

White paper version: 1.2 Date: 29th April 2011 AUTHORS: Vijeth R. Rajoli Krishna Chalamasandra

A complete guide for Installation, configuration and integration of Open Access Manager 9.0 with Cisco Unified Communications Manager 8.5, 8.6/Cisco Unity Connection 8.6 and Active Directory for Single Sign On.

Table of Contents

	4
1 Introduction	5
2 Configuring Domain Controller on Windows 2003 Server	5
3 Configuring DNS on Windows 2003 server domain controller	18
4 Configuring Windows client desktop as domain computer of domain controller	23
5 Brief history of OpenSSO and OpenAM	28
6 System requirements for OpenAM installation	28
6.1 OpenAM installation on Linux platform	28
6.2 OpenAM installation on Windows platform	29
7 Installation and Configuration of Apache Tomcat with HTTPS	30
7.1 Installation and configuration of Apache Tomcat on Linux platform	30
7.2 Installation and configuration of Apache Tomcat on Windows platform	31
8 Provisioning Active Directory for Single Sign-on	32
9 Deploying OpenSSO (OpenAM) Enterprise on Apache Tomcat	33
9.1 Deploying OpenSSO enterprise war on Apache Tomcat over Linux platform	33
9.2 Deploying OpenSSO enterprise war on Apache Tomcat over Windows platform.	33
10 Configuring OpenSSO Enterprise Using the GUI Configurator	34
10.1 Configuring Policies on OpenSSO server	38
10.1.1 Configuring Policies on OpenSSO server for Cisco Unified Communication Mana 8.5, 8.6 38	ger
10.1.2 Configuring Policies on OpenSSO server for Cisco Unity Connection 8.6	45
10.2 Configuring Windows Desktop SSO Authentication module instance	50
10.3 Configure J2EE Agent profile on OpenSSO server	51
10.3.1 Configure J2EE Agent Profile on OpenSSO server for Cisco Unified Communication Manager 8.5, 8.6	ons 51
10.3.2 Configure J2EE Agent Profile on OpenSSO server for Cisco Unity Connection 8.6	55
11 Undeploying/Removing OpenSSO Enterprise (OpenAM)	61
11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platforn	1 61
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platform 	n 61 orm.
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platforn 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfo 61 	n 61 orm.
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platform 61 12 Configuring Browser's for SSO 	n 61 orm. 61
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfo 61 12 Configuring Browser's for SSO 12.1 Internet Explorer 	n 61 orm. 61 62
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfo 61 12 Configuring Browser's for SSO 12.1 Internet Explorer 12.2 Mozilla Firefox 	n 61 orm. 61 62 62
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO	n 61 orm. 61 62 62 63
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 61 12 Configuring Browser's for SSO	n 61 orm. 61 62 62 63 64
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO	n 61 orm. 61 62 62 63 64 66
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO	161 prm. 61 62 62 63 64 66 66
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platform 12 Configuring Browser's for SSO	1 61 prm. 61 62 62 63 64 66 66
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platform 12 Configuring Browser's for SSO	161 prm. 61 62 62 63 63 64 66 67 67
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO. 12.1 Internet Explorer. 12.2 Mozilla Firefox 12.3 SSO Configurations test with browser 13 Configuring SSO on Cisco Unified Communications Manager 8.5 13.1.1 utils sso enable 13.1.2 utils sso disable 13.1.3 utils sso status 14 Configuring SSO on Cisco Unified Communications Manager 8.6 	161 61 62 62 63 63 66 66 67 67 67
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 61 12 Configuring Browser's for SSO	161 61 62 62 63 63 66 66 67 67 67 67 67 67
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO	161 61 62 62 63 63 66 67 67 67 67 67 67 67 67 69 69
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO	161 61 62 62 63 64 66 67 67 67 68 69 70 71
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO. 12.1 Internet Explorer. 12.2 Mozilla Firefox 12.3 SSO Configurations test with browser 13 Configuring SSO on Cisco Unified Communications Manager 8.5 13.1 Utils sso enable 13.1.2 utils sso disable 13.1.3 utils sso status 14 Configuring SSO on Cisco Unified Communications Manager 8.6 14.1 Utils sso enable 14.1.1 utils sso enable 14.1.2 utils sso disable 14.1.2 utils sso disable 14.1.3 utils sso status 	161 61 62 62 63 64 66 67 67 67 68 69 70 71
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO 12.1 Internet Explorer 12.2 Mozilla Firefox 12.3 SSO Configurations test with browser 13 Configuring SSO on Cisco Unified Communications Manager 8.5 13.1 Utils sso enable 13.1.2 Utils sso disable 13.1.3 Utils sso status 14 Configuring SSO on Cisco Unified Communications Manager 8.6 14.1 CUCM 8.6 SSO CLI Commands: 14.1.1 Utils sso enable 14.1.2 Utils sso disable 14.1.3 Utils sso disable 14.1.4 Utils sso disable 14.1.5 Utils sso disable 14.1.5 Utils sso disable 14.1.4 Utils sso disable 14.1.5 Utils sso disable 14.1.4 Utils sso disable 14.1.5 Utils sso disable 14.1.6 Utils sso disable 14.1.7 Utils sso disable 14.1.8 Utils sso disable 14.1.9 Utils sso disable 14.1.1 Utils sso disable 14.1.2 Utils sso disable 14.1.3 Utils sso disable 14.1.4 Utils sso disable 14.1.5 Utils sso disable 14.1.5 Utils sso disable 14.1.6 Utils sso disable 14.1.7 Utils sso disable 14.1.7 Utils sso disable 14.1.8 Utils sso disable<!--</td--><td>161 61 62 62 62 63 63 64 66 67 67 67 68 69 70 71 71</td>	161 61 62 62 62 63 63 64 66 67 67 67 68 69 70 71 71
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO	161 61 62 62 63 63 64 66 67 67 67 67 67 67 67 69 70 71 71 73
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platforn 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfor 61 12 Configuring Browser's for SSO	161 orm. 61 62 62 63 64 66 67 67 67 67 67 67 67 67 71 71 73 73
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfor 12 Configuring Browser's for SSO	161 61 62 62 62 63 63 66 67 67 67 67 67 67 67 71 71 73 74 74
 11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO. 12.1 Internet Explorer 12.2 Mozilla Firefox 12.3 SSO Configurations test with browser 13 Configuring SSO on Cisco Unified Communications Manager 8.5 13.1 CUCM 8.5 SSO CLI Commands: 13.1.1 utils sso enable 13.1.2 utils sso disable 13.1.3 utils sso status 14 Configuring SSO on Cisco Unified Communications Manager 8.6 14.1 CUCM 8.6 SSO CLI Commands: 14.1.1 utils sso enable 14.1.2 utils sso disable 14.1.3 utils sso status 14.2 CUCM 8.6 SSO GUI 15 Configuring SSO on Cisco Unity Connection 8.6 15.1 utils sso enable 15.1.1 utils sso enable 15.1.2 utils sso disable 15.1.2 utils sso disable 15.1.2 utils sso enable 	161 61 62 62 62 63 64 66 67 67 67 67 67 67 67 67 67 71 71 71 73 74 76 76
 11.1 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfore 12 Configuring Browser's for SSO. 12.1 Internet Explorer. 12.2 Mozilla Firefox 12.3 SSO Configurations test with browser 13 Configuring SSO on Cisco Unified Communications Manager 8.5 13.1 CUCM 8.5 SSO CLI Commands: 13.1.1 utils sso enable 13.1.2 utils sso status 14 Configuring SSO on Cisco Unified Communications Manager 8.6 14.1 CUCM 8.6 SSO CLI Commands: 14.1 CUCM 8.6 SSO CLI Commands: 14.1 Utils sso enable 14.1.2 utils sso status 14.2 CUCM 8.6 SSO GUI 15.1 CUCM 8.6 SSO GUI 15.1 Utils sso enable 15.1.1 utils sso enable 15.1.2 utils sso disable 15.1.3 utils sso status 	161 61 62 62 62 63 63 64 66 67 67 67 67 67 69 70 71 71 73 74 76 76 76
 11.1 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Linux Platform 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platford 61 12 Configuring Browser's for SSO	161 61 62 62 62 63 63 66 67 67 67 67 67 67 69 70 71 71 73 74 76 76 76 76
 11.1 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Linux Platforn 11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platfa 61 12 Configuring Browser's for SSO	1 61 61 62 62 62 62 63 64 66 67 67 67 67 67 67 67 70 71 71 73 74 76 76 78 79

16.2 Conf	guration of AMSFO components	79
16.2.1	Installation and configuration of Load Balancer	79
16.2.1.1	Installation of Load Balancer on Linux Platform.	79
16.2.1.2	Installation of Load Balancer on Windows platform.	
16.2.1.3	Configuration of Load Balancer for HTTP load balancing	
16.2.2	Installation and configuration of session failover components	108
16.2.2.1	Configuration of session failover components on Linux Platform	108
16.2.2.2	Configuration of session failover components of windows platform	115
16.2.3	Installation and configuration of OpenAM Enterprise servers for session	failover. 122
16.2.3.1	Installation of OpenAM Enterprise server 1	122
16.2.3.2	Installation of OpenAM Enterprise server 2	131
16.2.3.3	Configure OpenSSO Enterprise for Session Failover	137
16.3 Conf	iguring SSO on Cisco Unified Communications Manager with AMSFO	setup 138

Preface

This document will cover the installation and configuration of all the required software's which are essential for achieving Single Sign-on solution with Cisco Unified Communications Manager 8.5., which has been covered in respective chapters, here is the brief pictures of coverage on each chapter.

Chapter 1: This chapter covers brief introduction on the products which are installed and configured as part of this document.

Chapter 2: This chapter covers installation of Active Directory Service on Domain controller, Skip this chapter if you already have the domain controller setup in your environment.

Chapter 3: This chapter covers installation of DNS on domain controller, Skip this chapter if you already have the DNS configured on your domain controller.

Chapter 4: This chapter covers configuring the desktop as the domain computer of the above setup domain controller, Skip this chapter if your desktop is already a domain computer of the domain controller which is under test.

Chapter 5: This chapter covers brief introduction of OpenSSO and OpenAM.

Chapter 6: This chapter covers installation and configuration of Linux OS/Windows OS for OpenAM deployment.

Chapter 7: This chapter covers installation and configuration of Apache Tomcat with SSL on Linux and Windows Platform which is setup in the chapter 6.

Chapter 8: This chapter covers provisioning Active directory for Windows Desktop SSO Authentication.

Chapter 9: This chapter covers installing OpenSSO Enterprise on Linux /Windows platform.

Chapter 10: This chapter covers configuring OpenSSO with policies, agents and authentication module instance.

Chapter 11: This chapter covers un-installing OpenSSO Enterprise on Linux/Windows platform.

Chapter 12: This chapter covers configuring browsers for Single Sign-on.

Chapter 13: This chapter covers SSO Enable/Disable/Status on Cisco Unified Communications Manager 8.5

Chapter 14: This chapter covers SSO Enable/Disable/Status on Cisco Unified Communications Manager 8.6

Chapter 15: This chapter covers SSO Enable/Disable/Status on Cisco Unity Connection 8.6

Chapter 16: For the high availability of OpenSSO server, OpenSSO Enterprise session failover can be implemented. This chapter explains how to configure OpenSSO Enterprise session failover. Skip this chapter if you do not wish to have OpenSSO session failover.

1 Introduction

This document will cover the installation and configuration of all the required software components which are essential for achieving Single Sign-on solution with Cisco Unified Communications Manager 8.5.

Below is the list of products which are being installed and configured as part of this guide:

- Microsoft Windows 2003 server with SP2 \rightarrow for Domain Controller and DNS configurations. For instance in this guide, the domain controller is configured for the domain **vrajoli.com**
- Redhat Enterprise Linux(RHEL) 5.5 \rightarrow for OpenAM deployment.
- Microsoft Windows 2003 server \rightarrow for OpenAM deployment.
- Windows XP with SP3 \rightarrow Client Desktop

NOTE: If you are planning to in use Windows 2008 Server for configuring active directory, make sure Windows 2008 server has SP2 installed.

2 Configuring Domain Controller on Windows 2003 Server

Setting up active directory using the run command **dcpromo** is a straightforward procedure. To begin, from your windows 2003 server desktop go to **Start** click on **Run** and type **dcpromo** and hit **Enter.**

The "Welcome to the Active Directory Installation Wizard" should come up:



Click on Next. On the following window, you will get a warning about compatibility issues with other Operating Systems. Improve security settings in Windows Server 2003 affect older versions of windows:

Active Directory Installation Wizard
Operating System Compatibility Improved security settings in Windows Server 2003 affect older versions of Windows.
Domain controllers running Windows Server 2003 implement security settings that require clients and other servers to communicate with those domain controllers in a more secure way.
Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 or earlier, do not meet these requirements. Similarly, some non-Windows systems, including Apple Mac OS X and SAMBA clients, might not meet these requirements.
For more information, see <u>Compatibility Help</u> .
< <u>B</u> ack Cancel

After reading and evaluating the consequences, click Next. On the next screen, you will get two options. The first option asks you if you want the server to become a domain controller for a new domain or if you want the server to be an additional domain controller for for an existing domain:

e Direct	ory Installation Wizard 🤰 🤰
omain (Specif	Controller Type by the role you want this server to have.
Do you additio	uwant this server to become a domain controller for a new domain or an nal domain controller for an existing domain?
• Do	main controller for a new domain
Se Th	lect this option to create a new child domain, new domain tree, or new forest. is server will become the first domain controller in the new domain.
O <u>A</u> d	ditional domain controller for an existing domain
	Proceeding with this option will delete all local accounts on this server.
	All cryptographic keys will be deleted and should be exported before continuing.
	All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.
	< <u>B</u> ack <u>N</u> ext > Cancel

Select the first option and click Next. On the next window, you will get three options. the first option is to setup the domain in a new forest. Select this option if its the first domain controller on your organization, or if you want it to be totally independent from any forest.

Option two: Child domain in an existing domain tree. select this option if you want the domain to be a child domain from an existing domain. option three: Domain tree in an existing forest. if you don't want any of the above, select this option.

Active Directory Installation Wizard
Create New Domain Select which type of domain to create.
Create a new:
Domain in a new forest
Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.
C Child domain in an existing domain tree
If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.
O Domain tree in an existing forest
If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.
< <u>B</u> ack <u>N</u> ext > Cancel

In our case, choose the first option, and click Next. On the next screen, we need to type the full DNS name for the new domain:

Active Directory Installation Wizard	×
New Domain Name Specify a name for the new domain.	A
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.com).	
Full DNS name for new domain:	
vrajoli.com	
< <u>B</u> ack <u>N</u> ex	t > Cancel

Type the full DNS name like vrajoli.com, and click on Next. On the next screen, we need to choose the NETBIOS name. This is the name earlier version of windows users will be using to identify the new domain.

Active Directory Installation Wiz	zard 🗙		
NetBIOS Domain Name Specify a NetBIOS name for t	the new domain.		
This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.			
Domain NetBIOS name:	VRAJOLI		
	(Rack Neut) Cancel		
	< <u>Back</u> <u>N</u> ext> Cancel		

Choose the name, and click Next. On the next screen, you need to select the location of where you want to store the database and log files. for best performance store them in separate disks.

