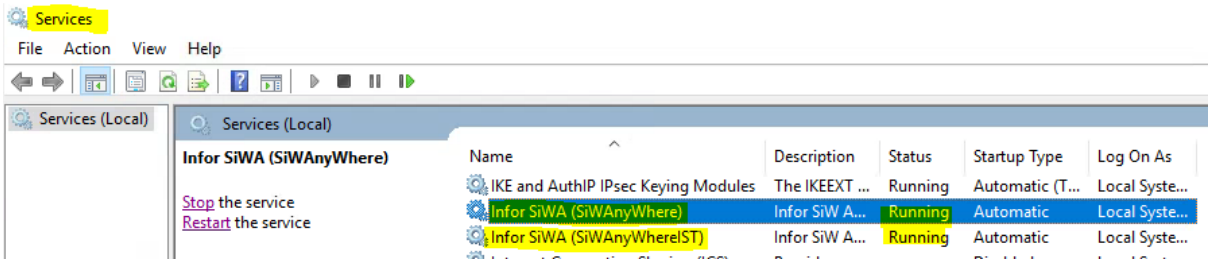
<Context sessionCookieName="JSESSIONID_{environmentID}">

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

context.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
  Licensed to the Apache Software Foundation (ASF) under one or more
  contributor license agreements.  See the NOTICE file distributed with
  this work for additional information regarding copyright ownership.
  The ASF licenses this file to You under the Apache License, Version 2.0
  (the "License"); you may not use this file except in compliance with
