Setup Guide for Secure Net-Link

Release 10

Publication Information

Release: Infor XA 9.2 & 10

Publication date: July 25, 2022

Contents

About this guide

This document describes the process to set up a secure Net-Link. The guide explains the requirements, WAR file deployment and configuration tasks.

Revision History

This table shows the chapters of the guide:

Version	Date	Author	Comments
0.1	14/Jun/2017	Michael Dillon	Initial Draft
0.2	11/Apr/2019	Singaravizhiyan R	Added Building WAR file and Workspace Net-Link URL configuration
1.0	10/16/2020	Development	WebSphere 9.x Configuration
2.0	06/19/2021	Development	WAR file redeployment
3.0	04/13/2022	Jany Khan Patan	IDFIONAPI WAR file deployment in WebSphere

Related documents

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

Contacting Infor

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

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

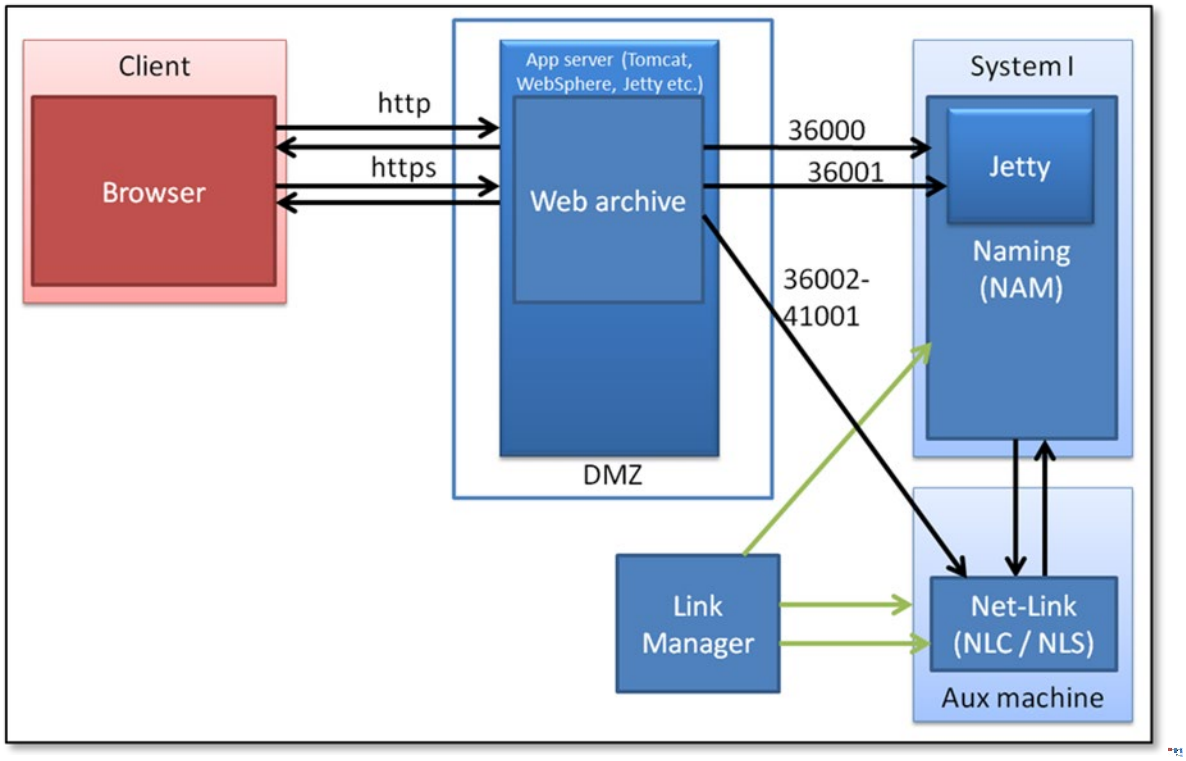
If you have comments about Infor documentation, contact documentation@infor.com.

Net-Link WAR file deployment

The standard installation process involves accessing the Net-Link through a URL to the IBMi due to which users are confined to a secure network. However, in some circumstances it is necessary to provide access to the users outside of the network. Although the platform is secure, and can be protected via firewall settings, connecting directly to IBMi from the web is not recommended.

Therefore, it is necessary to expose the Net-Link web server components to the web.

An example topology of the IDF components used for Net-Link in a container deployment scenario: The default ports used by IDF for http and https are typically 80 and 443 respectively.



The web components of Net-Link runs in a Servlet container. Examples of such a container are Apache Tomcat and IBM WebSphere. The components are packaged into a Web Archive (WAR)file.

Note: The container used for Systemi Workspace can also be used. This document explains how to obtain the WAR file, and to deploy it to these servers.

Fully Qualified Domain Names

For a Microsoft Windows deployment, we recommend that the Windows Server has a Fully Qualified Domain Name (FQDN) that can be used to address the Windows Server, both externally and internally (i.e. the Windows Server knows itself by this FQDN) within your enterprise.

For either a Microsoft Windows or IBMi deployment, we recommend that the IBMi server also has a FQDN that it can be used to address the Windows Server, both externally and internally (i.e. the IBMi knows itself by this FQDN) within your enterprise.

It is important to have FQDNs in place before you install System i Workspace, otherwise, the URL paths, SSL configuration and other settings created during the installation may be incorrect and cause failures when trying to access or use System i Workspace.

WAR file generation

The WAR file contains configuration details to communicate with the IBMi. Therefore, the file cannot be shipped with the IDF as a component. The file contains components that can change during the builds of IDF. Therefore, it is important to refresh the WAR file when a new build is applied to the global IDF environment.

Generate WAR file in XA R92

The current WAR file can be obtained by navigating to the URL http://{server}:{port}/NetLink/NetLink.war.

Caution: The URL is similar to the link used to access Net-Link.

Note:

- An alternative mechanism to obtain the WAR file has been created in XA R10 release. Previously, the war file was generated and downloaded from the server via the URL, as discussed above.
- This still works but as the war file is generated from global the contents are therefore at the build level that is current for the global environment. A new URL has been created that generates it from the environment (and at the build level of the environment)

  Error! Hyperlink reference not valid.

Generate WAR file in XA R10

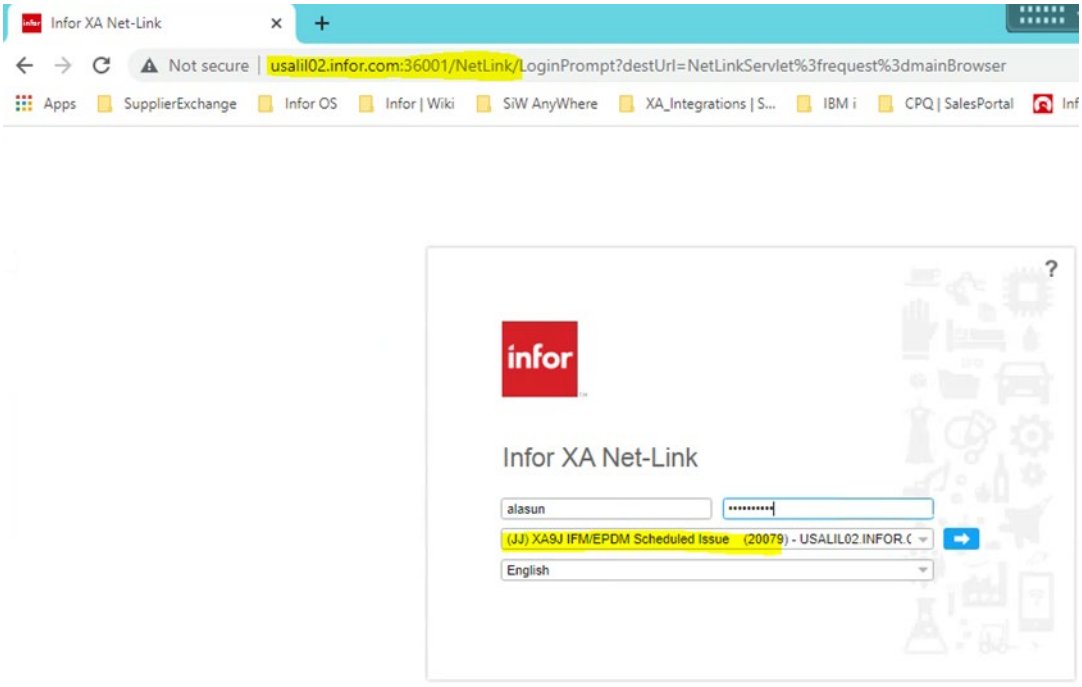
1 The user must be signed in to Net-Link for the environment that has the correct build.

2 Navigate to **Error! Hyperlink reference not valid.**

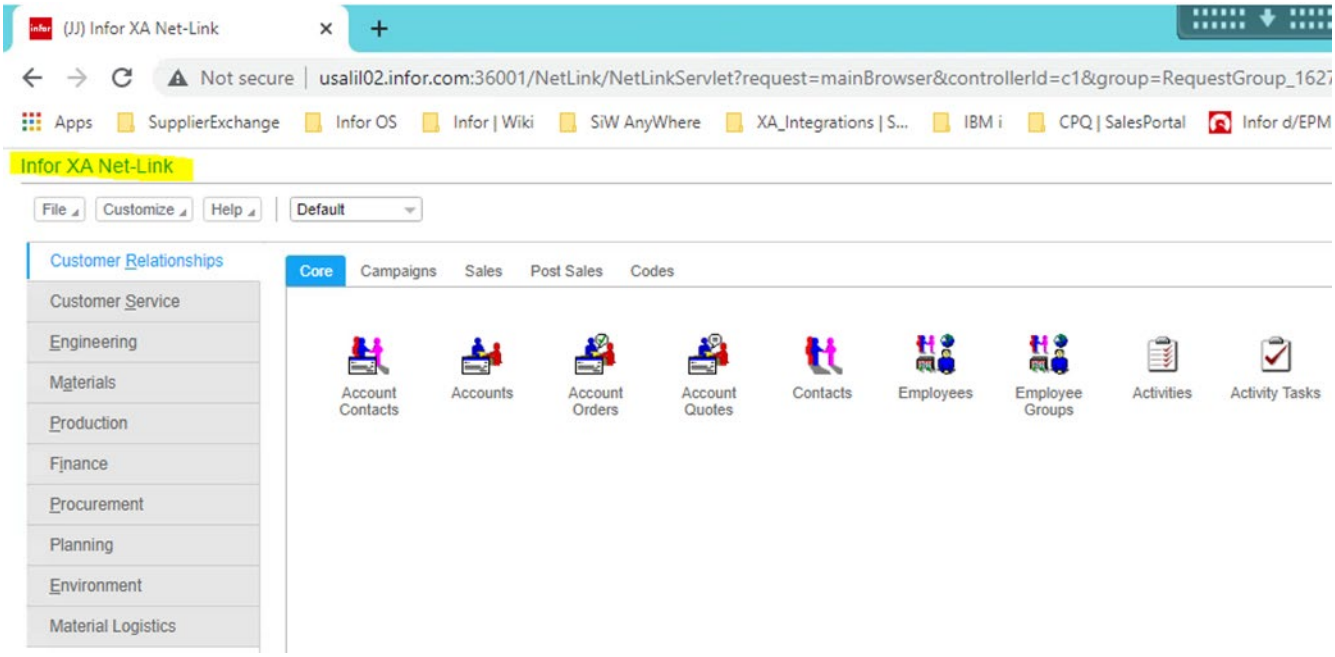
  where {server}, is the name of the IBMi which hosts IDF, and {port} is the port used for access to IDF components over HTTP.

  (For example: http://usalil02.infor.com:36001/NetLink/)

3 The Net-Link login prompt should be shown as below, then Sign into Net-Link for the correct environment using respective IBMi userID.



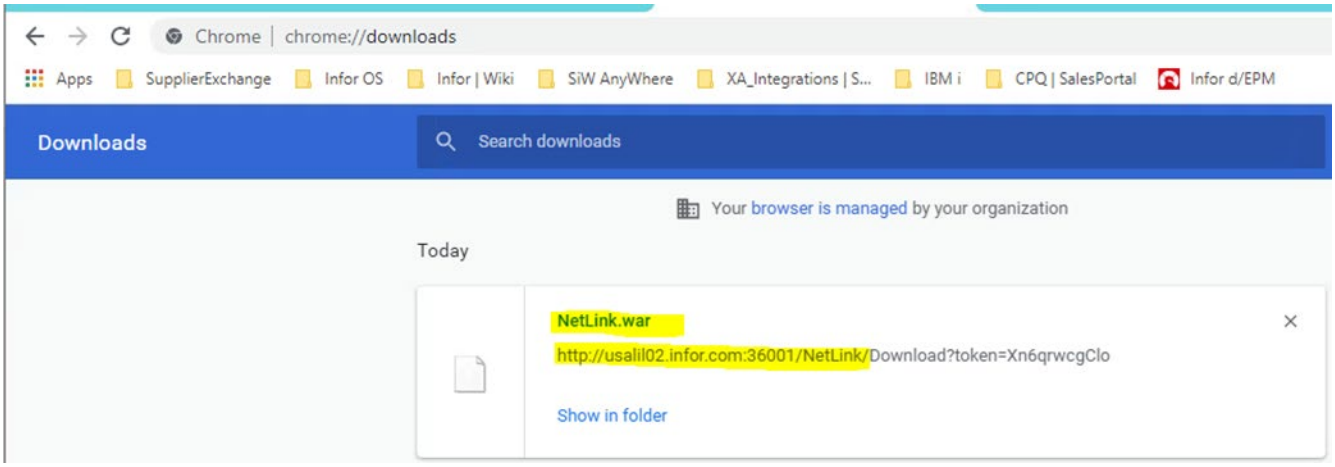
4 The Main Browser should display as below.



5 Either in a new tab (the browser session is shared between tabs), or in the current tab, navigate to **Error! Hyperlink reference not valid.**

where {server}, is the name of the IBMi which hosts IDF, and {port} is the port used for access to IDF components over HTTP.

6 The NetLink.war file should be generated and downloaded.



Building WAR file

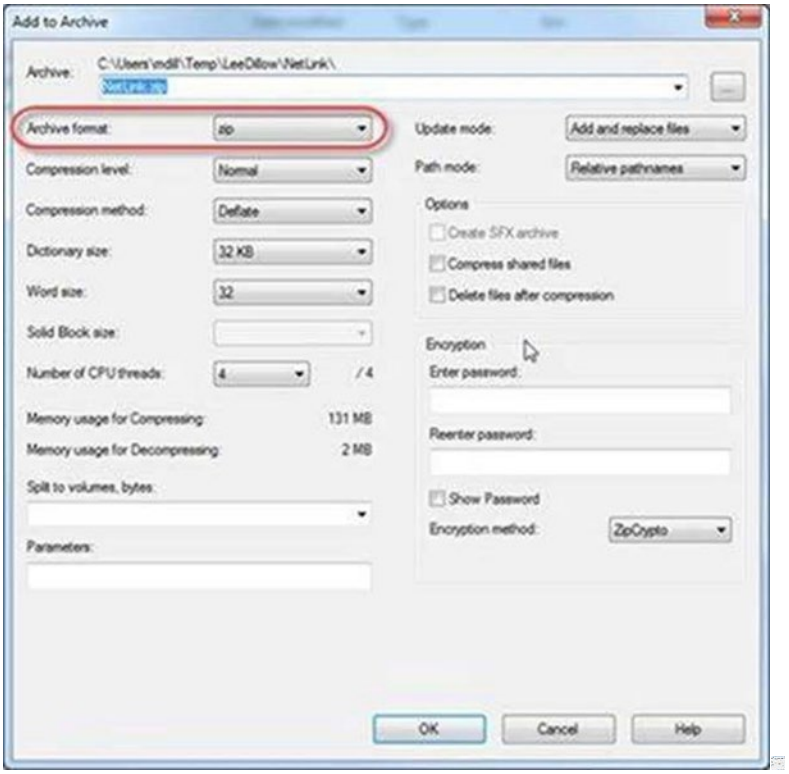
The Net-Link WAR file generation code is present only in Version 9.2 and 10. The `**Exception Encountered**` error message is displayed a previous version, the WAR file must bemanually built.

To build the file manually:

1 Extract the contents of the NetLink.war file to a new location using 7z.

2 Edit the WEB-INF/web.xml file and change all occurrences of nlbaiq05.infor.com (or the lower-case equivalent) with the Fully Qualified Domain Name (FQDN) of your iSeries.

3 Compress the contents to a new WAR file (named **NetLink.war**), ensuring that the structure matches that of the originally attached WAR file. Set the **Archive Format** field to zip.


Add to Archive
Archive:
C:\Users\mdll\Temp\LeeDillow\NetLink\
NetLink.zip
Archive format:
zip
Update mode:
Add and replace files
Compression level:
Normal
Path mode:
Relative pathnames
Compression method:
Deflate
Options
Dictionary size:
32 KB
Create SFX archive
Word size:
32
Compress shared files
Delete files after compression
Solid Block size:
Encryption
Number of CPU threads:
4
/ 4
Enter password:
Memory usage for Compressing:
131 MB
Reenter password:
Memory usage for Decompressing:
2 MB
Show Password
Split to volumes, bytes:
Encryption method:
ZipCrypto
Parameters:
OK
Cancel
Help

WAR file deployment

Tomcat (version 7.0 +)

The deployment of WAR file involves copying the WAR file to the root of the webapps folder of the Tomcat instance. The update is automatically loaded by Tomcat.

Note: If you are using WebSphere with version 8.5, please follow below steps in ***WebSphere (Version 8.5)*** section. Else, if you are using WebSphere with version 9.x and above, please follow below steps in ***WebSphere (Version 9.x)*** section.

WebSphere (version 8.5)

For deployment of WAR file using WebSphere, execute these steps:

1 Copy the WAR file to a location on the IFS of the iSeries which is preferably a 'scratch' folder. However, the location can also be in the root.

Note: If using the WebSphere instance of Systemi Workspace, make a copy of the plugin configuration (see the Systemi Workspace instructions for details).

2 Open the HTTP Administration console (http://{hostName}:2001/HTTPAdmin), and log in with

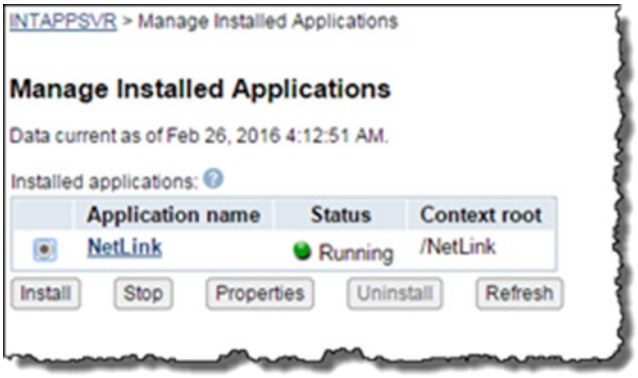
*SECADM authority.

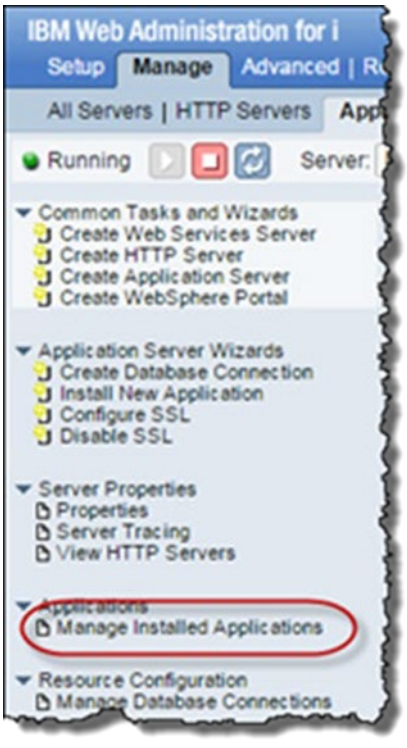
3 Select the Manage, and Application Servers tabs.

4 Specify a server instance in the Server field or select the instance used by Systemi Workspace.

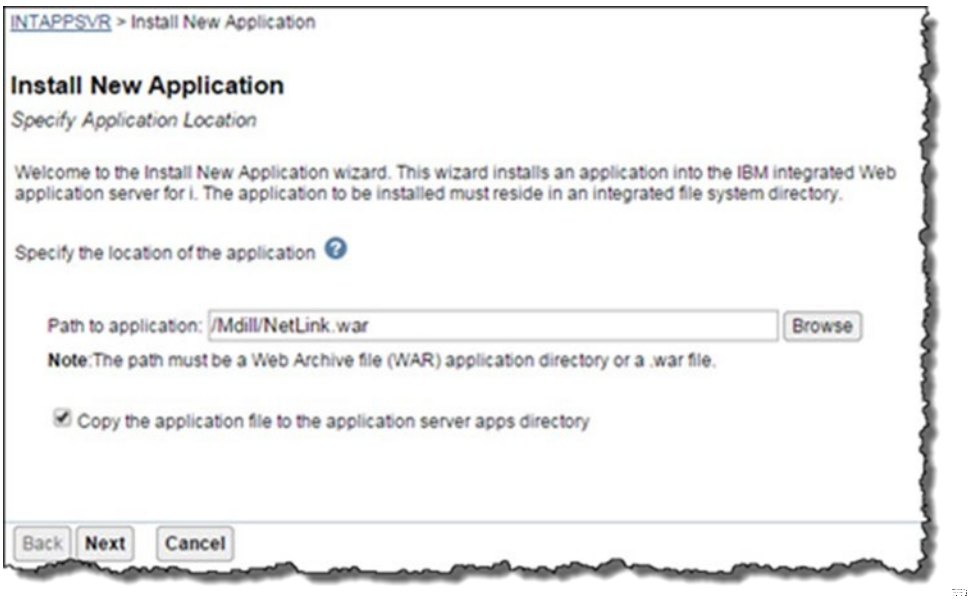
5 Select Manage > Manage Installed Applications.

6 Click **Install** to add Net-Link as a new application.

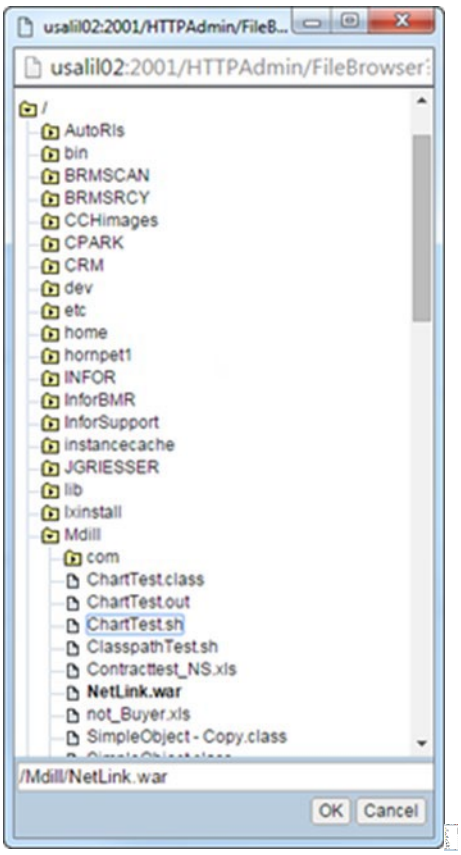




7 Specify the location of the WAR file (the location specified in Step 1) in the **Path to application** field.



Note: You can also use the Browse option to select the **File.**



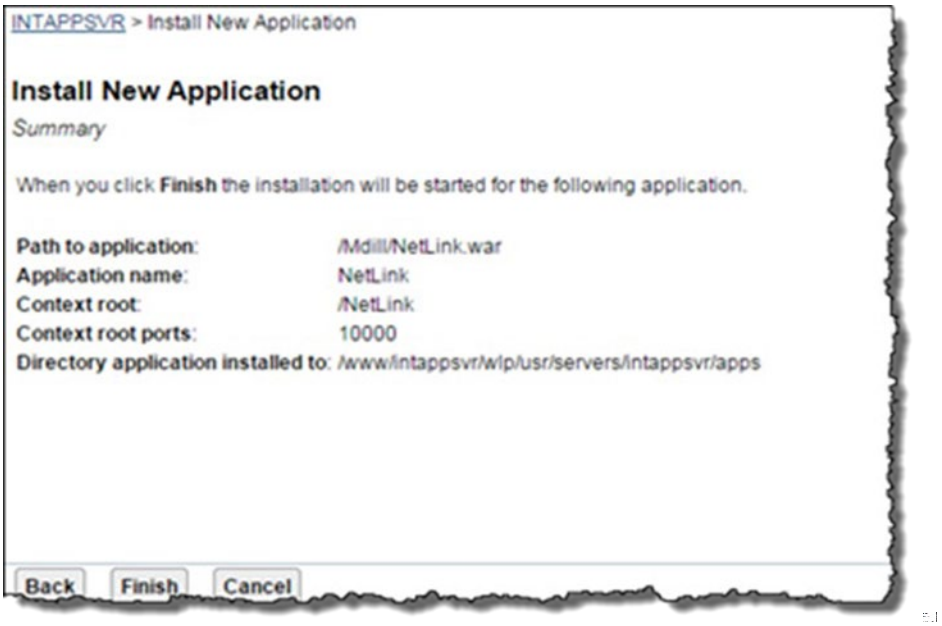
Note: Make sure that the location of the WAR file is correct.

8 Select the Copy the application file… check box.

9 Click Next. The Provide Options to perform the Install window is displayed.

10 Accept the default values for the **Application name** and **Context root**.

11 Click **Next**. The **Summary** window is displayed.



12 Review the content on the **Summary** window.

13 Click **Finish**.

Note: It is assumed that Systemi Workspace is already deployed to WebSphere.

WebSphere (version 9.x)

The deployment process utilizes the WebSphere Wizard function to create a Net-Link Applicationand associated HTTP server.

Check that you have the following subsystem running, and that all ADMIN jobs are running within the subsystem:

WRKSBSJOB QHTTPSVR

If the subsystem is not active, issue the following OS400 command:

STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

For deployment of WAR file using WebSphere, execute these steps:

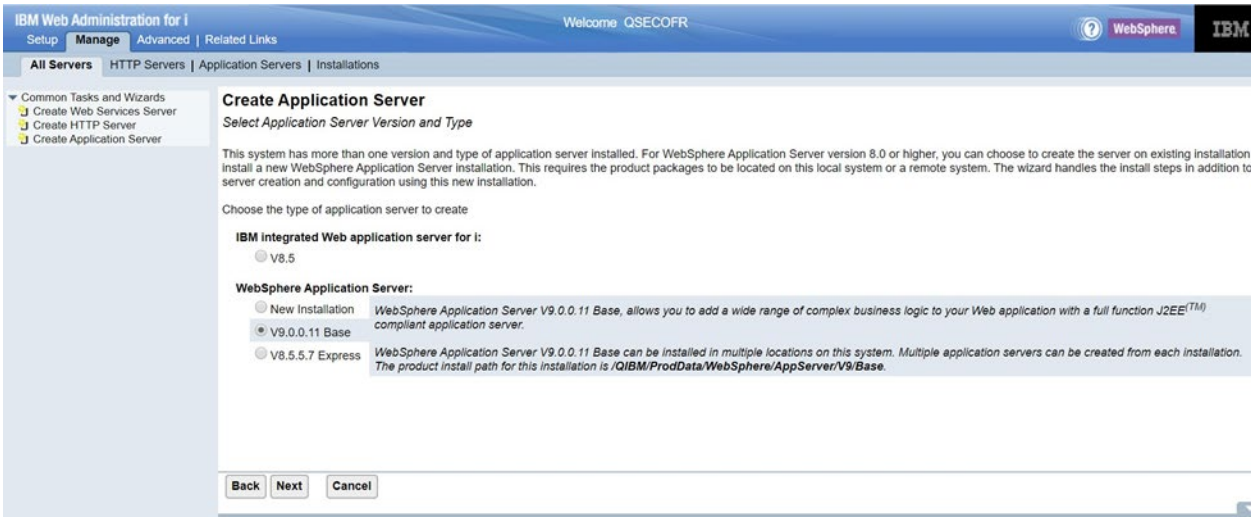
1 Copy the WAR file to a location on the IFS of the iSeries which is preferably a ‘scratch’ folder. However, the location can also be in the root.

2 Open the HTTP Administration console (http://{hostName}:2001/HTTPAdmin), and log in with *SECADM authority.

3 Select the **Manage**, and **All Servers** tab.

4 Select Create Application Server and Click Next.

5 Select V9.0.0.xx Base and Click Next.



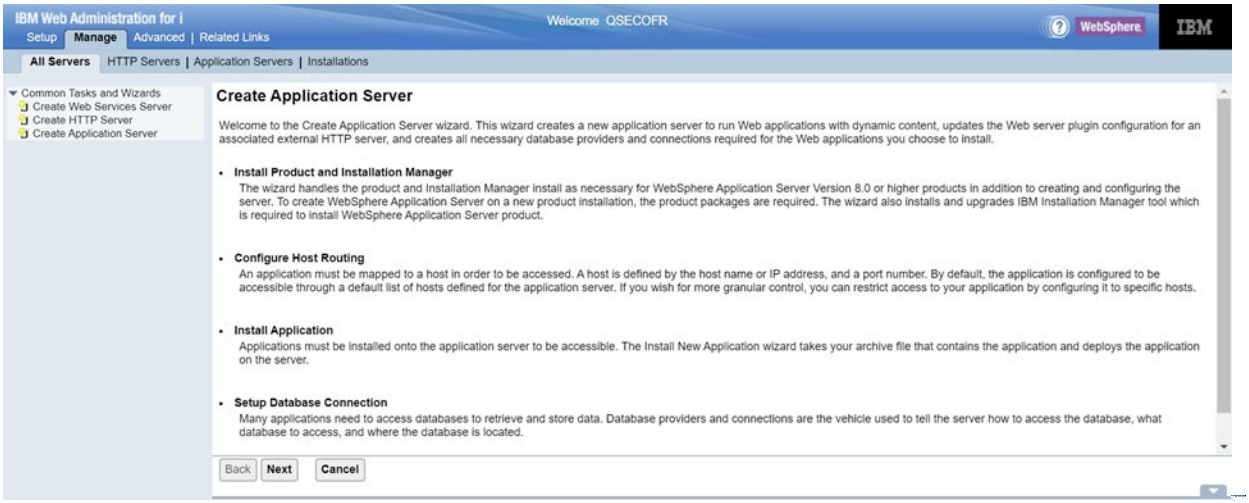
6 Enter appropriate Application server name and Server description and Click Next.

Suggested values

Application server name: NLAPPSVR

Server description: Net-Link Application Server

7 Click Next.



8 Select Create a new HTTP server (powered by Apache) and Click Next.

9 Enter appropriate HTTP server name and HTTP server description and Click Next.

Suggested values

Application server name: NLWEBSVR

HTTP server description: Net-Link Web server

IP address: All IP address

Port: 36001

Note: The port should be the same as that you have used in the **WAR file generation** section.