Active Directory Installation Wizard	×
Database and Log Folders Specify the folders to contain the Active Directory database and log files.	A
For best performance and recoverability, store the database and the log on s hard disks.	eparate
Where do you want to store the Active Directory database?	
Database folder:	
C:\WINDOWS\NTDS	iowse
Where do you want to store the Active Directory log?	
Log folder:	
C:\WINDOWS\NTDS B	r <u>o</u> wse
< <u>B</u> ack <u>Next</u> >	Cancel

Choose the location where you want the active directory database and logs, and click Next.

Next, the Shared system volume window will come up. here, you need to choose the location on where you want to store the SYSVOL files. this folder contains the domain public files and are replicated to all the domain controllers in the domain.

Active Directory Installation Wizard
Shared System Volume Specify the folder to be shared as the system volume.
The SYSVOL folder stores the server's copy of the domain's public files. The contents of the SYSVOL folder are replicated to all domain controllers in the domain.
The SYSVOL folder must be located on an NTFS volume.
Enter a location for the SYSVOL folder.
Eolder location:
C:\WINDOWS\SYSVOL Browse
< <u>B</u> ack <u>Next</u> Cancel

Choose the folder location, and click Next. On the next window, the DNS registration diagnostic will show up. here most likely you will get "**Diagnostic failed**" and will give you three options. First option: it will allow you to perform the DNS diagnostic again, if you have corrected the problem.

Option two: it gives you the option to allow the active directory wizard to install and configure DNS for you, and use this DNS as the primary DNS for this server. third option, it allows you to bypass this window if you plan to correct the problem later on.

Active Directory Installation Wizard	×
DNS Registration Diagnostics Verify DNS support, or install DNS on this computer.	
Diagnostic Failed	
The registration diagnostic has been run 1 time.	
Warning: Domain Controller functions like joining a domain, logging onto a domain, and Active Directory replication will not be available until the DNS infrastructure for Active Directory is correctly configured.	
The wizard could not determine the name and address of the DNS server with which this domain controller will be registered.	
For more information, including steps to correct this problem, see Help.	
I have corrected the problem. Perform the DNS diagnostic test again.	
 Install and configure the DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server. 	
\bigcirc I will correct the problem later by configuring DNS manually. (Advanced)	
< <u>B</u> ack <u>N</u> ext > Cance	el

We will choose the option to **Install and configure DNS server on this computer and set this computer to use this DNS server as its preferred DNS server.** then click Next.

On the next window, you need to choose what type or permissions you want for users and group objects. Here you will get two options. the first options: select this option if you run server programs with pre-windows 2000. option two: select this option, if you only run windows servers 2000 and windows servers 2003 on your domain.

Active Directory Installation Wizard
Permissions Select default permissions for user and group objects.
Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.
 Permissions compatible with pre-Windows 2000 server operating systems Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 domains. Anonymous users can read information on this domain. Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems Select this option if you run server programs only on Windows 2000 or Windows 2000 o
< <u>B</u> ack <u>N</u> ext > Cancel

Select the second option, and click Next. On the next window, you need to enter the **Directory services restore mode administrator password**. This password is used when you start the computer in directory services restore mode. This account is different from the domain administrator account.

Active Directory I	nstallation Wizaı	rd			×
Directory Serv This passwo Mode.	ices Restore Mo rd is used when you	ode Administ u start the corr	rator Passe aputer in Direc	vord ctory Services Res	store
Type and co when this se	nfirm the password rver is started in Dir	you want to a ectory Service	ssign to the A s Restore Mo	.dministrator accou ode.	unt used
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.				rator member	
Restore Mod	le <u>P</u> assword:	•••••			
<u>C</u> onfirm pass	word:	•••••			
For more info	rmation about Direc	ctory Services	Restore Mod	e, see <u>Active Dire</u>	ectory Help.
		[< <u>B</u> ack	<u>N</u> ext>	Cancel

Type your chosen password, and click Next. Next, you will get the summary of all the options you have chosen during the active directory wizard. remember, the domain administrator account password is the same as the current local administrator password.

A
es. 🔺
uter
_

Click Next. The active directory installation should begin.

Active Directory Installation Wizard
The wizard is configuring Active Directory. This process can take several minutes or considerably longer, depending on the options you have selected.
Starting

Duirng this process, Active Directory starts installing DNS and prompts you to insert the Windows Server 2003 CD-ROM, Please insert the CD-ROM and press OK.



Installation of DNS server and its configuration begins.

Windows Setup Installing DNS Server	×
Configuring Components Setup is making the configuration changes you requested.	X
Please wait while Setup configures the components. This may take several minutes, depending on the components selected.	
Status: Completing configuration of Management and Monitoring Tools	
< <u>B</u> ack. <u>N</u> ext >	



You will see below screen.

Active Directory Installation	Wizard	×
	Completing the Active Directory Installation Wizard	
	< <u>B</u> ack Finish Cancel	

Click on Finish and restart the computer. Active Directory should be now installed.

Active Directory Installation Wizard		
Windows must be restarted before the Directory Installation wizard take effort	he changes made by the Active ect.	
<u>R</u> estart Now	Don't Restart Now	

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

3 Configuring DNS on Windows 2003 server domain controller

DNS gets installed along with AD configuration, only the configuration has to be done on DNS Server.

To configure DNS, go to Start Menu \rightarrow Programs \rightarrow Administrative Tools \rightarrow DNS.

You will see the below screen. Under forward lookup zone, you see the domain controller configured.



Now Reverse Lookup Zone needs to be created. Right click on Reverse Lookup Zone and click on New Zone.



You will see below screen.

New Zone Wizard		×
	Welcome to the New Zone Wizard	
	This wizard helps you create a new zone for your DNS server.	
	A zone translates DNS names to related data, such as IP addresses or network services.	
	To continue, click Next.	
	< Back Next > Cancel Help	

Click on Next, you will see Zone type configuration wizard. Select Primary Zone.

New Zone Wizard
Zone Type The DNS server supports various types of zones and storage.
Select the type of zone you want to create: Primary zone Creates a copy of a zone that can be undated directly on this server.
 Secondary zone Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance. Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone. Store the zone in Active Directory (available only if DNS server is a domain controller)
< <u>B</u> ack <u>N</u> ext > Cancel Help

Click Next, you will be asked how you wish to replicate DNS date in the network. Select "To all domain controllers in the Active Directory domain"

New Zone Wizard 🛛 🔀
Active Directory Zone Replication Scope You can select how you want DNS data replicated throughout your network.
Select how you want zone data replicated:
🔘 To <u>a</u> ll DNS servers in the Active Directory forest vrajoli.com
\odot To all <u>D</u> NS servers in the Active Directory domain vrajoli.com
⊙ To all domain controllers in the Active Directory domain vrajoli.com
Choose this option if the zone should be loaded by Windows 2000 DNS servers running on the domain controllers in the same domain.
C To all domain controllers specified in the scope of the following application directory partition:
▼
< <u>B</u> ack <u>N</u> ext > Cancel Help

Click Next and then you will be asked to configure Reverse Lookup Zone name, enter the network ID and press Next.

New Zone Wizard
Reverse Lookup Zone Name A reverse lookup zone translates IP addresses into DNS names.
To identify the reverse lookup zone, type the network ID or the name of the zone. Network ID: 10 .78 .85 . The network ID is the portion of the IP addresses that belongs to this zone. Enter the network ID in its normal (not reversed) order. If you use a zero in the network ID, it will appear in the zone name. For example, network ID 10 would create zone 10.in-addr.arpa, and network ID 10.0 would create zone 0.10.in-addr.arpa.
Reverse lookup zone name:
85.78.10.in-addr.arpa For more information on creating a reverse lookup zone, click Help. < Back

Select the type of dynamic updates that DNS Zone accepts. Click on "Allow only Secure dynamic updates" and press next.

New Zone Wizard 🔀 🔀 🔀
Dynamic Update You can specify that this DNS zone accepts secure, nonsecure, or no dynamic updates.
Dynamic updates enable DNS client computers to register and dynamically update their resource records with a DNS server whenever changes occur. Select the type of dynamic updates you want to allow:
 Allow only secure dynamic updates (recommended for Active Directory) This option is available only for Active Directory-integrated zones. Allow both nonsecure and secure dynamic updates Dynamic updates of resource records are accepted from any client. This option is a significant security vulnerability because updates can be accepted from untrusted sources. Do not allow dynamic updates Dynamic updates of resource records are not accepted by this zone. You must update these records manually.
< <u>B</u> ack <u>N</u> ext > Cancel Help

With this New Zone creation is successfully completed.



Now configure the Local Area Connection properties for this server.

- In the Local Area Connection Properties dialog box, click Internet Protocol (TCP/IP), and then click Properties.
- In the **Internet Protocols (TCP/IP) Properties** dialog box, click **Use the following IP address**, and then type the static IP address, subnet mask, and default gateway for this server.
- In **Preferred DNS**, type the IP address of this server.
- In **Alternate DNS**, type the IP address of another internal DNS server, or leave this box blank.
- When you finish setting up the static addresses for your DNS, click **OK**, and then click **Close**.

4 Configuring Windows client desktop as domain computer of domain controller

In this example, we will be using Windows XP desktop for joining to the vrajoli.com domain. Create a DNS entry on DNS server for this client host (windows xp)

Configuring LAN properties for this client desktop.

- In the Local Area Connection Properties dialog box, click Internet Protocol (TCP/IP), and then click Properties.
- In the **Internet Protocols (TCP/IP) Properties** dialog box, click **Use the following IP address**, and then type the static IP address, subnet mask, and default gateway for this server.
- In **Preferred DNS**, type the IP address of DNS server (vrajoli).
- In **Alternate DNS**, type the IP address of another internal DNS server, or leave this box blank.
- When you finish setting up the static addresses for your DNS, click **OK**, and then click **Close**.

Make a DNS entry for this Client desktop. Open DNS utility on domain controller (Administrative Tools \rightarrow DNS), under forward lookup zone, create a new host under domain name (vrajoli.com). Click on checkbox to create associated reverse pointer. Verify that Client desktop host got added to DNS.

Change the computer name to one which you wish as below. Right click on My Computer \rightarrow Properties. Go to Computer Name tab and click on Change button.



System Properties			? 🛿
System Restore General Co	Automa mputer Name	tic Updates Hardware	Remote Advanced
Windows us on the netw	es the following info ork.	ormation to identify	your computer
Computer description:			
	For example: ''k Computer''.	(itchen Computer''	or ''Mary's
Full computer name:	VJTH.		
Workgroup: WORKGROUP			
To use the Network Id domain and create a lo ID.	entification Wizard cal user account, c	to join a click Network	Network ID
To rename this compu	er or join a domain,	click Change.	Change
	ОК	Cance	Apply

Click on More Button on the Computer Name Changed window, and enter Primary DNS Suffix of this computer with the DNS name (DNS running on Domain controller). In our case the DNS name is vrajoli.com. Press OK.

DNS Suffix and NetBIOS Computer Name
Primary DNS suffix of this computer: vrajoli.com
Change primary DNS suffix when domain membership changes
NetBIOS computer name: VJTH
This name is used for interoperability with older computers and services.
OK Cancel

Select the "Domain" radio button then put in your domain name, not including the . extension (in this example we used the domain "vrajoli" but when joining the computer to a domain, we will only type "vrajoli")

Computer Name Changes
You can change the name and the membership of this computer. Changes may affect access to network resources.
Computer name:
WTH
Full computer name: VJTH.vrajoli.com More
⊙ Domain:
vrajoli
Workgroup: WORKGROUP
OK Cancel

Press "OK". Then you will be presented with a user name and password prompt. Enter the user name and password of a Domain Administrator

Computer Nam	e Changes 🛛 😨 💈
7	E Sta
Enter the name a to join the domain User name:	nd password of an account with permission
Decruord	

Press "OK" and after a minute or two you will receive a message welcoming you to the domain.

Comput	er Name Changes	
(į)	Welcome to the vrajoli d	lomain,
	ОК	

Then you will receive a message telling you that a reboot is required; click "OK" to that, and the properties window. Then click "Yes" when you are prompted to reboot.

Computer Name Changes		
į)	You must restart this computer for the changes to t	ake effect.

And we're finished. You have just learnt how to add a Windows XP computer to a Windows Server 2003 domain

After the XP computer boots to Control-Alt-Delete you may need to change it from logging onto itself (which *will* use the local info) to logging onto the domain. To do this, press Ctrl-Alt-Del, then the "Options >>>" button on the log on screen. Then select the domain from the drop-down box

Log On to Windows			
Copyright © 1985 Microsoft Corpora	-2001 tion Microsoft Windows Xp Professional Microsoft		
User name:	vijeth		
Password: Log on to:	VRAJOLI		
	ENG VJTH (this computer) VRAJOLI OK Cancel Shut Down Options <<		

After that you can log on using domain credentials

5 Brief history of OpenSSO and OpenAM

OpenSSO is an open source access management and federation server platform originally created by Sun Microsystems. The main purpose of OpenSSO is to provide an easy and powerful way to enable using Single Sign-On with many legacy software products. Oracle completed the acquisition of Sun Microsystems in February 2010 and announced that OpenSSO would no longer be their strategic product. OpenSSO will continue to be developed and supported by ForgeRock under the name of OpenAM.

More information about OpenAM is available at http://www.forgerock.com/openam.html

6 System requirements for OpenAM installation

Active directory, domain controller and DNS should be installed and configured before getting started with OpenAM.

6.1 **OpenAM installation on Linux platform**

- Get the compatible hardware for installing RHEL 3/4/5 version (32bit/64bit)
- Install the RHEL and make sure the installation is successful.
- After the successful installation, configure the network settings and get the machine up in the network.
- Configure the hostname for this OpenAM host machine and create DNS entry for this host on the above DNS setup.
- Configure DNS and domain name, which should point to the above configured AD and DNS setup.
- Install JAVA on this machine, Latest version of JAVA can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html, Latest version of JAVA as on 13-Sep-2010 is JDK 6 Update 21.

NOTE: The latest version of java (JDK 6 Update 21) has some issue with Kerberos; please visit <u>http://forums.sun.com/thread.jspa?threadID=5448003</u> to know more.

You can use JDK 6 Update 20, which can be downloaded from http://java.sun.com/products/archive/j2se/6u20/index.html

• Define JAVA_HOME, JRE_HOME environment variables in your user profile (.bash_profile) as below:

export JAVA_HOME=/usr/java/jdk1.6.0_20

export JRE_HOME=/usr/java/jdk1.6.0_20/jre

• Create java keystore which is required for enabling SSL on Tomcat which will be installed and configured in the section 7.1

Execute **'\$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA -validity 1825**' command on the terminal, default keystore password is **'changeit'**.

Next you will be prompted to input certain requests. When prompted for 'Enter the first name and last name' enter the FQDN(hostname.domainname) of your OpenAM host (*ex:vrajlnx.vrajoli.com*).

Example:

[root@vrajlnx ~]# \$JAVA_HOME/bin/keytool -genkey -alias tomcat -keyalg RSA - validity 1825

Enter keystore password:

What is your first and last name?

[Unknown]: vrajlnx.vrajoli.com

What is the name of your organizational unit?

[Unknown]: IPCBU

What is the name of your organization?

[Unknown]: CSIPL

What is the name of your City or Locality?

[Unknown]: Bengaluru

What is the name of your State or Province?

[Unknown]: Karnataka

What is the two-letter country code for this unit?