  the License.  You may obtain a copy of the License at

      http://www.apache.org/licenses/LICENSE-2.0

  Unless required by applicable law or agreed to in writing, software
  distributed under the License is distributed on an "AS IS" BASIS,
  WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
  See the License for the specific language governing permissions and
  limitations under the License.
-->
<!-- The contents of this file will be loaded for each web application -->
<Context sessionCookieName="JSESSIONID_L2MEG">

    <!-- Default set of monitored resources. If one of these changes, the    -->
    <!-- web application will be reloaded.                                   -->
    <WatchedResource>WEB-INF/web.xml</WatchedResource>
    <WatchedResource>WEB-INF/tomcat-web.xml</WatchedResource>
    <WatchedResource>${catalina.base}/conf/web.xml</WatchedResource>

    <!-- Uncomment this to disable session persistence across Tomcat restarts -->
    <!--
```

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



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

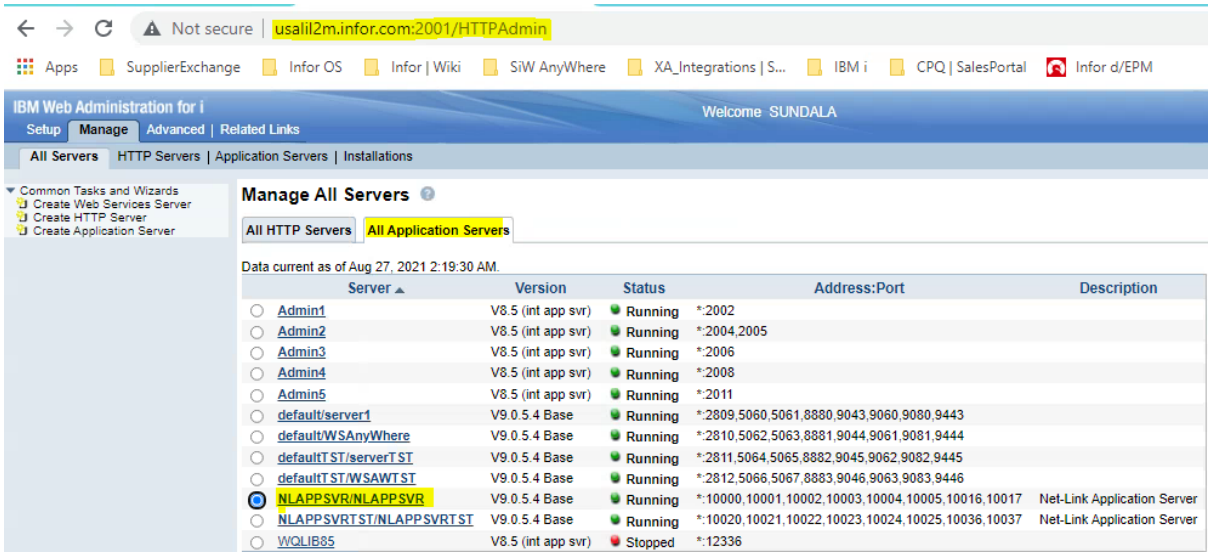