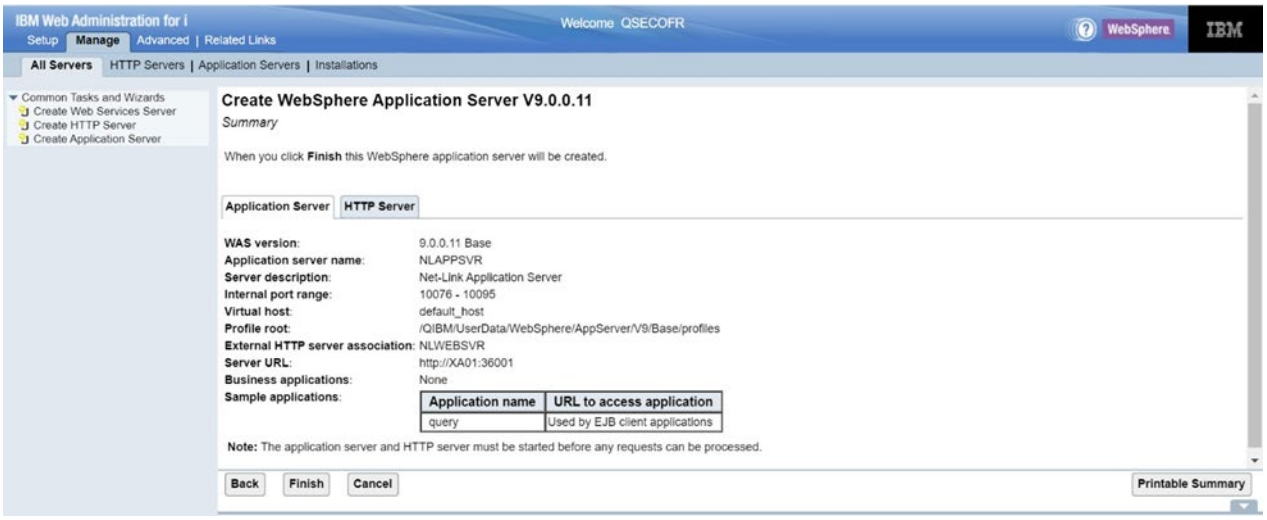
Note: If you receive the below Warning that the port is already configured by another application is displayed. Enter a new port, which hasn't been configured by another application, please make a note of the new port and click Next *to* continue the wizard using the port (36001), which is already been configured by another application. You will be asked to change the port (36001) to the new port by following **Appendix A** at the end of this wizard.

10 Accept the default First port in range: default values and Click Next.

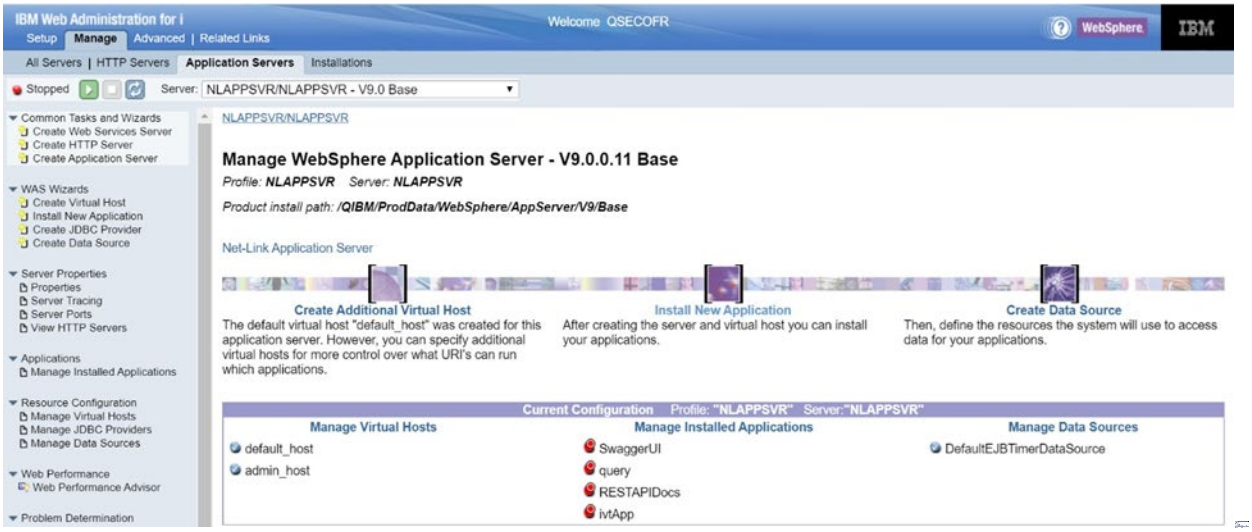
11 Deselect Default Applications and Click Next.

12 Select Do not configure Identity Tokens and Click Next.

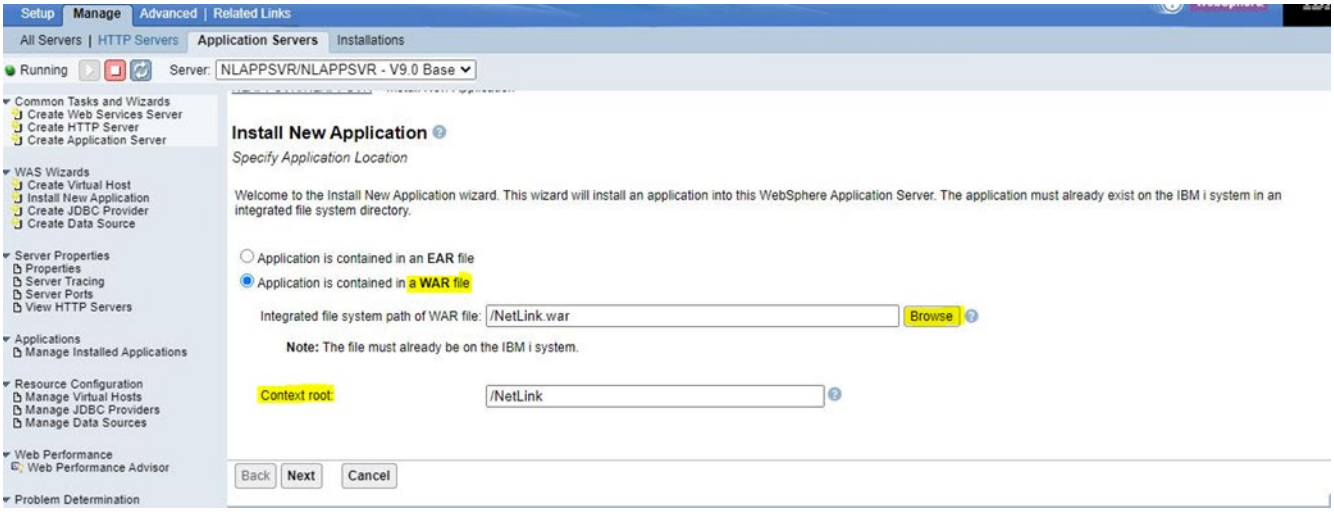
13 Review the Summary and Click **Finish.**



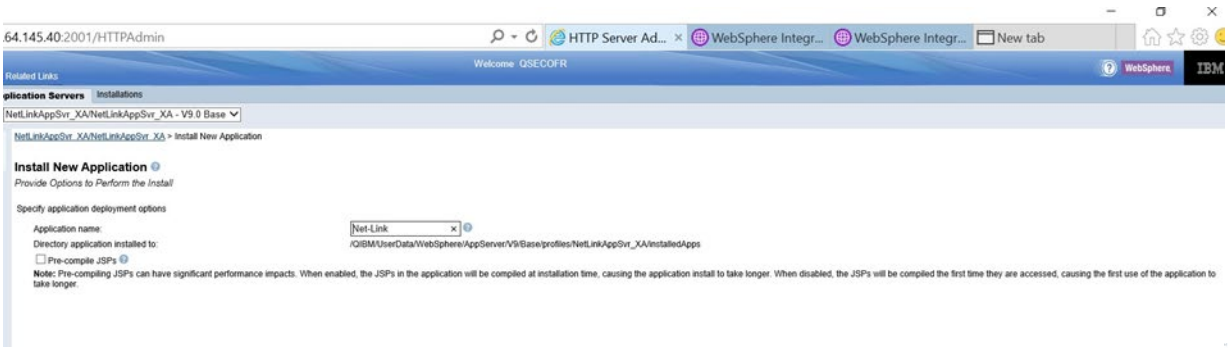
14 Select **Install New Application** from the *WAS Wizards* menu.



15 Select **Application is contained in a WAR file** and click **Browse** to locate and select the WAR file located on the IFS from Step **1**and then at Context root field, update with ***/myContexRoot*** value (for eg:/NetLink) and Click **Next.**

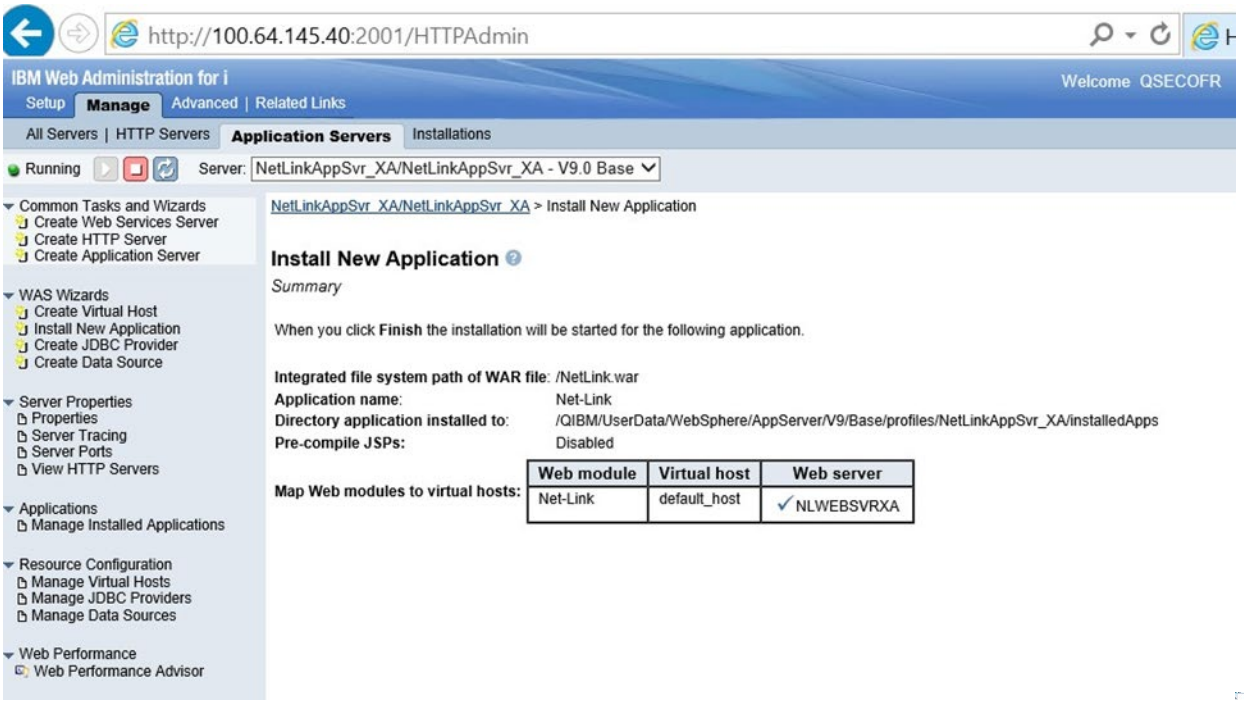


16 Click **Next.**



17 Check the Web server checkbox and Click **Next.**

18 Click Finish.

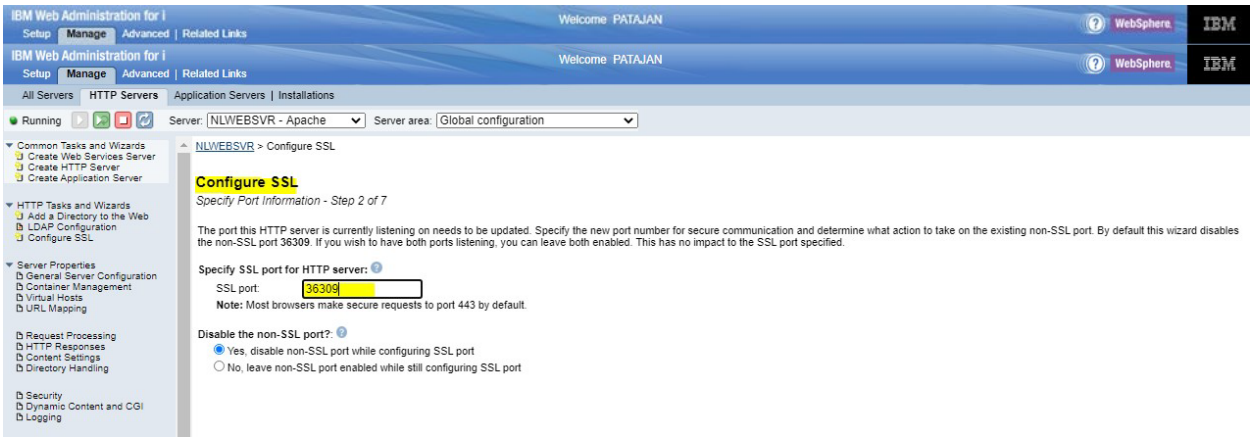


19 If you did not change the port (36001) to the new port and continued with the warning ‘port is already configured by anotherapplication’ in **Step 9 – see Appendix A** and then continue with the below section “**Configure SSL**”.

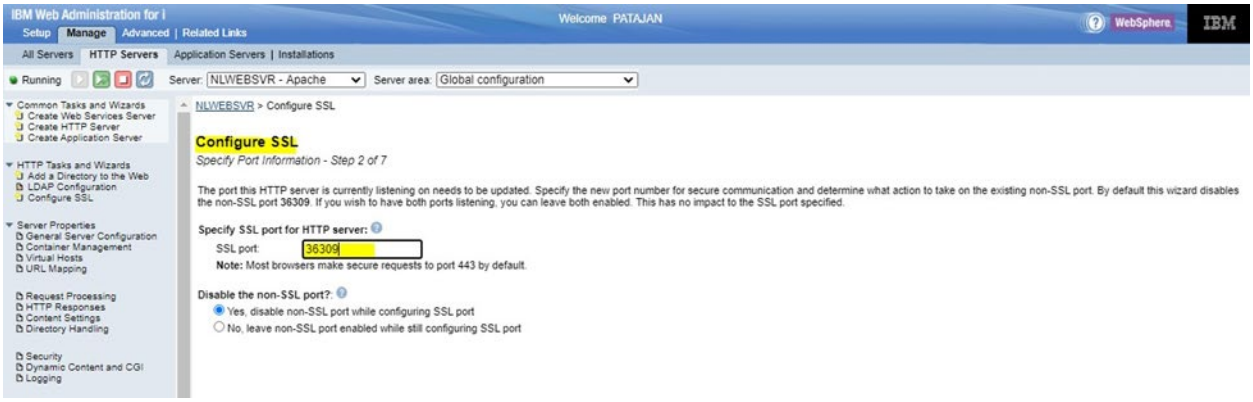
Application logs are available in the following folders.

/QIBM/UserData/WebSphere/AppServer/V9/Base/profiles//logs/ Configure SSL:

20 Select Manage tab | Select HTTP Servers tab | Select Configure SSL – (HTTP Tasks and Wizards) Click **Next**.



21 Enter required SSL port.

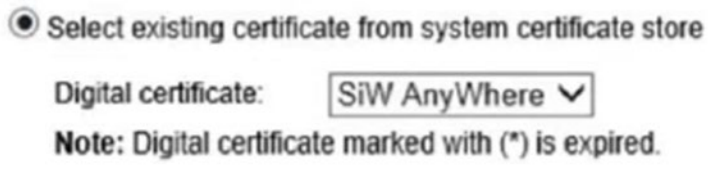


Note: If you have received the warning ‘port is already configured by another application’ in **Step 9** and performed Port Warning Rest instructions by following Appendix A, then specify that new SSL Port for HTTP server, which has been used in Appendix A. Otherwise, proceed with the port (36001) at **Step 9,** which should be same as a port that you have used in the **WAR file generation** section.

Select **Yes**, **disable non-SSL port while configuring SSL port**.Click **Next**.

22 Enter the system certificate store password. Click **Next**.

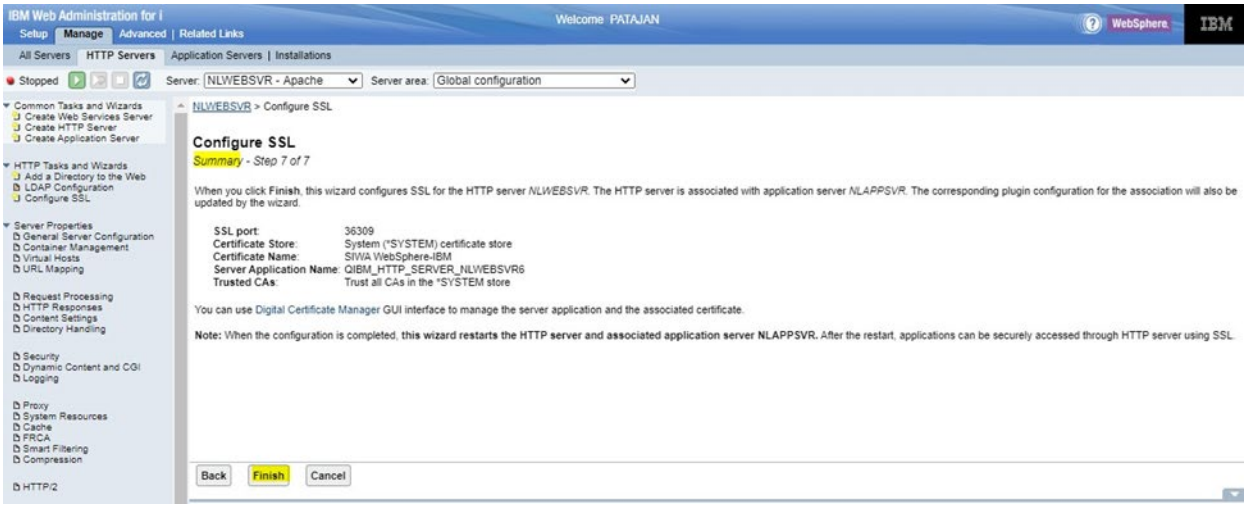
23 Select an existing certificate from the system certificate store, which you have created in ***Creating a local Certificate of Authority*** section, at the time of SiWA WebSphere installation using the ***System i Workspace AnyWhere Installation & Administration Guide***. Click **Next**.



24 Select Trust all CAs in the *SYSTEM store. Click Next.

25 Select Restart the server immediately after the wizard. Click Next.

26 Check that the summary is correct and Click Finish.



The wizard configures SSL for the HTTP server *NLWEBSVR*. The HTTP server is associated with application server *NLAPPSVR*. The corresponding plugin configuration for the associationwill also be updated by the wizard.

SSL port:	36309
Certificate Store:	System (*SYSTEM) certificate store
Certificate Name:	<certificate_name>
Server Application Name:	QIBM_HTTP_SERVER_NLWEBSVR
Trusted CAs:	Trust all CAs in the *SYSTEM store

Note: When the configuration is completed, **this wizard restarts the HTTP server and associated applicationserver NetLinkAppSvr_XA.** After the restart, applications can be securely accessed through HTTP server usingSSL.

27 Now try to access the NetLink using below URL.

https:///{hostname}:{port}/NetLink Hostname→ FQDN of the iseries machinePort→ SSL Port number

(For example: https://usalil2m.infor.com:36309/NetLink)

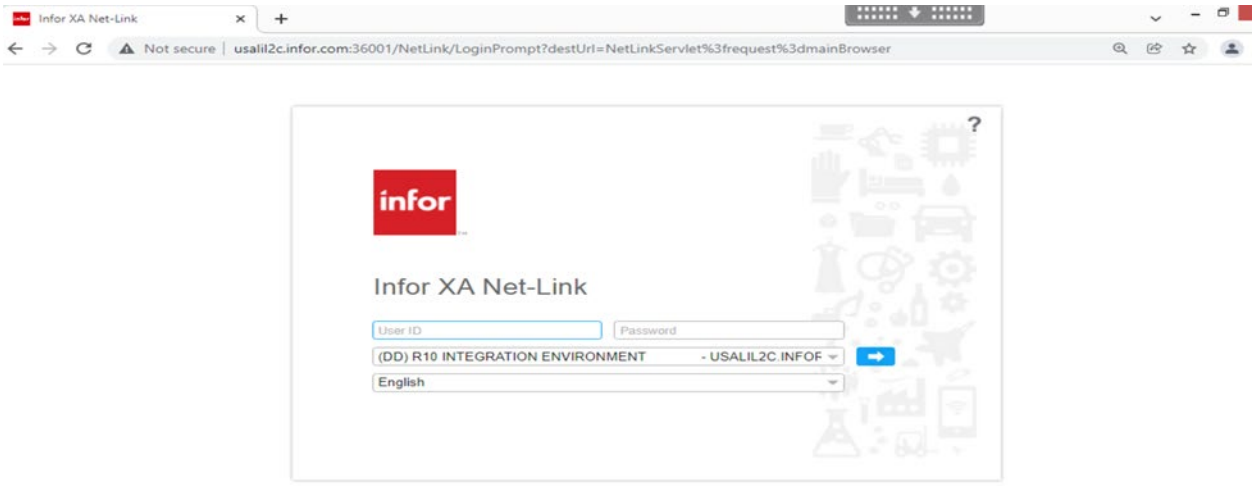
Application logs are contained in the following folders.

/QIBM/UserData/WebSphere/AppServer/V9/Base/profiles//logs/

IDFIONAPI WAR file deployment

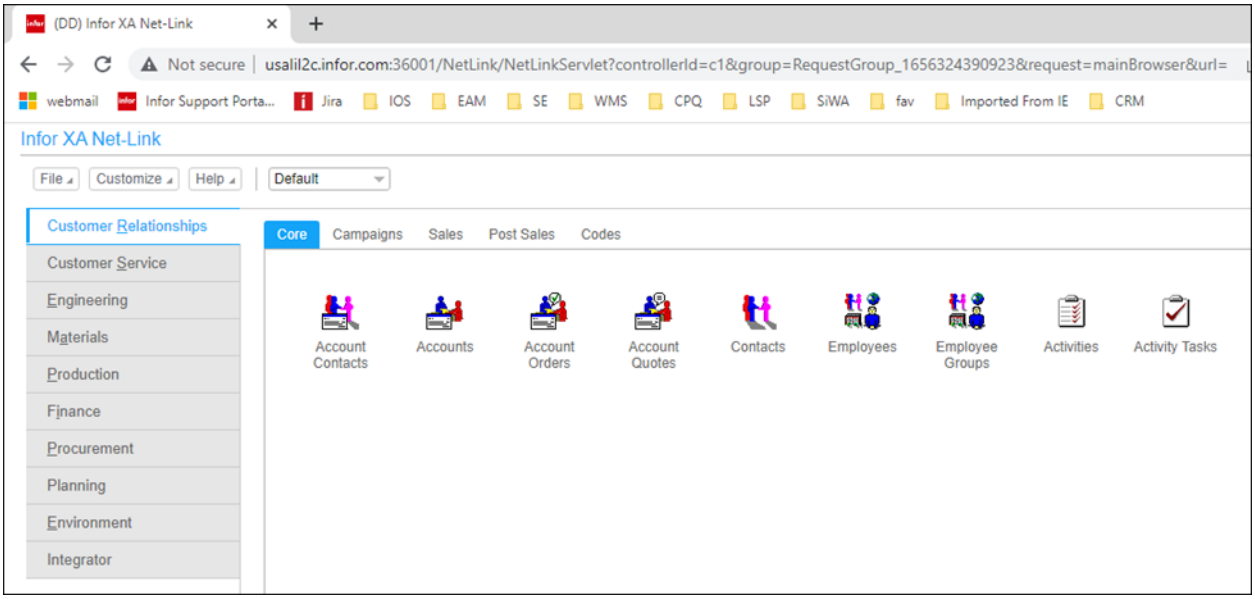
The ION API component of IDF will need to be deployed to a location visible to ION. It is expected that this will be the same location as the SiWA / Net-Link server (WebSphere).

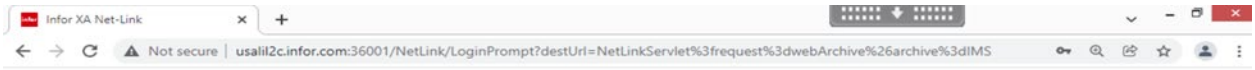
Log in to Net-Link for the environment." http://usalil2c.infor.com:36001/NetLink"



In the Address bar, replace the "/NetLinkServlet?....." with "/WebArchive?archive=IMS"

(e.g. "http://usalil2c.infor.com:36001/NetLink/WebArchive?archive=IMS"), and press enter.



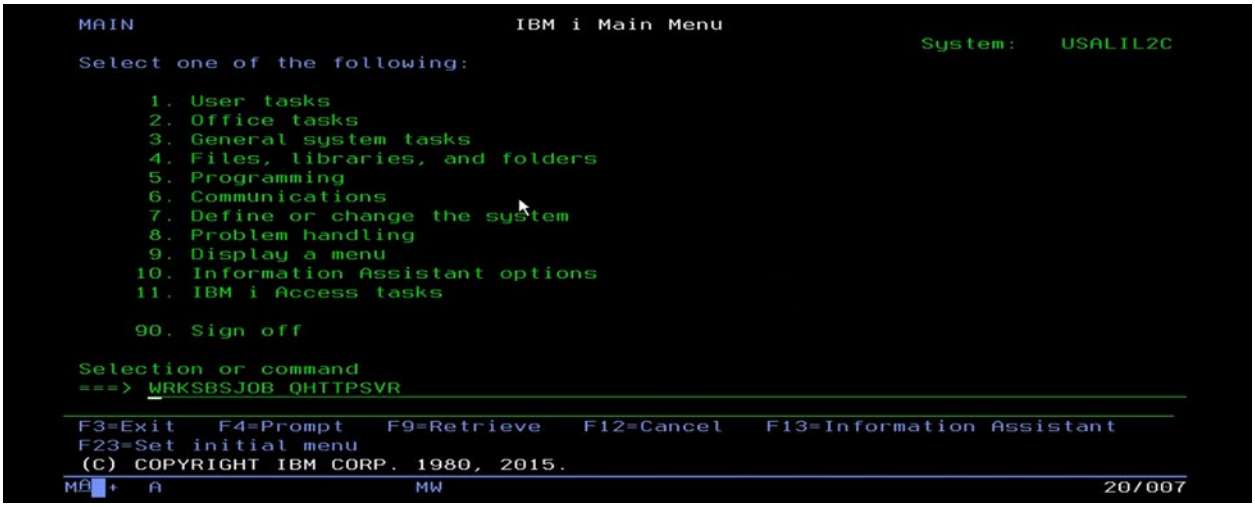


The deployment war file should be generated and downloaded to the local machine.

The deployment process utilizes the WebSphere Wizard function to create a Net-Link Application and associated HTTP server.

Check that you have the following subsystem running, and that all ADMIN jobs are running within the subsystem:

WRKSBSJOB QHTTPSVR



If the subsystem is not active, issue the following OS400 command:

STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

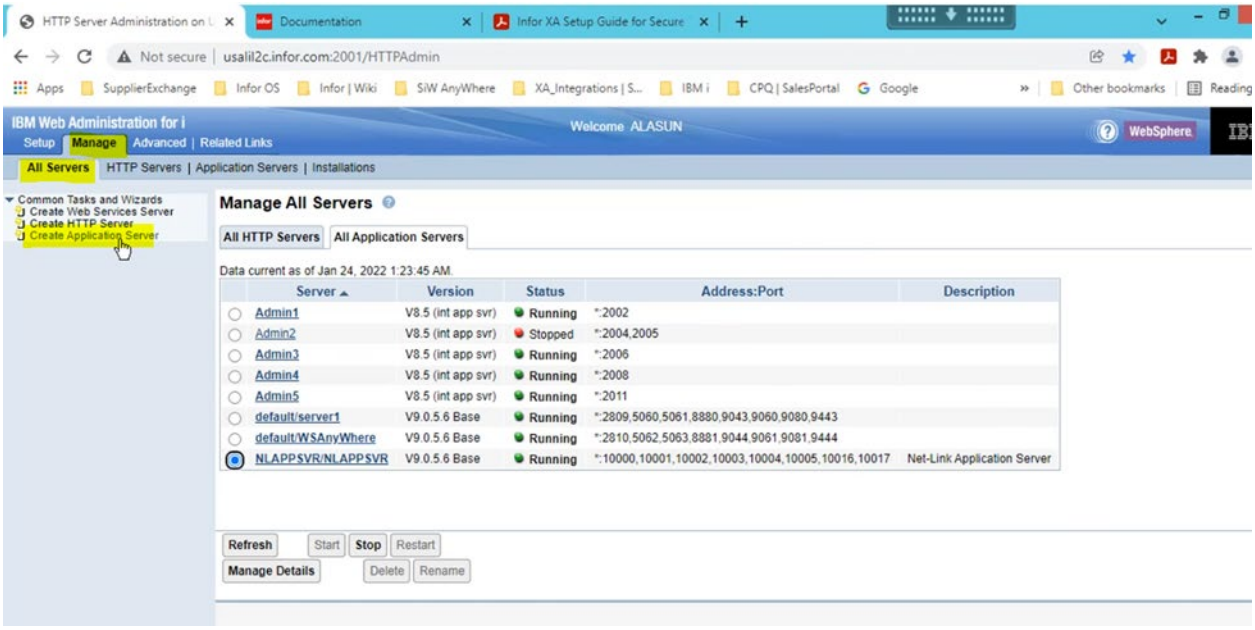
For deployment of WAR file using WebSphere, execute below steps:

1 Copy the WAR file to a location on the IFS of the iSeries which is preferably a ‘temp’ folder. However, the location can also be in the root.

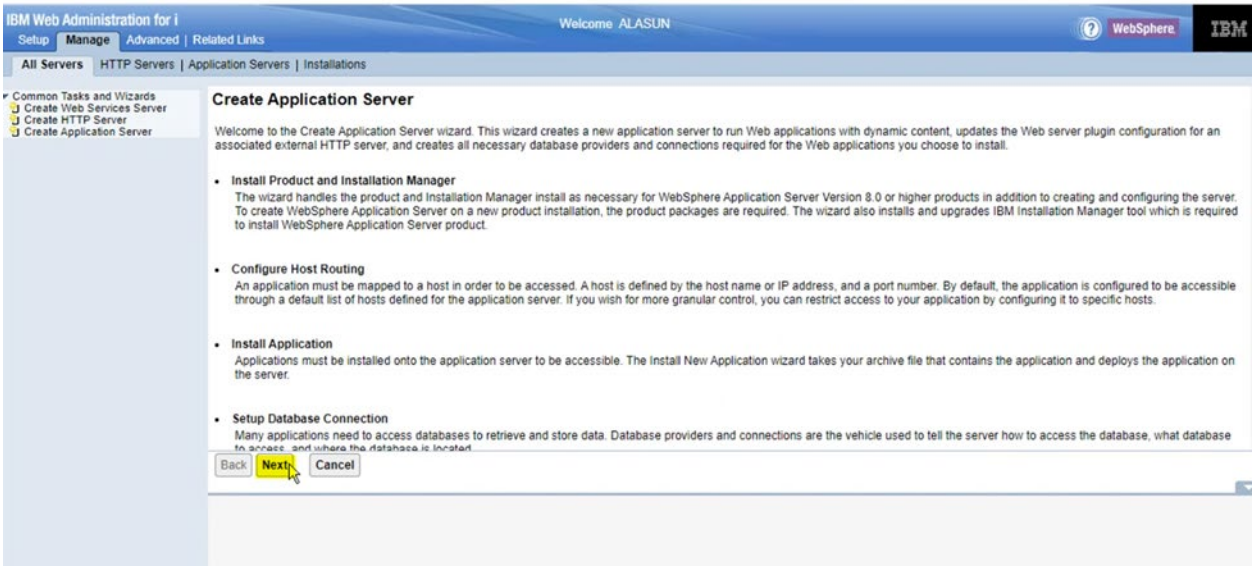
2 Open the HTTP Administration console (**Error! Hyperlink reference not valid.**)

Ex:(http://ualil2c.infor.com:2001/HTTPAdmin), and log in with *SECADM authority.