[Unknown]: IN

Is CN=vrajlnx.vrajoli.com, OU=IPCBU, O=CSIPL, L=Bengaluru, ST=Karnataka, C=IN correct?

[no]: yes

Enter key password for <tomcat>

(RETURN if same as keystore password):

[root@vrajlnx ~]#

6.2 OpenAM installation on Windows platform

- Install Windows OS (XP/2003 Server/2008 Server/Windows7/Vista).
- After successful installation, configure the network settings and get the machine up in the network.
- Join this computer to the domain controller (ex: vrajoli.com), refer to the section 4 for the procedure to be followed for joining the computer to the domain controller.
- Install JAVA on this machine, Latest version of JAVA can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html, Latest version of JAVA as on 13-Sep-2010 is JDK 6 Update 21.

NOTE: The latest version of java (JDK 6 Update 21) has some issue with Kerberos; please visit <u>http://forums.sun.com/thread.jspa?threadID=5448003</u> to know more.

You can use JDK 6 Update 20, which can be downloaded from http://java.sun.com/products/archive/j2se/6u20/index.html

- Create java keystore which is required for enabling SSL on Tomcat which will be installed and configured in the section 7.2
- Open the command prompt and execute the below command. In this test setup, I have JAVA installed under *c:\Program Files\Java*. Please enter the right path of keytool.exe in your setup when executing this command. The default keystore password is **changeit**

C:\>"c:\Program Files\Java\jdk1.6.0_20\bin\keytool.exe" -genkey -alias tomcat -keyalg RSA -validity 1825 -keystore c:\keystore Enter keystore password: What is your first and last name? [Unknown]: vrajlnx.vrajoli.com What is the name of your organizational unit? [Unknown]: IPCBU What is the name of your organization? [Unknown]: CSIPL What is the name of your City or Locality? [Unknown]: Bengaluru What is the name of your State or Province? [Unknown]: Karnataka What is the two-letter country code for this unit? [Unknown]: IN Is CN=vrajlnx.vrajoli.com, OU=IPCBU, O=CSIPL, L=Bengaluru, ST=Karnataka, C=IN corr ect? [no]: yes Enter key password for <tomcat>

(RETURN if same as keystore password):

Keystore will be created under c:\>

7 Installation and Configuration of Apache Tomcat with HTTPS

7.1 Installation and configuration of Apache Tomcat on Linux platform

- Download the latest version of Apache Tomcat; refer to http://tomcat.apache.org/index.html for the latest version, download the zip/tar archives specific to your processor architecture(32bit/64bit). We use apache-tomcat-7.0.0 in this guide.
- Copy the downloaded apache-tomcat-7.0.0.tar.gz to the specific location on OpenAM server which was setup in section 6.1
- Extract the apache-tomcat-7.0.0.tar.gz archive. In this guide, we are extracting it under root home directory (/root)

• Increase the JVM heap size on tomcat, by setting JAVA_OPTS = "\$JAVA_OPTS - Xmx1024m -XX:MaxPermSize=256m -Xms512m property in the catalina.sh under /root /apache-tomcat-7.0.0/bin directory.

<u>Example:</u> JAVA_OPTS="\$JAVA_OPTS -Xmx1024m -XX:MaxPermSize=256m -Xms512m - Djava.util.logging.manager=org.apache.juli.ClassLoaderLogManager"

- Open the server.xml file under /root/apache-tomcat-7.0.0/conf directory,
 - ✓ <u>Comment the 8080 connector port:</u> Make the code read as below

<!-- <Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" /> -->

✓ <u>Uncomment the 8443 connector port:</u> Remove <!-- code at the beginning and --> at the end of 8443 connector, make the code read as below

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS" />

Save the **server.xml** file after doing above changes.

- Start the tomcat by executing startup.sh under /root/ apache-tomcat-7.0.0/bin directory.
- Launch a browser and go to: https://localhost:8443/tomcat.gif, if your certificate is self-signed, your browser will warn you. You should tell the browser to import the certificate and proceed. You should then see the little Tomcat logo. If you do, you're done configuring Tomcat.

7.2 Installation and configuration of Apache Tomcat on Windows platform

- Download the latest version of Apache Tomcat for windows platform; refer to http://tomcat.apache.org/index.html for the latest version, download the tomcat service installer (32-bit/64-bit Windows Service Installer apache-tomcat-7.0.0.exe). We use apache-tomcat-7.0.0 in this guide.
- Install the apache-tomcat-7.0.0.exe. in this guide, tomcat is installed under *c:\Program Files\Apache Software Foundation\Tomcat 7.0*
- Set the JAVA_HOME, JRE_HOME and JAVA_OPTS environment variables by creating a file called **setenv.bat** under *c*:*Program Files\Apache Software Foundation\Tomcat 7.0\bin* and set the above variables.

Content of **setenv.bat** in testing this guide:

set JAVA_HOME=c:\Program Files\Java\jdk1.6.0_20 set JRE_HOME=c:\Program Files\Java\jdk1.6.0_20\jre set JAVA_OPTS=%JAVA_OPTS% -Xms512m -Xmx1024m

- Open the **server.xml** file under **c:\Program Files\Apache Software** Foundation\Tomcat 7.0\conf folder,
 - ✓ <u>Comment the 8080 connector port:</u>

Make the code read as below
<!-- <Connector port="8080" protocol="HTTP/1.1"

connectionTimeout="20000"

redirectPort="8443" /> -->

✓ <u>Uncomment the 8443 connector port:</u>

Remove <!-- code at the beginning and --> at the end of 8443 connector, in this 8443 connector we have added two more attributes **keystoreFile** (location of the keystore file which was created in section 6.2, in this test it was created under C:\keystore) and **keystoreType**. Since we have keystore created with default password 'changeit', no need to set keystorePass attribute. Make the code read as below:

<Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true"

maxThreads="150" scheme="https" secure="true"

clientAuth="false" sslProtocol="TLS"

keystoreFile="C:\keystore"

keystoreType="JKS" />

Save the **server.xml** file after doing above changes.

- Start the tomcat service from services.msc utility or from Administrative Tools → Services → Apache Tomcat 7 → Start
- Launch a browser and go to: https://localhost:8443/tomcat.gif, if your certificate is self-signed, your browser will warn you. You should tell the browser to import the certificate and proceed. You should then see the little Tomcat logo. If you do, you're done configuring Tomcat.

8 Provisioning Active Directory for Single Sign-on

- Login to AD Server.
- From the Start menu, go to Programs>Administration Tools. Select Active Directory Users and Computers.
- Go to Users > New > Users and create a new user with the OpenSSO Enterprise host name as the User ID (example: *vrajlnx*).
- The OpenSSO Enterprise host name should not include the domain name.
- Create keytab file on the AD server using below command from the command prompt.

ktpass -princ HTTP/hostname.domainname@DCDOMAIN -pass password mapuser userName-out hostname.HTTP.keytab -ptype KRB5_NT_PRINCIPAL target DCDOMAIN

Example:

ktpass -princ HTTP/vrajlnx.vrajoli.com@VRAJOLI.COM -pass <password> -mapuser vrajlnx -out vrajlnx.HTTP.keytab -ptype KRB5_NT_PRINCIPAL -target VRAJOLI.COM

• After successful creation of keytab file, copy the keytab file to some location on the OpenAM server, this path will later be specified in OpenAM configuration.

For OpenAM configured on Linux, you can create a directory under root, and copy the above keytab file. *Example: /root/keytab/ vrajlnx.HTTP.keytab*

For OpenAM configured on Windows, you can create a directory under C:\>, and copy the above keytab file. *Example: c:/keytab/ vrajlnx.HTTP.keytab*

9 Deploying OpenSSO (OpenAM) Enterprise on Apache Tomcat

9.1 Deploying OpenSSO enterprise war on Apache Tomcat over Linux platform

- Visit to forgerock site http://www.forgerock.com/downloads.html and download the stable release OpenAM Release9 / February 7, 2010(20100207)
- Copy the openam_release9_20100207.zip to OpenAM server to any location and unzip it.
- Stop the tomcat service if running on this OpenAM server.
- After unzipping, copy opensso.war file under opensso/deployable-war directory and paste it under /root/apache-tomcat-7.0.0/webapps directory.
- Start the tomcat by executing startup.sh under /root/ apache-tomcat-7.0.0/bin directory.

9.2 Deploying OpenSSO enterprise war on Apache Tomcat over Windows platform

- Visit to forgerock site http://www.forgerock.com/downloads.html and download the stable release OpenAM Release9 / February 7, 2010(20100207)
- Copy the openam_release9_20100207.zip to OpenAM server to specific location and unzip it.
- Stop the tomcat service if running on this OpenAM server. (Administrative Tools → Services → Apache Tomcat 7 → Stop)
- After unzipping, copy opensso.war file under opensso\deployable-war folder and paste it under *c:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps* folder.
- Start the tomcat from Administrative Tools \rightarrow Services \rightarrow Apache Tomcat 7 \rightarrow Start

10Configuring OpenSSO Enterprise Using the GUI Configurator

OpenAM server and policy agents require FQDNs for the host name of the machines where you will do your installations. You can **NOT** use a host name like "localhost" and can **NOT** use numeric IP addresses like "192.168.1.2" as host names either, else it will **cause problems** in installation, configuration and usage

When accessing the OpenAM for the first time, you should use FQDN of OpenAM server in the URL (<u>https://vrajlnx.vrajoli.com:8443/opensso</u>). When you access OpenSSO Enterprise for the first time, you will be directed to the Configurator, to perform the OpenSSO Enterprise initial configuration. You will see the below screenshot when accessed the OpenSSO for the first time.



Select the configuration option:

• **Default Configuration**: You specify and confirm passwords for the OpenSSO Enterprise administrator (amAdmin) and the default policy agent user (UrlAccessAgent), which is the policy agent user that connects to OpenSSO Enterprise server. The Configurator uses default values for the other configuration settings.

The default policy agent user is also referred to as an application user. This user can connect to OpenSSO Enterprise server from a client such as the client SDK or a distributed authentication UI server.

Choose Default Configuration for development environments or simple demonstration purposes when you just want to evaluate OpenSSO Enterprise features. Click Create Default Configuration and continue with Configuring OpenSSO Enterprise With the Default Configuration.

OR

• **Custom Configuration**: You specify the configuration settings that meet the specific requirements for your deployment (or accept the default settings). Choose Custom Configuration for production and more complex environments. For example, a multi-server installation with several OpenSSO Enterprise instances behind a load balancer. Click Create New Configuration and continue with Configuring OpenSSO Enterprise with a Custom Configuration.

For Custom configuration, refer to Chapter 14.

In this section, we will select Default Configuration and move further.

When the configuration is complete, the Configurator displays a link to the OpenSSO

Enterprise Administration Console to perform any additional configuration required for your



deployment.

If a problem occurred during the configuration, the Configurator displays an error message. If you can, correct the error and retry the configuration.

Also, check the web container log files and the install.log, which if created, will be in the configuration directory (default /opensso). These logs might contain information about the

cause of a configuration problem.

By default, OpenSSO will be deployed under /root/opensso directory on Linux platform, on windows platform OpenSSO will be deployed under C:\opensso

Click on Proceed to login.

You will see the below screen. Login with amAdmin username and password you created during creating the default configuration.



Login to OpenSSO server with amAdmin username and password

Go to Access Control tab and click on / (Top Level Realm), then go to Authentication tab as shown below.
🥹 OpenSSO - Mozilla Firefox								
<u>Eile E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>I</u>	<u>H</u> elp							
🔇 🔊 - C 🗙 🏠 💽 vrajol.com https:	//vrajlnx.vrajoli.com:8443/op	ensso/realm/Realm	Properties?Realn	nProperties.t 🏠 🖞	+ 🛃 + Google	P		
🖬 1 OpenSSO 🔅								
VERSION					LOG	OUT HELP		
User: amAdmin Server: vrajinx.vrajoli.com								
OpenSSO 🔤								
		ĥ				Sun" Microsystems, Inc.		
General Authentication Serv	vices Data Stores	Privileges	Policies	Subjects	Agents	- 22-		
/ (Top Level Realm)	/ (Top Level Realm)							
(Top Level Realm) - Authentication			S	ave Reset	Back to A	ccess Control		
Core * Authenticatio	n Chaining							
 Module Instances 								
Core								
All Core Settings								
Organization Authentication Config	uration: IdapService	~						
Administrator Authentication Configuration: IdapService								
Default Success Login URL								
Current Values /opensso/con	sole <u>^</u> Rem	ove						
						~		
Done						🔒 F110% 🛷		

Click on **All Core Settings...** button in the above screen, set the User Profile to **Ignored** as shown below, Click the Save button to save the configuration.

🥹 OpenSSO - Mozilla Firefox				
Ele Edit View History Bookmarks Tools Help				
C X 🏠 🐻 vrajoli.com https://vrajlnx.vraj	oli.com:8443/opensso/authentication/AuthPropert	ies 🏠 +	🛃 - Google	P
1 OpenSSO +				+
VERSION			LOG OUT	HELP ^
User: amAdmin Server: vrajlnx.vrajoli.com				10
OpenSSO				
			Sun" Mic	Java
			2-2-2-2 (2-2-2-2-2-2-2-2-2-2-2-2-2-2-2-2	
Core		Save Reset	Back to Authen	tication
Realm Attributes				
User Profile:	 ○ Dynamic ○ Dynamic with User Alias ● Ignored ○ Required 			
Administrator Authentication Configuration:	⊖ [empty] ⊚ IdapService			
User Profile Dynamic Creation Default Roles				
Current Values	Remove			
Done	1		<u> </u>	F110% 🕷

10.1 Configuring Policies on OpenSSO server

10.1.1 Configuring Policies on OpenSSO server for Cisco Unified Communication Manager 8.5, 8.6

Login to OpenSSO server with amAdmin username and password

Go to Access Control tab and click on / (Top Level Realm). You will see the below screen after clicking on / (Top Level Realm).

🕄 OpenSSO - Mozi	lla Firefox						
File Edit View History Bookmarks Tools Help							
C C X	🕎 💌 vraioli com I	https://vrailnx.v	raioli.com:8443/or	ensso/task/Home?t	Home.tabCom	mon. TabHref=1&iato. par 🏠 🔹 Google	
OpenSSO	*						
VERSION						LOG OUT HELP	
User: amAdmin Serv	ver: vrajlnx.vrajoli.com					<u>«</u>	
OpenSSO						Java	
					Tomo ya i	Sun" Microsystems, In	
Common Tasks	Access Control	Federation	Web Services	Configuration	Sessions		
A realm is the unit that defined within the real configuration data.	t OpenSSO uses to or m. The top level realm	ganize configura is created wher	tion information. Au you deploy OpenS	thentication properti SO. The top level rea	es, authorization alm is the root	on policies, data stores, subjects and other data can be of the OpenSSO instance and contains OpenSSO	
Realms							
×.;	Search						
Realms (1 Item(s))	_	-	_	_	-		
Realm Name					Locati	ion	
/ (Top Level F	, Realm)				/		
Dono						فد ایم ا	

Go to policies tab and add a new policy, enter the PolicyName.