If you want to install and run multiple instances of SiW AnyWhere WebSphere in a single IBMi server using unique ports for each individual installation, please follow the below additional settings for each SiW AnyWhere installations:

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:

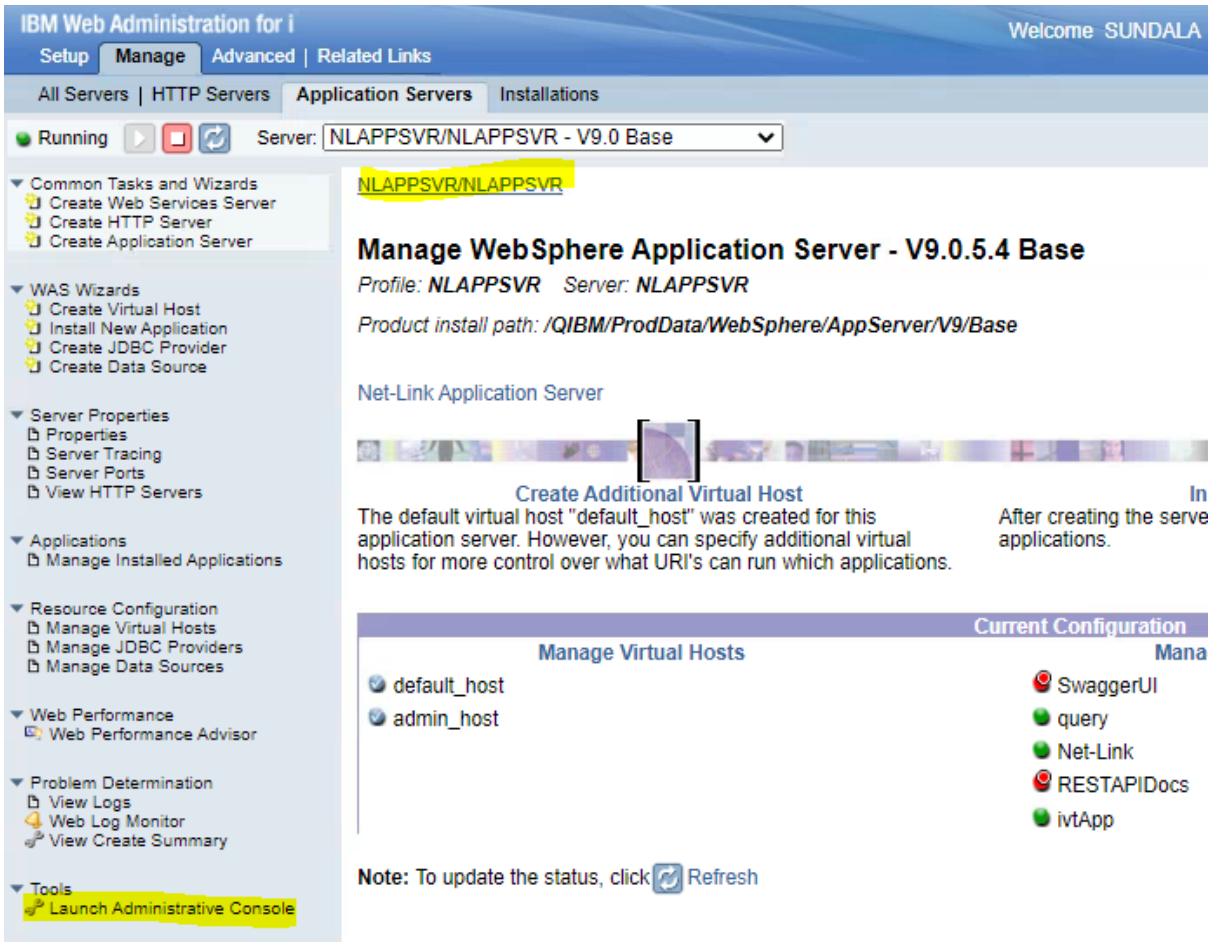
http://<hostname>:2001/HTTPAdmin

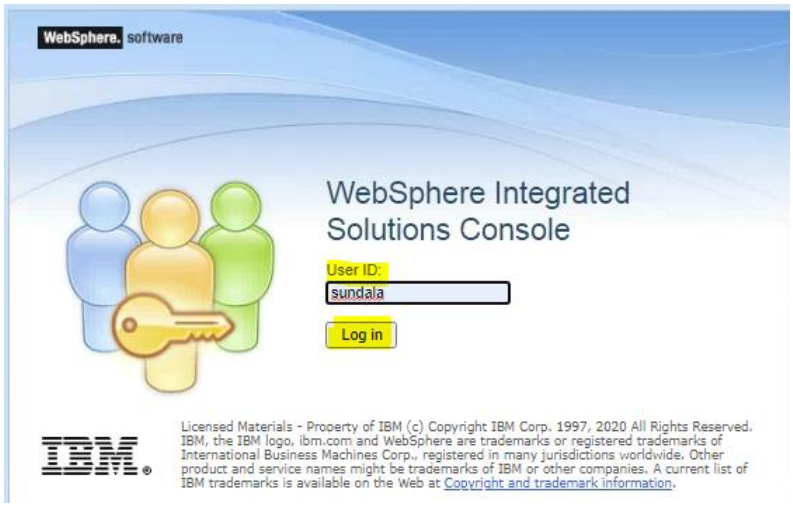
where <hostname> is FQDN of IBMi server

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

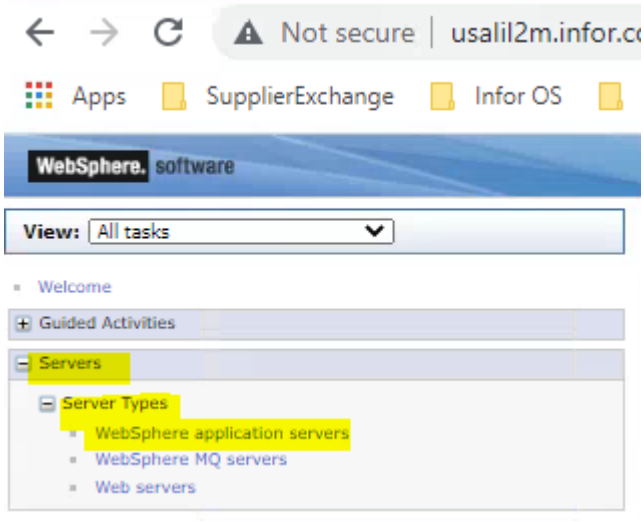