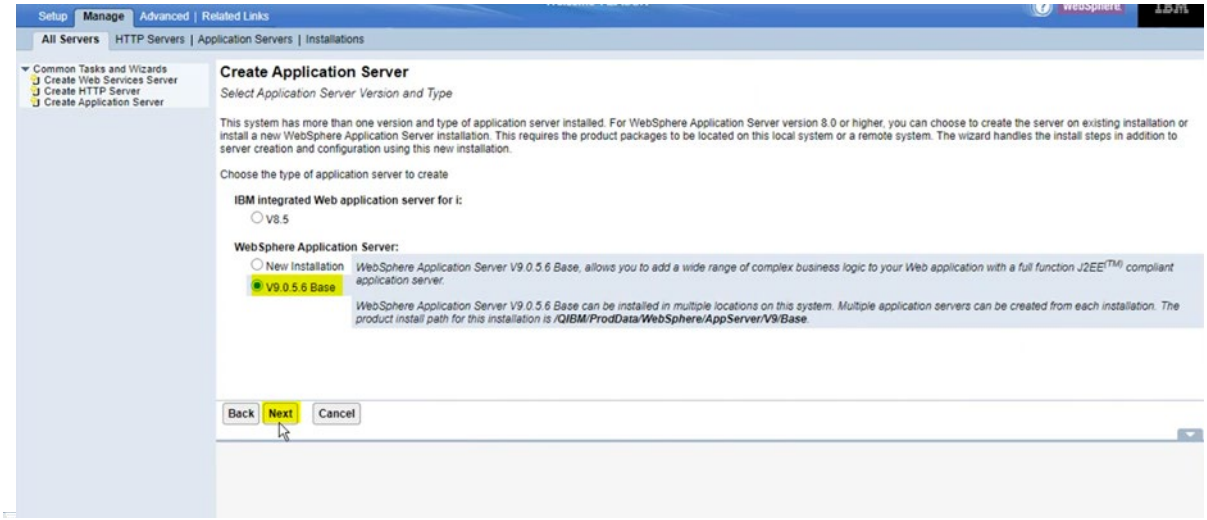
3 Select the Manage, and All Servers tab.



Select Create Application Server and Click Next.



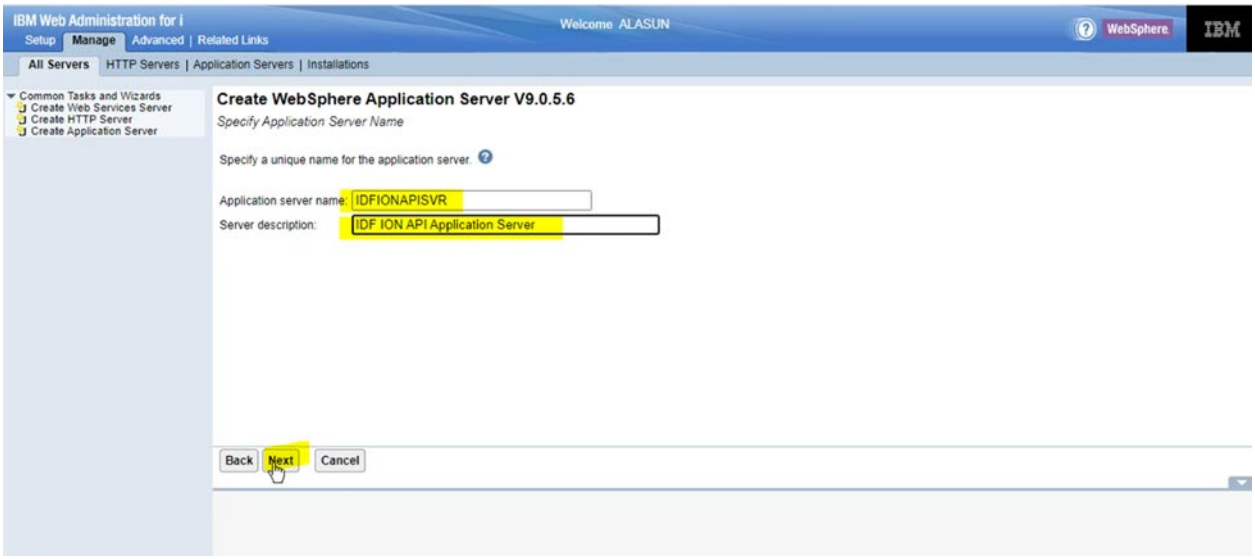
Select V9.0.0.xx Base and Click Next.



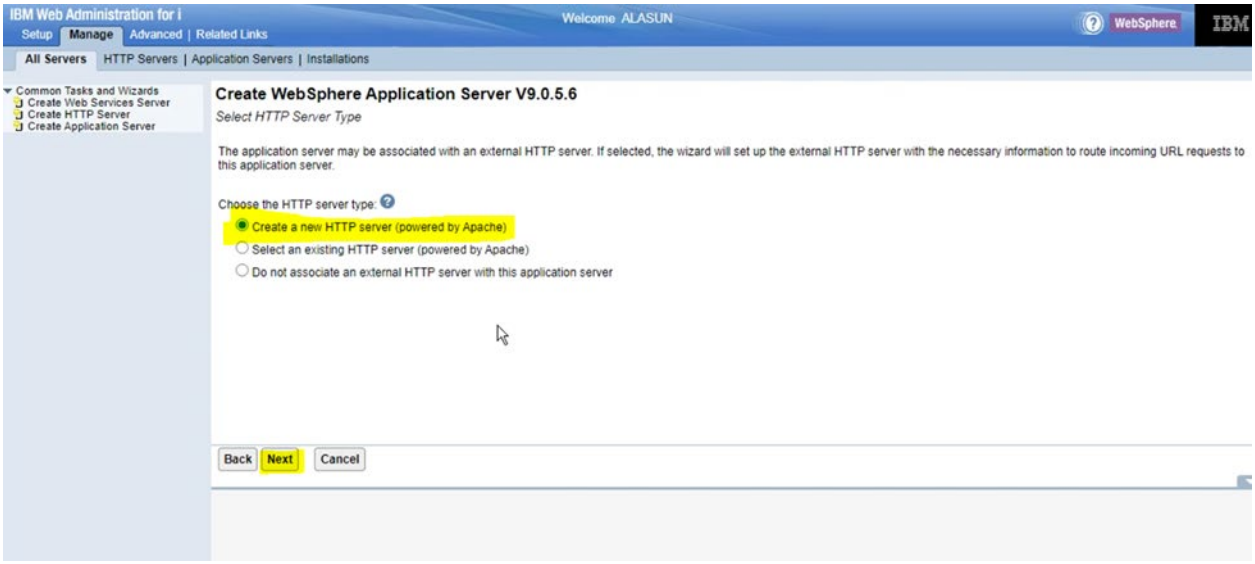
Enter below Application server name, description and Click Next.

Application server name: IDFIONAPISVR

Server description: IDF ION API Application Server



Select Create a new **HTTP server** and Click **Next.**



Enter below HTTP server name, HTTP server description and Click Next.

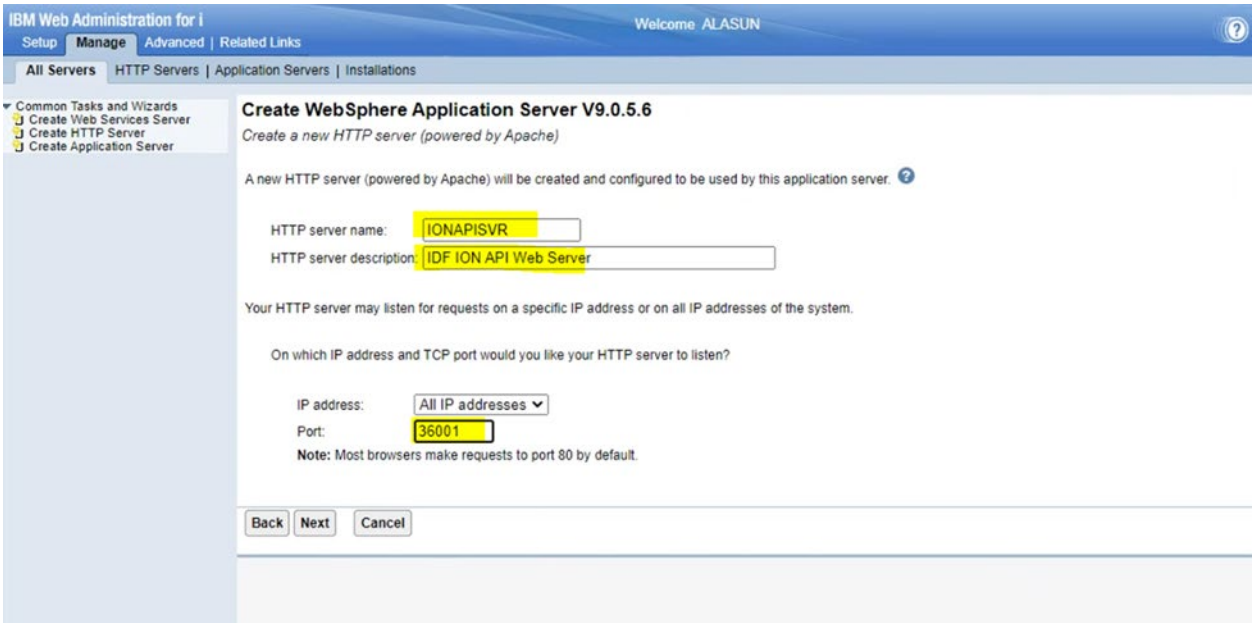
HTTP server name: IONAPISVR

HTTP server description: IDF ION API Web Server

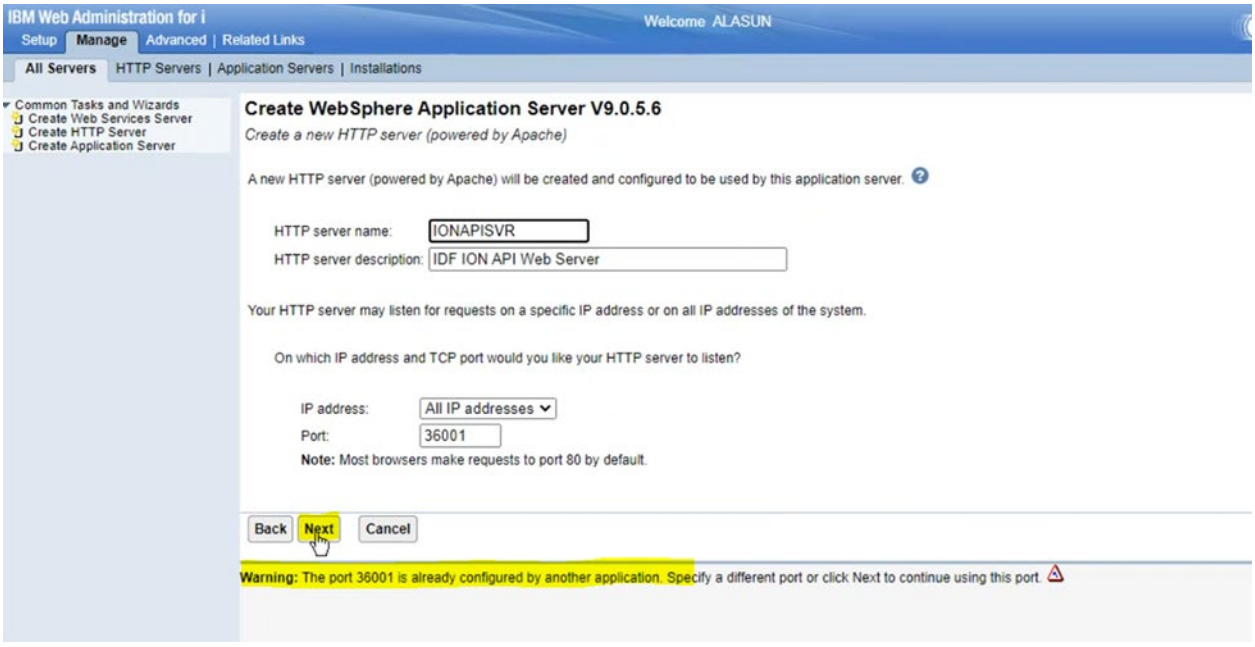
IP address: All IP address

Port: 36001

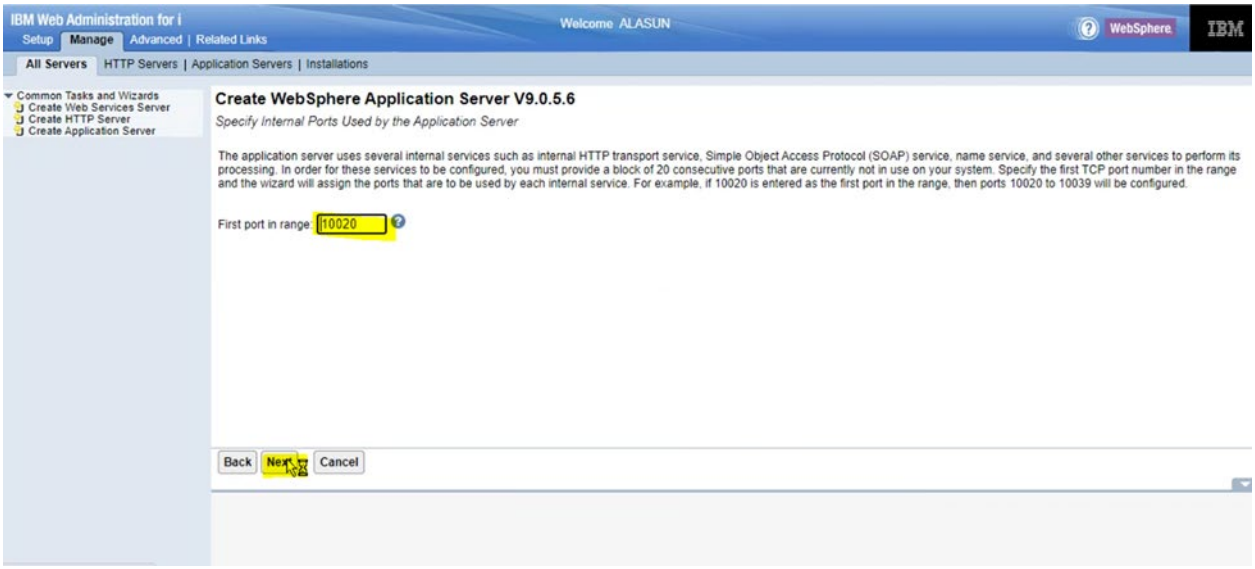
Note: The port should be the same as that you have used in the WAR file generation section



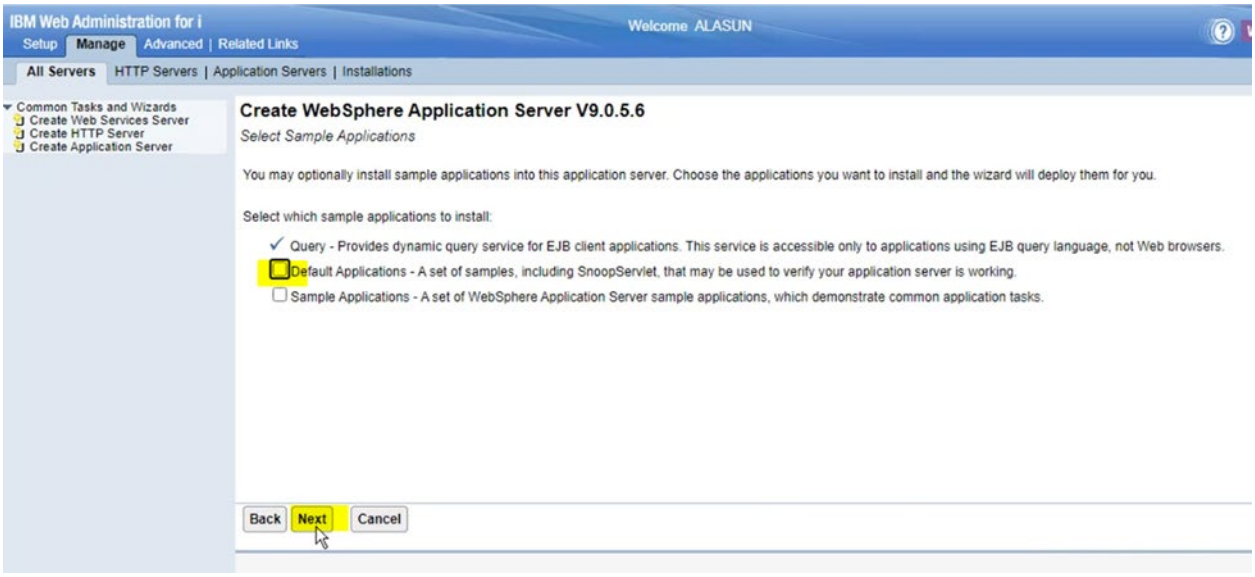
Click next again



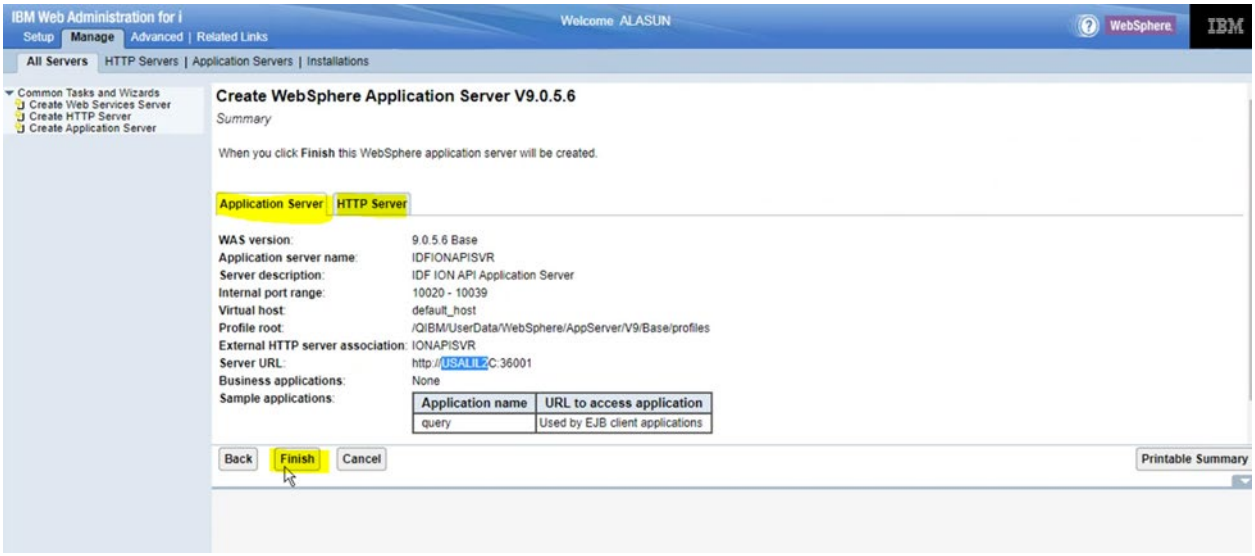
Accept the default **First port in range**: default values and Click Next.



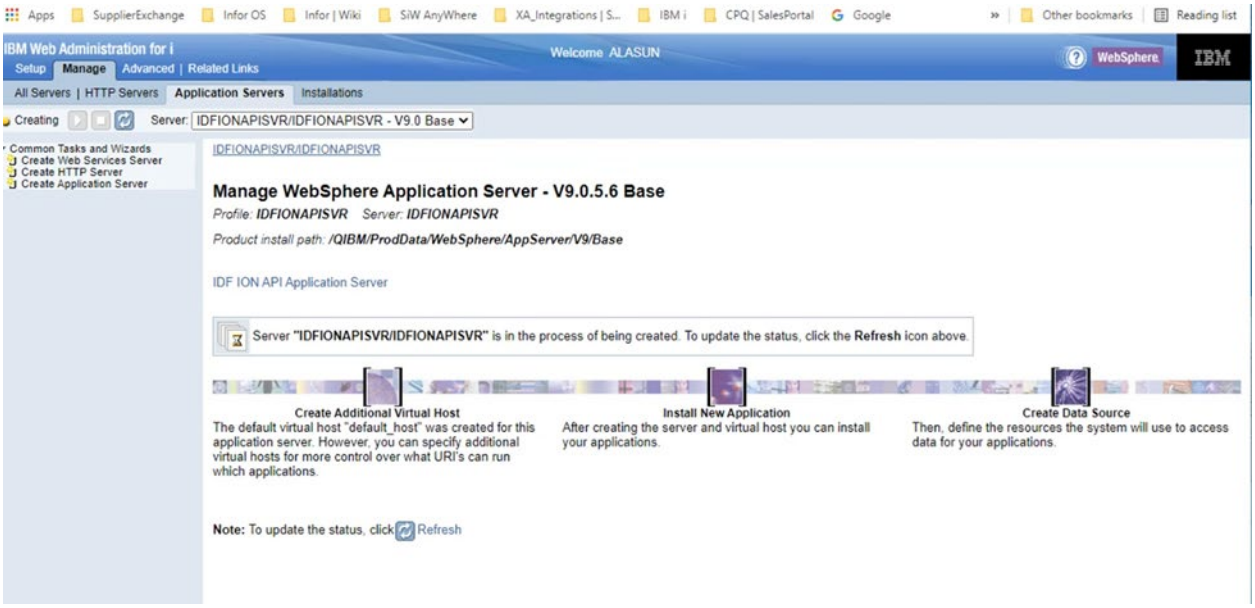
Deselect Default Applications and Click Next.



Review the Summary and Click **Finish.**

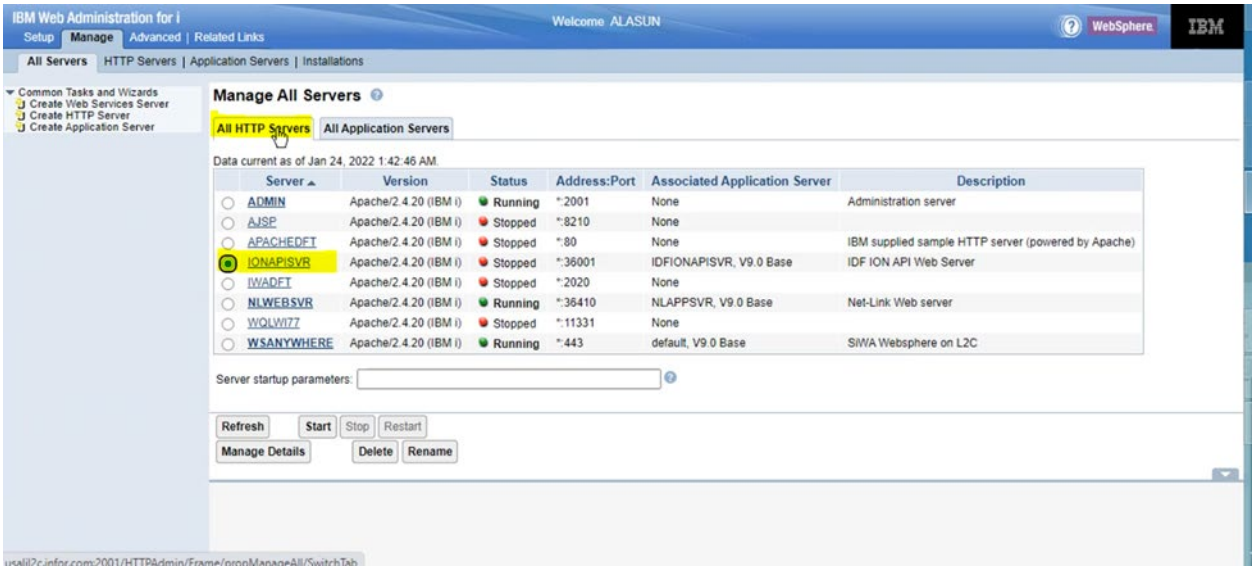


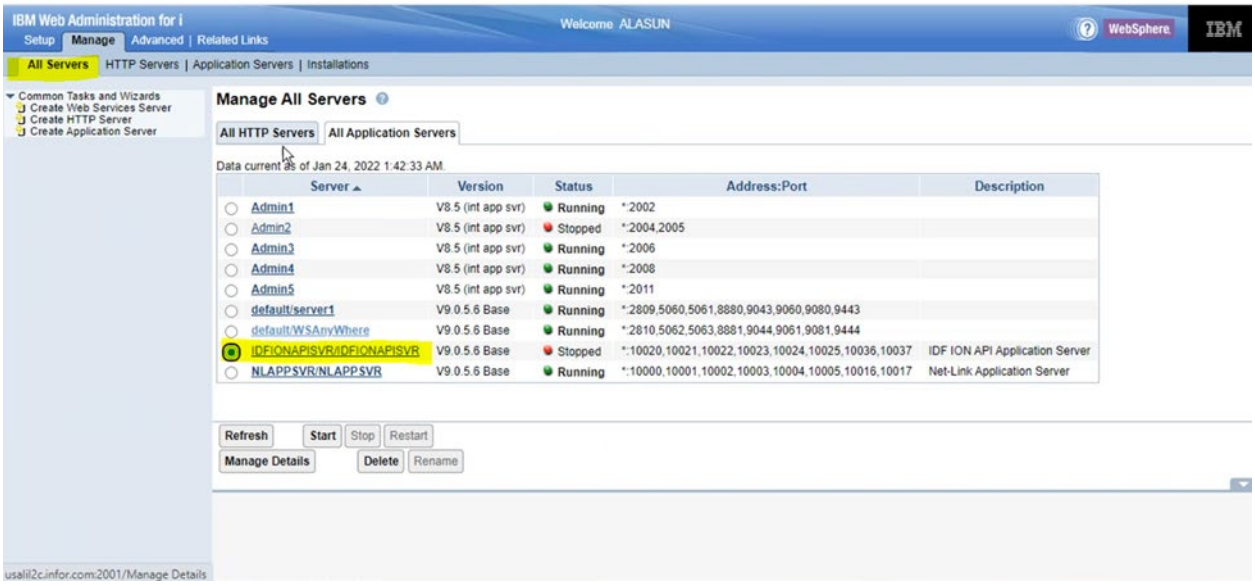
Wait until the creation process is completed



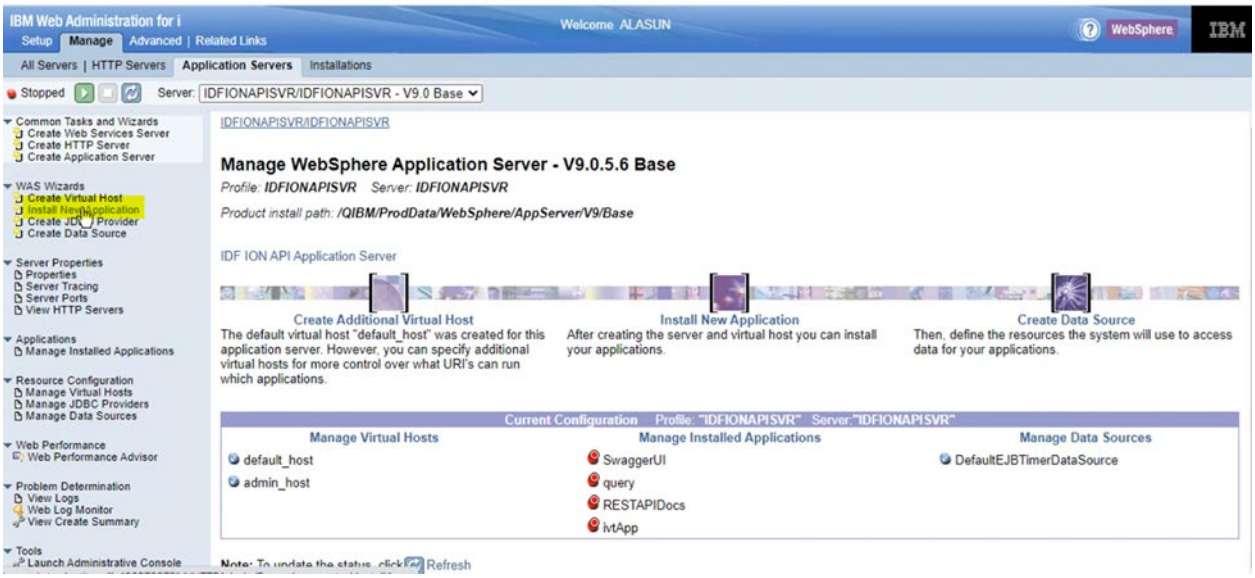
Click on refresh to update the status

Check for the created servers in All servers.