🕲 OpenSS(0 - Mozilla Firefo	x						
Eile Edit 1	/iew Hi <u>s</u> tory <u>B</u> ool	kmarks <u>T</u> ools	<u>H</u> elp					
	C 🗙 🏠 🗷 🗤	ajoli.com http:	s://vrajlnx.vrajoli	i.com:8443/op	ensso/policy/	PolicyNormalA	Ndd	☆ • 🚺• Google 🖉
OpenSS	0	+						
VERSION]							LOG OUT HELP
User: amAdr	min Server: vrajlnx.v	rajoli.com						٢
OpenSSO								Java
24.00								Sun ⁴⁴ Microsystems, Inc.
General	Authentication	Services	Data Stores	Privileges	Policies	Subjects	Agents	
/ (Top Level)	Realm)							
(Top Level)	Realm) - Policies							Back to Access Control
*	Sea	urch						
Policies (0	ltem/c))		_	_	_	_	_	
New Polic	v New Referral	Delete						
Name	,	Pro	tected Resourc	es				
There are r	no policies.							
Done								🔒 🦑 .

Create a new Rule from the Policy Configuration page. You will see the below screen. select service type as "URL Policy Agent (with resource name)"



Enter the Rule Name and Resource URL as Web Application URL. In our case it will be CUCM User application URL (https://<CUCM FQDN>:8443/*).

Check GET and POST check box and press Finish button.

🕑 Ор	enSSO - N	lozilla Firefox		
<u>F</u> ile <u>E</u>	dit <u>V</u> iew	History Bookmarks Tools	<u>H</u> elp	
< >	· C ×	🕻 🏠 🌆 vrajoli.com https://	vrajlnx.vrajoli.com:8443/opensso/policy/S	electServiceTyr 🏠 - 🚺 - Google 🛛 🔎
De Op	enSSO	*		-
VER	SION			LOG OUT HELP
User:	<i>«</i> .			
Oper	ISSO			juj lava"
1	_			Sun [®] Microsystems, Inc.
Step	2 of <mark>2</mark> : Ne	w Rule		Back Finish Cancel * Indicates required field
* So Typ	ervice be:	URL Policy Agent		
* N	ame:	CUCMUser		
* R Nar	esource ne:	https://vrajolicucm1.vra	joli.com:8443/*	
Actio	ns			
* 0	ne or mor	e actions are required.		
Ac	tions (2 It	em(s))		
	Action	*	Value	
	GET		●Allow ○Deny	
	POST		● Allow ○ Deny	
Done				🔒 F110% 🏕

Create another rule for the requests involving query patterns (*?*) in Find and List pages of CUCMUser application

🔮 OpenSSO - Mozili	a Firefox			
<u>File Edit View Histo</u>	ry <u>B</u> ookmarks <u>T</u> ools	Help		
🔇 🔊 - C 🗙 🏠	wrajoli.com https://	/vrajlnx.vrajoli.com:8443/opensso/policy/SelectServiceTyr 🏠	- Google 🔎	
S OpenSSO	÷		-	
VERSION			LOG OUT HELP	
User: amAdmin Ser	ver: vrajlnx.vrajoli.com		«	
OpenSSO			jej lava	
			Sun [®] Microsystems, Inc.	
Step 2 of 2: New Ru	lle		Back Finish Cancel * Indicates required field	
* Service URL Policy Agent Type:				
*Name: C	CUCMUser_QueryPatt	erns		
* Resource h Name:	ttps://vrajolicucm1.vra	joli.com:8443/*?*		
Actions * One or more act	tions are required.			
Actions (2 Item(s	i))			
Action		Value		
GET		● Allow ○ Deny		
POST		● Allow ○ Deny		
Done			🔒 F110% 🦑	

From CUCM 8.6 release, SSO support is provided for RTMT application as well. To achieve SSO for RTMT, along with the above policy rules, one more new rule should be created for the requests involving RTMT query patterns (*?*?*),

🔮 Oper	nSSO - Mozilla Firefox					
	🗸 C 🗙 🏠 🚮 vrajoli.com http	ps://vrajlnx.vrajoli.com:8443/opensso/policy/SelectService' ☆ 🔹 👪 - Google	P			
🚮 Oper	nSSO +		-			
VERS	SION	LOG OUT	HELP ^			
User: a	amAdmin Server: vrajlnx.vrajoli	.com	4			
Opens	SSO		E) lava			
		Sua" Micr	osystems, inc.			
Step 2	of 2: New Rule	Back Finish * Indicates requi	Cancel ired field			
* Service URL Policy Agent Type:						
* Na	me: RTMT_Query					
*	https://vrajolicucm1.vra	ajoli.com:8443/*?*?*				
Res Nam	ie:					
Action * On Acti	s e or more actions are require ions (2 Item(s))	ed.				
	Action 🔺	Value				
☑ (GET	● Allow ○ Deny				
F	POST	● Allow ○ Deny	~			
<			>			
Done			🔒 F110%			

Click on New Button under Subjects on the Policy Configuration page. Select subject type as "Authenticated Users".



Enter the Subject Name and Click Finish. Now Policy is created with defining Rules and Subjects. Click on Finish button.



Click on New button under Conditions. Under select condition type, select Active Session Time and click next button.

OpenSSO - Mozilia Firefox		
Elle Edit View History Bookmarks Loois I	Heip	
• C × 🏠 📾 vrajoli.com https://v	vrajInx.vrajoli.com:8443/opensso/policy/PolicyNormalAd 😭 🕤 🎦 Google	<u></u>
si OpenSSO ÷		
VERSION		UT HELP
User: amAdmin Server: vrajinx.vrajoli.com		<u></u> ,
OpenSSO		Java"
		Sun [®] Microsystems, Inc.
Step 1 of 2: Select Condition Type	Back Ne	xt Cancel
	* Indicates	required field
* Type: Active Session Time 		
Authentication by Module Characteristics by Module Inst Authentication by Module Inst	ain tance	
Authentication Level (greater	than or equal to)	
Authentication Level (less that	an or equal to)	
Authentication to a Realm Ourrent Session Presenting		
☐ Identity Membership		
O IP Address/DNS Name		
O LDAP Filter Condition	• 200703.00	
Resource/Environment/IP Add Time (day, date, time, and time)	dress nezone)	
O Time (day, date, time, and tim		
Done		E110%
🥹 OpenSSO - Mozilla Firefox		
<u>File Edit View History Bookmarks Tools</u>	Help	
🔣 🔹 😴 🗶 🏫 🖾 vrajoli.com https:/	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🎲 🕤 🛂 - Goog	le 🔎
Solution of the second	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 🍷 🛂 - Goog	le 🔎
VERSION	//vrajinx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏫 🍵 👪 - Goog	G OUT HELP
C X A Les vrajoli.com https:/ OpenSSO VERSION	//vrajinx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏫 🍵 👪 - Goog	GOUT HELP
VERSION User: amAdmin Server: vrajinx.vrajoli.com	//vrajinx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏫 🍵 👪 - Goog	
VERSION User: amAdmin Server: vrajinx.vrajoli.com OpenSSO	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 🅤 🛂 - Goog	G OUT HELP
VERSION User: amAdmin Server: vrajlnx.vrajoli.com OpenSSO	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🛛 🔮 - Goog	le P G OUT HELP ýjava Sun [®] Microsystems, Inc
VERSION User: amAdmin Server: vrajlnx.vrajoli.com OpenSSO	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🛛 😫 - Goog	le P GOUT HELP Java Sun [®] Microsystems, Inc
C Image: Comparison of the state of t	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🛛 😫 - Goog LO ssion Time	e P G OUT HELP java Sun [®] Microsystems, Inc
C X Yrajoli.com https:/ OpenSSO * VERSION User: amAdmin Server: vrajinx.vrajoli.com OpenSSO Step 2 of 2: New Condition - Active Sec	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🛛 😫 - Goog LO n ssion Time Back F * Indice	e P G OUT HELP Java Sun [®] Microsystems, Inc Finish Cancel ates required field
C X Yesiol.com https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🛛 😫 - Goog LO ssion Time Back F * Indica	e P G OUT HELP java Sun [®] Microsystems, Inc Finish Cancel ates required field
C X Yespectrum https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🚺 - Goog LO ssion Time Back F * Indica CUCMUser	e P G OUT HELP java Sun [®] Microsystems, Inc Finish Cancel ates required field
C X Yesoloicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🚺 - Goog LO ssion Time Back F * Indica CUCMUser 120	e P G OUT HELP java Sun [®] Microsystems, Inc Finish Cancel ates required field
C X Yesolicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🚺 - Goog LO ssion Time Back F * Indica CUCMUser 120 No 💌	e P G OUT HELP java Sun [®] Microsystems, Inc Finish Cancel ates required field
C X Yesolicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🚺 - Goog LO ssion Time Back F * Indica CUCMUser 120 No 👻	e P G OUT HELP java Sun" Microsystems, Inc Finish Cancel ates required field
C X Yesolicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🔛 - Goog LO ssion Time Back F * Indica CUCMUser 120 No 💌	e
C X Yesolicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🔛 - Goog LO ssion Time Back F * Indice CUCMUser 120 No v	e P G OUT HELP java Sun" Microsystems, Inc Finish Cancel ates required field
C X Yesolicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🔛 - Goog LO ssion Time Back F * Indice CUCMUser 120 No v	e
C X Yesoloicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 🔛 - Goog LO ssion Time Back F * Indice CUCMUser 120 No v	e
C X Yesoloicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 💽 🍇 - Goog LO ssion Time Back F * Indice CUCMUser 120 No v	e
C X Yesoloicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 💽 🍇 - Goog LO ssion Time Back F * Indice CUCMUser 120 No v	e
C X Yead Community (Community): OpenSSO VERSION User: amAdmin Server: vrajInx.vrajoli.com OpenSSO Step 2 of 2: New Condition - Active See * Name: * Maximum Session Time (minutes): * Terminate Session:	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 - 💽 🍇 - Goog LO ssion Time Back F * Indice CUCMUser 120 No 💌	e
C X Yesoloicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 😭 - 💽 😫 - Goog LO ssion Time Back F * Indice CUCMUser 120 No 💌	e
C X Yesoloicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 😭 - 💽 😫 - Goog LO ssion Time Back F * Indice CUCMUser 120 No 💌	e
C X Yesoloicom https://	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 😭 - 💽 😫 - Goog LO ssion Time Back F * Indice CUCMUser 120 No 💌	e
C Version OpenSSO VERSION User: amAdmin Server: vrajinx.vrajoli.com OpenSSO Step 2 of 2: New Condition - Active See * Name: * Maximum Session Time (minutes): * Terminate Session:	//vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 😭 - 🚱 - Goog ssion Time Back F * Indice CUCMUser 120 No V	GOUT HELP GOUT HELP Java Sun [®] Microsystems, Inc Sinish Cancel ates required field

Configure active session timeout as 120 minutes.

10.1.2 Configuring Policies on OpenSSO server for Cisco Unity Connection 8.6

Login to OpenSSO server with amAdmin username and password. Go to Access Control tab and click on / (Top Level Realm). You will see the below screen after clicking on / (Top Level Realm).

🥹 OpenSSO - Mozi	lla Firefox					
Eile Edit View His	tory <u>B</u> ookmarks]	ools <u>H</u> elp				
🔇 🖸 - C 🗙	🏠 🗷 vrajoli.com	https://vrajlnx.v	rajoli.com:8443/op	oensso/task/Home?I	Home.tabCon	nmon.TabHref=1&jato.paç 🟠 🔹 🚮 Google 🛛 🔎
🗷 OpenSSO	+					
VERSION						LOG OUT HELP
User: amAdmin Serv	er: vrajlnx.vrajoli.com					<u>چ</u>
OpenSSO						Java
Common Tasks	Access Control	Federation	Web Services	Configuration	Sessions	Self - Microsystems, IRC.
A realm is the unit that	OpenSSO uses to o	rganize configura	ation information. Au	thentication propert	ies, authorizat	tion policies, data stores, subjects and other data can be
configuration data.	III. The top level realin	TIS Created when	ryou deploy Opens	SO. The top lever le	aim is the roo	tor the OpenSSO instance and contains OpenSSO
Realms						
*	Search					
Realms (1 Item(s))	_	_	_	_	_	
New Delete						
🗵 🗄 Realm Name					🔺 Loca	tion
/ (Top Level R	ealm)				1	
Done						🔒 🏶 🛒

Go to policies tab and add a new policy, enter the PolicyName.

🕹 OpenSSO - Mozilla Firefox	
Elle Edit View History Bookmarks Tools Help	
🕜 🗁 😋 🗶 🏠 🖾 vrajoli.com https://vrajlnx.vrajoli.com:8443/opensso/policy/PolicyNormalAdd 🏠 🖓 🔀 Go	ogle 🔎
Ø OpenSSO ↔	1
VERSION	OG OUT HELP
User: amAdmin Server: vrajlnx:vrajoli.com	j,
UpenSSU	Java
Conserve Authentiastian Services Date Stores Brivileges Delisies Subjects Agents	Sun" Microsystems, Inc.
General Authentication Services Data stores Frivileges Folicies Subjects Agents	
/ (Top Level Realm)	
(Top Level Realm) - Policies Back t	o Access Control
* Search	
Policies (0 Itam/s))	
New Policy New Referral Delete	
Name Protected Resources	_
There are no policies.	
Done	🔒 🦑 .

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

Create a new Rule from the Policy Configuration page. You will see the below screen. select service type as "URL Policy Agent (with resource name)"

🔮 OpenSSO - Mozilla Firefox	
Elle Edit View History Bookmarks Iools Help	
🕢 🕞 C 🗙 🏠 🔄 vrajoli.com https://vrajlnx.vrajoli.com:8443/opensso/policy/PolicyNormalEdit	습 • 🛃 Google 🖉
🖉 OpenSSO 🔅	
VERSION	LOG OUT HELP
User: amAdmin Server: vrajlnx.vrajoli.com	<u>, s</u>
OpenSSO	Java [*]
	Sun [®] Microsystems, Inc.
Step 1 of 2: Select Service Type for the Rule	Back Next Cancel * Indicates required field
* Service Type: ODiscovery Service (with resource name) OLiberty Personal Profile Service (with resource name) © URL Policy Agent (with resource name)	
Done	🔒 🦑 🔬

Then create rules for Cisco Unity Connection application(s) with below resource URL configured in protected resources.

- https://<FQDN>:8443/*
- https://<FQDN>:8443/*?*
- https://<FQDN>/*
- https://<FQDN>/*?*
- http:/<FQDN>/*
- http:/<FQDN>/*?*

where fqdn is the fully qualified domain name of Cisco Unity Connection server. Below is the snapshot of OpenSSO Policy configured for Unity Connection server.

🥹 OpenSSO - Mozilla Firefox							
🕼 🗁 C 🔀 🏠 🔝 vrajoli.com https://vrajhx.vrajoli.com:8443/opensso/policy/Policy?Policy:tblSearch 😭 🕤 🛂 - Google 🖉							
See OpenSSO *							
VERSION					LC	DG OUT HELP	
User: amAdmin Server: vrajlnx.v	/rajoli.com					<u>, (</u>	
OpenSSO						Java	
	. 7	1		-	1	Sun [®] Microsystems, Inc.	
General Authentication	Services	Data Stores	Privileges	Policies	Subjects	Agents	
/ (Top Level Realm) (Top Level Realm) - Policies * Sea Policies (26 - 26 of 26) New Policy New Referral	rch Delete		_	_	Back t	o Access Control	
🗵 🗉 Name 🔺	Protected Re	sources					
UCSSO https://ucsso238.vrajoli.com/* http://ucsso238.vrajoli.com/* https://ucsso238.vrajoli.com/*?* https://ucsso238.vrajoli.com/*?* https://ucsso238.vrajoli.com/*?*							
Page: 2 of 2	Go 🕑	N 6+D					
Done						🔒 F110%	

Click on New Button under Subjects on the Policy Configuration page. Select subject type as "Authenticated Users".