1 Launch the IBM WebSphere Administrative Console to make configuration changes, shown as below:



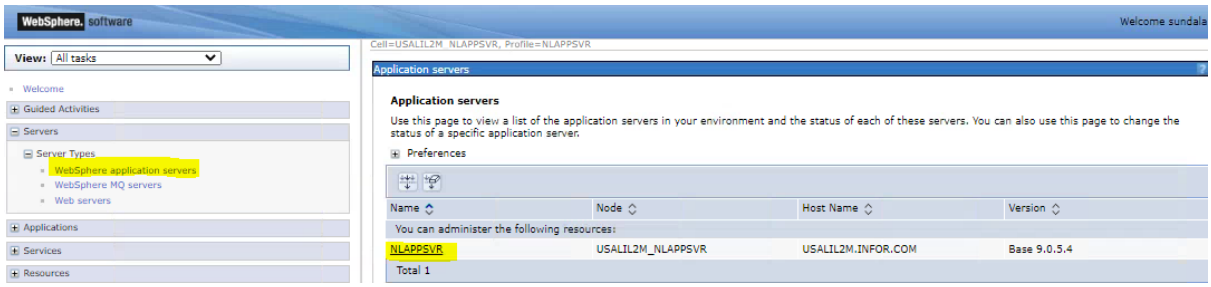


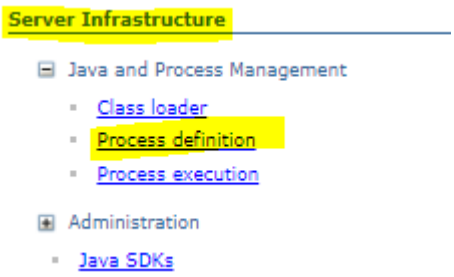
1 From the menus on the left-hand side, select **Servers** > **Server Types** > **WebSphere Application Servers**

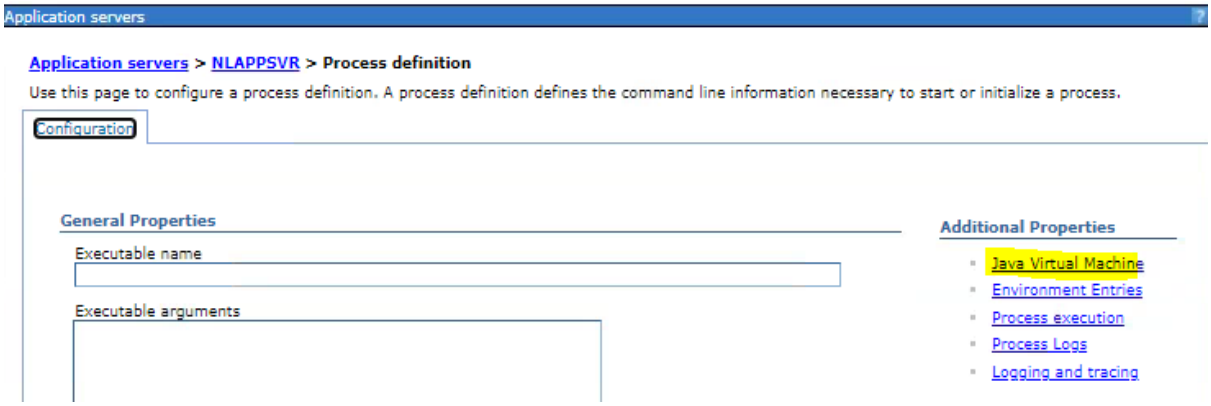


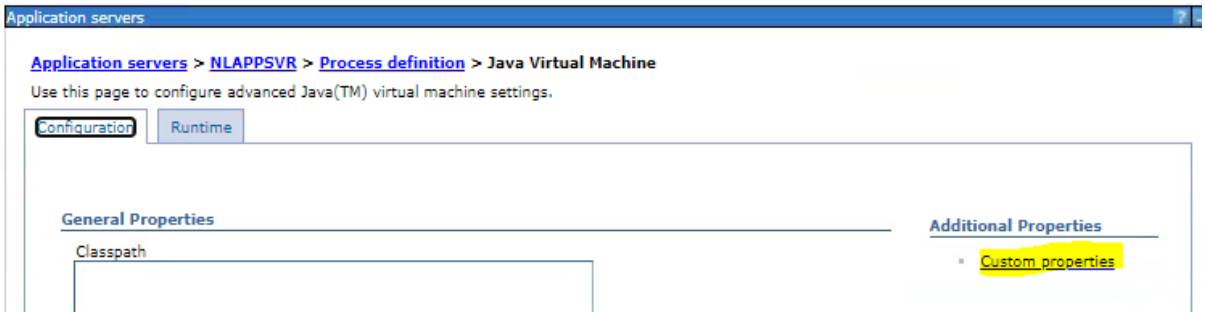
1 Click on the Net-Link configured WebSphere Application server and then navigate to

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

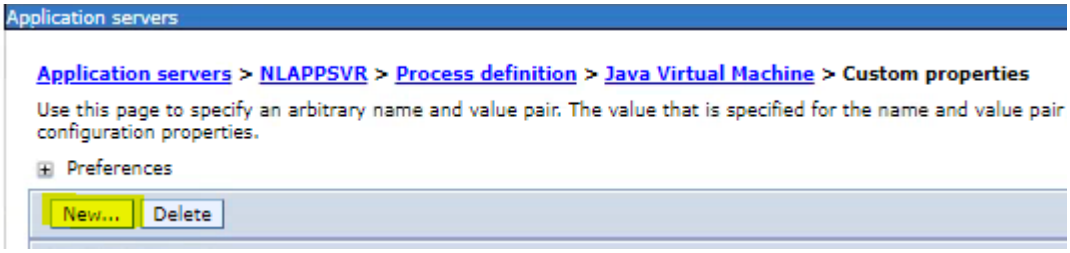




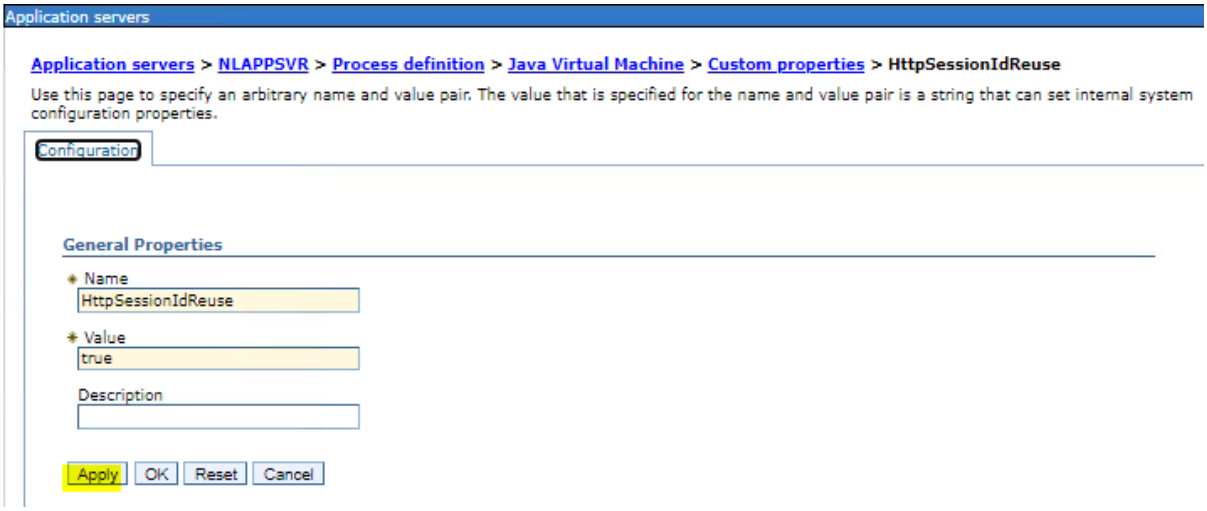