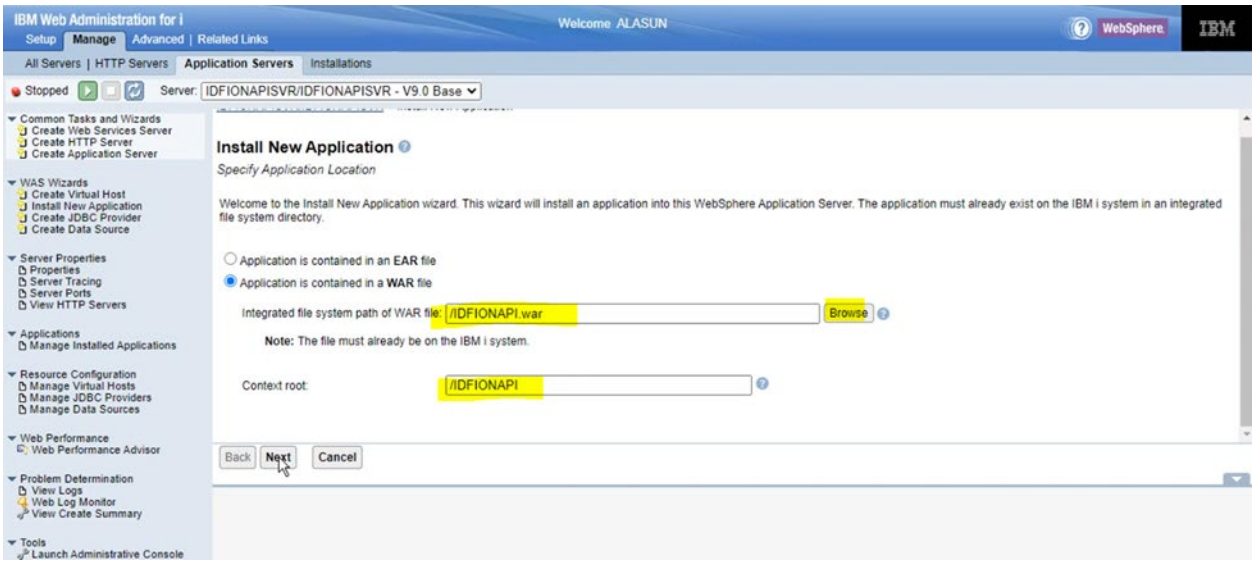




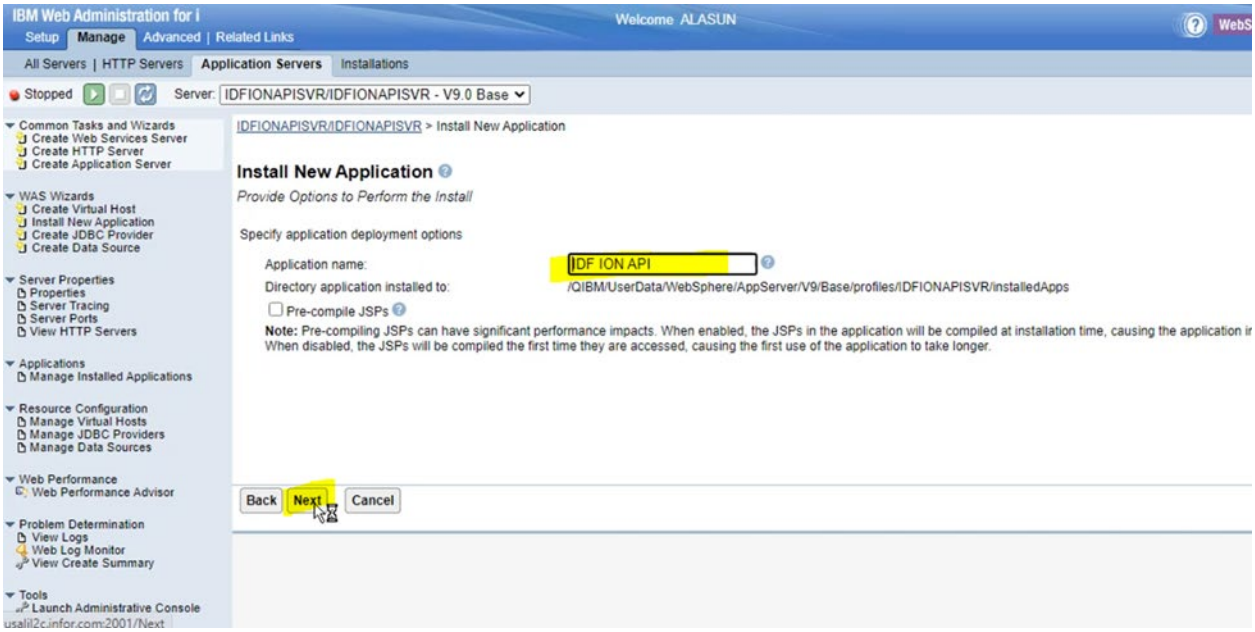
Click on the created application server (**IDFIONAPISVR**) and Select **Install New Application** from the WAS Wizards menu.



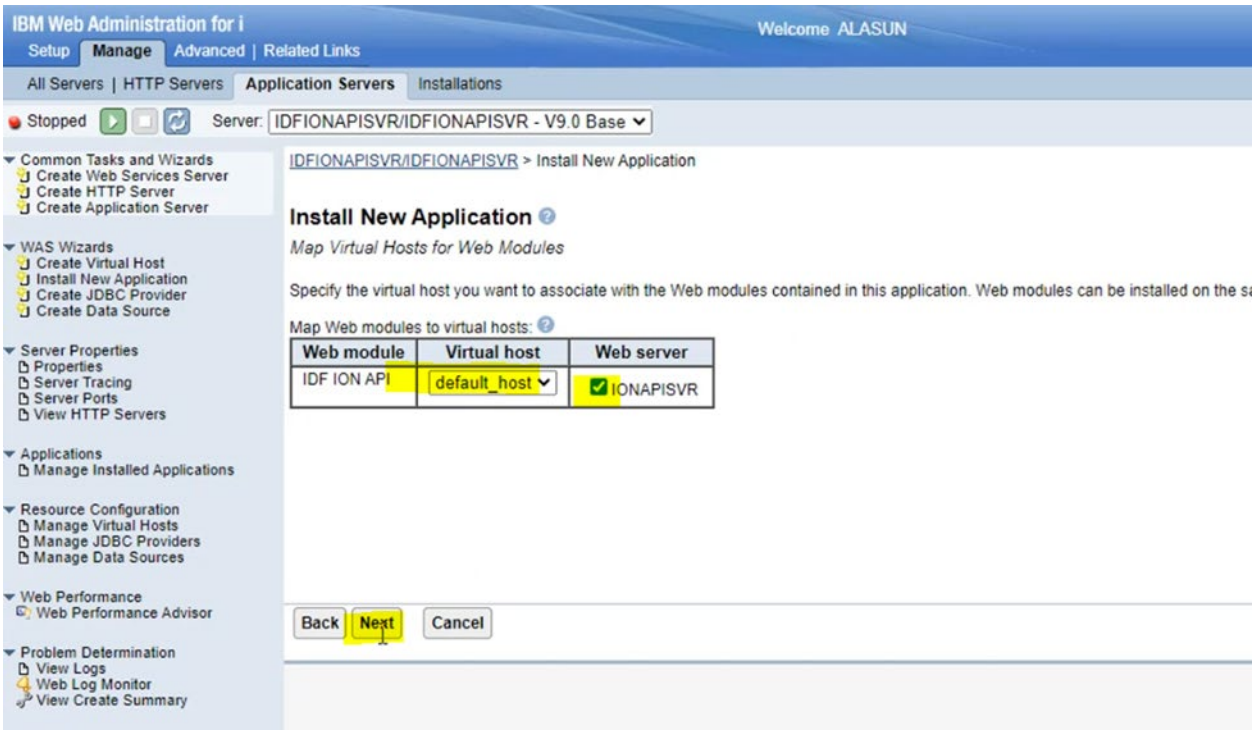
Select **Application is contained in a WAR file** and click **Browse** to locate and select the WAR file located on the IFS from Step 1 and then at Context root field, update with /myContexRoot value (for eg:/IDFIONAPI) and Click **Next.**



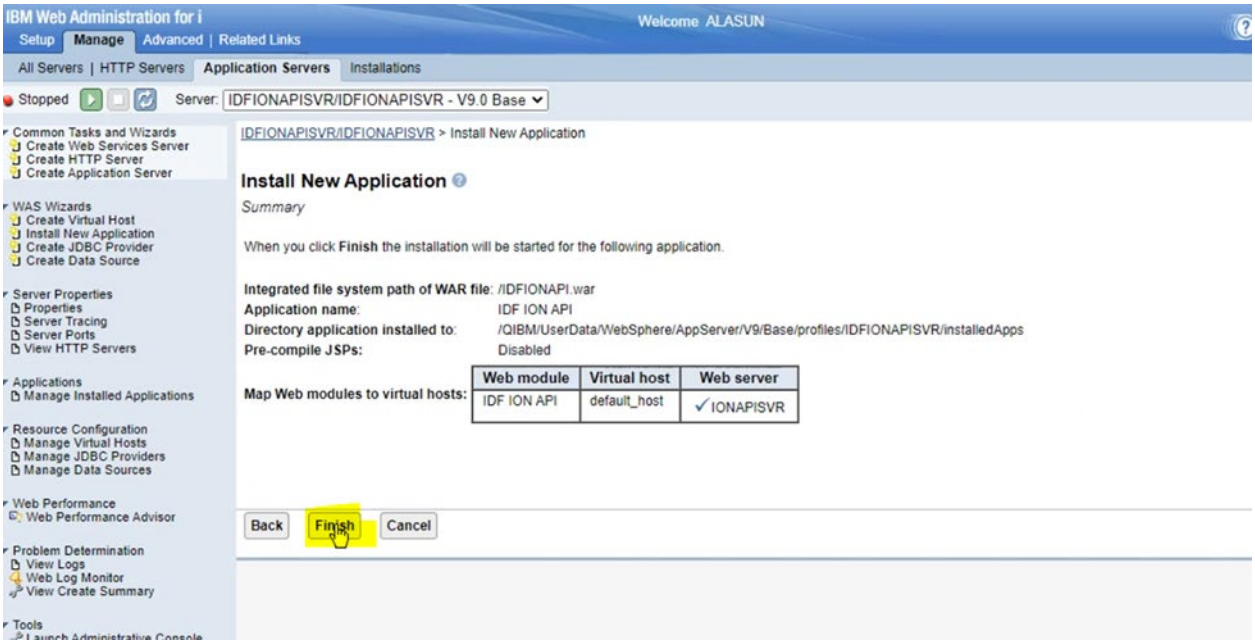
Click Next.



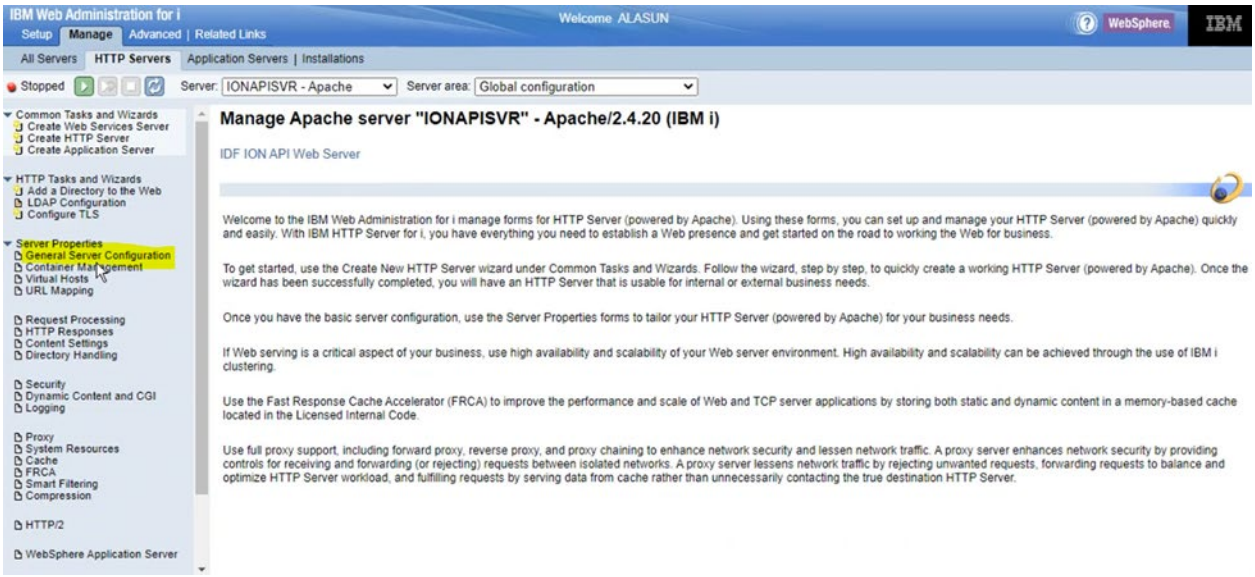
Check the Web server checkbox and Click Next.



Click on Finish.



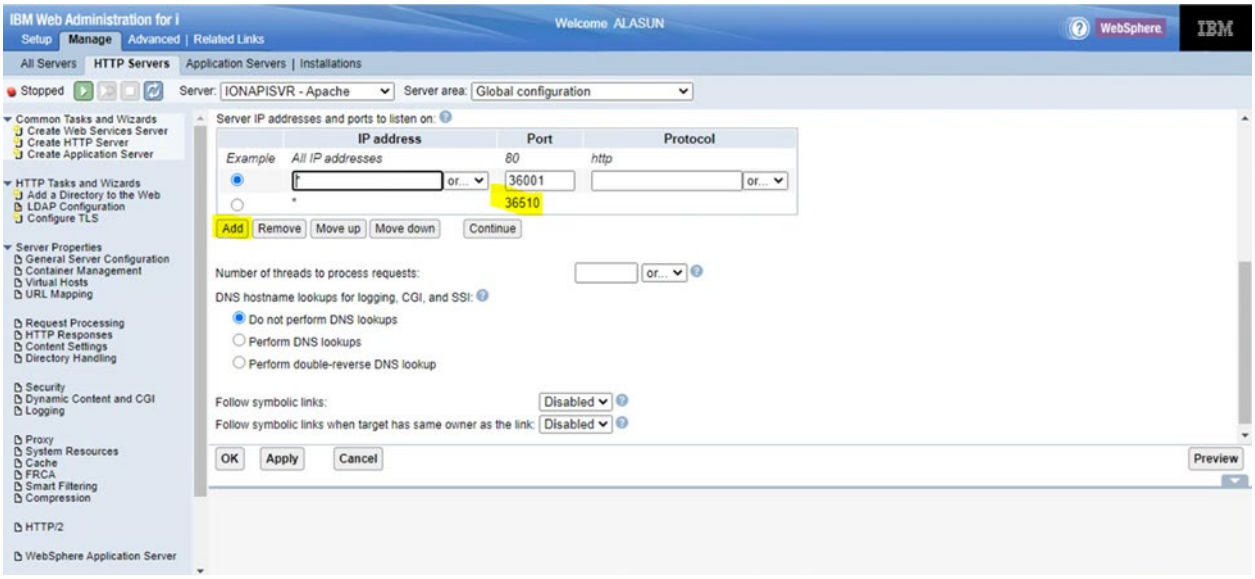
Now go to manage http servers, in **IDFIONAPI Web Server**, click on general server configuration**.**



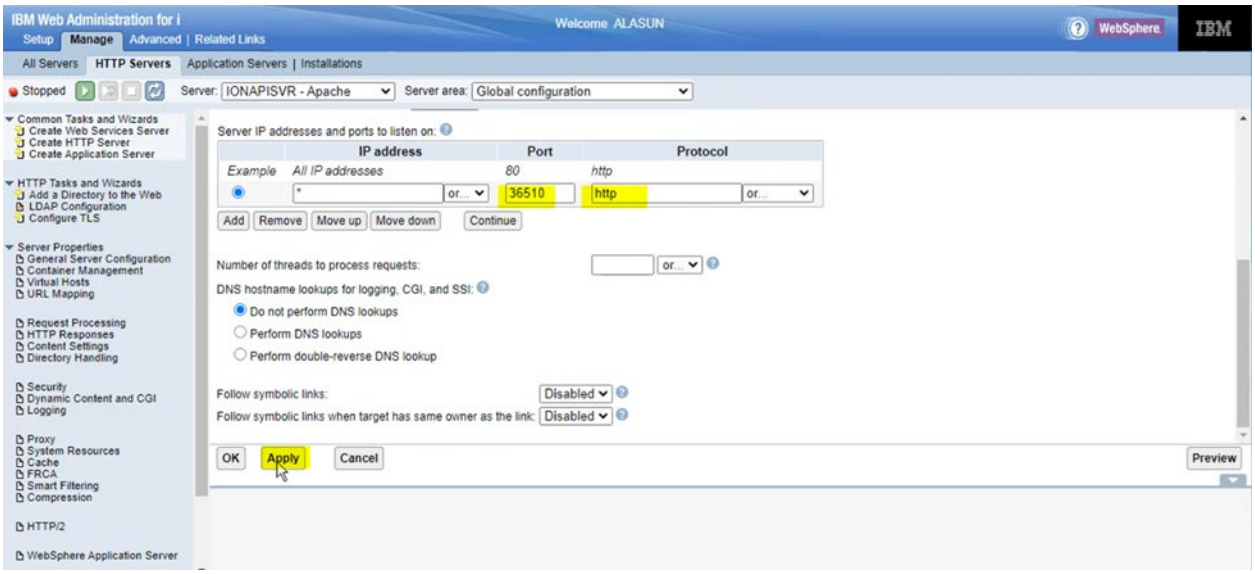
Click on add to add the new port and remove the old port

Port: 36510

Protocol: http

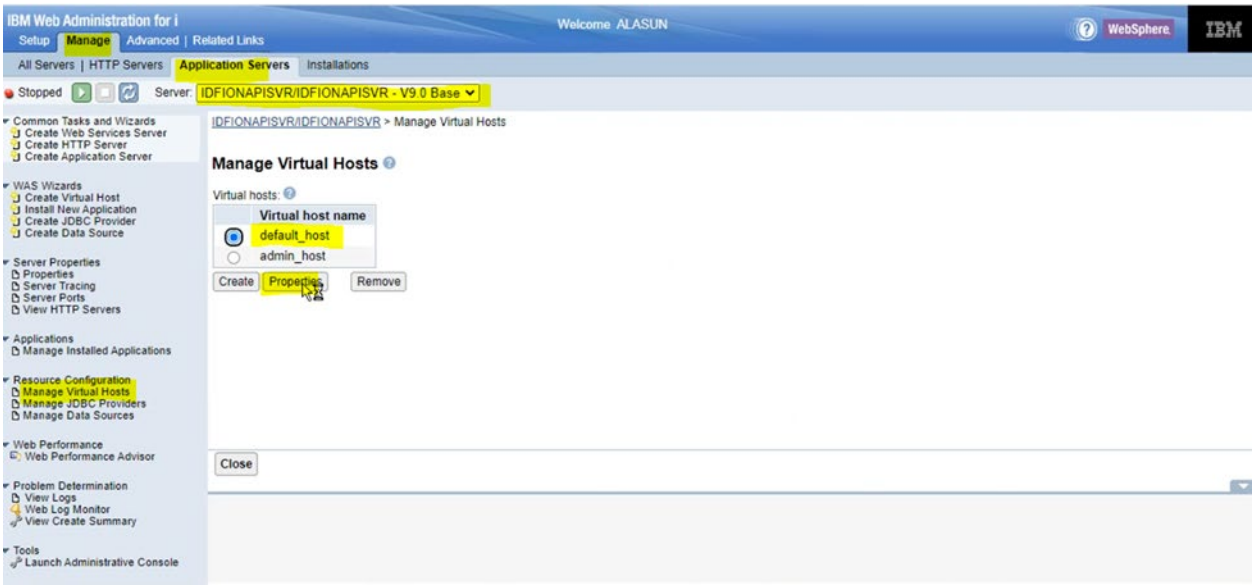


Click on Apply then ok.

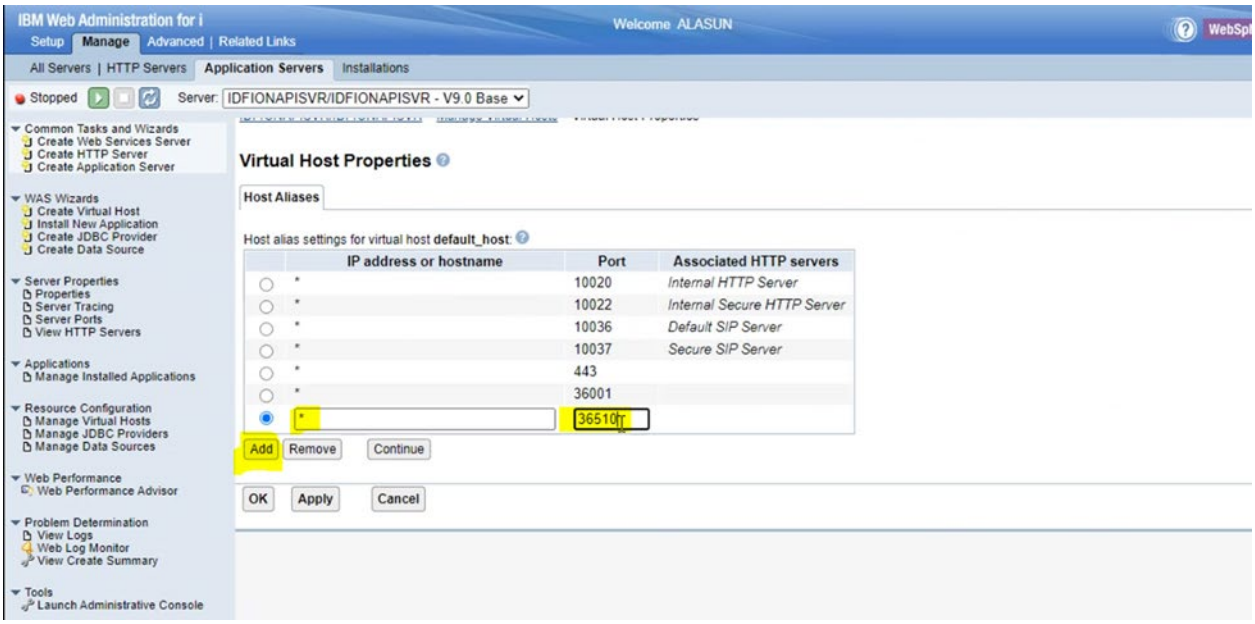


Select the **Manage Virtual Hosts** under **Resource Configuration** from the IDFIONAPISVR Application server, as shown in below screenshot.

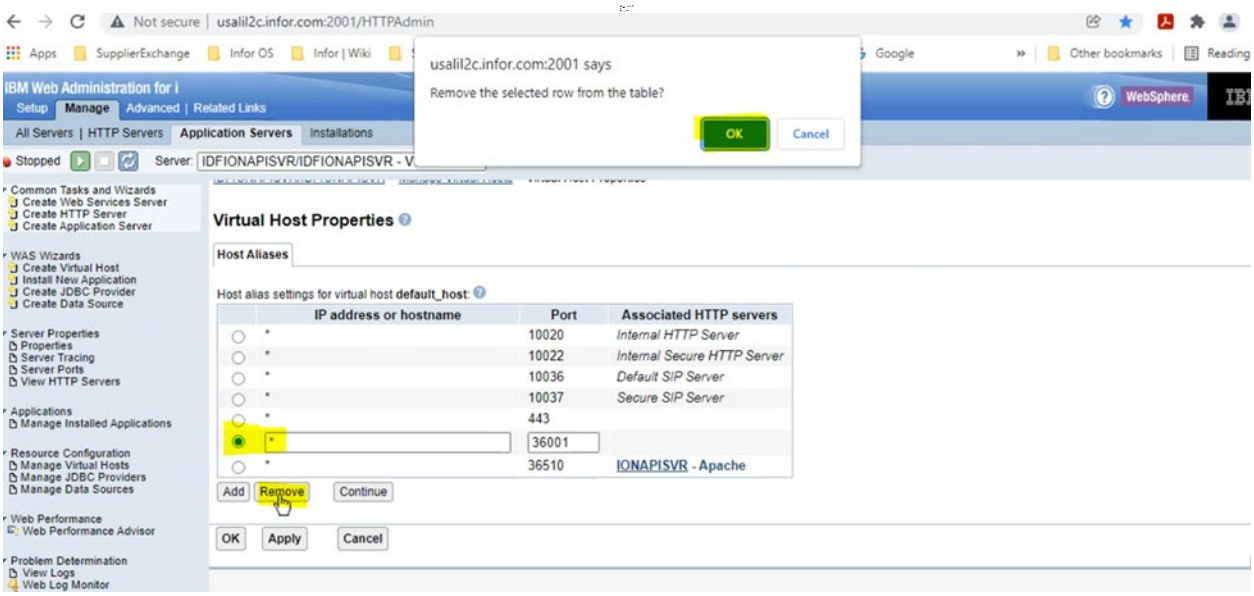
Select the default host and Click Properties



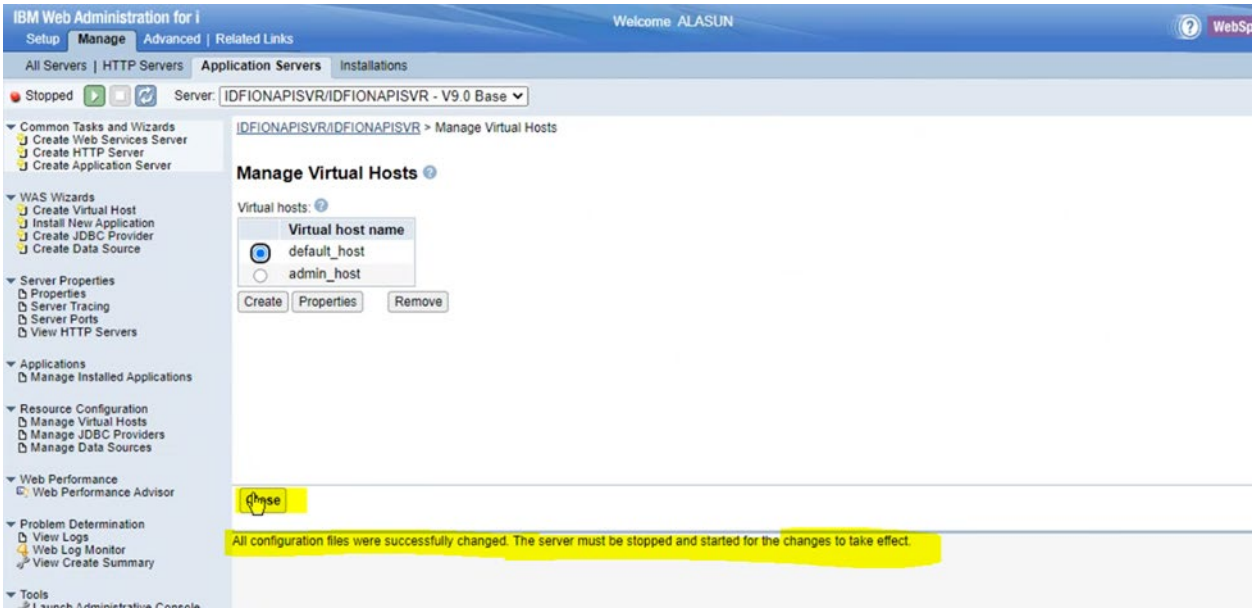
Click Add to add a Host Aliases (In the below example, added 36510 as a port).



Select the **36001** port and Click Remove. Click **Apply**.

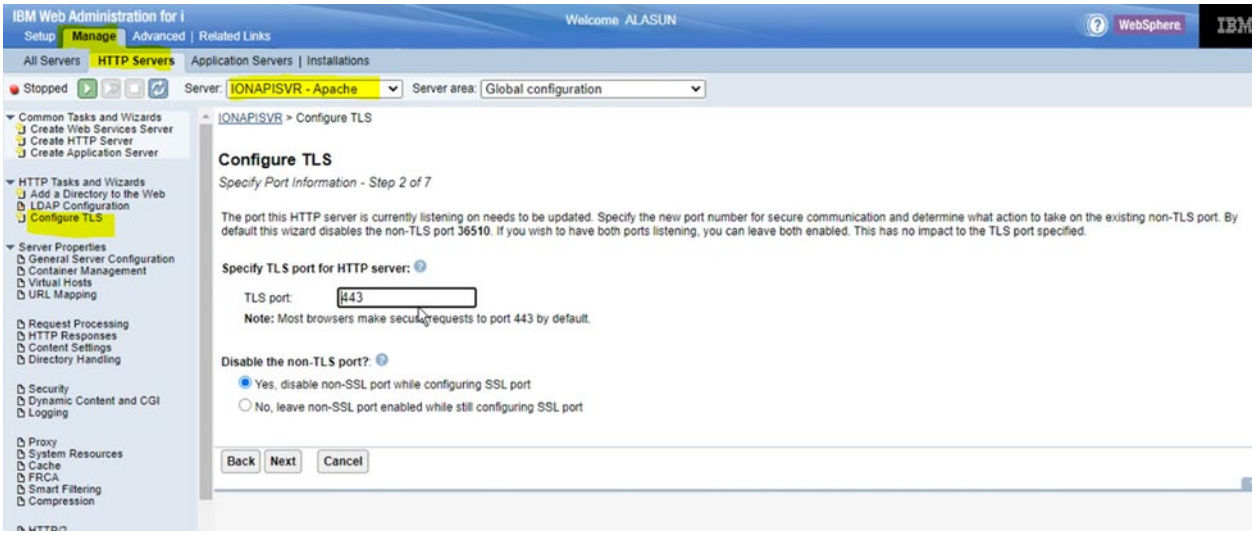


Click on close. As all configuration is saved, server must be **restarted**.

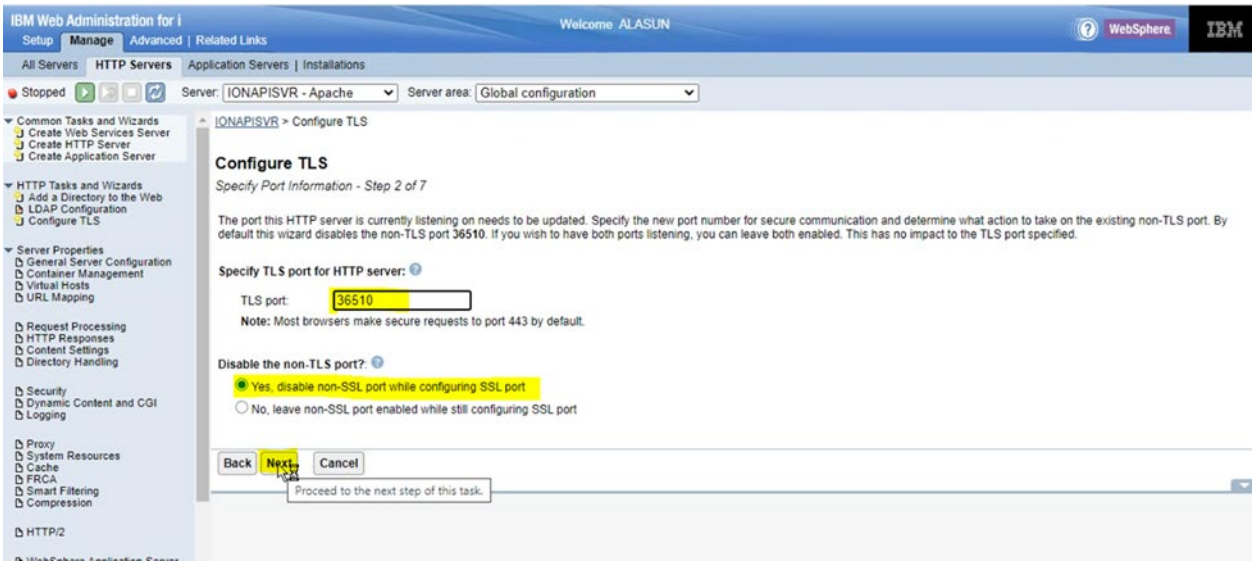


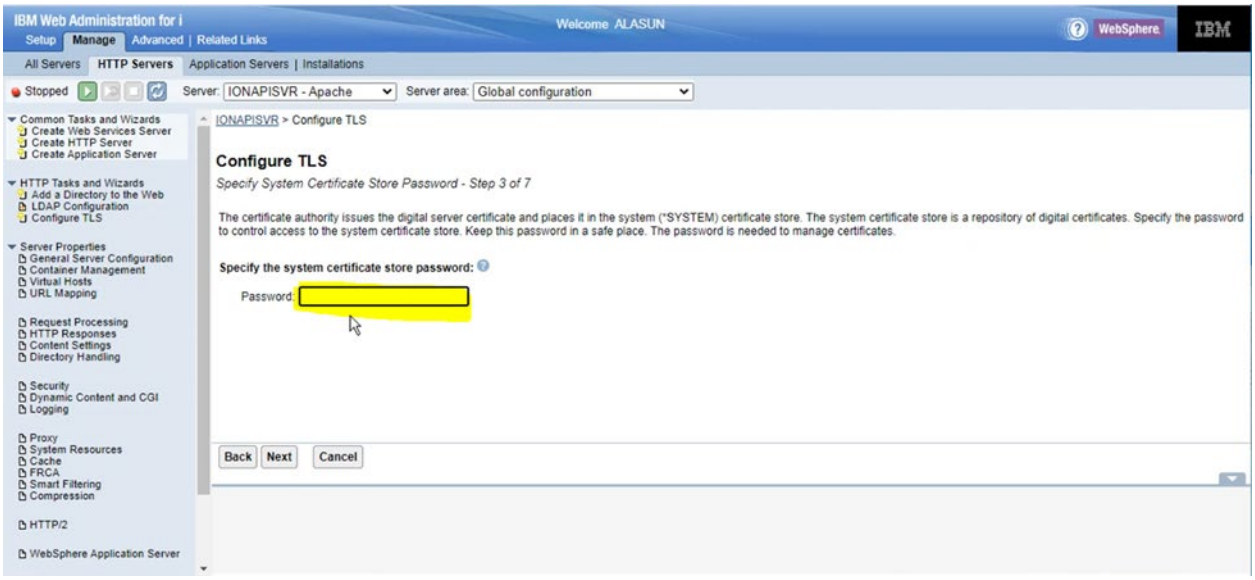
Configuring TLS:

Select Manage tab | Select HTTP Servers tab | Select Configure TLS – (HTTP Tasks and Wizards).