Copyright © 2010 Cisco Systems, Inc. All rights reserved.

Enter the Subject Name and Click Finish. Now Policy is created with defining Rules and Subjects. Click on Finish button

🥹 OpenSSO - Mozilla Firefox	
🕢 🗸 🖒 🐨 Vrajol.com https://vrajlnx.vrajol.com:8443/opensso/policy/PMAuthenticatedUser	습 🔹 🚼 🔹 Google 🖉
Some Section S	-
VERSION	LOG OUT HELP
User: amAdmin Server: vrajlnx.vrajoli.com	<u>(</u>
OpenSSO	Java"
	Sun [®] Microsystems, Inc.
Step 2 of 2: New Subject - Authenticated Users	Back Finish Cancel
	* Indicates required field
* Name: UCSSO	
Exclusive:	
Done	🔒 F110% 🚽

Click on New button under Conditions. Under select condition type, select Active Session Time and click next button

🔮 OpenSSO - Mozilla Firefox	
Eile Edit View History Bookmarks Tools Help	
🕜 🕞 C 🔀 🏡 🔚 vrajoli.com https://vrajlnx.vrajoli.com:8443/opensso/policy/PolicyNormalAd 🏠	- Google 🔎
CopenSSO *	
VERSION	LOG OUT HELP
User: amAdmin Server: vrajlnx.vrajoli.com	« .
OpenSSO	ji j
	Sun* Microsystems, Inc.
Step 1 of 2: Select Condition Type	Back Next Cancel * Indicates required field
Authentication by Module Chain Authentication by Module Instance Authentication Level (greater than or equal to) Authentication to a Realm Current Session Properties Identity Membership IP Address/DNS Name LDAP Filter Condition Resource/Environment/IP Address Time (day, date, time, and timezone)	
Done	🔒 F110% 🌌

Configure active session timeout as 120 minutes

🥹 OpenSSO - Mozilla Firefox		
🚱 🕞 C 🗙 🏠 🜆 vrajoli.com https://v	rajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessionCo	n 🗘 🔹 🛃 - Google 🛛 🔎
S OpenSSO +		-
VERSION		LOG OUT HELP
User: amAdmin Server: vrajlnx.vrajoli.com		Ľ,
OpenSSO		Java"
		Sun [®] Microsystems, Inc.
Stop 2 of 2: Now Condition Active Sec	aion Timol	Back Finish Cancel
Step 2 of 2. New Condition - Active Ses		* Indicates required field
* Namo:	10250	
* Maximum Cassian Time (minutes):		
maximum Session Time (minutes):	120	
* Terminate Session:	No 💌	
Done		🔒 F110%

Copyright $\ensuremath{\mathbb{C}}$ 2010 Cisco Systems, Inc. All rights reserved.

10.2 Configuring Windows Desktop SSO Authentication module instance

The Windows Desktop SSO Authentication Module enables OpenSSO Enterprise to work with Kerberos tokens. The user presents the Kerberos token, previously issued by a Kerberos Distribution Center, to OpenSSO Enterprise using the SPNEGO protocol. The client browser sends back a SPNEGO token embedded with a Kerberos token. The OpenSSO Windows Desktop SSO Authentication module retrieves the Kerberos token and authenticates the user using the Java GSS API. If authentication is successful, the OpenSSO Windows Desktop SSO Authentication module returns an SSOToken to the client.

- Copy the keytab files to OpenAM server, which was created in section 8.
- Log into the OpenSSO Enterprise administration console as amAdmin.
- Go to Access Control > Default Realm > Authentication.
- In the Module Instances page, click New.
- Enter a name for the new login module, and then select Windows Desktop SSO. Click OK.

In this test, Module instance with name 'CUCMUser' is created.

- In the Module Instances page, click the name of the new login module (*Example: CUCMUser*) and provide the following information:
- Service Principal: HTTP/ openAMhost.example.com@EXAMPLE.COM
- Keytab File Name: /root/keytab/openAMhost.HTTP.keytab
- Kerberos Realm: EXAMPLE.COM
- Kerberos Server Name: Kerberos.example.com
- If multiple Kerberos Domain Controllers exist for failover purposes, all Kerberos Domain Controllers can be set using a colon (:) as the separator.
- Return Principal with Domain Name: False
- Authentication Level: 22
- Restart the OpenSSO Enterprise server.

🥹 OpenSSO - Mozilla Firefox			_ 🗆 🔀
<u>Eile Edit View History Bookmarks Tools Help</u>			
🔇 🖂 🗸 🕜 🔝 vrajoli.com https://v	rajlnx.vrajoli.com:8443/opensso/authentication/AuthProper	ties?AuthPrope 🏠 🚽 🚼 - Google	P
🖬 1 OpenSSO 🔅			+
VERSION		LOG OUT	HELP
User: amAdmin Server: vrajlnx.vrajoli.com			k
OpenSSO			E
		Sun ^w A	Java Aicrosystems, Inc.
Windows Desktop SSO		Save Reset Back to Authe	entication
Desiles Attails start			
Realm Attributes			
Service Principal:	HTTP/vrajlnx.vrajoli.com@VRAJOLI.COM		
Keytab File Name:	/root/keytab/vrajlnx.HTTP.keytab		
Kerberos Realm:	VRAJOLI.COM		
Kerberos Server Name:	ssoad.VRAJOLI.COM		
Return Principal with Domain Name:	Enabled		
Authentication Level:	22		
		Save Reset Back to Authe	entication
Done		🔒 I	F110% 🕷

10.3 Configure J2EE Agent profile on OpenSSO server

10.3.1 Configure J2EE Agent Profile on OpenSSO server for Cisco Unified Communications Manager 8.5, 8.6

Perform the following tasks in OpenSSO Enterprise Console. The key steps of this task involve creating an agent name (ID) and an agent password.

- Log in to OpenSSO Enterprise Console as a user with AgentAdmin privileges, such as amadmin.
- Click the Access Control tab.
- Click the name of the realm to which the agent will belong, such as the following: /(Top Level Realm).
- Click the Agents tab.
- Click the J2EE tab.
- Click New in the agent section.
- Enter values for the following fields:
- Name: Enter the name or identity of the agent. This is the agent profile name, which is the name the agent uses to log into OpenSSO Enterprise. Multi-byte names are not accepted.

NOTE: while enabling SSO on Cisco Unified Communications Manager or Cisco Unity Connection, when requested for "Enter the name of the profile configured for this policy agent", the above configured agent name should be entered.

• Password: Enter the agent password. However, it must be the same password entered in the agent profile password file that is used by the agentadmin utility to install the agent.

NOTE: while enabling SSO on Cisco Unified Communications Manager or Cisco Unity Connection, when requested for "Enter the password of the profile name", the above configured password should be entered.

- Re-Enter Password: Confirm the password.
- In the Server URL field, enter the OpenSSO Enterprise server URL.

For example: https://<OpenAM FQDN>:8443/opensso

• In the Agent URL field, enter the URL for the agent application.

For example: https://<Cisco Unified Communications Manager FQDN>:8443/agentapp

• Click Create.

The Console creates the agent profile and displays the J2EE Agent page again with a link to the new agent profile.

🕲 OpenSSC) - Mozilla Firefo	эх										X
<u>Eile Edit V</u>	iew Hi <u>s</u> tory <u>B</u> oo	kmarks <u>T</u> ools	<u>H</u> elp									
	2 × 🏠 🗷	rajoli.com https	s://vrajlnx.vrajoli	.com:8443/op	ensso/agent	config/Agents	s		습 • 🔮	• Google		P
OpenSSC 🖉)	*										÷
VERSION										LOG OUT	HELP	^
User: amAdn OpenSSO	nin Server: vrajlnx.	vrajoli.com								Sun [®] Micr	Java Java	
General	Authentication	Services	Data Stores	Privileges	Policies	Subjects	Agents					
Web	J2EE Web Se	ervice Provider	Web Service	Client STS	Client 2	.2 Agents	Agent Authentio	ator				
/ (Top Level F J2EE J2EE agents	Realm) protect Java applic	cation servers su	uch as Glassfish, I	BM WebSpher	e Applicatic	on Server and	Oracle WebLog	ic Applicatic	Bac on Server.	k to Access	Control	1
*	Se	arch										
Agent (0 Ag	gent) Doloto	_	_	_	-	_	_	-	_	_	_	
Name	Delete	Reno	siton/'s Location	1								
There are n	o entities.	Itepo	skory a Locator	•							_	
*	Se	arch										
Group (0 G	roup) Delete	_	_	_	_	_	_	_	_	_	-	
Name												
There are n	o entities.											
												*
Done											<u></u>	*

🥹 OpenSSO - Mozilla F	irefox	
<u>Eile Edit View History</u>	Bookmarks Tools Help	
🕢 🖓 🖯 🕻	vrajoli.com https://vrajlnx.vrajoli.com:8443/opensso/agentconfig/Agents	🗘 • 🛂• Google 🖉
OpenSSO	*	
VERSION		LOG OUT HELP
User: amAdmin Server: vi	ajlnx.vrajoli.com	<u>«</u>
OpenSSO		Java
		Sun" Microsystems, Inc.
New Agent		Create Cancel * Indicates required field
*Name:	CUCMUser	
* Password:	••••••	
*Re-Enter Password:	•••••	
Configuration:	○Local	lized is the OpenSSO Server
* Server URL:	https://vrajlnx.vrajoli.com:8443/opensso	
	protocol://host:port/deploymentUri e.g. http://opensso.sample.com:58080/opensso	
* Agent URL:	https://vrajcucm1.vrajoli.com:8443/agentapp	
	protocol.most.poi/deploymenton e.g. http://agent1.sample.com.1234/agentapp	
Done		<u>د</u> ک

Click on the J2EE agent created above, go to Application tab, and under Login processing enter new Login Form URIs.

- For CCMUser webapp: /ccmuser/WEB-INF/pages/logon.jsp
- For CUCiMOC: /cucm-uds/WEB-INF/pages/logon.jsp

Starting from CUCM 8.6 release, SSO support is provided for other applications like Cisco Unified CM Administration, Cisco Unified Serviceability, Cisco Unified Reporting, Cisco Unified OS Administration, Disaster Recovery System and RTMT along with Cisco Unified CM User Options and CUCiMOC, for these new applications, you need to configure below Login Form URIs.

٠	For Cisco Unified CM Administration:	/ccmadmin/WEB-INF/pages/logon.jsp
•	For Cisco Unified Serviceability:	/ccmservice/WEB-INF/pages/logon.jsp
•	For Cisco Unified Reporting:	/cucreports/WEB-INF/pages/logon.jsp
•	For Cisco Unified OS Administration:	/cmplatform/WEB-INF/pages/logon.jsp
•	For Disaster Recovery System:	/drf/WEB-INF/pages/logon.jsp
•	For Real Time Monitoring Tool (RTMT):	/ast/WEB-INF/pages/logon.jsp

🔮 OpenSSO - Mozilla Fi	refox				
<u>File Edit View History B</u>	ookmarks <u>T</u> ool	; <u>H</u> elp			
🔇 🖂 - C 🗙 🏠 🔝	vrajoli.com https	://vrajlnx.vrajoli.com:8443	opensso/agentconfig/	GenericAgentProfile?Gen	ericAgen 🏠 🕤 🚼 🖕 Google 🛛 🔎
5. OpenSSO	÷				
VERSION					LOG OUT HELP
User: amAdmin Server: v	rajlnx.vrajoli.co	m			۷,
OpenSSO					Java"
					Sun" Microsystems, Inc.
Global Applicatio	n SSO	OpenSSO Services	Miscellaneous	Advanced	
Edit CUCMUser					Save Reset Back to Main Page
Inheritance Settings	Export Config	uration			
	× No	Enforced LIRI			
 Login Processing 	Pro	ocessing	 Response Att 	ibutes Processing	 Privilege Attributes Processing
Logout Processing	≈ No Pro	t Enforced IP ocessing	 Common Attri Processing 	outes Fetching	 Custom Authentication Processing
 Access Denied URI Processing 	× Pro Pro	ofile Attributes ocessing	 Session Attrib 	utes Processing	
Login Processing					
Login Form URI					
Current Values	/ccmuser/WEF	B-INE/pages/logon isp	Remove		
	/cucm-uds/WE	B-INF/pages/logon.jsp			
		1			
			2		
New Value		Add			
https://wrailpy.wraioli.com:94	1 43/opensso/2000	tconfig/GenericAgentDrofile	2Generic Agent Profile +	abCommon TabHrof-46	001#lbli oggut Processing

Go to OpenSSO Services tab, Under Login URL add OpenSSO Login URL as https://<OpenSSO FQDN>:8443/opensso/UI/Login?module=<WindowsDesktopSSO_Module>

WindowsDesktopSSO_Module should be same as the one created in section 10.2

Ex: https://<OpenAM FQDN>:8443/opensso/UI/Login?module=CUCMUser

OpenSSU -	Mozilla Firerox	T 1					
Eile Edit View	History Bookmark	cs <u>L</u> ools I	<u>H</u> elp				
Con C		i.com https:	//vrajlnx.vrajoli.com:8443/oper	nsso/agentconfig/Generic	AgentProfile?Gener	icAgentProfile ☆ • 🚺 🕤 Google	
1 OpenSS	0	4		_	_		-
VERSION						LC	
User: amAdn	nin Server: vrajln	ıx.∨rajoli.c	om				<u>\$</u> ,
OpenSSO							Java
						41	Sun [®] Microsystems, Inc.
Global	Application	SSO	OpenSSO Services	Miscellaneous	Advanced		
		2					
Edit CUCML	Jser					Save Reset Ba	ack to Main Page
Inheritance	Settings Ex	mort Confi	ouration				
Innernarioe	Cottings	port com	gulation				
Solution ≥ Login URL	× Authentic	cation Ser	vice 🔹 User Data Cac	the Service			
✤ Logout UR	L × Policy Cl	lient Servi	ce 🔹 Session Client	Service			
Login URL							
avgin							
OpenSSO	Login URL						
Se	lected:		lononana/III/Login2modu			-	
inu -	ps.//vrajinx.vrajon	.0011.0443	sopensso/orcogin/modu		Move Up		
					Move Down		
					Move to Top		
					Move to Botto	on	
					Delete		
				~			
				Add			
Deno							0 E1100/ 🔅
Done							🔒 FII0% 🦛 🔅

10.3.2 Configure J2EE Agent Profile on OpenSSO server for Cisco Unity Connection 8.6

Perform the following tasks in OpenSSO Enterprise Console. The key steps of this task involve creating an agent name (ID) and an agent password.

- Log in to OpenSSO Enterprise Console as a user with AgentAdmin privileges, such as amadmin.
- Click the Access Control tab.
- Click the name of the realm to which the agent will belong, such as the following: /(Top Level Realm).
- Click the Agents tab.
- Click the J2EE tab.
- Click New in the agent section.
- Enter values for the following fields:
- Name: Enter the name or identity of the agent. This is the agent profile name, which is the name the agent uses to log into OpenSSO Enterprise. Multi-byte names are not accepted.