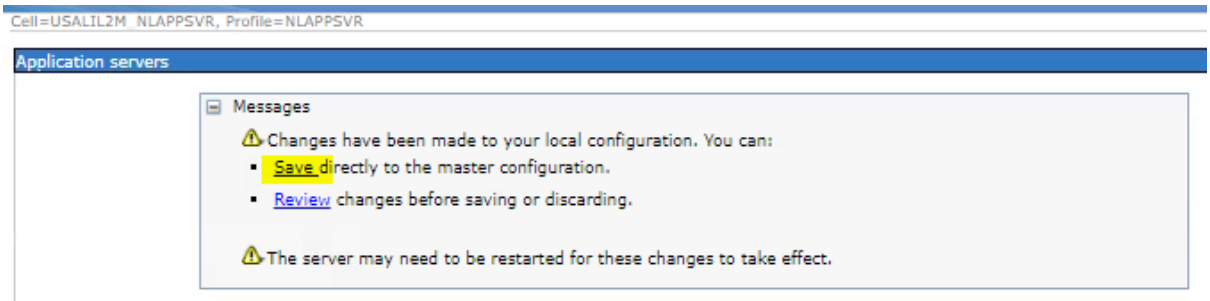
1) Click on **New** and add a new Custom Property for the JVM to reuse the sessionId, shown as below:

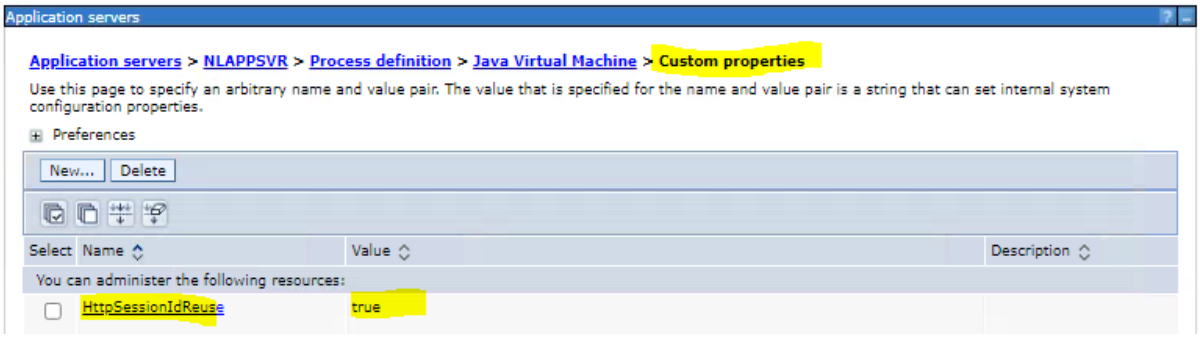


Use System Property Name: ***HttpSessionIdReuse*** and System Property Value: ***true***



2) Save your changes and restart the Application Server.



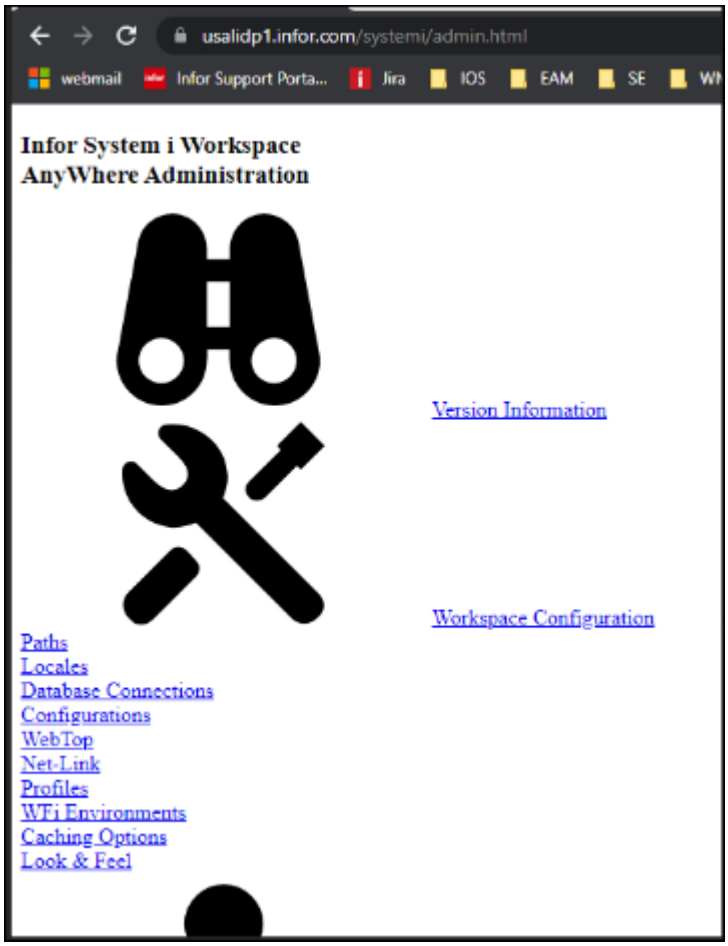


Note: SSO cannot be implemented for the second instance of SiWA, as we are using single WebSphere for 2 SiWA. This is a limitation,

Appendix H 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.

