INSTALLATION & CONFIGURATION – SSO

Parul Garg#1, Dr. Yashpal Singh*2

#1Research Scholar #2Associate Professor

#1Research Scholar Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Kabalana, Jhajjar, Haryana,

#2Department of Computer Science & Engineering, Ganga Institute of Technology and Management, Kabalana, Jhajjar, Haryana,

MDU university, parulgarg22@gmail.com, 9999405236

Abstract—This paper is a case study on a project to provide the installation and configuration to Single Sign On (SSO) solution to web based applications that use the mainframe as the data store.

It is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. Conversely it is the property whereby a single action of signing out may terminates access to multiple software systems.

This paper begins with a thorough description of the high level business requirements project to provide the installation and configuration to Single Sign On (SSO) solution to web based applications that use the mainframe as the data store.

Keywords—SSO, password, authentication, replication, application, installer, Admin

INTRODUCTION

Single sign-on (SSO) is a method of access control that enables a user to log in once and gain access to the resources of multiple software systems without being prompted to log in again (enter Id and password) thus this may consume less time.[1] "Single sign-on (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.”[2]

Single Sign-On (SSO) is a key feature of the Enterprise Portal that eases user interaction with the many component systems available to the user in a portal environment. Once the user is authenticated to the enterprise portal, he/she can use the portal, to access external applications. With SSO in the Enterprise Portal, the user can access different systems and applications without having to repeatedly enter his or her user information for authentication.

RELATED WORK

• Configuring Single Sign-On using fusion middleware Administrator’s guide for oracle WebCenter. [15]
• Setting up ADFS and enabling Single Sign-On to office 365
• Identity and access management solution
• Identify infrastructure for development
• Protocol and SSO client/server architecture [16]

WHY SHOULD WE USE SSO

• A Typical net user needs at least nine passwords.[3]
• 30% never change passwords, 29% less than once a year.
70% have forgotten a password at least once[4]  
35% of people use the same password for multiple apps.  
60% of people cycle two passwords across all applications.

INSTALLATION &CONFIGURATION OF CA   SITEMINDER ADMINISTRATIVE UI(WAMUI)

Administrative UI Prerequisite Installation

The installation is done using a generic account i.e “smuser”. The “root” user privilege is used to unzip the Administrative UI Prerequisite Installer and WAM UI binaries.[5]

Login to Linux server and copy Administrative UI Prerequisite installer under the path say :

root@spado # /var/WAMUI_Installable

Change the permission of the files as shown in the below screenshot:

root@spado # chmod 755 adminui-pre-req-12.52-sp01-cr02-linux.bin

root@spado # chmod 755 ca-adminui-12.52-sp01-cr02-linux.bin

Exit from the current user and switch to “smuser” as shown in the screenshot:

u5127488@spado # sudo su - smuser

Navigate to the installation path

smuser@spado: /var/WAMUI_Installable

Exit from the current user and switch to “smuser”

Navigate to the installation path

smuser@spado: /var/WAMUI_Installable
Run the following command from /var/WAMUI_Installable as shown in the below screenshot to start the Administrative UI Prerequisite installation[6]

```bash
./adminui-pre-req-12.52-sp01-cr02-linux.bin -i console
```

Press enter to accept the License Agreement and continue with the installation as shown in the below screenshot
Screen5: accept the License Agreement

Type the command: `Y` under the license agreement page to accept the License Agreement and continue further. See below the below screenshot.

Screen6: the command: `Y` under the license agreement page to accept the License Agreement

Select the default Installation Folder `/usr/app/netegrity/CA` location for installing the Administrative UI Server as shown in the below screenshot.

Screen7: the default Installation Folder location for installing the Administrative UI Server

694 www.ijergs.org
Screen8: Supply Installation formalities

Check the Pre-Installation Summary and press <Enter> to continue as shown in the below screenshot.

Screen9: Pre-Installation Summary

The Admin UI Prerequisite installation is completed successfully under the path /usr/app/netegrity/CA/siteminder/adminui
Screen10: The Admin UI Prerequisite installation is completed as shown above

Administrative UI (WAM) Installation

Login to Linux server and copy Admin UI installer under the path say [8]

root@spado # cd /var/WAMUI_Installable

Change the permission of the files as shown in the below screenshot.

root@spado # chmod 755 ca-adminui-12.52-sp01-cr02-linux.bin

Screen11: Change the permission of the files as shown in the below screenshot.