NOTE: while enabling SSO on Cisco Unified Communications Manager or Cisco Unity Connection, when requested for "Enter the name of the profile configured for this policy agent", the above configured agent name should be entered.

• Password: Enter the agent password. However, it must be the same password entered in the agent profile password file that is used by the agentadmin utility to install the agent.

NOTE: while enabling SSO on Cisco Unified Communications Manager or Cisco Unity Connection, when requested for "Enter the password of the profile name", the above configured password should be entered.

- Re-Enter Password: Confirm the password.
- In the Server URL field, enter the OpenSSO Enterprise server URL.
- For example: https://<OpenAM FQDN>:8443/opensso
- In the Agent URL field, enter the URL for the agent application.
- For example: https://<Cisco Unity Connection FQDN>:8443/agentapp
- Click Create.

The Console creates the agent profile and displays the J2EE Agent page again with a link to the

new agent profile.

🔮 OpenSSO - Mozilla Firefox	
Elle Edit View History Bookmarks Tools Help	
🔇 💽 😋 🗙 🏠 🗟 vrajoli.com https://vrajlnx.vrajoli.com:8443/opensso/agentconfig/Agents 🎲 र 🐉 Google	P
I OpenSSO *	÷
VERSION	HELP ^
User: amAdmin Server: vrajlnx vrajoli com	j,
UpenSSU	Java
General Authentication Services Data Stores Privilenes Policies Subjects Agents	Alcrosystems, Inc.
Web J2EE Web Service Provider Web Service Client S1S Client 2.2 Agents Agent Authenticator	
/ (Top Level Realm)	
J2EE Back to Acces	s Control
J2EE agents protect Java application servers such as Glassfish, IBM WebSphere Application Server and Oracle WebLogic Application Server.	
* Search	
Agent (0 Agent)	
New Delete	
Name Repository's Location	
There are no entities.	
- Search	
Group (0 Group)	
New Delete	
Name	
There are no ensures.	
	~
Done	🙆 🌴 🚲

😻 OpenSSO - Mozilla	a Firefox
🚱 🖸 - C 🗙 🏠	🔚 vrajol.com https://vrajhx.vrajol.com:8443/opensso/agentconfig/Agents 😭 🔹 🚼 - Google 🖉
Moren SSO	*
VERSION	LOG OUT HELP
User: amAdmin Ser	ver: vrajlnx.vrajoli.com
OpenSSO	java"
	Sun" Microsystems, Inc.
New Agent	Create Cancel * Indicates required field
* Name:	CUCSSO
* Password:	•••••
* Re-Enter Password:	•••••
Configuration:	◯ Local
	Where agent properties are stored. Local is the server on which the agent is running. Centralized is the OpenSSO Server
* Server URL:	https://vrajInx.vrajoli.com:8443/opensso
	protocol://host:port/deploymentUri e.g. http://opensso.sample.com:58080/opensso
* Agent URL:	https://ucsso238.vrajoli.com:8443/agentapp
	protocol://host:port/deploymentUri e.g. http://agent1.sample.com:1234/agentapp
Done	🔒 F110%

Click on the J2EE agent created above, go to Application tab, and under Login processing enter new Login Form URIs.

- For Cisco Unity Connection Administration:
- For Cisco Unity Connection Serviceability:
- For Cisco Personal Communications Assistant:
- For Cisco Unity Connection Web Inbox:
- For Cisco Unified CM User option:
- For CUCiMOC:
- For Cisco Unified CM Administration:
- For Cisco Unified Serviceability:
- For Cisco Unified Reporting:
- For Cisco Unified OS Administration:
- For Disaster Recovery System:
- For Real Time Monitoring Tool (RTMT):

/cuadmin/WEB-INF/pages/logon.jsp /cuservice/WEB-INF/pages/logon.jsp /ciscopca/WEB-INF/pages/logon.jsp /inbox/WEB-INF/pages/logon.jsp /ccmuser/WEB-INF/pages/logon.jsp /cucm-uds/WEB-INF/pages/logon.jsp /ccmservice/WEB-INF/pages/logon.jsp /cucreports/WEB-INF/pages/logon.jsp /cmplatform/WEB-INF/pages/logon.jsp /drf/WEB-INF/pages/logon.jsp

🥹 OpenSSO - Mozilla Fire	fox					
🔇 🗩 C 🗙 🏠 🔝	vrajoi.com https	:://vrajlnx.vrajoli.com:8443/oper	nsso/agentconfig/Gener	icAgentProfile	🏠 📲 🗧 Google	P
Moren SSO	+					-
VERSION					LOG OUT	HELP ^
User: amAdmin Server: \	rajlnx.vrajoli.c	om				Ś,
OpenSSO						Java
		1			Sun [™]	Microsystems, Inc.
Global Applicatio	n SSO	OpenSSO Services	Miscellaneous	Advanced		
			🕤 Info	rmation		
			Profile wa	s updated.		
Edit CUCSSO					Save Reset Back to M	lain Page
Inhoritoneo Cottingo	Export Cont	Suration				
Innentance Settings	Export Com	iguration				
✤ Login Processing	*	Not Enforced URI Proces	sing × Respon	se Attributes Processing	Privilege Attributes Processing	
* Logout Processing	*	Not Enforced IP Processi	ing × Commo	n Attributes Fetching Processing	 Custom Authentication Processing 	
* Access Denied URI Pro	cessing *	Profile Attributes Process	ang session	Attributes Processing		
Login Processing						
Login Form URI						
Current Values	/cuadmin/WE	EB-INF/pages/logon.jsp	Remove			
	/cuservice/W /ciscopca/W	/EB-INF/pages/logon.jsp EB-INF/pages/logon.jsp				
	/inbox/WEB-	INF/pages/logon.jsp				
			×]			
New Value		Add				
List of absolute U	RIs correspor	iding to an application's we	eb.xml form-login-pa	age element. (property name: com	.sun.identity.agents.config.login.form)	
Hot-swap: Yes		• · · · · · · · · · · · · · · · · · · ·			·,····,	
⊨xampie: /BankApp/jsp/logi	n.jsp					
Done						🔒 F110% .:

Under the Application tab, in the section titled "Not Enforced URI Processing" add the following URI:

🕑 OpenSSO - Mozilla Firefox 📃 🗌 🗙
🌏 🕞 C 🗶 💩 🔚 venjak.com https://vrajnx.vrajok.com:8443/opensso/agentconfig/GenericAgentProfile?GenericAgentProfile.tabCommon.TabHref= 😭 - 🛛 😽 – Google 🔊
openSSO *
Not Enforced URI Processing
Not Enforced URIs
Current Values //inbox/gadgets/msg/msg-gadget.xnl A Remove
New Value Add
List of URIs for which protection is not enforced by the Agent. (property name: com.sun.identity.agents.config.notenforced.un) Hot-swap: Yes Examples: /BankApp/public/* /BankApp/images/*
Invert Not Enabled
Enforced URIs: Inverts protection of URIs specified in Not Enforced URIs list. When set to true, it indicates that the URIs specified should be enforced and all other URIs should be not enforced by the Agent. (property name: com.sun.identity.agents.config.notenforced.uri.invert) Hot-swap: Yes
Not Enforced URIs 🔽 Enabled
Cache Enabled: Enables the caching of the Not Enforced URIs list evaluation results. (property name: com.sun.identity.agents.config.notenforced.uri.cache.enable) Hot-swap: Yes
Not Enforced URIs 1000
Cache Size: Size of the cache to be used if caching of not enforced URI list evaluation results is enabled. (property name: com.sun.identity.agents.config.notenforced.uri.cache.size) Hot-swap: Yes
Refresh Session Enabled
Idle Time: Indicates if opensso session idle time should be refreshed or reset for not enforced URIs. (property name: com.sun.identity.agents.config.notenforced.refresh.session.idletime) Hot-swap: Yes
Done

/inbox/gadgets/msg/msg-gadget.xml

Go to OpenSSO Services tab, Under Login URL add OpenSSO Login URL as https://<OpenSSO FQDN>:8443/opensso/UI/Login?module=<WindowsDesktopSSO_Module>

WindowsDesktopSSO_Module should be same as the one created in section 10.2

Ex: https://<OpenAM FQDN>:8443/opensso/UI/Login?module=CUCMUser

🥹 OpenSSO - Mozilla Firefox	×			
🌀 🗁 😋 🗶 🏠 🔚 vrajol.com https://vrajnx.vrajol.com:8443/opensso/agentconfig/GenericAgentProfile?GenericAgentProfile.tabCommon.TabHref= 🏠 🕘 🚷 - Google	P			
openSSO *	-			
VERSION LOG OUT HELP	^			
User: amAdmin Server: vrajinx.vrajoli.com				
OpenSSO Sara				
Su ^a " Micropitent, Inc				
Global Application SSO OpenSSO Services Miscellaneous Advanced				
	1			
Edit CUCSSO Save Reset Back to Main Page	I.			
Inheritance Settings Export Configuration				
Logia IIBL V Authoritaction Sociale V Loss Data Costa Service				
Logan DRL - Authenucation Service - Session Clark Service				
	c .			
Login URL				
OpenSSO Login URL				
Selected:				
ntips://vrajinz.vrajoii.com.o443/opensoi/or/Login/module=hannara				
Move Down				
Move to Top				
Move to Botton				
Delete				
Add				
OpenSSO login page URL. (property name: com.sun.identity.agents.config.login.url)				
Hot-swap: Yes				
Example. http://host.port/opensso/Ul/Login				
Login URL Schabled				
name: com.sun.identity.agents.config.login.url.prioritized)	~			
Done di F110	%			

11Undeploying/Removing OpenSSO Enterprise (OpenAM)

11.1 Uninstalling OpenSSO Enterprise (OpemAM) Server deployed on Linux Platform.

- Stop the tomcat running on OpenAM server, by executing shutdown.sh under /root/ apache-tomcat-7.0.0/bin directory.
- Remove the following directories and all of their contents:
 - ✓ ConfigurationDirectory is the directory created when the OpenSSO Enterprise instance is initially conf.igured using the Configurator. The default directory is **opensso** in the home directory of the user running the Configurator. If the Configurator is run by root, ConfigurationDirectory is created in the root home directory (/root).
 - ✓ user-home-directory.openssocfg where user-home-directory is the home directory of the user who deployed the opensso.war file. If this user is root, the directory is /.openssocfg.

Remove the opensso.war file from webapps directory of the tomcat.

Example: /root/ apache-tomcat-7.0.0/webapps

• Start the tomcat on OpenAM Server, by executing startup.sh under /root/ apachetomcat-7.0.0/bin directory

11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server deployed on Windows Platform.

- Stop the tomcat service if running on this OpenAM server. (Administrative Tools → Services → Apache Tomcat 7 → Stop)
- Delete the **opensso** and **.openssocfg** folder from the user home directory.
- Delete the **opensso.war** file from the webapps folder of tomcat. *Example:* c:*Program Files\Apache Software Foundation\Tomcat 7.0\webapps*
- Start the tomcat from Administrative Tools \rightarrow Services \rightarrow Apache Tomcat 7 \rightarrow Start

12 Configuring Browser's for SSO

Standard browser clients like Internet Explorer, Fire Fox and Safari have the capability to handle HTTP 401: Negotiate. The steps to enable this capability for Internet Explorer 6/7/8 and Mozilla Firefox is explained below:

12.1 Internet Explorer

Steps to setup Internet Explorer for SSO -

- Supported version 6.X onwards.
- In the Tool menu, go to Internet Options > Advanced > Security.

Select the check box for Integrated Windows Authentication option

- Go to Tools \rightarrow Internet Options \rightarrow Security > Local Intranet.
 - ✓ Select Custom Level. In the User Authentication/Logon panel/option, select the Automatic Logon Only in Intranet Zone option.
 - ✓ Go to Sites and select all of the options.
 - ✓ Click Advanced and add the OpenSSO Enterprise to the local zone (if it is not added already).
- Additionally for IE7 and IE8 browsers, go to Tools> Internet Options> Security tab> Uncheck the "Enable Protected Mode" check box. (requires restarting Internet Explorer)
- For windows machines(Windows7/Windows 2008 and other higher versions) with extended Protection for Authentication enabled, disable extended Protection for Authentication by creating registry entry Under registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\, Add DWORD value SuppressExtendedProtection 0x02

12.2 Mozilla Firefox

Steps to setup FireFox for SSO –

- Supported version 3.x onwards.
- Open Firefox browser.
- At the address field, type about:config.
- In the Filter, type network.n

• Double click on network.negotiate-auth.trusted-uris. This preference lists the sites that are permitted to engage in SPNEGO Authentication with the browser. Enter a commadelimited list of trusted domains or URLs. Example:vrajoli.com

12.3 SSO Configurations test with browser

- Logon to domain computer which is member of domain controller *(Example: vrajoli.com)*
- Configure the browser capable for SSO, described in section 12.1 and 12.2
- Browse for <u>https://<OpenAM</u> FQDN>:8443/opensso/UI/Login?module= <WindowsDesktopSSO_Module>, WindowsDesktopSSO_Module should be same as configured in section 10.2.

In this test, it will be: <u>https://vrajlnx.vrajoli.com:8443/opensso/UI/Login?module=CUCMUser</u>

• You should see **You're logged in** message as shown in below screen shot, which tells all the above configurations are correct.



13 Configuring SSO on Cisco Unified Communications Manager 8.5

Before enabling SSO on CUCM 8.5, below configurations has to be done on CUCM.

- Logon to Cisco Unified Serviceability and activate Cisco DirSync service.
- Logon to Cisco Unified CM Administration, go to System → LDAP → LDAP System, check the 'Enable Synchronizing from LDAP Server' checkbox and save. Go to System → LDAP →LDAP Directory, create a new directory agreement with configuring LDAP Directory information and LDAP server information, save the configuration and click on 'Perform Full Sync' button.
- Upon completion of directory sync, AD users are imported to CUCM.
- On Cisco Unified CM Administration page, go to User Management → End User, verify all the AD users are available and LDAP Sync Status is Active.

• Associate respective User Group to the end users and save.

Since we configure CUCM to talk to OpenAM over https while enabling SSO, we need to import OpenAM server certificate into Call Manager tomcat-trust store before enabling the SSO on CUCM.

To get the OpenAM server certificate, Login to OpenAM URL (https://<OpenAM FQDN>:8443/opensso), click on the security icon at the bottom right corner. Click on the Details tab of Certificate Viewer window, click on export button and save it your desktop.



After getting OpenAM server certificate, Logon to CUCM OS Administration page, go to Security → Certificate Management, Click Upload Certificate button

In the Upload Certificate window, Select certificate name as 'tomcat-trust' and browse for the saved OpenAM certificate and upload it.

Now we have OpenAM server certificate added into CUCM Tomcat-trust store.

13.1 CUCM 8.5 SSO CLI Commands:

There are three CLI command available for managing SSO on CUCM 8.5, they are.