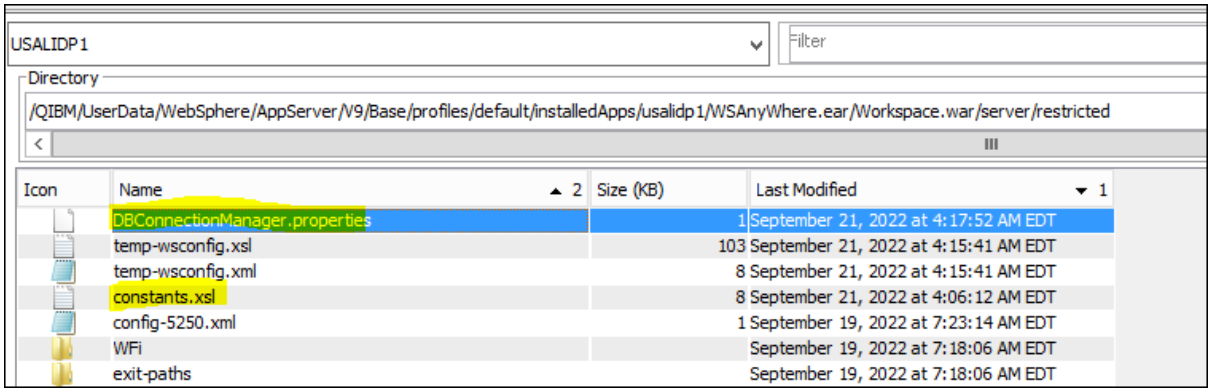
Though the previous SiWA installation is deleted on WebSphere or Tomcat, the previous installation data will be stored in IBMi server and same old configuration might be re-used in new installation due to using same User Key.

IBMi Deployment:

Go to below folder in IFS.

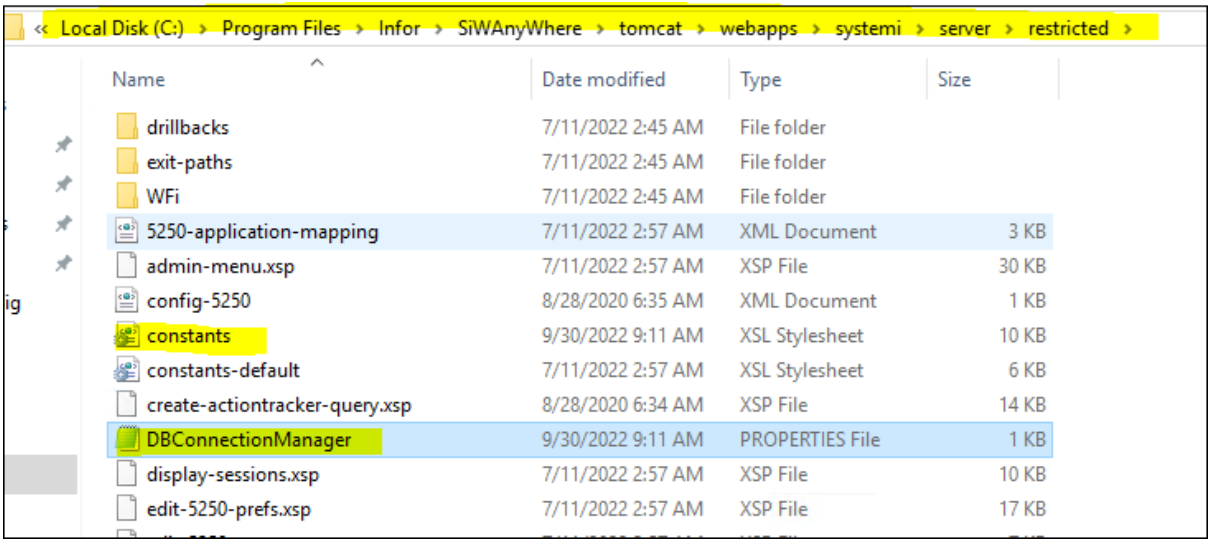
/QIBM/UserData/WebSphere/AppServer/V9/Base/profiles/<ProfileName>/installedApps/<NodeName>/WSAnyWhere.ear/Workspace.war/server/restricted