Exit from the current user and switch to “smuser” as shown in the screenshot

u5127488@spado # sudo su - smuser

Screen12: Exit from the current user and switch to “smuser” as shown

696  www.ijergs.org
Navigate to the installation path

```
smuser@spado: cd /usr/app/CA_WAMUI_Installable
```

Screen13: Navigate to the installation path

Run the following command from /var/WAMUI_Installable as shown in the below screenshot to start the CA Siteminder Administrative UI (WAM UI) installation.

```
./ca-adminui-12.52-sp01-cr02-linux.bin -i console
```

Screen14: start the CA Siteminder Administrative UI (WAM UI) installation

Press enter to accept the License Agreement and continue with the installation as shown in the below screenshot.
License Agreement

Use of the CA SiteMinder Administrative UI Installer requires acceptance of the following License Agreement:

CA, Inc. ("CA")

End User license Agreement (the "Agreement") for the CA software product that is being installed as well as the associated documentation and any SHL, as defined below, included within the product ("the Product").

Carefully read the following terms and conditions regarding your use of the Product before installing and using the Product. Throughout this Agreement, you will be referred to as "You" or "Licensee.

By selecting the "I accept the terms of the License Agreement" radio button below, and then clicking on the "Next" button, you are

(1) Representing that you are not a minor, and have full legal capacity and have the authority to bind yourself and your employer, as applicable, to the terms of this Agreement;

(2) Authorizing on behalf of yourself and/or as an authorized representative of your employer, as applicable, to be bound by this Agreement.

By selecting the "I do not accept the terms of the License Agreement" radio button below, and then clicking on the "Cancel" button, the installation process will cease.

PRESS <ENTER> TO CONTINUE.

Screen15: acceptance License Agreement

PRESS <ENTER> TO CONTINUE:

relating to third party software which are set forth below this Agreement, constitutes the complete Agreement between the parties regarding this subject matter and that it supersedes any information licensee has received relating to the subject matter of this Agreement, except that this Agreement (excluding the third party terms below) will be superseded by any written agreement executed by both licensee and CA, granting licensee a license to use the product. This Agreement may only be amended by a written Agreement signed by authorized representatives of both parties.

Select the "I accept the terms of the License Agreement" radio button, and then click on the "Next" button to accept the terms and conditions of this Agreement as set forth above and proceed with the installation process.

Select the "I do not accept the terms of the License Agreement" radio button and then click on the "Cancel" button to halt the installation process.

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y

Screen16: accept the License Agreement

Type the command: Y under the license agreement page to accept the License Agreement and continue further. See below the below screenshot.
Screen 17: accept the License Agreement and continue

Choose the installation path /usr/app/netegrity/CA for CA Siteminder Administrative UI installation.

Screen 18: the installation path for CA Siteminder Administrative UI installation

Select JBOSS as the Application Server by pressing 1 and continue with the installation.
Screen19: Select JBOSS as the Application Server by pressing 1 and continue with the installation

Check the **Application Server Information** as shown in the below screenshot. Select the JBoss Folder path `/usr/app/netegrity/CA/siteminder/adminui`

Screen20: Check the **Application Server Information** as shown

Choose the Java virtual Machine already installed on the system by selecting 1 as shown in the below screenshot.
Screen21: Choose the Java virtual Machine already installed on the system by selecting 1 as shown

Check the Pre-Installation Summary and press <Enter> to continue as shown in the below screenshot.

Screen22: Check the Pre-Installation Summary and press <Enter> to continue as shown

The Admin UI Prerequisite installation is completed successfully under the path /usr/app/netegrity/CA/siteminder/adminui
Screen23: The Admin UI Prerequisite installation is completed successfully under the path

Run the above command. Start the JBOSS Server from /usr/app/netegrity/CA/siteminder/adminui/bin by running the below command. [10]

```
root@spado #./run.sh -b spado.host.mobistar.be
```

Screen24: Start the JBOSS Server

The below screenshot shows that JBOSS Server is up and running.
that JBOSS Serve

Execute the below script from the CA Siteminder installation directory

directory

Check the policy server is up and running under the path /usr/app/netegrity/CA/siteminder

We can also check the Policy Server process by using the below command:

Execute the XPSRegClient utility from /usr/app/netegrity/CA/siteminder/bin to supply the super user account name (siteminder) and password (*******). The Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.[11]

root@sorel: /XPSRegClient siteminder:******* -adminui-setup -vT
Screen28: Policy Server uses these credentials to verify that the registration request is valid and that the trusted relationship can be established.

The below screenshot shows the successful execution of XPSRegClient utility.

Screen29: shows the successful execution of XPSRegClient utility.