Give the port number (36510) select radio button for “Yes, disable non-SSL…” and Click Next.





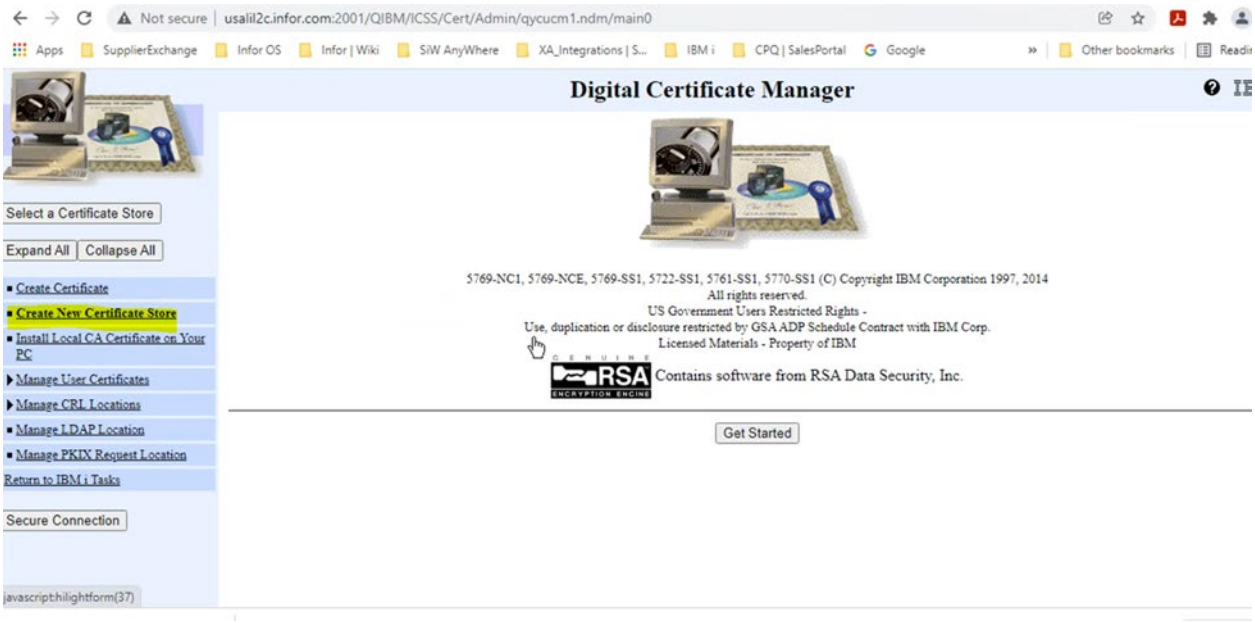
If the required system certificate store password is available on hand then enter it.

If you are sure about the password, then you can reset the password and use it.

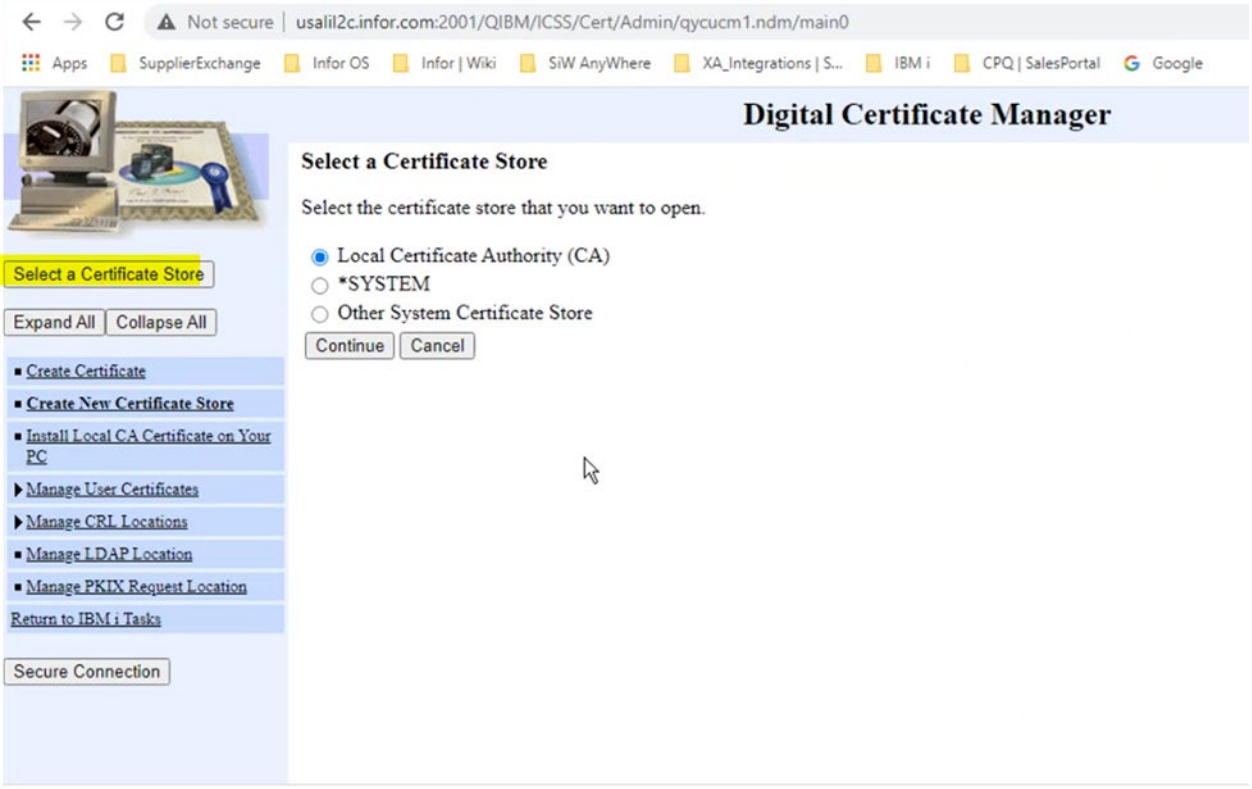
Follow “***Creating a local Certificate of Authority***” from ***System i Workspace AnyWhere Installation & Administration Guide*** to re-generate password and use here.

Example re-generation steps below:

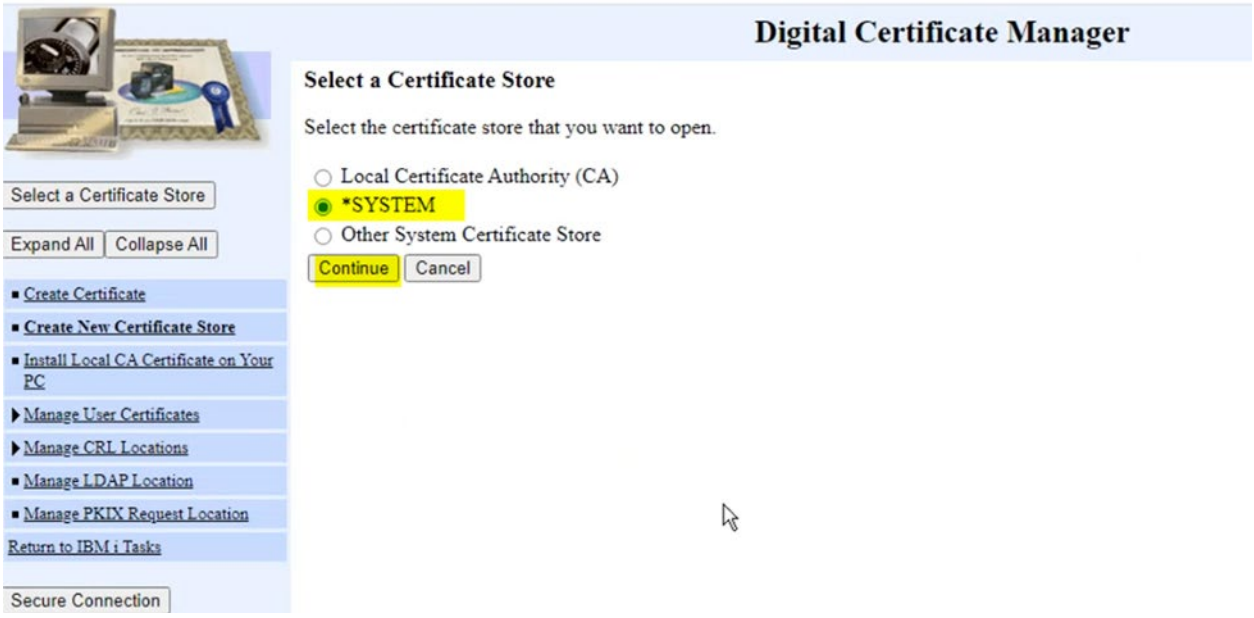
http://usalil2c.infor.com:2001/QIBM/ICSS/Cert/Admin/qycucm1.ndm/main0



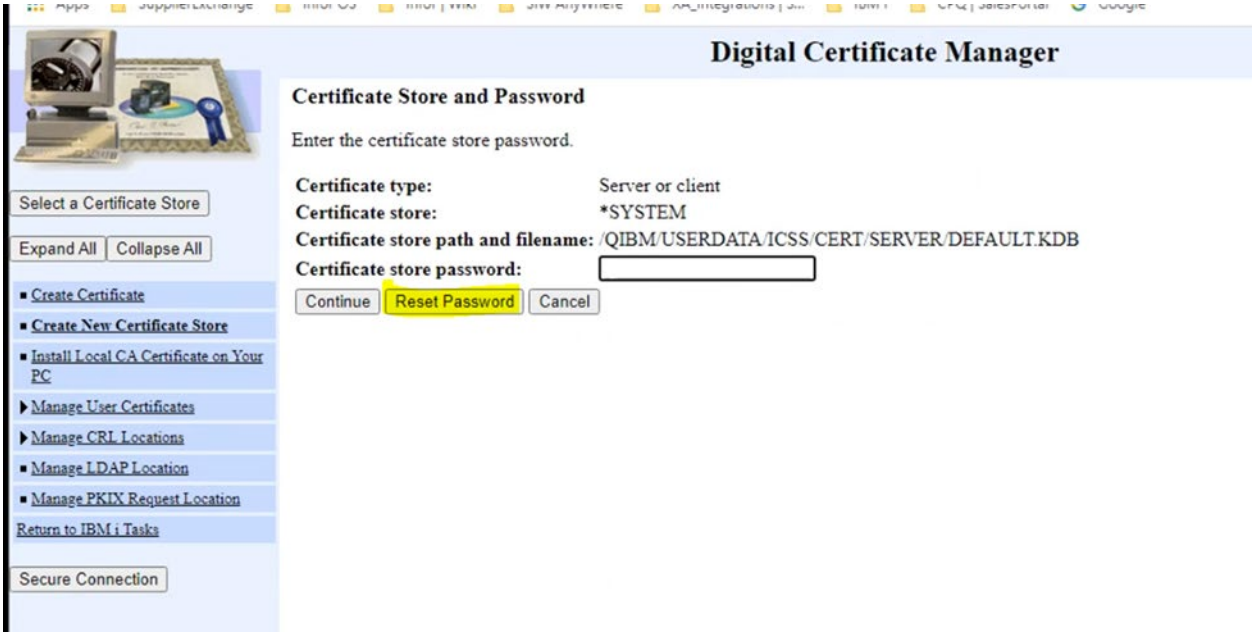
Select a Certificate Store.



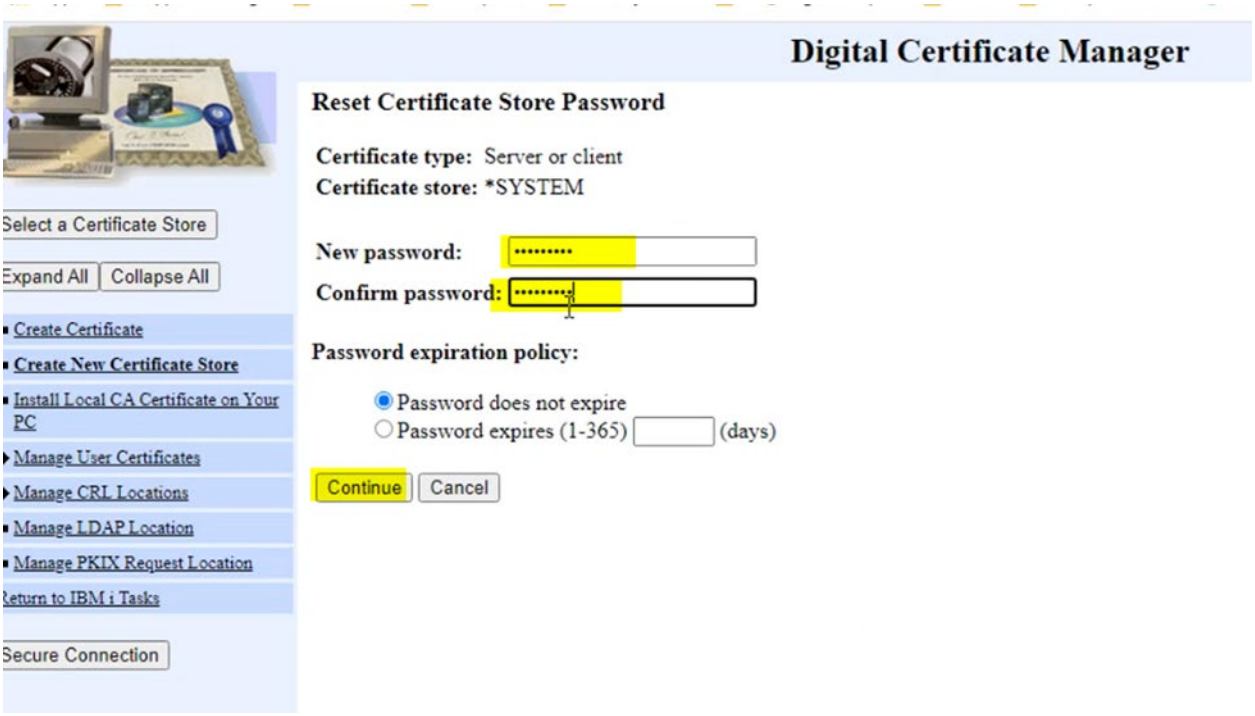
Select ***SYSTEM** and click Continue.



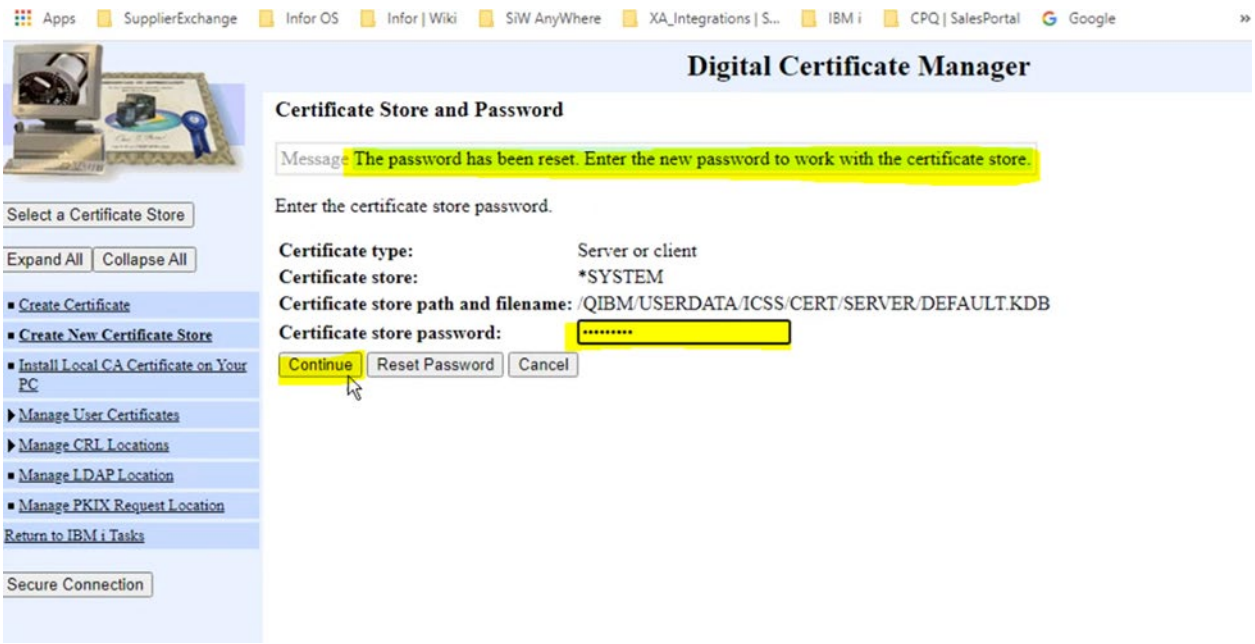
Click on reset password



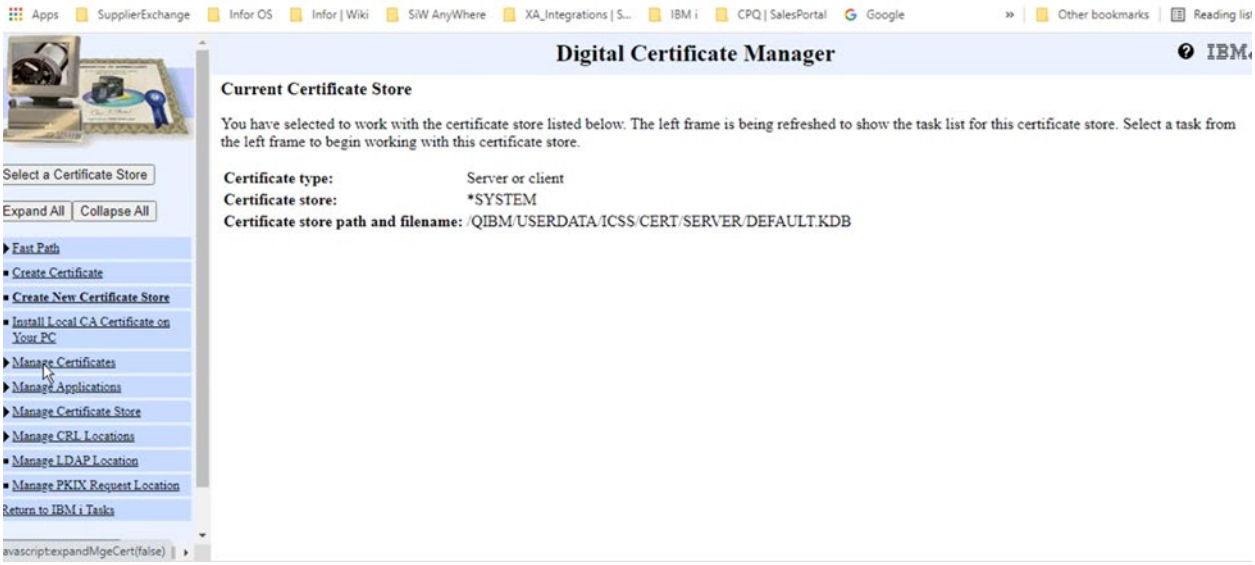
Enter and confirm the password and click on continue.



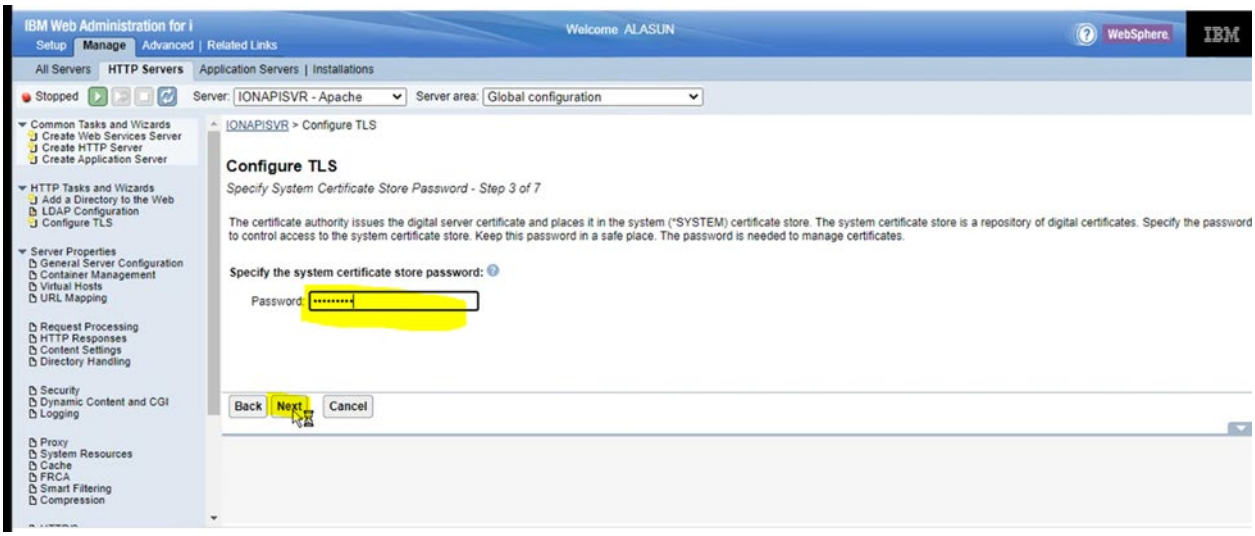
Enter the password and click on continue.



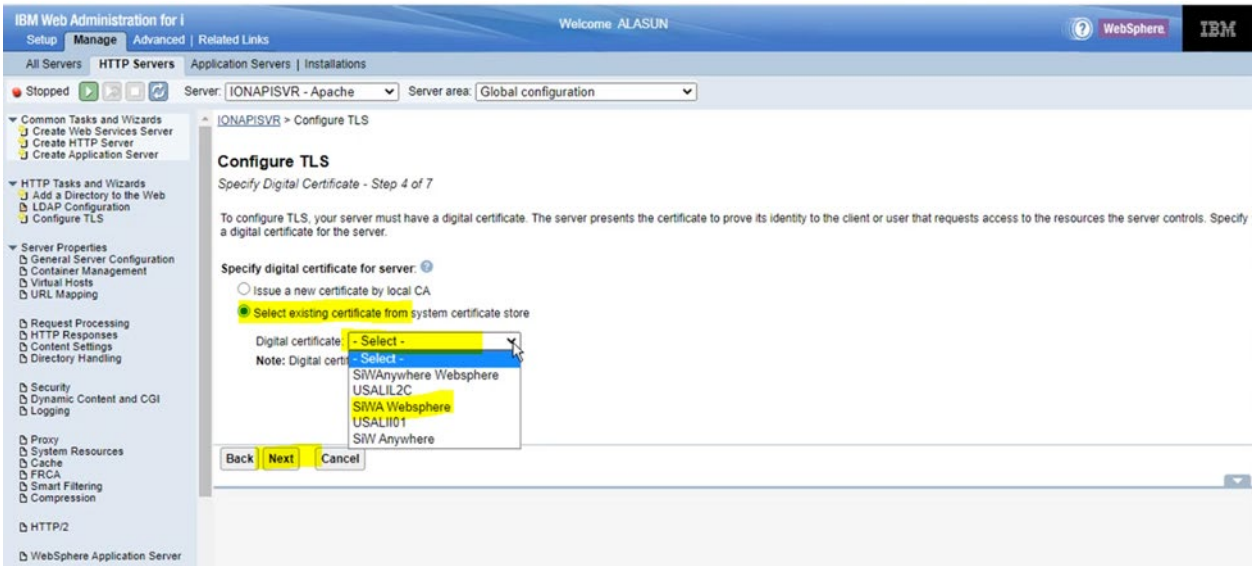
Password got changed.



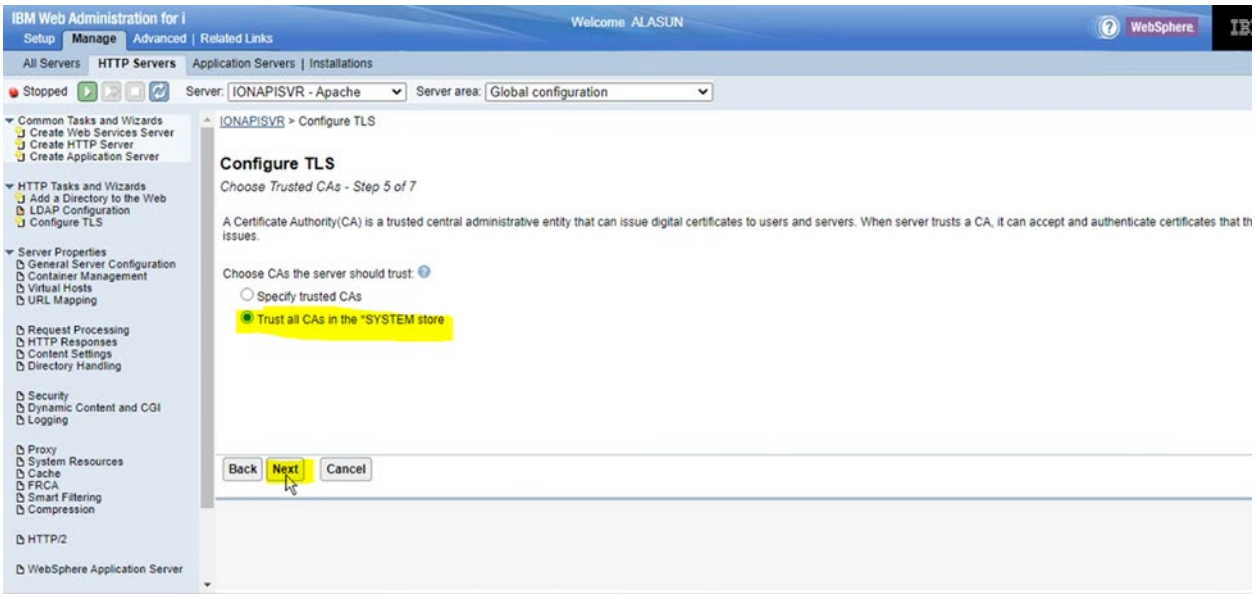
Enter the new password in the TLS page and click on next.



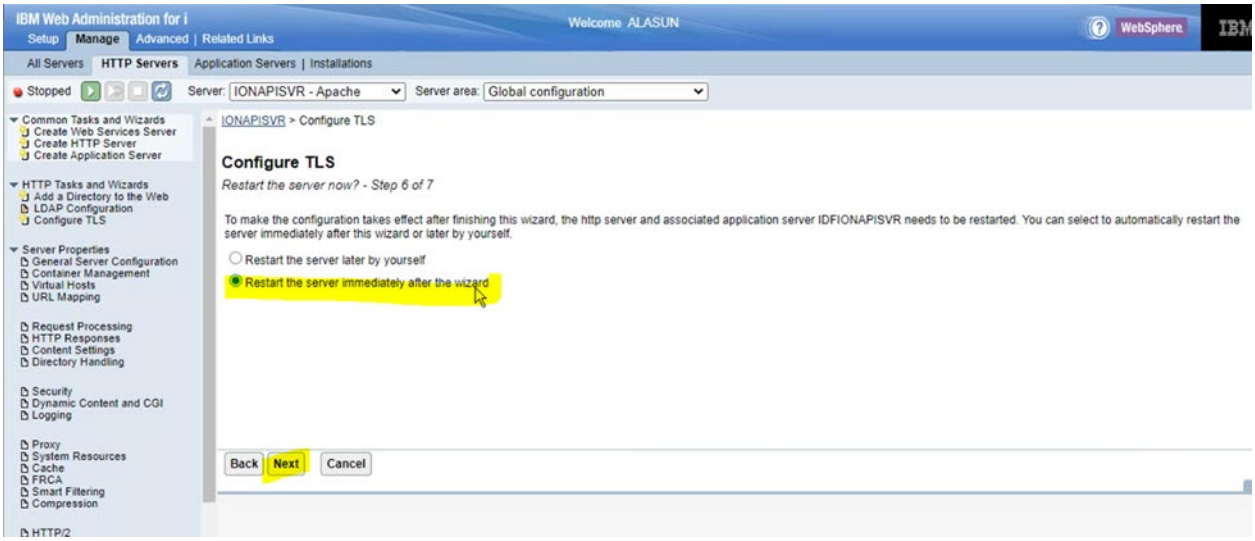
Select existing certificate from system certificate store. And select SIWA WebSphere.



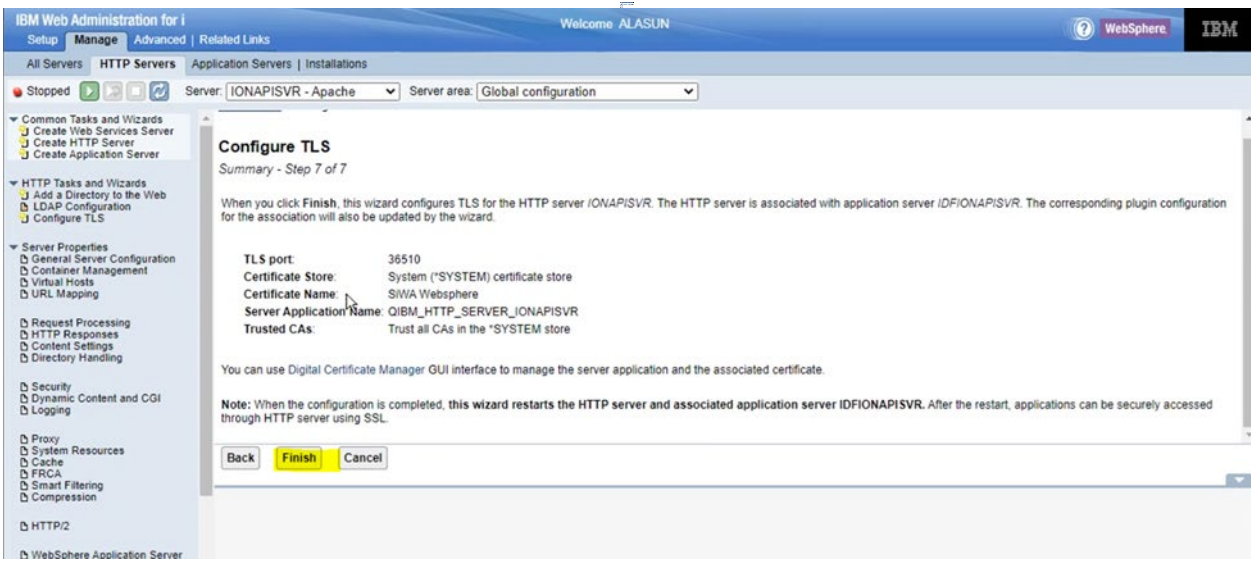
Select “Trust all CAs in the “SYSTEM store”” and click on next.