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



Windows Deployment:

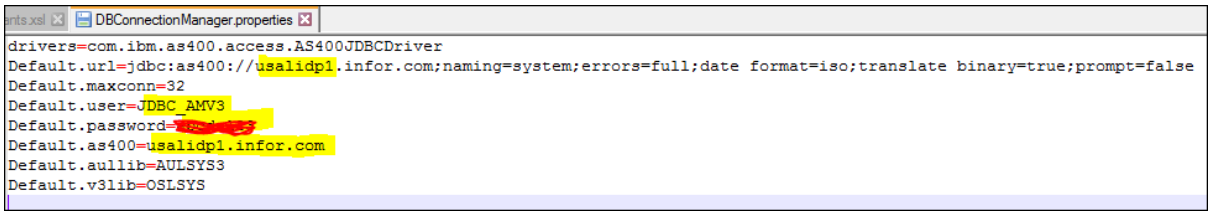
Go to SiWA Tomcat installation folder, tomcat -> webapps -> systemi -> server - > restricted folder.



For example validate below details in constants.xsl file:

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

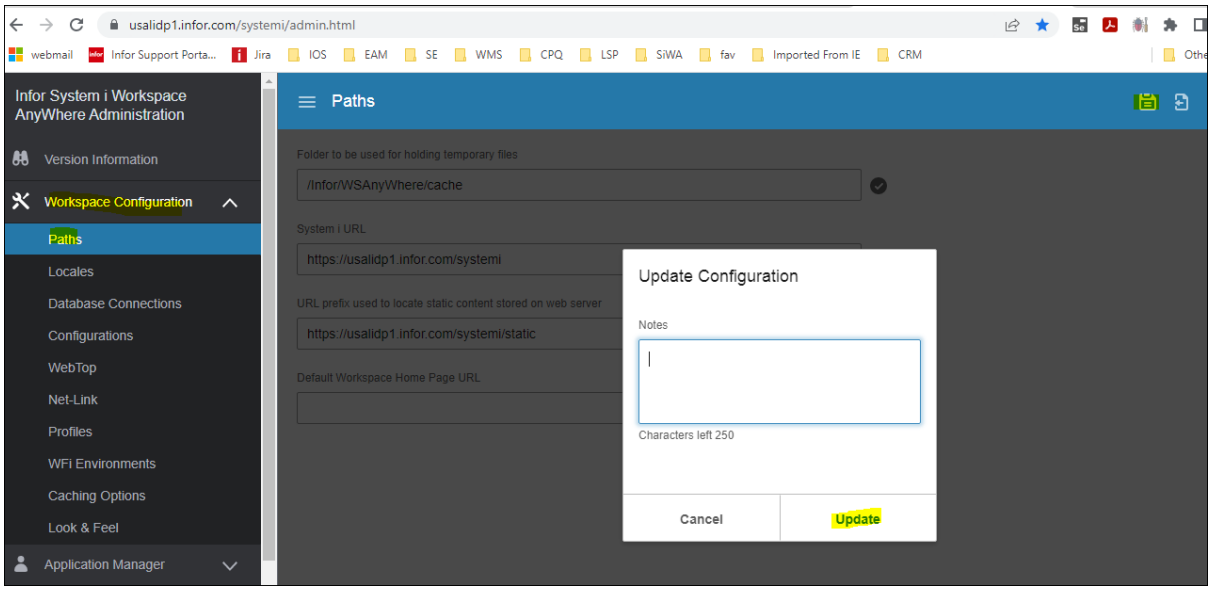
For example validate below details in DBConnectionManager.properties file.



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.