If we have run the

```
./XPSRegClient siteminder:******** -adminui-setup -vT
```
on one Policy Server and we want to register other Policy Server with the same WAMUI then run the below command on the second Policy Server:

```
./XPSRegClient siteminder:******** -adminui -vT
```
Screen30: Policy Server with the same WAMUI

LOGIN TO WAM UI BY USING URL

Login to WAM UI by using the URL:  http://spado.host.mobistar.be/iam/siteminder/adminui

Provide the username, Password and Server information to login to WAM UI.

Screen31: Welcome to CA siteminder

The WAM UI is shown below:
Steps to configure Additional Policy Server Connections for the Administrative UI

By default, the Administrative UI is configured with a single Policy Server. You can configure additional Policy Server connections and can administer these servers from the Administrative UI.

For the Administrative UI to connect to multiple Policy Servers, use an external administrator store. An external user store is a requirement for extra Policy Server connections. Create the administrator accounts for the administrator identities in the store. The accounts enable the Administrative UI to locate administrator records in the external store.[12][13]

Follow these steps:

1. Configure a connection from the Administrative UI to an external administrator user store.

Note: If the Administrative UI is using the policy store as its source of administrator identities, you cannot configure extra Policy Server connections.

2. Run the registration tool.

3. Configure the connection to the Policy Server.

4. Configure a connection from the Admin UI to an external administrative user store

Login to WAM UI and click on Configure Administrative Authentication as mentioned in the screenshot:
Screen33: Administrator page

Click on Start the Configuration Wizard as shown in screenshot.

Screen34: configuration setup

Follow the steps and click on Next.
Screen35: Follow steps for configuration

Select the Directory Type as **OpenLDAP**.

Screen36: directory type OpenLDAP

Enter the Connection Details as shown below.

- **Username**: uid=smuser_acc,ou=production,ou=system,o=mobistar.be
- **Password**: *********
- **Host**: sounder.host.mobistar.be
- **Port**: 389

Screen37: Assigning host no
Provide the rest of the details and you will get the Policy Server Connection listed under Admin UI as shown in the below screenshot.

Screen38: the Policy Server Connection listed under Admin UI

REGISTRATION TOOL

Run the registration tool

To run the registration use the below command:

```
./XPSRegClient smuser_acc:******** adminui -vT
```

Screen39: registration under registory tool
Configure the Connection to the Policy Server

You configure the connection so the Administrative UI can be used to manage CA SiteMinder objects.

To configure a Policy Server connection

Log into the Administrative UI with an account that has super user permissions.

Click Administration, Admin UI.

Click Policy Server Connections, Register Policy Server Connection.

Screen40: Policy Server Connections

Type a connection name in the Name field.

Type the Policy Server host name or IP address in the Policy Server Host field.

Type the Policy Server authentication port in the Policy Server Port field.

Note: This value must match the value in the Authentication port (TCP) field on the Settings tab in the Policy Server Management Console. The default authentication port is 44442. To determine the port number, open the Settings tab in the Policy Server Management Console.

Type the client name and passphrase you created using the registration tool in the respective fields.

Select a FIPS mode:

If you installed the Policy Server in FIPS-compatibility mode, select Compatibility mode.

If you installed the Policy Server in FIPS-only mode, select FIPS only mode.
Screen41: Policy Server in FIPS-compatibility mode

Click Submit.

The values should match the entries as mentioned in the screenshot.

Screen42: The values should match the entries as shown

The connection between the Administrativell UI and the Policy Server is configured. The Administrativell UI login screen contains a list of Policy Servers to which the Administrativell UI is registered. By default, the Policy Server that was registered first is the default connection.
If the primary policy server is down, you can switch to the secondary policy server at the time of login.

If you want to switch to another policy server connection, you can use the drop down menu for the same as shown in the below screenshot.
CONCLUSION

Decentralized systems are so common and authentication is an important aspect of them. Using SSO a big problem is solved: Managing large population across the globe of applications and services. When implementing authentication for a new application, consider integration it with the SSO. The results of the analysis conducted for this paper indicate that technology issues are the main factors implementing SSO and MFA within organisations; this is partly due to complexities of existing technical infrastructures and workflow processes. SSO is here to stay. [14]

REFERENCES:


[5]. SAPCRM tutorial http://sapcrmtutorial.blogspot.in/2014_05_01_archive.html

[6]. https://www.linkedin.com/pulse/more-momentum-clean-energy-bill-gates

[7]. https://docops.ca.com/ca-single-sign-on-12-52-sp1/en/installing/administrative-user-interface-installation/additional-policy-server-connections-for-the-administrative-ui


[12]. https://docops.ca.com/ca-single-sign-on-12-52-sp1/en/troubleshooting/administrative-ui-troubleshooting


[16]. Setting http://docs.oracle.com/cd/E21764_01/webcenter.1111/e12405/wadm_security_SSO.htm#WCADM3434