Select restart the server immediately option and click next.



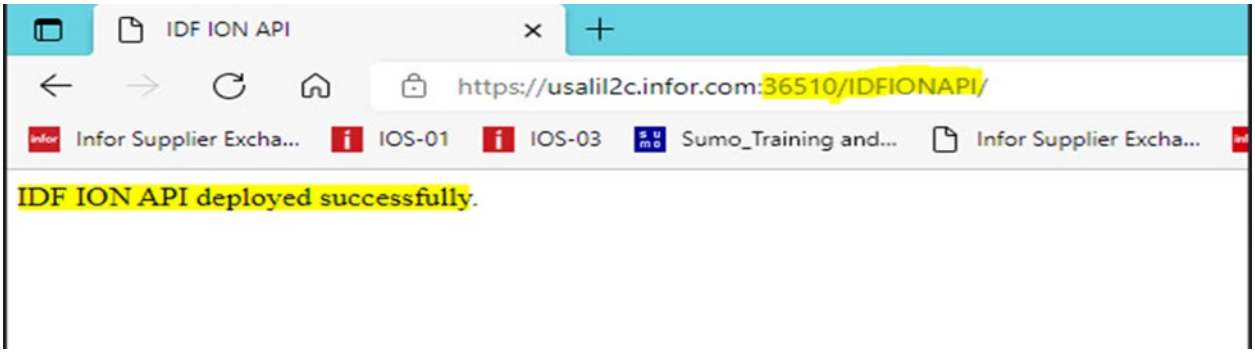
Click on finish and the servers will be restarted.



After restart validate if the IDFIONAPI deployment is successful.

https://usalil2c.infor.com:36510/IDFIONAPI/

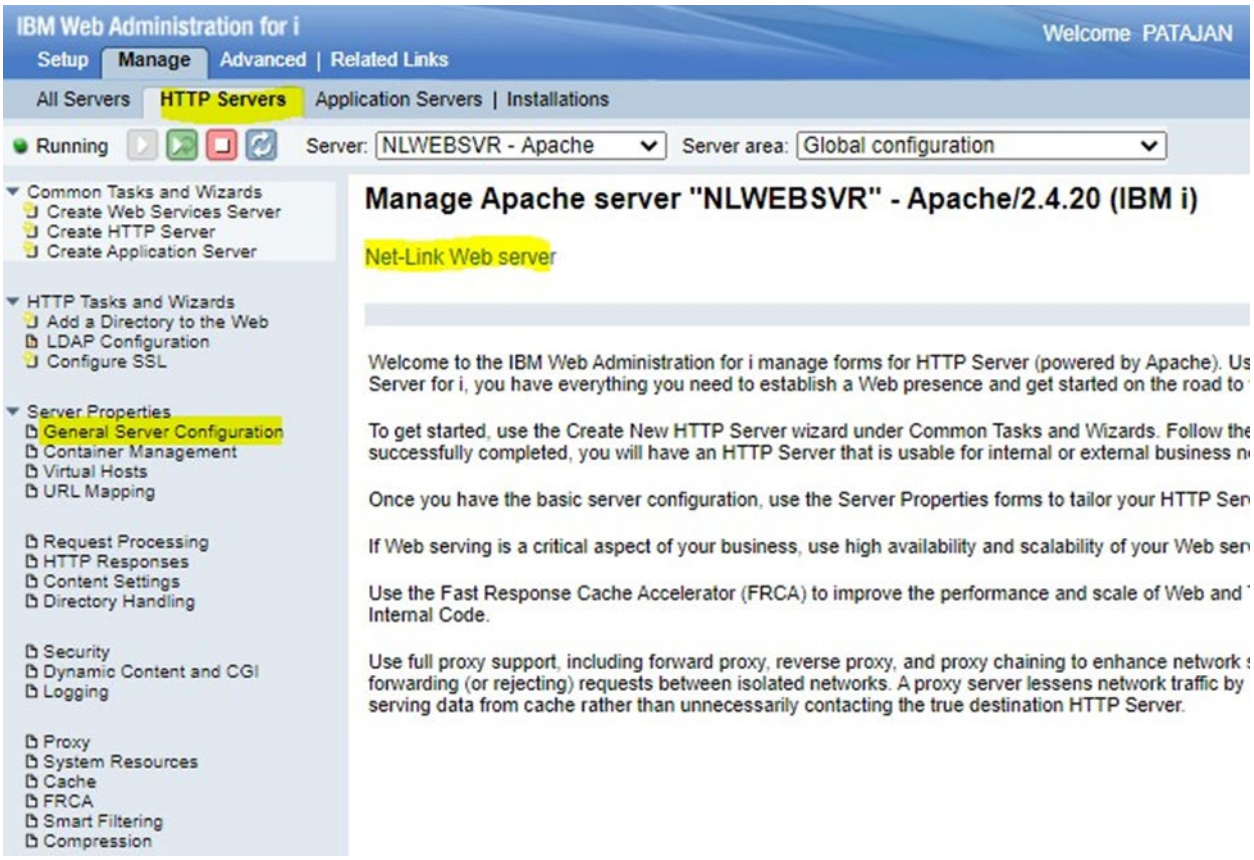
“IDF ION API deployed successfully” will be displayed.


IDF ION API
https://usalil2c.infor.com:36510/IDFIONAPI/
Infor Supplier Excha...
IOS-01
IOS-03
Sumo_Training and...
Infor Supplier Excha...
IDF ION API deployed successfully.

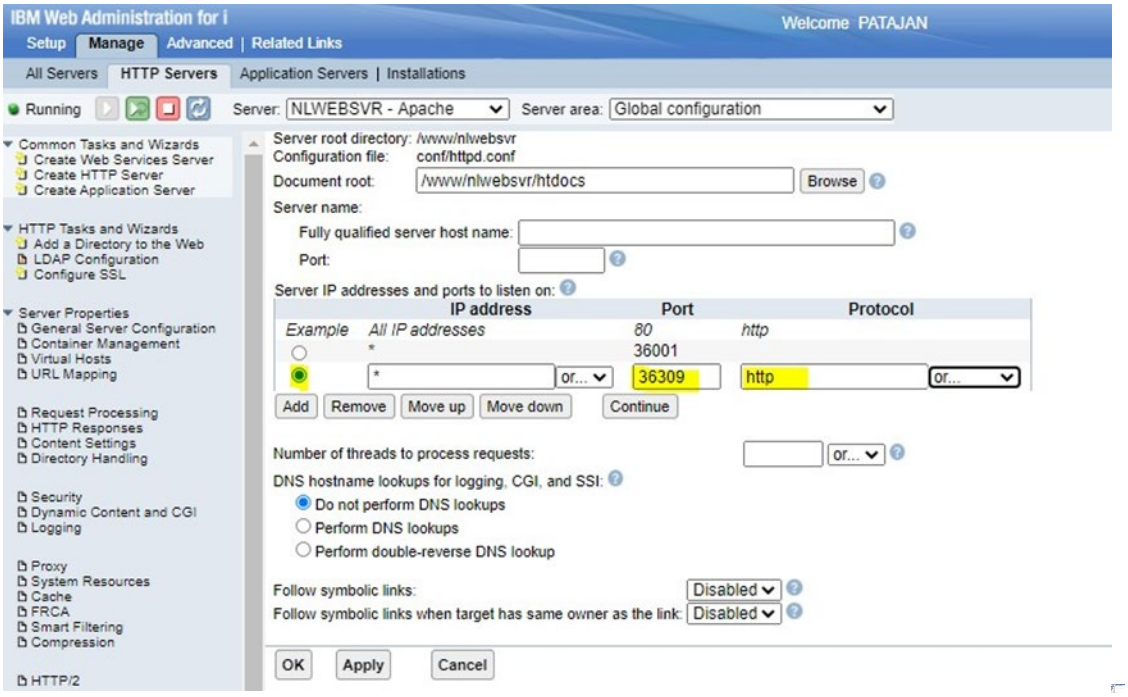
Appendix A Port Warning Reset

Follow these steps if you need to reset the assigned default Net-Link port.

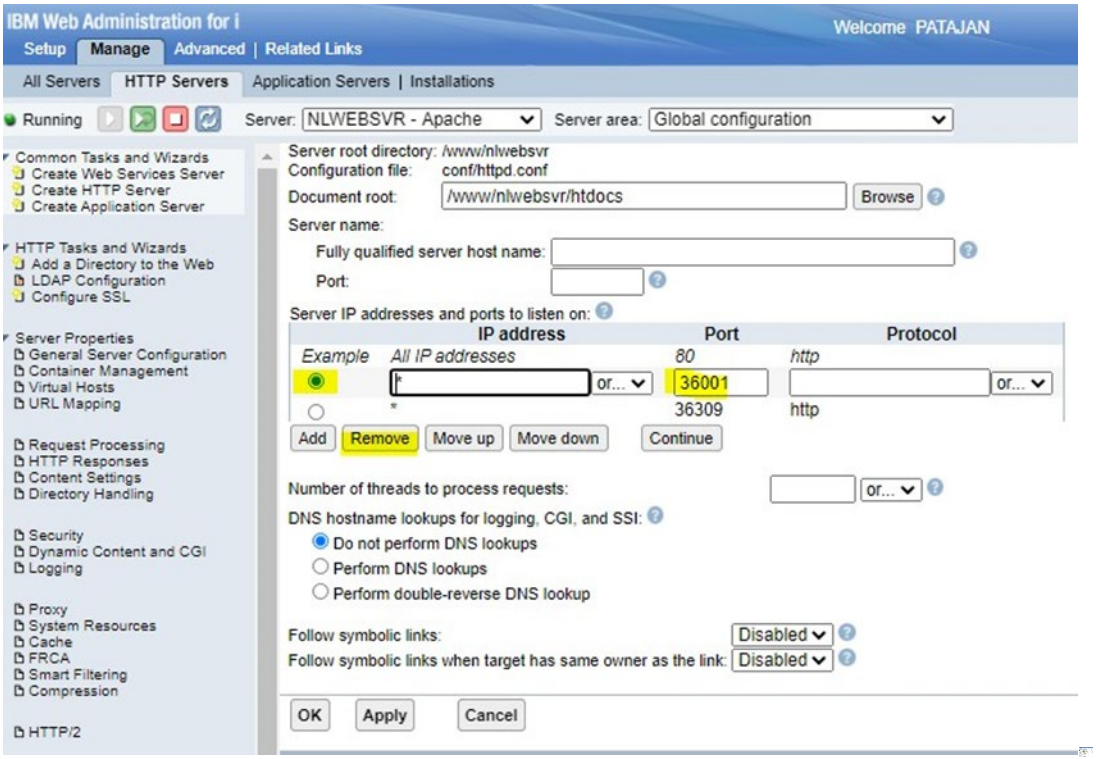
1 Select the General Server Configuration under Server Properties from the Net-Link HTTP server, as shown in below screenshot.



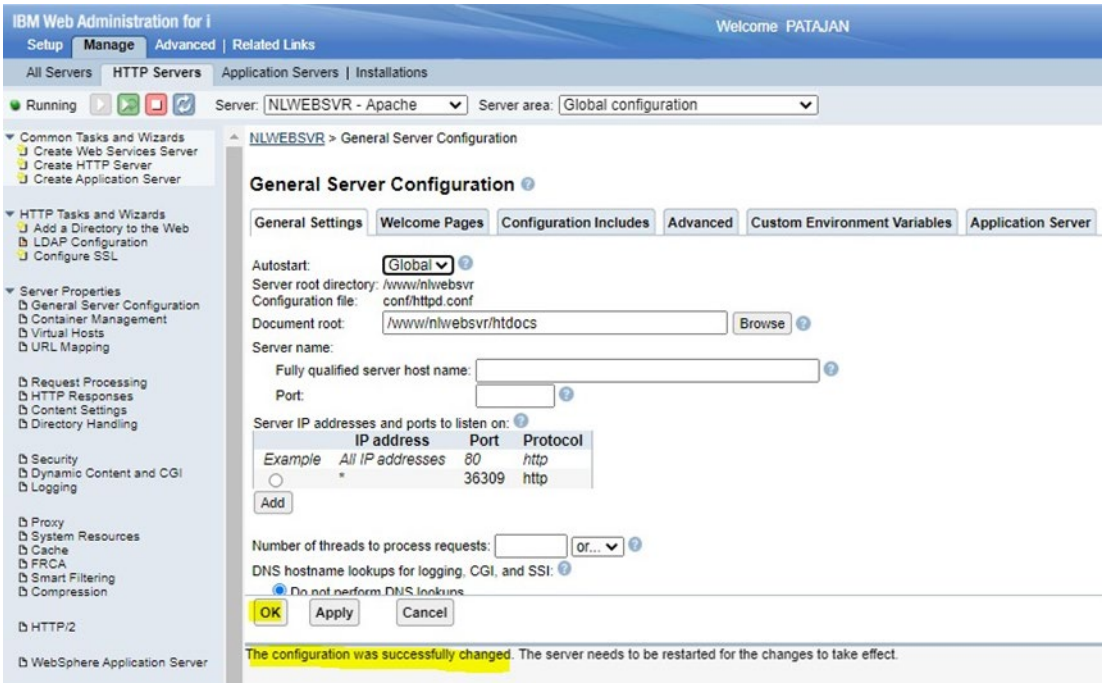
2 Navigate to General settings and Click Add to add a new port with http as a protocol (In thebelow example, added 36309 as a new unused port).



3 Select the 36001 port and Click on **Remove**.

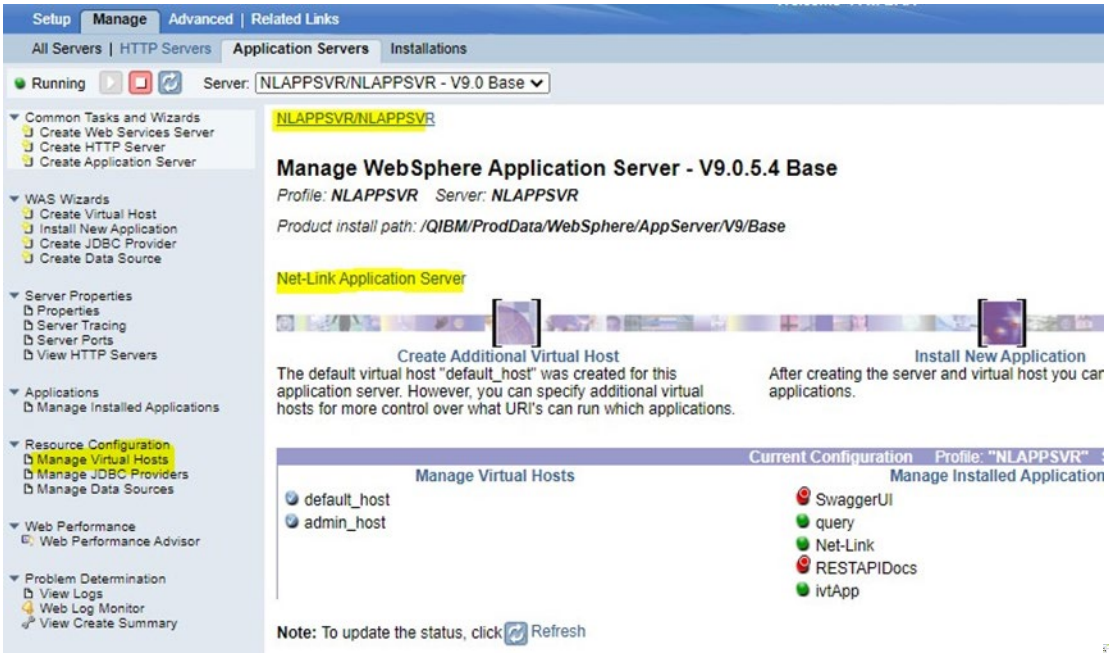


4 Click Apply.



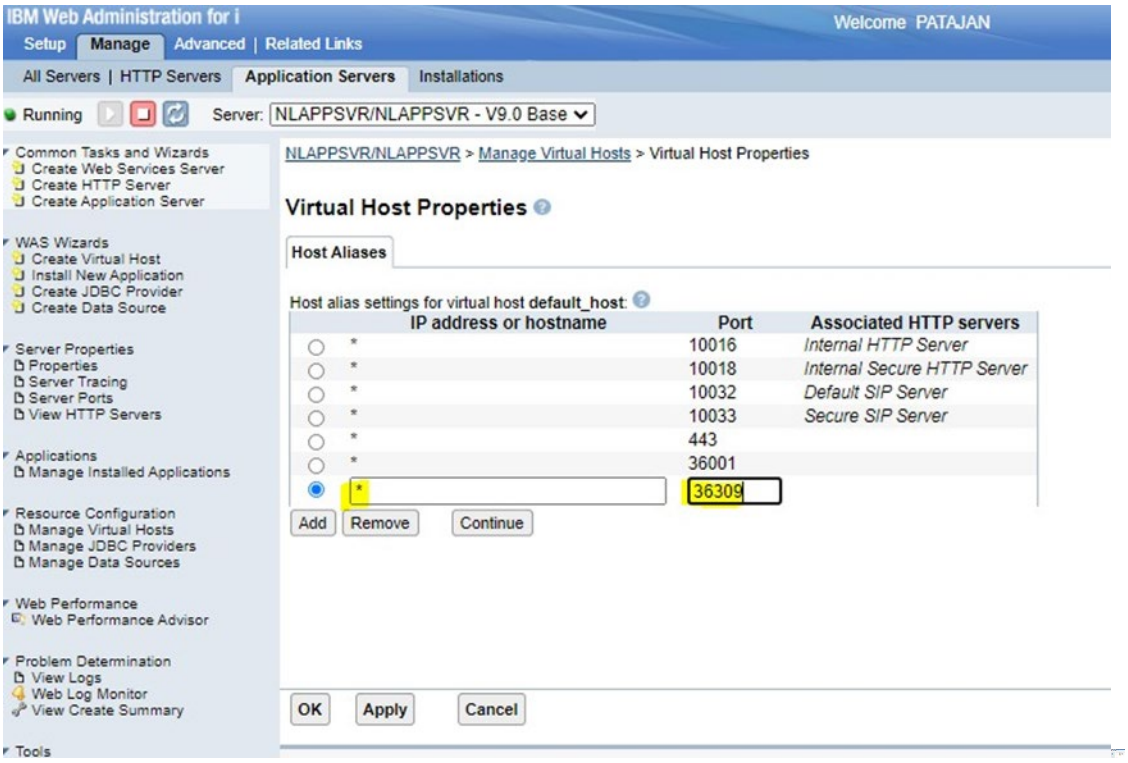
5 Click **OK** then Click **Close**.

6 Select the Manage Virtual Hosts under Resource Configuration from the Net-Link Application server, as shown in below screenshot.

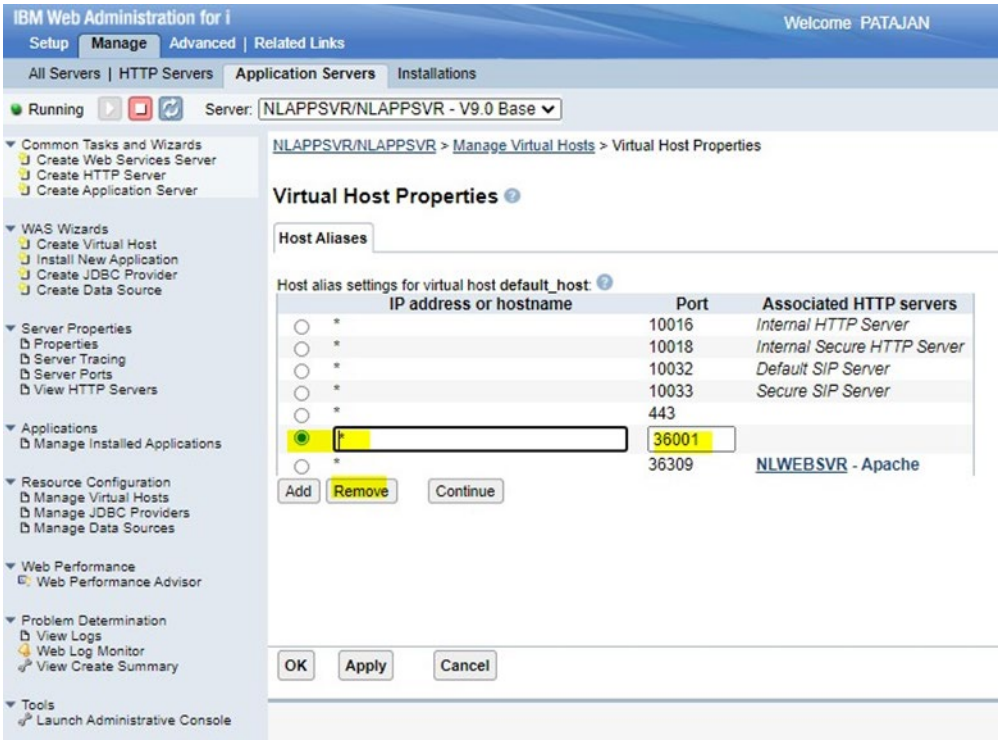


7 Select the default host and Click **Properties**.

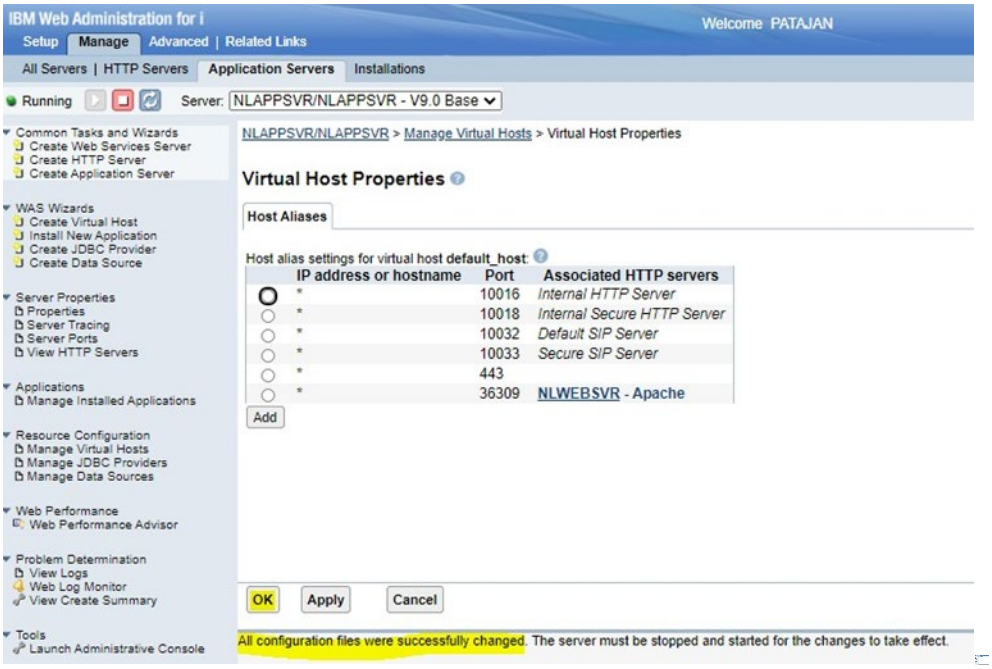
8 Click **Add** to add a Host Aliases (In the below example, added 36309 as a port).



9 Select the 36001 port and Click **Remove**. Click **Apply.**



10 Click **OK** then Click **Close**.

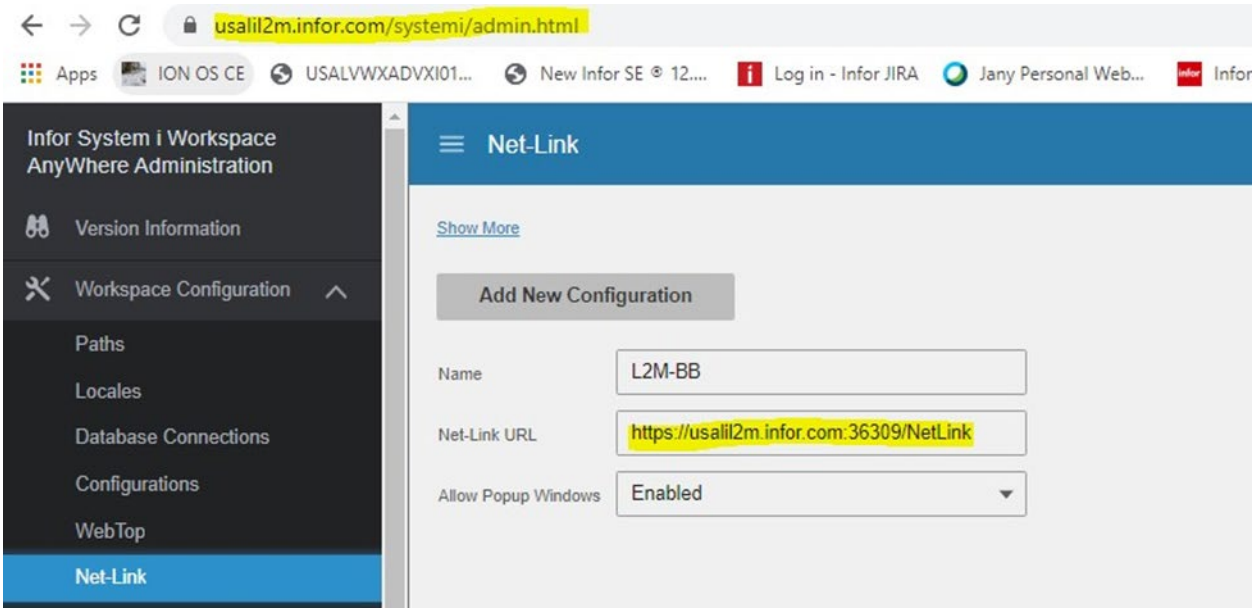


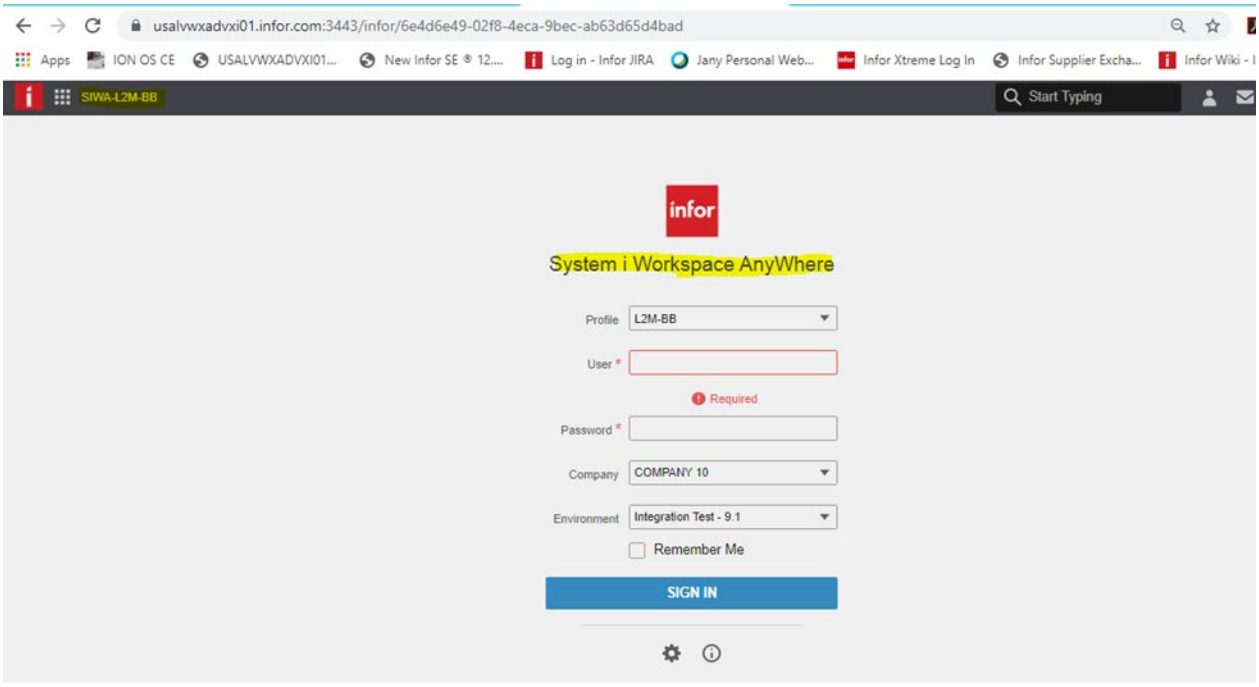
Restart both the Net-Link HTTP and Application servers to make sure changes has been reflected successfully.