- utils sso enable
- utils sso disable
- utils sso status

13.1.1 utils sso enable

Enables SSO based authentication

This command will start the wizard for enabling SSO on the CUCM. It will ask for

- 1) OpenAM server URL
- 2) Relative path for policy agent deployment
- 3) Profile name configured for this policy agent on the AM server
- 4) Password for the above
- 5) Module name configured for Windows Desktop SSO

admin:utils sso enable ***** W A R N I N G ***** This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): yes
Enter URL of the Open Access Manager (OpenAM) server: https://vrajlnx.vrajoli.com:8443/opensso
Enter the relative path where the policy agent should be deployed: agentapp
Enter the name of the profile configured for this policy agent: CUCMUser
Enter the password of the profile name: ********
Enter the login module instance name configured for Windows Desktop SSO: CUCMUser
Validating connectivity and profile with Open Access Manager (OpenAM) Server: https://vrajlnx.vrajoli.com:8443/opensso
Valid profile Enabling SSO This will take upto 5 minutes
SSO Enable Success
Please make sure to execute this command on all the nodes in the cluster. admin:

13.1.2 utils sso disable

Disables SSO based authentication, no parameters required.

admin:utils sso disable ***** W A R N I N G ***** This command will restart Tomcat for successful completion. This command needs to be executed on all the nodes in the cluster. Do you want to continue (yes/no): yes Disabling SSO configuration. This will take upto 5 minutes Disable SSO Success Please make sure to execute this command on all the nodes in the cluster.

13.1.3 utils sso status

Provides the status of SSO on this CUCM 8.5, no parameters required.

• When SSO is Disabled:

admin:utils sso status SSO Status: Disabled

• When SSO is Enabled:



14 Configuring SSO on Cisco Unified Communications Manager 8.6

With CUCM 8.6, SSO is extended to below CUCM Applications along with CCMUser and CUCiMOC.

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified OS Administration
- Disaster Recovery System
- RTMT

Before enabling SSO on CUCM 8.6, below configurations has to be done on CUCM.

- Logon to Cisco Unified Serviceability and activate Cisco DirSync service.
- Logon to Cisco Unified CM Administration, go to System 🛛 LDAP 🖓 LDAP System, check the 'Enable Synchronizing from LDAP Server' checkbox and save. Go to System 🖾 LDAP 🖾 LDAP Directory, create a new directory agreement with configuring LDAP Directory information and LDAP server information, save the configuration and click on 'Perform Full Sync' button.
- Upon completion of directory sync, AD users are imported to CUCM.
- On Cisco Unified CM Administration page, go to User Management 2 End User, verify all the AD users are available and LDAP Sync Status is Active.
- Associate respective User Group to the end users and save. For an end user to access the SSO enabled applications like Cisco Unified CM Administration, Cisco Unified Serviceability, Cisco Unified Reporting, Cisco Unified OS Administration and RTMT, end user should have '**Standard Audit Users'**, '**Standard CCM Super Users'** User Groups associated.

Since we configure CUCM to talk to OpenAM over https while enabling SSO, we need to import OpenAM server certificate into Call Manager tomcat-trust store before enabling the SSO on CUCM.

14.1 CUCM 8.6 SSO CLI Commands:

14.1.1 utils sso enable

This command will enable SSO for below options selectively.

Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)

Cisco Unified CM User Options (CUCM End User options)

Cisco Unified Operating System Administration (CUCM OS Admin, DRF)

Cisco Unified Data Service (CUCiMOC)

RTMT

This command will start the wizard for enabling SSO on the CUCM. It will ask for

- 1) OpenAM server URL
- 2) Relative path for policy agent deployment
- 3) Profile name configured for this policy agent on the AM server
- 4) Password for the above
- 5) Module name configured for Windows Desktop SSO

admin:utils sso enable
This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): y
List of apps for which SSO can be enabled
1) Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)
2) Cisco Unified CM User Options (CUCM End User options)
3) Cisco Unified Operating System Administration (CUCM OS Admin, DRF)
4) Cisco Unified Data Service (CUCiMOC)
5) RTMT
Do you want to enable SSO for Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) (yes/no):y
Do you want to enable SSO for Cisco Unified CM User Options (CUCM End User options) (yes/no):y
Do you want to enable SSO for Cisco Unified Operating System Administration (CUCM OS Admin, DRF) (yes/no):y
Do you want to enable SSO for Cisco Unified Data Service (CUCiMOC) (yes/no):y
Do you want to enable SSO for RTMT (yes/no):y
Enter URL of the Open Access Manager (OpenAM) server: https://vrajlnx.vrajoli.com:8443/opensso
Enter the relative path where the policy agent should be deployed: agentapp
Enter the name of the profile configured for this policy agent: cucmsso238
Enter the password of the profile name: ********
Enter the login module instance name configured for Windows Desktop SSO: Harihara
Validating connectivity and profile with Open Access Manager (OpenAM) Server: https://vrajlnx.vrajoli.com:8443/opensso
Valid profile
Valid module name
Enabling SSO This will take upto 5 minutes
SSO Enable Success
Please make sure to execute this command on all the nodes in the cluster. admin:

14.1.2 utils sso disable

Disables SSO for SSO enabled options.

admin:utils sso disable
***** \Im A R N I N G ***** This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): y
List of apps for which SSO can be disabled
1) Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)
2) Cisco Unified CM User Options (CUCM End User options)
3) Cisco Unified Operating System Administration (CUCM OS Admin, DRF)
4) Cisco Unified Data Service (CUCiMOC)
5) RTMT
Do you want to disable SSO for Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) (yes/no):y
Do you want to disable SSO for Cisco Unified CM User Options (CUCM End User options) (yes/no):y
Do you want to disable SSO for Cisco Unified Operating System Administration (CUCM OS Admin, DRF) (yes/no):y
Do you want to disable SSO for Cisco Unified Data Service (CUCiMOC) (yes/no):y
Do you want to disable SSO for RTMT (yes/no):y
Disabling SSO configuration. This will take upto 5 minutes
Disable SSO Success
Please make sure to execute this command on all the nodes in the cluster. admin:

14.1.3 utils sso status

Displays the list of SSO enabled applications.

admin:utils sso status SSO Status: Disabled

14.2 CUCM 8.6 SSO GUI

From CUCM 8.6 release, SSO configurations (SSO enable/disable/status) are supported from GUI as well.

To configure SSO from GUI, Logon to Cisco Unified OS Administration, Go to Security \rightarrow Single Sign on and you will see below configuration page.

cisco	Cisco Unified Operating System Administration For Cisco Unified Communications Solutions				
Show - S	ettings - Security - Software Upgrades - Services - Help -				
SSO Applications Configuration					
Save					
-Status					
A Warning:Changing the SSO settings causes an immediate Tomcat restart					
Server Settings:					
Enter URI	of the Open Access Manager(OpenAM) server*				
Enter the relative path where the policy agent should be deployed*					
Enter the name of the profile configured for this policy agent*					
Enter the password of the profile name*					
Enter the login module instance name configured for Windows Desktop SSO*					
⊂					
Select	All Application name	SSO Status			
	Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)	Disabled			
	Cisco Unified CM User Options (CUCM End User options)	Disabled			
	Cisco Unified Operating System Administration (CUCM OS Admin, DRF)	Disabled			
	Cisco Unified Data Service (CUCiMOC)	Disabled			
	RTMT	Disabled			

- Save

(i) *- indicates required item.

For enabling SSO from GUI, the same parameters were requested as requested from CLI. All the inputs will be validated before enabling SSO to selected application. Check box is provided for selecting the application(s), set the check-box to select the application for enabling SSO and click on save button. After successful validation of all the inputs, a pop-up window is displayed saying *'Enabling/Disabling SSO for the applications will cause Tomcat to restart. Do you want to continue?'* press OK button if you want to proceed else click Cancel button to cancel.

Below is the snapshot when SSO is enabled for all applications.
Cisco Unified Operating System Administration For Cisco Unified Communications Solutions							
Show - Settings - Set	curity ▼ Software Upgrades ▼ Services ▼ Help ▼						
SSO Applications Conf	iguration						
Save							
- Status Warning:Changing t	he SSO settings causes an immediate Tomcat restar	t					
- Server Settings:	M		1				
Enter ORL of the Open Access Manager(OpenAM) server* https://vrajinx.vrajoli.com:8443/opensso							
Enter the relative path where the policy agent should be deployed* agentapp							
Enter the name of the profile configured for this policy agent* cucmsso239							
Enter the password of th	e profile name*						
Enter the login module in	stance name configured for Windows Desktop SSO*	Harihara					
– Select Applications –							
Select All	Application name			SSO Status			
	Cisco Unified CM Administration (CUCM Admin, CU	Serviceability, CU Reporting)		Enabled			
	Cisco Unified CM User Options (CUCM End User op	tions)		Enabled			
	Cisco Unified Operating System Administration (CUCM OS Admin, DRF)						
	Cisco Unified Data Service (CUCiMOC)			Enabled			
	RTMT			Enabled			
Save							

(i) *- indicates required item.

To disable SSO enabled application(s), uncheck the check box of the SSO enabled application(s), then click on save button. pop-up window is displayed saying 'Enabling/Disabling SSO for the applications will cause Tomcat to restart. Do you want to continue?' press OK button if you want to proceed else click Cancel button to cancel.

15 Configuring SSO on Cisco Unity Connection 8.6

Before enabling SSO on CUCM 8.6, below configurations has to be done on Cisco Unity Connection.

- Import users to Unity Connection either directly from LDAP server **OR** from CUCM, however users imported from CUCM must first be imported from LDAP to CUCM). Users must be configured with the appropriate roles to log in to Cisco Unity Connection Administration, or Cisco Unity Connection Serviceability.
- For co-res and stand-alone Connection server, users accounts that will access Cisco Unity Connection Administration and Cisco Unity Connection Serviceability, must have the "System Administrator" role. To give a user the "System Administrator" role, select the user in Cisco Unity Connection Administration, choose Edit/Roles from the menu, then select "System Administrator" from the available roles, and add it to the user's Assigned Roles
- Since we configure CUCM to talk to OpenAM over https while enabling SSO, we need to import OpenAM server certificate into Call Manager tomcat-trust store before enabling the SSO on Unity Connection.

15.1 CUC 8.6 SSO CLI Commands

There are three CLI command available for managing SSO on CUCM 8.5, they are.

• utils sso enable

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

- utils sso disable
- utils sso status

15.1.1 utils sso enable

Enables SSO based authentication. Connection offers following options for enabling SSO:

- Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)
- Cisco Unified CM User Options (CUCM End User options)
- Cisco Unified Operating System Administration (CUCM OS Admin, DRF)
- Cisco Unity Connection PCA and Web Inbox
- Cisco Unity Connection Administration
- Cisco Unified Data Service (CUCiMOC)
- RTMT

This command will start the wizard for enabling SSO on the CUCM. It will ask for

- 1) OpenAM server URL
- 2) Relative path for policy agent deployment
- 3) Profile name configured for this policy agent on the AM server
- 4) Password for the above
- 5) Module name configured for Windows Desktop SSO

admin:utils sso enable
This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): yes
List of apps for which SSO can be enabled
1) Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)
2) Cisco Unified CM User Options (CUCM End User options)
3) Cisco Unified Operating System Administration (CUCM OS Admin, DRF)
4) Cisco Unity Connection PCA and Web Inbox
5) Cisco Unity Connection Administration
6) Cisco Unified Data Service (CUCiMOC)
7) RTHT
Do you want to enable SSO for Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) (yes/no):yes
Do you want to enable SSO for Cisco Unified CM User Options (CUCM End User options) (yes/no):yes
Do you want to enable SSO for Cisco Unified Operating System Administration (CUCM OS Admin, DRF) (yes/no):yes
Do you want to enable SSO for Cisco Unity Connection PCA and Web Inbox (yes/no):yes
Do you want to enable SSO for Cisco Unity Connection Administration (yes/no):yes
Do you want to enable SSO for Cisco Unified Data Service (CUCiMOC) (yes/no):yes
Do you want to enable SSO for RTMT (yes/no):yes
Enter URL of the Open Access Manager (OpenAM) server: https://vrajlnx.vrajoli.com:8443/opensso
Enter the relative path where the policy agent should be deployed: agentapp
Enter the name of the profile configured for this policy agent: ucsso
Enter the password of the profile name: *********

Enter the login module instance name configured for Windows Desktop SSO: Harihara

15.1.2 utils sso disable

Disables SSO based authentication, no parameters required.

```
admin:utils sso disable
This command will restart Tomcat for successful completion.
This command needs to be executed on all the nodes in the cluster.
Do you want to continue (yes/no): y
List of apps for which SSO can be disabled
)) Cisco Unified Operating System Administration (CUCM OS Admin, DRF)
4) Cisco Unity Connection PCA and Web Inbox
 Cisco Unity Connection Administration
7) RTMT
o you want to disable SSO for Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) (yes/no):y
o you want to disable SSO for Cisco Unified CM User Options (CUCM End User options) (yes/no):y
o you want to disable 330 for Cisco Unified Operating System Administration (CUCM OS Admin, DRF) (yes/no):y
o you want to disable SSO for Cisco Unity Connection PCA and Web Inbox (yes/no):y
 o you want to disable SSO for Cisco Unity Connection Administration (yes/no):y
 o you want to disable SSO for Cisco Unified Data Service (CUCiMOC) (yes/no):y
 you want to disable SSO for RTMT (yes/no):y
```

15.1.3 utils sso status

Provides the status of SSO on UC 8.6, no parameters required

admin:utils sso status SSO Status: Disabled

15.2 Cisco Unity Connection 8.6 SSO GUI

To configure SSO from GUI, Logon to Cisco Unified OS Administration, Go to Security \rightarrow Single Sign on and you will see below configuration page.

cisco For t	co Unified Operating System Administration Cisco Unified Communications Solutions					
Show - Setting	gs ▼ Security ▼ Software Upgrades ▼ Services ▼ Help ▼					
SSO Applicat	ions Configuration					
Save						
Ctatua						
Warning:	hanging the SSO settings causes an immediate Tomcat restart					
Server Setti	ngs:					
Enter URL of	he Open Access Manager(OpenAM) server*					
Enter the relative path where the policy agent should be deployed*						
Enter the nan	ne of the profile configured for this policy agent*					
Enter the pas	sword of the profile name*					
Enter the logi	n module instance name configured for Windows Desktop SSO* Universal_SSO					
Select Appli	cations					
Select All	Application name	SSO Status				
	Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)	Disabled				
	Cisco Unified CM User Options (CUCM End User options)	Disabled				
	Cisco Unified Operating System Administration (CUCM OS Admin, DRF)	Disabled				
	Cisco Unity Connection PCA and Web Inbox	Disabled				
	Cisco Unity Connection Administration	Disabled				
	Cisco Unified Data Service (CUCiMOC)	Disabled				
	PTMT	Disabled				

For enabling SSO from GUI, the same parameters were requested as requested from CLI. All the inputs will be validated before enabling SSO to selected application. Check box is provided for selecting the application(s), set the check-box to select the application for enabling SSO and click on save button. After successful validation of all the inputs, a pop-up window is displayed saying 'Enabling/Disabling SSO for the applications will cause Tomcat to restart. Do you want to continue?' press OK button if you want to proceed else click Cancel button to cancel.