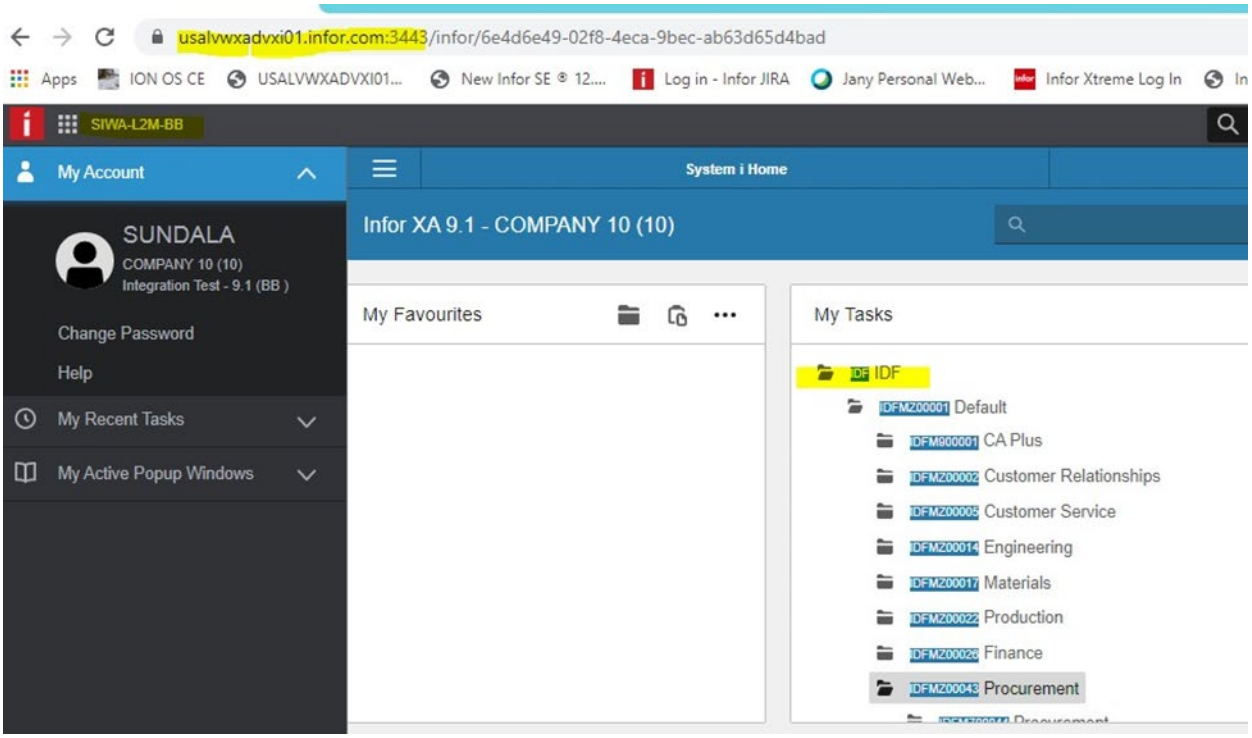
Appendix B Workspace Net-Link URL configuration

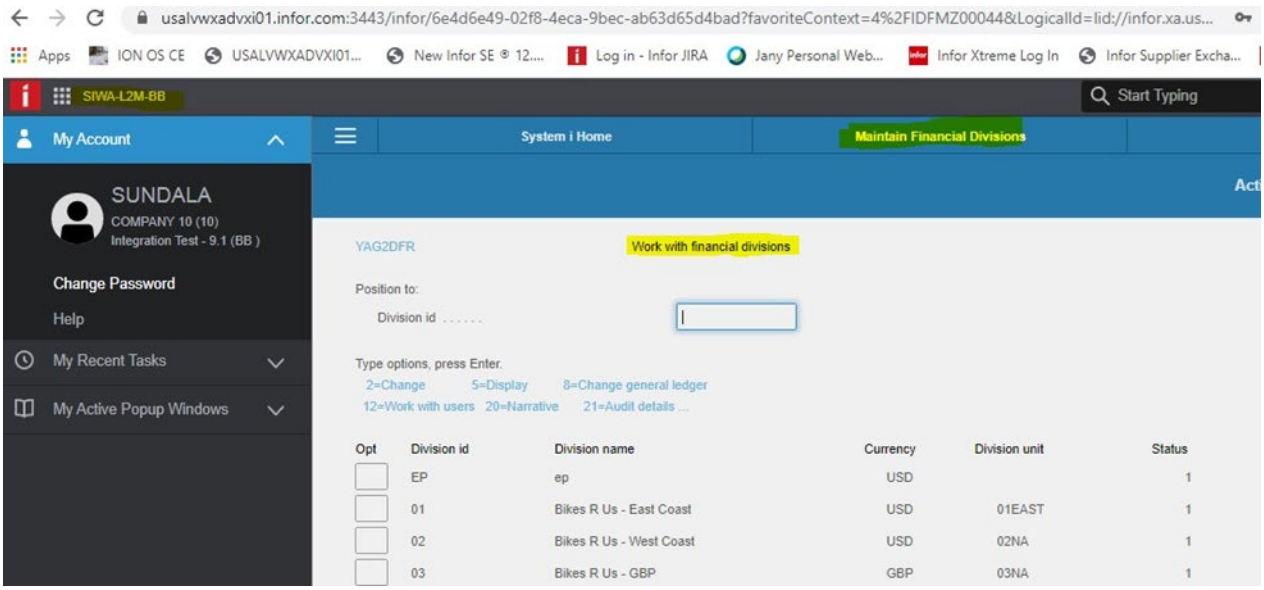
The Net-Link URL is set up in the admin.html file as http://iseries:port/NetLink. to the URL must now refer to the web app running inside WebSphere (with ssl). In the Workspace URL (Refer address bar) replace '/systemi' with '/NetLink' (For example: https://usalil2m.infor.com:36309/NetLink).

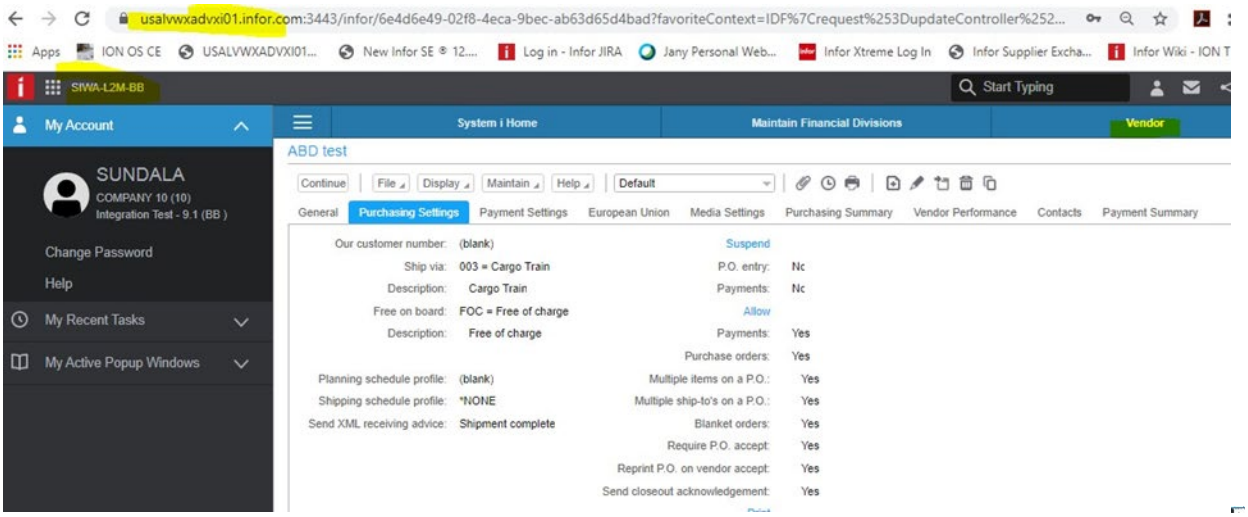
The below screenshot represents that, we are able to launch and access the System i Workspace Anywhere WebSphere application using the Infor OS on premise.




usalvwxadvxi01.infor.com:3443/infor/6e4d6e49-02f8-4eca-9bec-ab63d65d4bad
Apps
ION OS CE
USALVWXADVXI01...
New Infor SE ® 12....
Log in - Infor JIRA
Jany Personal Web...
Infor Xtreme Log In
Infor Supplier Excha...
Infor Wiki - I
SIWA-L2M-BB
Start Typing
infor
System i Workspace AnyWhere
Profile
L2M-BB
User *
Required
Password *
Company
COMPANY 10
Environment
Integration Test - 9.1
Remember Me
SIGN IN


usalvwxadvxi01.infor.com:3443/infor/6e4d6e49-02f8-4eca-9bec-ab63d65d4bad
Apps
ION OS CE
USALVWXADVXI01...
New Infor SE ® 12....
Log in - Infor JIRA
Jany Personal Web...
Infor Xtreme Log In
SIWA-L2M-BB
My Account
SUNDALA
COMPANY 10 (10)
Integration Test - 9.1 (BB)
Change Password
Help
My Recent Tasks
My Active Popup Windows
System i Home
Infor XA 9.1 - COMPANY 10 (10)
My Favourites
My Tasks
IDF
IDFMZ00001 Default
IDFM900001 CA Plus
IDFMZ00002 Customer Relationships
IDFMZ00005 Customer Service
IDFMZ00014 Engineering
IDFMZ00017 Materials
IDFMZ00022 Production
IDFMZ00023 Finance
IDFMZ00043 Procurement


usalvwxadvxi01.infor.com:3443/infor/6e4d6e49-02f8-4eca-9bec-ab63d65d4bad?favoriteContext=4%2FIDFMZ00044&LogicalId=lid://infor.xa.us...
Apps
ION OS CE
USALVWXADVXI01...
New Infor SE ® 12....
Log in - Infor JIRA
Jany Personal Web...
Infor Xtreme Log In
Infor Supplier Excha...
SIWA-L2M-BB
Start Typing
My Account
SUNDALA
COMPANY 10 (10)
Integration Test - 9.1 (BB)
Change Password
Help
My Recent Tasks
My Active Popup Windows
System i Home
Maintain Financial Divisions
YAG2DFR
Work with financial divisions
Position to:
Division id . . . . . .
Type options, press Enter.
2=Change 5=Display 8=Change general ledger
12=Work with users 20=Narrative 21=Audit details ...
Opt
Division id
Division name
Currency
Division unit
Status
EP
ep
USD
1
01
Bikes R Us - East Coast
USD
01EAST
1
02
Bikes R Us - West Coast
USD
02NA
1
03
Bikes R Us - GBP
GBP
03NA
1


usalvwxadvxi01.infor.com:3443/infor/6e4d6e49-02f8-4eca-9bec-ab63d65d4bad?favoriteContext=IDF%7Crequest%253DupdateController%252...
Apps
ION OS CE
USALVWXADVXI01...
New Infor SE ® 12....
Log in - Infor JIRA
Jany Personal Web...
Infor Xtreme Log In
Infor Supplier Excha...
Infor Wiki - ION T
SIWA-L2M-BB
Start Typing
My Account
SUNDALA
COMPANY 10 (10)
Integration Test - 9.1 (BB)
Change Password
Help
My Recent Tasks
My Active Popup Windows
System i Home
Maintain Financial Divisions
Vendor
ABD test
Continue
File
Display
Maintain
Help
Default
General
Purchasing Settings
Payment Settings
European Union
Media Settings
Purchasing Summary
Vendor Performance
Contacts
Payment Summary
Our customer number: (blank)
Ship via: 003 = Cargo Train
Description: Cargo Train
Free on board: FOC = Free of charge
Description: Free of charge
Planning schedule profile: (blank)
Shipping schedule profile: *NONE
Send XML receiving advice: Shipment complete
Suspend
P.O. entry: Nc
Payments: Nc
Allow
Payments: Yes
Purchase orders: Yes
Multiple items on a P.O.: Yes
Multiple ship-to's on a P.O.: Yes
Blanket orders: Yes
Require P.O. accept: Yes
Reprint P.O. on vendor accept: Yes
Send closeout acknowledgement: Yes

Appendix C WAR file redeployment

WAR file redeployment

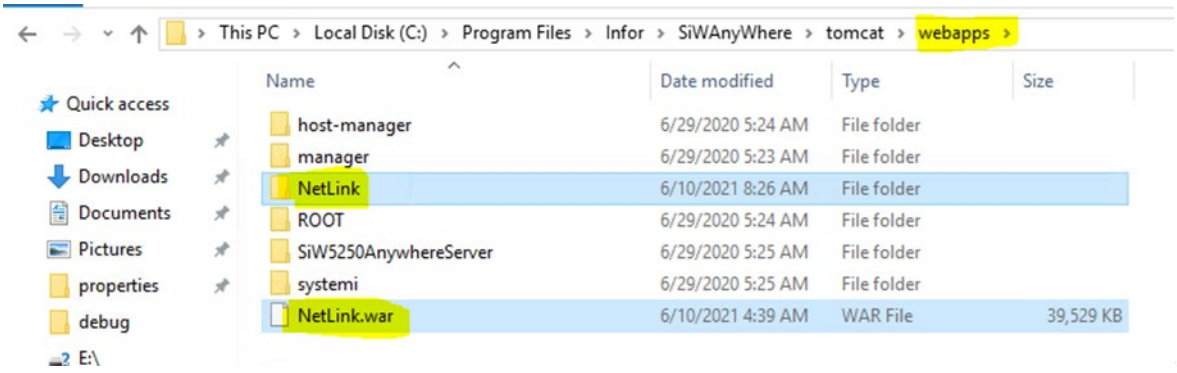
This section explains about the procedure on Net-Link WAR file redeployment. We perform this section only, whenever we want to redeploy the Net-Link war file with new changes.

WAR file generation

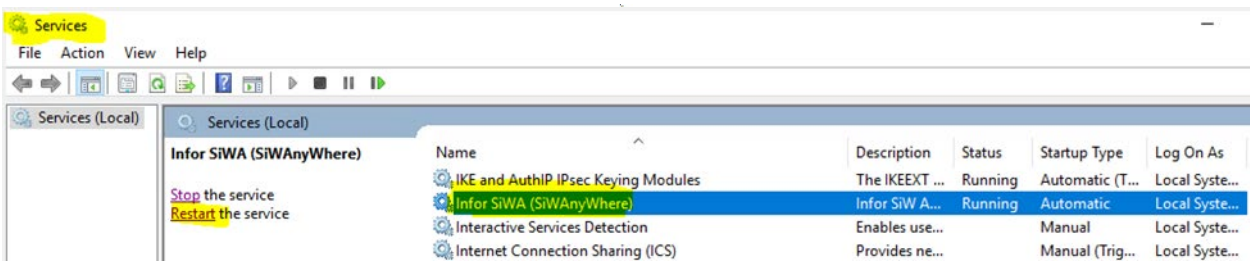
Follow the "**WAR file generation**" section above in this document.

Tomcat (version 7.0 +)

- Delete or take the backup of the ***NetLink.war*** file & ***NetLink*** folder from the root of the ***webapps*** folder of theTomcat instance, shown as below.



- The redeployment of WAR file involves copying the WAR file to the root of the ***webapps*** folder of the Tomcat instance. The update is automatically loaded by Tomcat.
- Restart the Infor SiWA service from Windows→ Services, shown as below.



WebSphere (version 9.x)

Check that you have the following subsystem running, and that all ADMIN jobs are running within the subsystem:

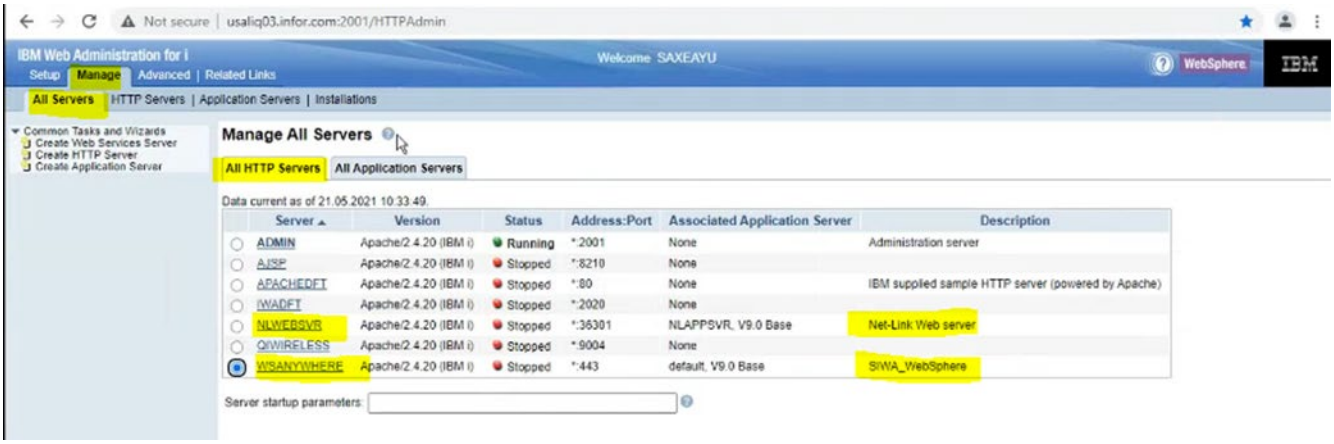
WRKSBSJOB QHTTPSVR

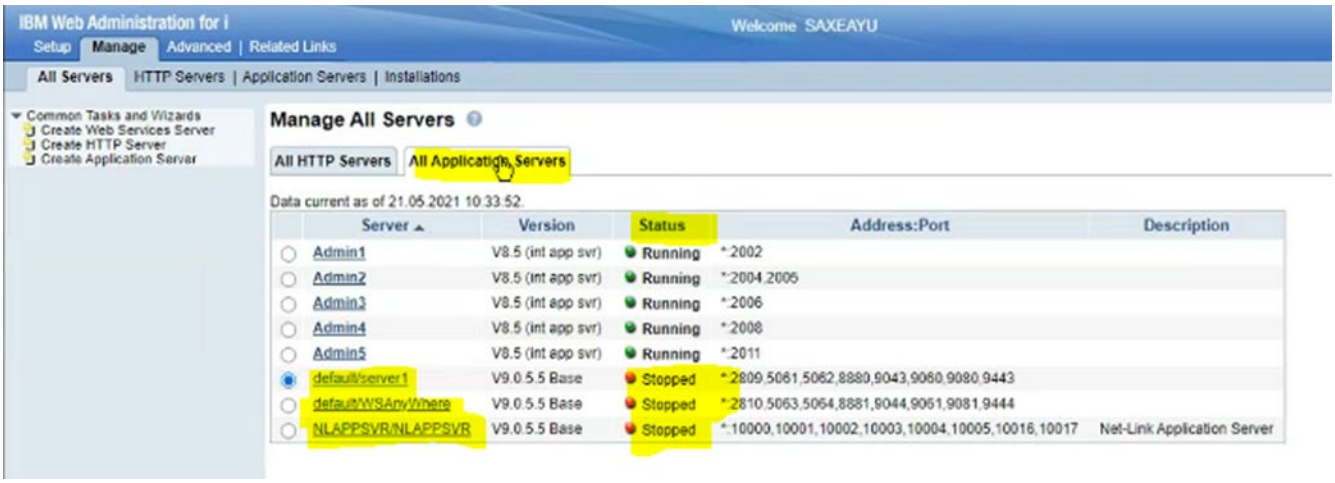
If the subsystem is not active, issue the following OS400 command:

STRTCPSVR SERVER(*HTTP) HTTPSVR(*ADMIN)

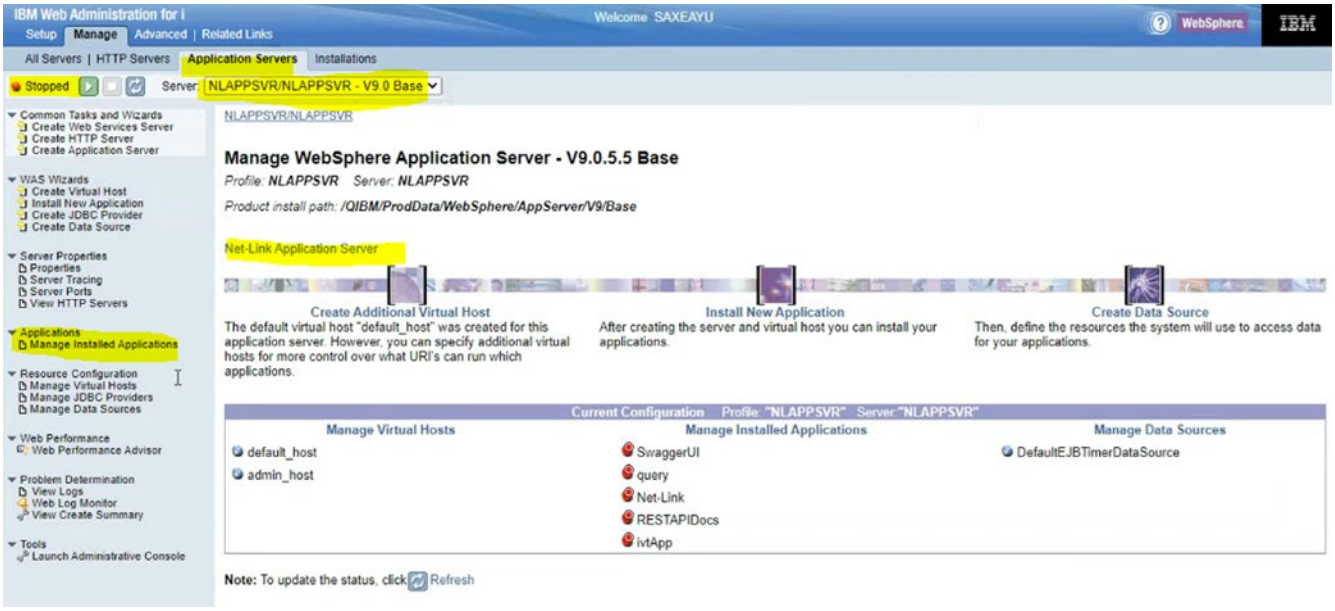
For deployment of WAR file using WebSphere, execute below steps:

1. Replace the existing Net-Link WAR file with the new Net-Link WAR file on the IFS of the iSeries which is preferably a ‘scratch’ folder.However, the location can also be in the root.
2. Open the HTTP Administration console (http://{hostName}:2001/HTTPAdmin), and log in with *SECADM authority.
3. Stop the HTTP server and its associated Application server instances for both the SiWA & NetLink applications.

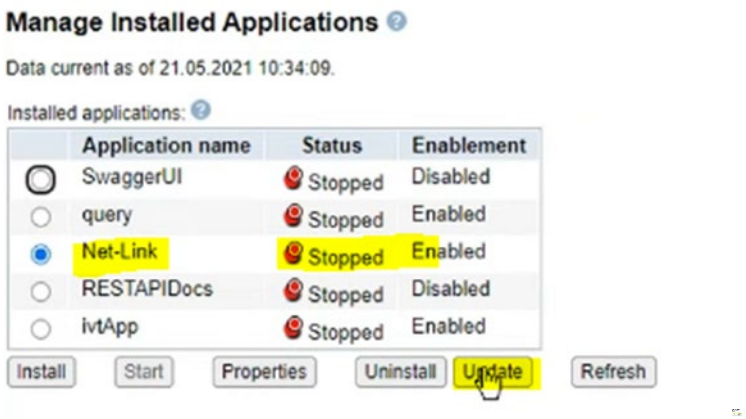




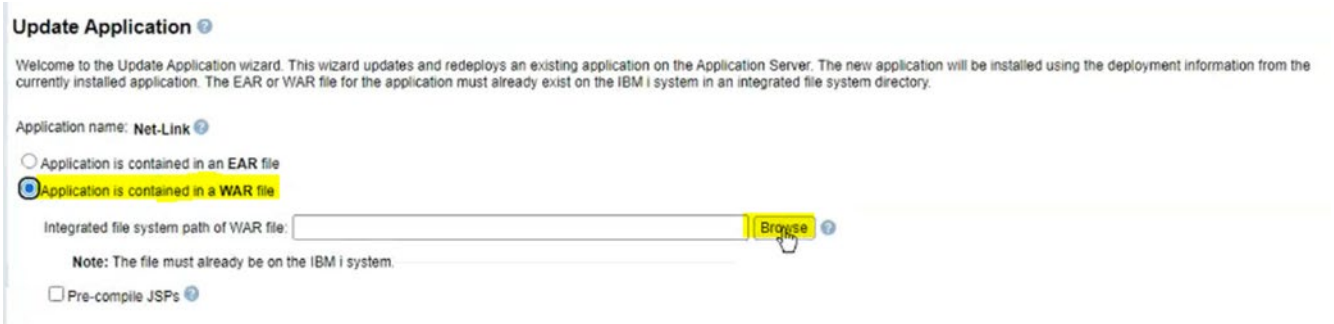
4 Click on the Net-Link application server (NLAPPSVR/NLAPPSVR) and then Select ***Manage Installed Applications*** under ***Applications***.

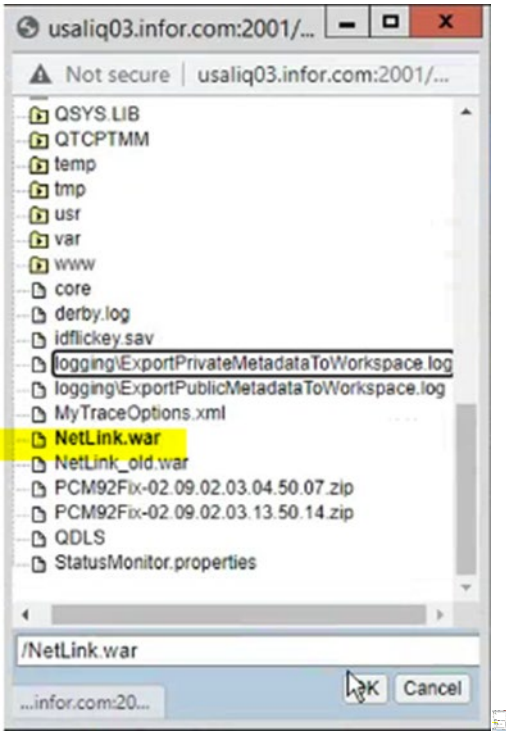


5 Select the Net-Link application and click on ***Update***, shown as below.

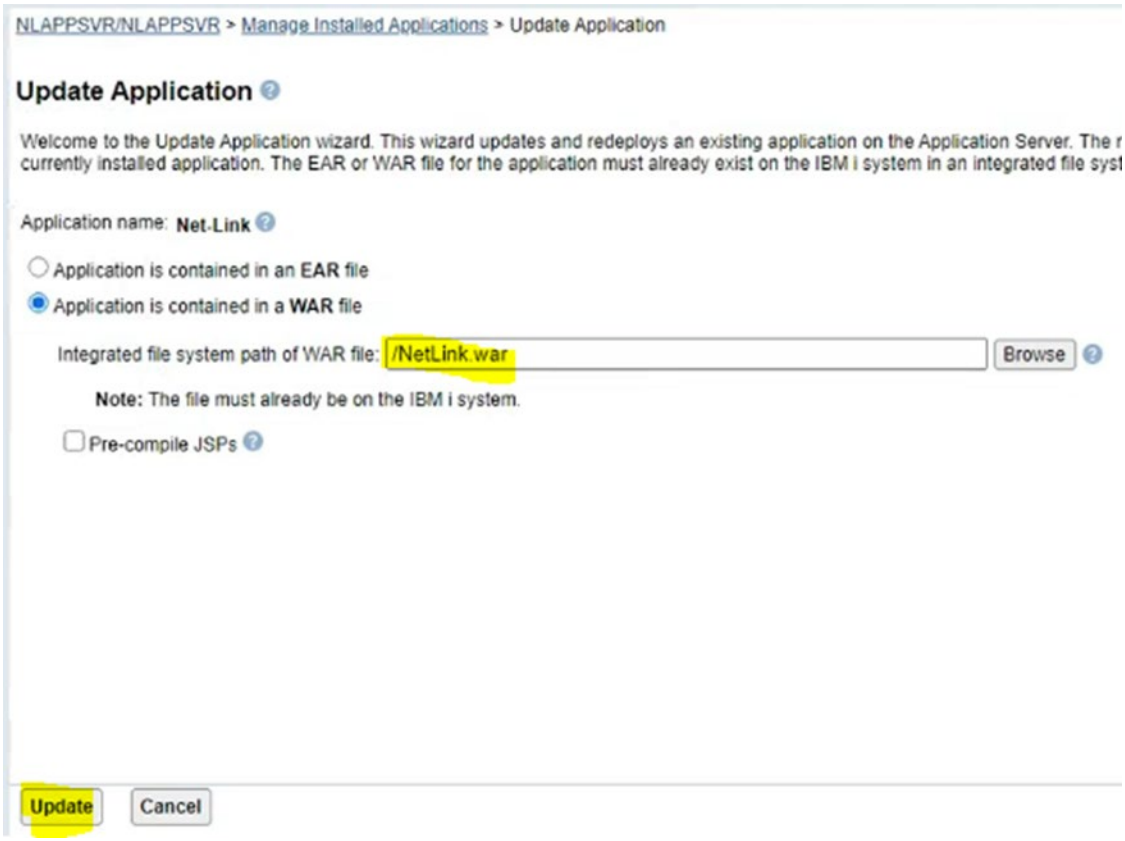


6 Select the ***Application is connected in a WAR file***, click on ***Browse*** and select the Net-Link war file and click on ***OK***.

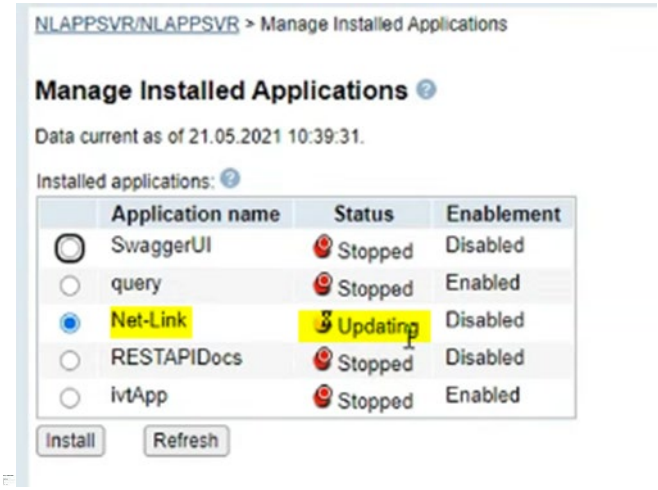




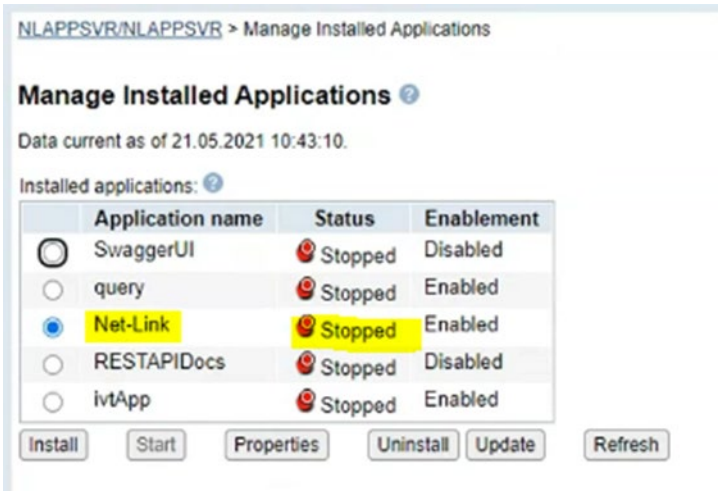
7 Click on **Update.**



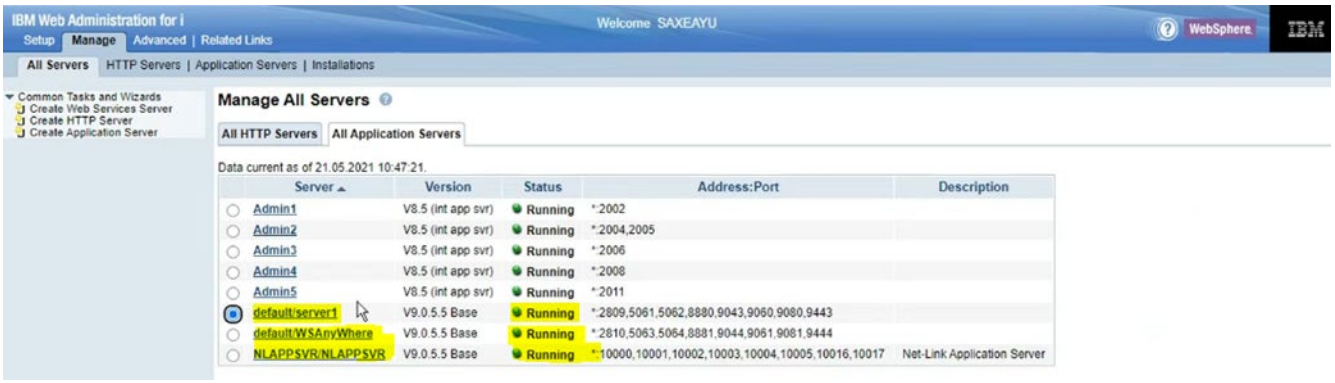
8 The Status of the Net-Link is now changed to Updating.

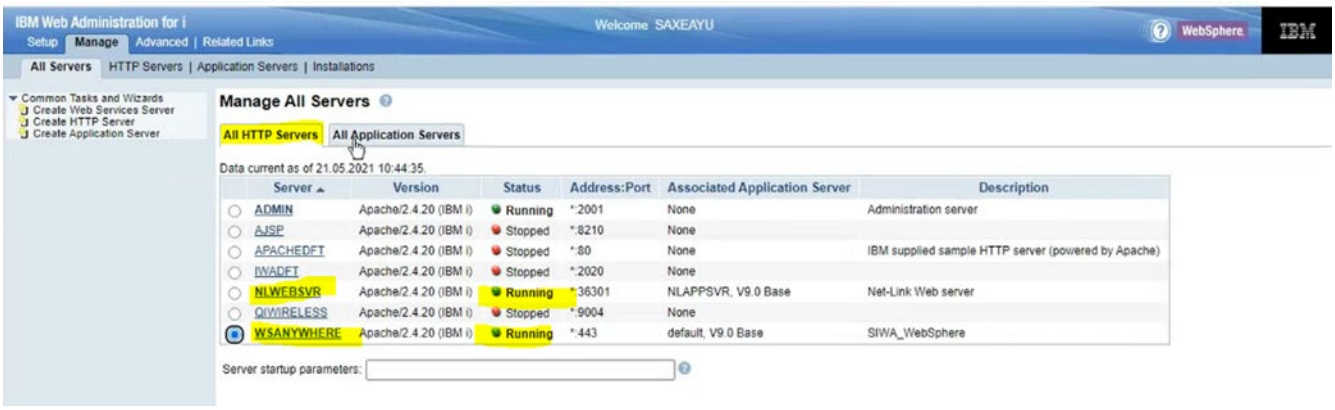


9 After successful update, the status of the Net-Link will change to Stopped.



10 Start the HTTP server and its associated Application server instances for both the SiWA & NetLink applications.





Appendix D Configuring SiWA IBMi WAS with single port

Configuring all XA web components to use a single HTTP server and port on WebSphere

To simplify web security for XA deployments where all web related components are running on a single IBM i server, a single HTTP server can be used when deploying through a firewall. The components include SiW Anywhere and Net-Link. These instructions will provide the basics for configuring this type of environment.

Approach

Install all components on a single IBM i server

Setup SIWA on SSL port 443 (default, can be different)

Setup Net-Link on another port

Net-Link is on 36001 by default

Install NetLink.war in a new WAS profile

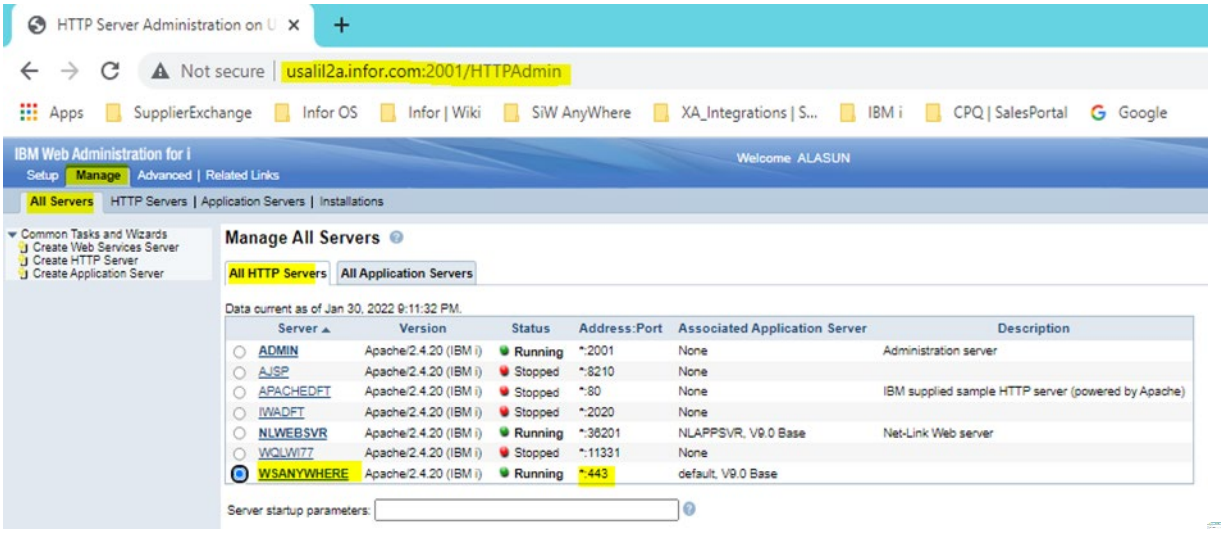
SiW Anywhere HTTPD.conf changes

1 Login to IBMi Web Administration, using the below URL (where **hostname**, is the FQDN of the IBMi server)

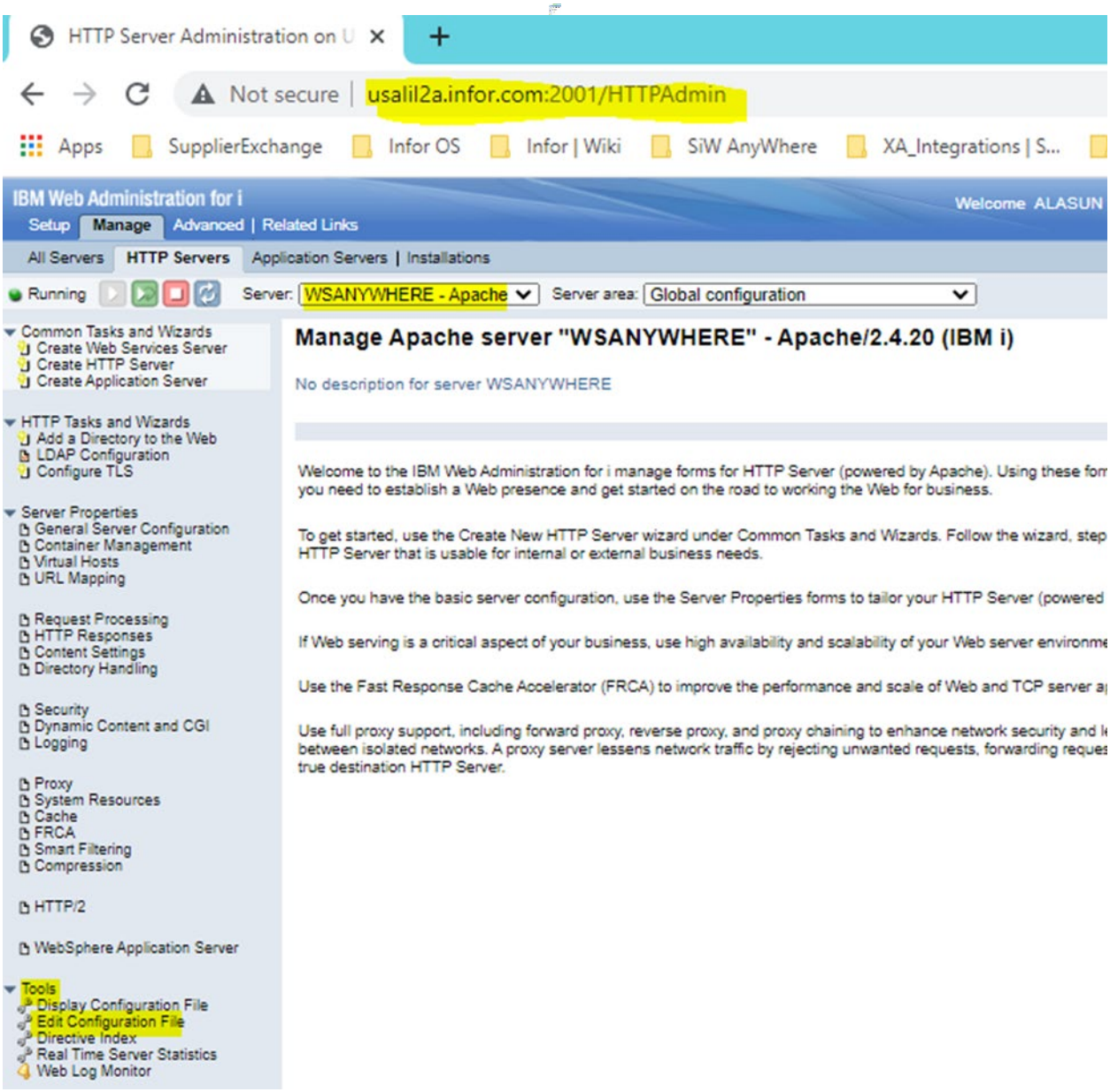
Error! Hyperlink reference not valid.

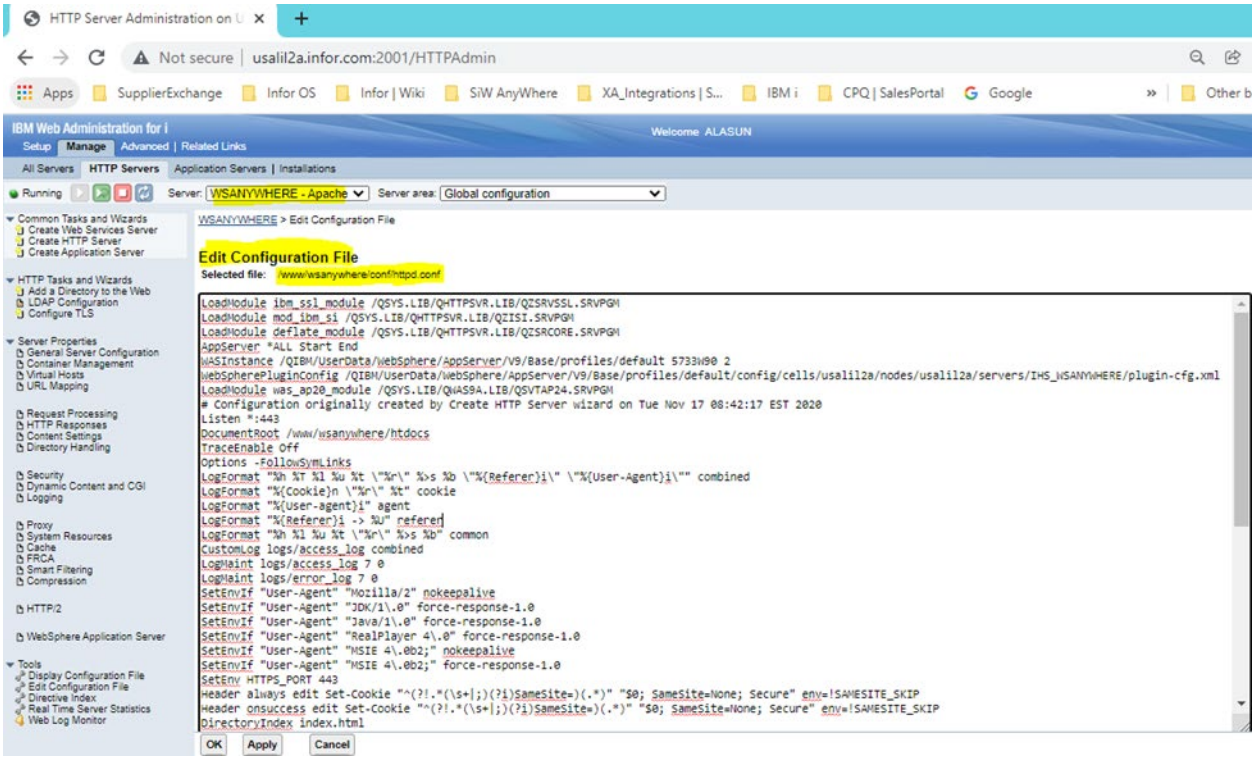
(For example: http://usalil2a:2001/HTTPAdmin)

2 Navigate to **Manage** -> **All Servers** -> **All HTTP Servers,** click on the SiWA configured HTTP server, which is running on 443 port (for example: *WSANYWHERE*) shown as below.



3 On WSANYWHERE HTTP Server, open the httpd.conf file by navigating to **Tools** -> **Edit Configuration File**, shown as below.


HTTP Server Administration on U
Not secure
usalil2a.infor.com:2001/HTTPAdmin
Apps
SupplierExchange
Infor OS
Infor | Wiki
SiW AnyWhere
XA_Integrations | S...
IBM Web Administration for i
Welcome ALASUN
Setup
Manage
Advanced | Related Links
All Servers
HTTP Servers
Application Servers | Installations
Running
Server: WSANYWHERE - Apache
Server area: Global configuration
Common Tasks and Wizards
Create Web Services Server
Create HTTP Server
Create Application Server
HTTP Tasks and Wizards
Add a Directory to the Web
LDAP Configuration
Configure TLS
Server Properties
General Server Configuration
Container Management
Virtual Hosts
URL Mapping
Request Processing
HTTP Responses
Content Settings
Directory Handling
Security
Dynamic Content and CGI
Logging
Proxy
System Resources
Cache
FRCA
Smart Filtering
Compression
HTTP/2
WebSphere Application Server
Tools
Display Configuration File
Edit Configuration File
Directive Index
Real Time Server Statistics
Web Log Monitor
Manage Apache server "WSANYWHERE" - Apache/2.4.20 (IBM i)
No description for server WSANYWHERE
Welcome to the IBM Web Administration for i manage forms for HTTP Server (powered by Apache). Using these for
you need to establish a Web presence and get started on the road to working the Web for business.
To get started, use the Create New HTTP Server wizard under Common Tasks and Wizards. Follow the wizard, step
HTTP Server that is usable for internal or external business needs.
Once you have the basic server configuration, use the Server Properties forms to tailor your HTTP Server (powered
If Web serving is a critical aspect of your business, use high availability and scalability of your Web server environme
Use the Fast Response Cache Accelerator (FRCA) to improve the performance and scale of Web and TCP server a
Use full proxy support, including forward proxy, reverse proxy, and proxy chaining to enhance network security and
between isolated networks. A proxy server lessens network traffic by rejecting unwanted requests, forwarding reques
true destination HTTP Server.

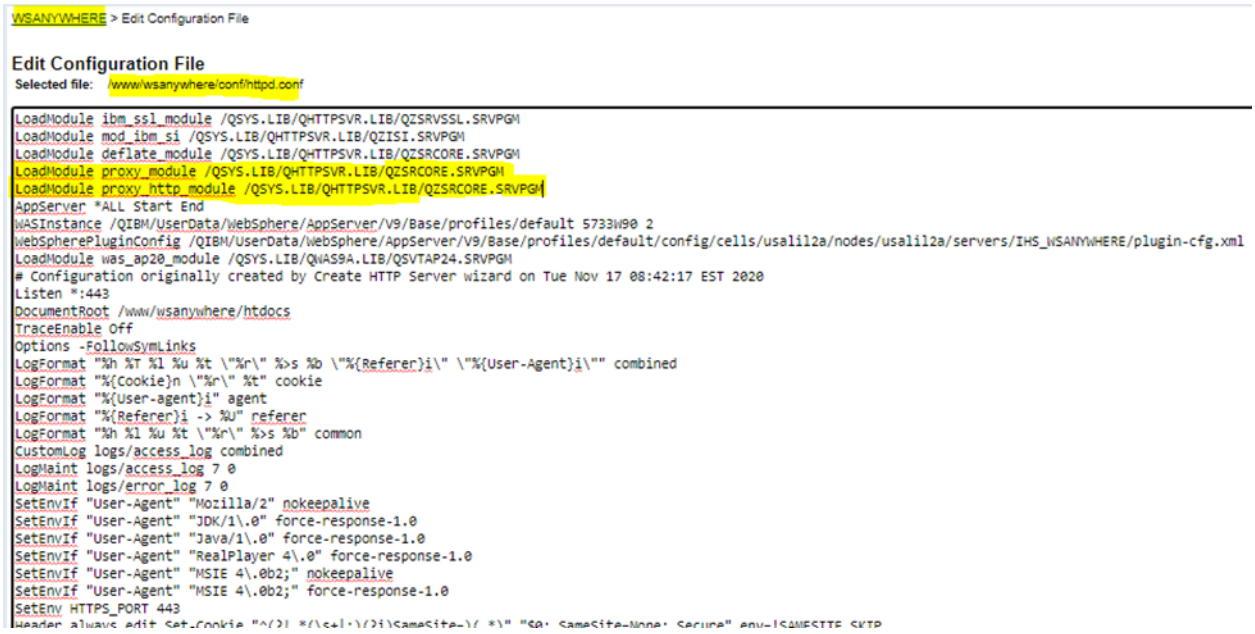


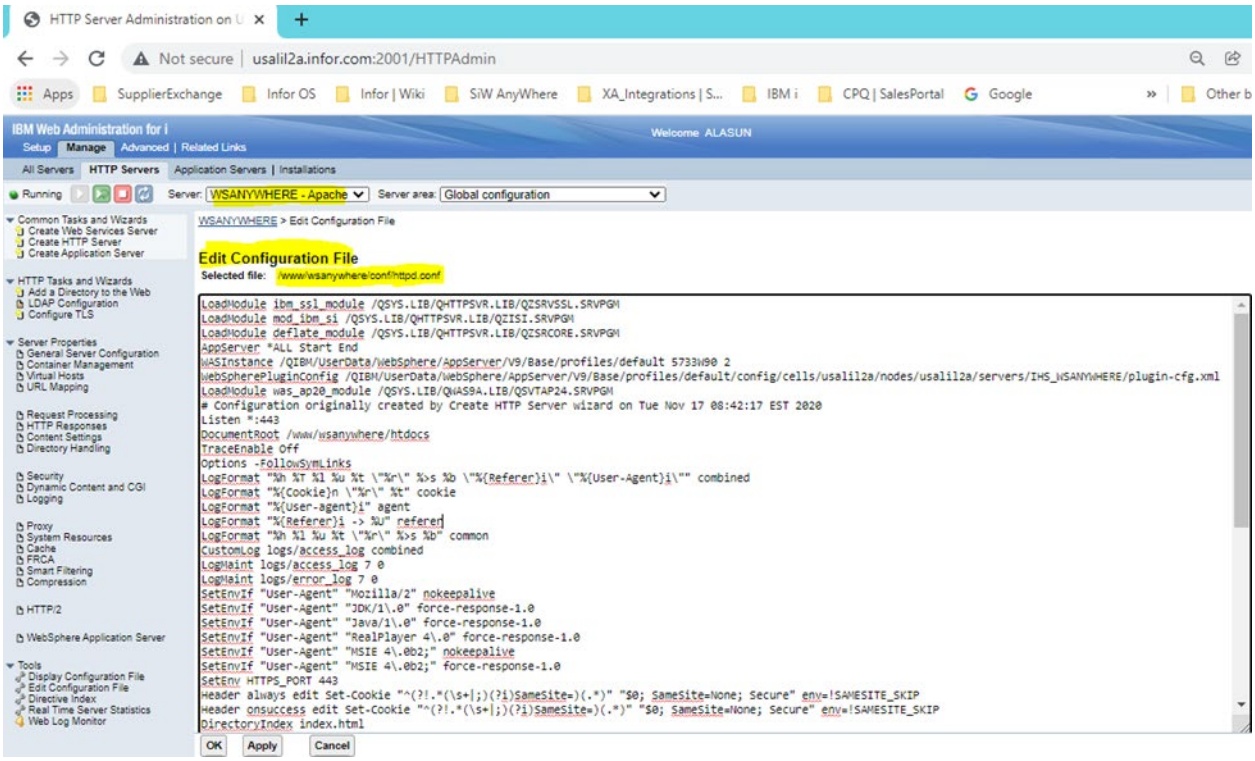
4 It is suggestible to take a backup of httd.conf file, before proceeding with any changes.

5 Add the below statements to the httpd.conf file in the SiWA environment. If these LoadModule statements already exist be sure they are not commented out.

LoadModule proxy_module /QSYS.LIB/QHTTPSVR.LIB/QZSRCORE.SRVPGM

LoadModule proxy_http_module /QSYS.LIB/QHTTPSVR.LIB/QZSRCORE.SRVPGM





6 Add the below statements to the virtual host section for SSL for SiWA. The virtual host section would be between the **<VirtualHost.443>** and **</VirtualHost>** lines. There will be other statements in this section as well.

Note: The Net-Link proxypass would point to the IDF SSL web server and port if NetLink.war is deployed in an app server connected to an SSL enabled HTTP server. If not, use the standard IDF Net-link server and port.

<VirtualHost *:443>

Set SSL application for NetLink proxy if using SSL

SSLProxyAppName QIBM_HTTP_SERVER_WSANYWHERE

SSLProxyEngine on

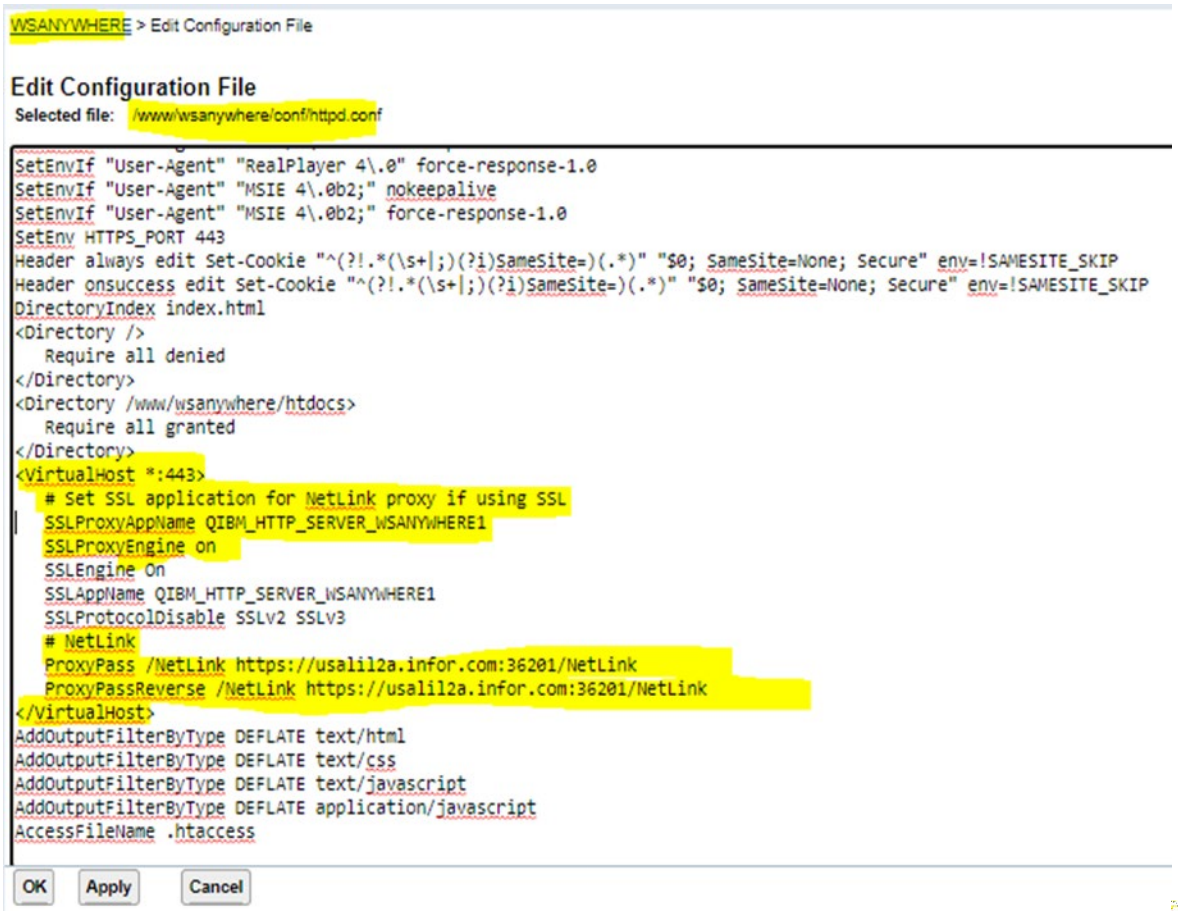
NetLink

ProxyPass /NetLink https://myibmi.infor.com:port/NetLink

ProxyPassReverse /NetLink https://myibmi.infor.com:port/NetLink

</VirtualHost>

(Where ***myibmi*** is the hostname of IBMi server and ***port*** is Net-Link running port, for example shown as below)



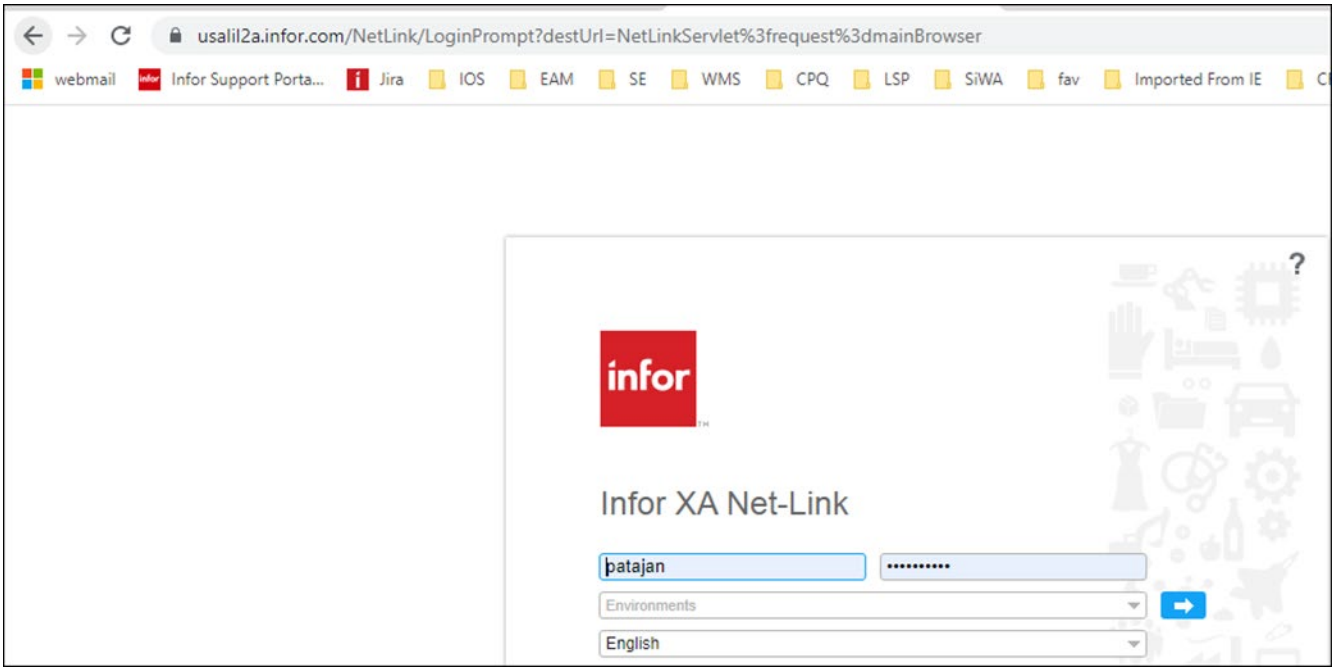
Caution: The parameter value of ***SSLProxyAppName*** should match with ***SSLAppName.***

For example shown as below:

7 Click on **Apply** and **OK**.

8 Restart the SIWA configured HTTP server and its associated Application server.

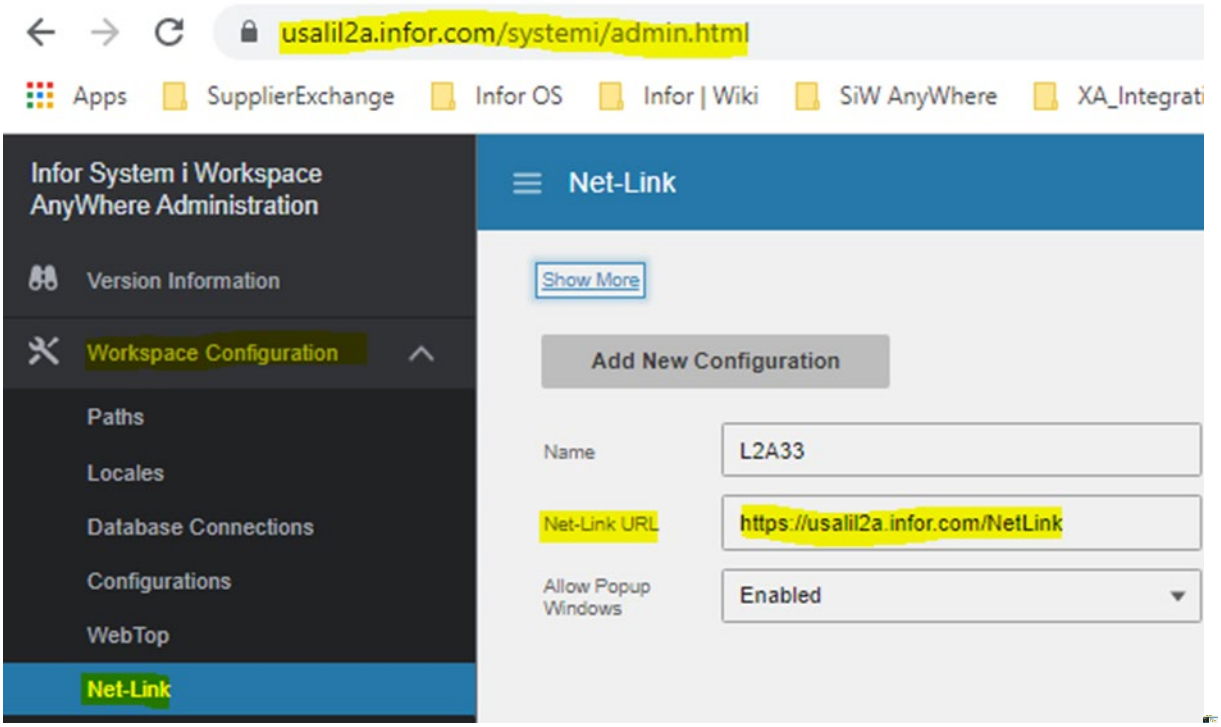
9 Verify if NetLink application is launching with same 443 port or without port as now.



SiW Anywhere Admin settings

Once the above settings are deployed and validated, log into SiWA Admin and update the Net-Link URL to use the same server and port that SiWA is using.

For example, if you had Net-Link set to **`https://usalil2a.infor.com:36201/NetLink`**, then it should be changed to **`https://usalil2a.infor.com/NetLink`**, to use the SiWA server and port that will be opened in the firewall.


usalil2a.infor.com/systemi/admin.html
Apps
SupplierExchange
Infor OS
Infor | Wiki
SiW AnyWhere
XA_Integrati
Infor System i Workspace AnyWhere Administration
Version Information
Workspace Configuration
Paths
Locales
Database Connections
Configurations
WebTop
Net-Link
Net-Link
Show More
Add New Configuration
Name
L2A33
Net-Link URL
https://usalil2a.infor.com/NetLink
Allow Popup Windows
Enabled