Below is the snapshot when SSO is enabled for all applications.

cisco	Cisco Unified Operating System Admini For Cisco Unified Communications Solutions	stration				
Show -	Settings - Security - Software Upgrades - Services - Help -					
SSO Ap	plications Configuration					
Save						
Status						
🔔 War	ning:Changing the SSO settings causes an immediate Tomcat resta	rt				
Server	Settings:					
Enter U	Enter URL of the Open Access Manager(OpenAM) server* https://vrajlnx.vrajoli.com:8443/opensso					
Enter th	e relative path where the policy agent should be deployed*	agentapp	entapp			
Enter the name of the profile configured for this policy agent*						
Enter th	e password of the profile name*					
Enter th	e login module instance name configured for Windows Deskton SS	X Haribara				
2						
Select	Applications					
Sele	t All Application name		SSO Status			
	Cisco Unified CM Administration (CUCM Admin, CU Servic	eability, CU Reporting)	Enabled			
	Cisco Unified CM User Options (CUCM End User options)		Enabled			
	Cisco Unified Operating System Administration (CUCM OS	Admin, DRF)	Enabled			
	Cisco Unity Connection PCA and Web Inbox		Enabled			
	Cisco Unity Connection Administration		Enabled			
	Cisco Unified Data Service (CUCiMOC)		Enabled			
	RTMT		Enabled			
Save]					

(i) *- indicates required item.

16 OpenSSO Enterprise Session Failover

NOTE: Refer this chapter if you wish to configure the session failover

Session failover ensures that session data remains accessible to OpenSSO Enterprise servers and OpenSSO Enterprise Policy Agents. Service requests are routed to a failover server, the user's session continues uninterrupted, and no user data is lost. The OpenSSO Enterprise Session Service maintains authenticated session states and continues processing new client requests subsequent to the failure. In most cases, without session failover, after system failure and subsequent service recovery, the user would have to re-authenticate.

Session failover is critical when end-users' transactions involve financial data or other sensitive information that is difficult to recover when a system failure occurs. With session failover, when a system failover occurs, the user's transaction can proceed uninterrupted. Session failover is less important if end-users are, for example, reading but not writing data.

When you configure OpenSSO Enterprise for session failover, the user's authenticated session state is stored in the Berkeley Database in the event of a single hardware or software failure. In session failover deployments, you configure the OpenSSO Enterprise servers to communicate with Message Queue brokers which manage session state persistence in the Berkeley Database. This configuration enables the users session to fail over to a backup OpenSSO Enterprise server without losing any session state information. The user does not have to login again. The backup OpenSSO Enterprise server is determined among the available servers in the configuration list by an internal algorithm.

This type of deployment ensures the state availability even if one of the OpenSSO Enterprise servers is inaccessible due to scheduled maintenance, hardware failure, or software failure. However, the single load balancer can be a single point of failure. When this load balancer is inaccessible, no OpenSSO Enterprise

16.1 Requirements for AMSFO

Key components that are required for basic session failover in an OpenSSO Enterprise deployment for high availability are:

- A single load balancer distributes the workload among multiple OpenSSO Enterprise This increases transaction throughput, and ensures failover when a system failure occurs.
- Multiple OpenSSO Enterprise servers with respective embedded Directory Servers act as backups when system failure occurs. Embedded Directory Servers ensure that replicated configuration data is always available even during system failure.
- When OpenSSO Enterprise is configured for session failover, a Java Message Queue Broker Cluster replicates session data and stores it in the Berkeley Database. When a system failure occurs, the replicated session data is made available to Policy Agents so that the end-user does not lose data and does not have to re-authenticate after system recovery.
- Multiple Berkeley Databases are used to store session data, and are configured for session failover. If one Berkeley Database fails, the working Berkeley Database can provide session data to the OpenSSO Enterprise servers for session validation.

In all examples in this chapter, load balancers represent the only access points to OpenSSO Enterprise servers. An access point can be any hardware or software that acts as a load balancer, and is associated with a site, that is installed in front of OpenSSO Enterprise servers. Policy Agents interact with OpenSSO Enterprise servers through these access points.

16.2 Configuration of AMSFO components

16.2.1 Installation and configuration of Load Balancer

16.2.1.1 Installation of Load Balancer on Linux Platform.

To configure load balancer on Linux platform, install the Red Hat Enterprise Linux 5.5 (lower version of RHEL can also be used). Once RHEL is installed, configure network settings and create an entry in DNS servers for this RHEL host. Once everything is configured on this RHEL server, we will install Sun Java System Web Server application for load balancing.

In this guide we will be configuring Sun Java System Web Server as the load balancer; you can get the Sun Java System Web Server setup file from <u>https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_SMI-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=SJWS-7-TechPrvw-OTH-G-Beta@CDS-CDS_SMI_URL.</u>

On the above download page, select the platform as Linux and download the installation file.

Copy the installation file to the above RHEL server at any location and run the setup.

[root@ssoloadbal Sun Java System Web Server]# ./setup

Welcome to the Oracle iPlanet Web Server 7.0.9 installation wizard.

Copyright (c) 2007, 2010, Oracle and/or its affiliates. All rights reserved. Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

You will be asked to specify preferences that determine how Oracle iPlanet Web Server 7.0.9 is installed and configured.

The installation program pauses as questions are presented so you can read the information and make your choice. When you are ready to continue, press Enter (Return on some keyboards).

<Press ENTER to Continue>

Some questions require that you provide more detailed information. Some questions also display default values in brackets []. For example, yes is the default answer to the following question:

Are you sure? [yes]

To accept the default, press Enter.

To provide a different answer, type the information at the command prompt and then press Enter.

<Press ENTER to Continue>

Oracle iPlanet Web Server components will be installed in the directory listed below, referred to as the installation directory. To use the specified

directory, press Enter. To use a different directory, enter the full path of the directory and press Enter.

Oracle iPlanet Web Server Installation Directory [/opt/oracle/webserver7] {"<" goes back, "!" exits}:

Specified directory /opt/oracle/webserver7 does not exist

Create Directory? [Yes/No] [yes] {"<" goes back, "!" exits} yes

Select the Type of Installation

- 1. Express
- 2. Custom
- 3. Exit

What would you like to do [1] {"<" goes back, "!" exits}?1

Choose a user name and password. You must remember this user name and password to administer the Web Server after installation.

Administrator User Name [admin] {"<" goes back, "!" exits} Administrator Password: Retype Password:

Product : Oracle iPlanet Web Server Location : /opt/oracle/webserver7 Disk Space : 231.37 MB

Administration Command Line Interface

Copyright © 2010 Cisco Systems, Inc. All rights reserved.

Server Core

Start Administration Server [yes/no] [yes] {"<" goes back, "!" exits}: yes

Ready to Install

- 1. Install Now
- 2. Start Over
- 3. Exit Installation

What would you like to do [1] {"<" goes back, "!" exits}?1

Installing Oracle iPlanet Web Server |-1%-----75%-----100%| Installation Successful.

Refer to the installation log file at: /opt/oracle/webserver7/setup/install.log for more details.

Next Steps:

- You can access the Administration Console by accessing the following URL:

https://ssoloadbal.vrajoli.com:8989

[root@ssoloadbal Sun Java System Web Server]#

16.2.1.2 Installation of Load Balancer on Windows platform.

To configure load balancer on windows platform, install Windows XP SP2/Windows server 2003. Once windows OS is installed, configure network settings and create an entry in DNS servers for this host. Once everything is configured on this windows machine, we will install Sun Java System Web Server application for load balancing.

In this guide we will be configuring Sun Java System Web Server as the load balancer; you can get the Sun Java System Web Server setup file from <u>https://cds.sun.com/is-bin/INTERSHOP.enfinity/WFS/CDS-CDS_SMI-Site/en_US/-/USD/ViewProductDetail-Start?ProductRef=SJWS-7-TechPrvw-OTH-G-Beta@CDS-CDS_SMI_URL.</u>

On the above download page, select the platform as windows xp/windows server 2003 and download the installation file.

Copy the installation file to the above windows server at any location and run the setup.

Below is the example of setup done in this guide

C:\Documents and Settings\Administrator\Desktop\sjsws-7_0u1-windows-i586>dir

Volume in drive C has no label.

Volume Serial Number is 1C23-BFE7

Directory of C:\Documents and Settings\Administrator\Desktop\sjsws-7_0u1-windowsi586

.

09/25/2010 10:35 PM <DIR>

09/25/2010 10:35 PM <DIR> ..

09/25/2010 10:35 PM <DIR> Legal

09/25/2010 01:20 PM 751 README.txt

09/25/2010 01:22 PM 20,603 setup.exe

09/25/2010 10:34 PM <DIR> WebServer

2 File(s) 21,354 bytes

4 Dir(s) 8,806,412,288 bytes free

C:\Documents and Settings\Administrator\Desktop\sjsws-7_0u1-windowsi586>setup.exe

🕵 Sun Java System Web Server 7.0U1 Install Wizard

🥵 Sun Java System V	Veb Server 7.0U1 Install Wizard	
Java™ Bava™ Enterprise System	Welcome to the Sun Java System Web Server 7.0U1 installation wiz used to install the Web Server.	ard. This wizard is
	& Back Next >	Cancel Help
🥵 Sun Java System V	Veb Server 7.0U1 Install Wizard	
<u>چ</u>	Software License Agreement	
Java	Sun Microsystems, Inc. ("Sun") SOFTWARE LICENSE AGREEMENT ENTITLEMENT for SOFTWARE	("SLA") and
Java™ Enterprise System	A. ENTITLEMENT for SOFTWARE. Capitalized terms not defined in th Entitlement have the meanings ascribed to them in the SLA (attache below as Section B). These terms will supersede any inconsistent o conflicting terms in the SLA.	iis d m
CCA.	Licensee ("You"): The entity receiving the Software from Sun.	
555	Effective Date: Date You receive the Software.	-
227	Do you agree with the terms of this license?	1 annord
	• Yes	
@Sun	© No	
	≪ Back Next ≫	Cancel Help

<u></u>	Select Installation Directory	
lava	Installation Directory:	
	C:\Program Files\Sun\WebServer7	Brows
Java ³³⁴		
System		
System		

Cancel

Help

<u></u>	Select the Type of Installation	
Java™ Enterprise System	 Select the type of installation you want to perform, then click Next. Express The easiest installation, with standard options installed automatically. Custom Custom installation based on user choices. 	

Sun

≪ Back

Next >

🙋 Sun Java System Web Server 7.0U1 Install Wizard

Java™ Java™ Enterprise System	Administration Server Setti Choose a user name and pa password to administer the v Administrator User Name Administrator Password Retype Password	ngs assword. You must remember this user Web Server after installation. admin ********	name and	
	Back Next 📎		Cancel	Help
🐣 Sun Java System V	Veb Server 7.0U1 Install V	Vizard		_ 🗆 🛛
*	Ready to Install			
Java	Product : Sun Java System	Web Server		
Java™	Location : C:\Program File	s\SunWebServer7		
Enterprise System	Disk Space : 239.79 MB			
	Administration Command	Line Interface		
	Server Core			
122	Sample Applications			
	Language Pack for Server	Core		
sun	Language Pack for Admini	stration Command Line Interface		
	& Back Install No	w >	Cancel	Help

🕵 Sun Java System Web Server 7.0U1 Install Wizard



Services											
File Action View	Help										
🏶 Services (Local)	🍇 Services (Local)	Services (Local)									
	Sun Java System Web Server 7.0	Name A	Description Status	Startup Type	Log On As						
	Administration Server	🆓 OfficeScan NT Listener	Receives c Started	Automatic	Local System						
	Start the cervice	Service OfficeScan NT Proxy Service	Scans net	Manual	Local System						
		Contraction Contractico Contra	Performs R Started	Automatic	Local System						
		Performance Logs and Alerts	Collects pe	Manual	Network S						
		No. 10 Plug and Play	Enables a c Started	Automatic	Local System						
		Portable Media Serial Number Service	Retrieves t	Manual	Local System						
		Print Spooler	Loads files Started	Automatic	Local System						
		Protected Storage	Provides pr Started	Automatic	Local System						
		QoS RSVP	Provides n	Manual	Local System						
		Remote Access Auto Connection Manager	Creates a	Manual	Local System						
		Remote Access Connection Manager	Creates a Started	Manual	Local System						
		Remote Desktop Help Session Manager	Manages a	Manual	Local System						
		Remote Packet Capture Protocol v.0 (experimental)	Allows to c	Manual	Local System						
		Remote Procedure Call (RPC)	Provides th Started	Automatic	Network S						
		Remote Procedure Call (RPC) Locator	Manages t	Manual	Network S						
		Remote Registry	Enables re Started	Automatic	Local Service						
		Removable Storage		Manual	Local System						
		Routing and Remote Access	Offers rout	Disabled	Local System						
		SafeNet Log Service	Allows logg Started	Automatic	Local System						
		M SafeNet Token Service	Token serv Started	Automatic	Local System						
		Mg SafeNet Virtual Channel Monitor	Required f Started	Automatic	Local System						
		Secondary Logon	Enables st Started	Automatic	Local System						
		Security Accounts Manager	Stores sec Started	Automatic	Local System						
		and Security Center	Monitors s	Automatic	Local System						
		and Server	Supports n Started	Automatic	Local System						
		n Shell Hardware Detection	Provides n Started	Automatic	Local System						
		ng Smart Card	Manages a Started	Automatic	Local Service						
		Sular Winds Tr TP Server	Soldr Willius	Manual	Local System						
		Soundmax Agent Service	Starteu Fachles dia - Started	Manual	Local System						
		Sup Java Suctam Web Server 7.0 (https://www.ioli.labyp.urajoli.com)	Enables uis Starteu	Manual	Local Sustem						
		Sup Java System Web Server 7.0 (https://ajoinabxp.vrajoin.com/		Manual	Local System						
		Suctor Event Notification	Tra Start	Automatic	Local System						
		System Restore Service	Per Stop	Automatic	Local System						
		Task Scheduler	Pause	Automatic	Local System						
			Resume	Automatic	Local Service						
		Telephony	Pro	Manual	Local System						
		Telnet	ED: All Tasks	Disabled	Local System						
		Terminal Services	Allo	Manual	Local System						
		Themes	Pro Refresh	Automatic	Local System						
		Uninterruptible Power Supply	Ma Properties	Manual	Local Service						
		Universal Plug and Play Device Host	Pro	Manual	Local Service						
		WNC Server Version 4	Help	Automatic	Local System						
		Volume Shadow Copy	Manages a	Manual	Local System						
		WebClient	Enables Wi Started	Automatic	Local Service						



16.2.1.3 Configuration of Load Balancer for HTTP load balancing

Browse the Load Balancer URL, <u>https://ssoloadbal.vrajoli.com:8989</u>, you will be presented with below login page, Login to the admin console.



After login, you will see below page,

VERSION VERSION VERSION VERSION VERSION VERSION VERSION VERSION Variable Value Version V		?token=83078020-6029-41c9- ☆ 🔹 🛃 - Google	/serverTasksGenera	com:8989/admingui/admingu	soloadbal.vrajoli	vrajol.com https://s	🗩 C X 🏠
er: admin Server: ssoloadbal.vrajoli.com acter IPlanet Web Server Sommon Tasks To access information about a task, select the "I" info button. To understand the terminology, click here. Configuration Tasks Select Configuration is ecoloadbal vraiali.com Edit Configuration is ecoloadbal vraiali.com Edit Configuration Edit Configuration Start/Stop Instances Edit Java Settings Log Preferences and Archival Log Preferences and Archival Log Preferences and Archival Request Server Certificate View Summary New Configuration New Configuration View Summary New Configuration View Configuration View Configuration View Configuration View Configuration View Configuration View Configuration View Summary New Configuration View Summary View Summary New Configuration View Configuration View Configuration View Configuration View Configuration View Summary New Configuration View Summary New Configuration View Summary New Configuration View Summary New Configuration New Virtual Server New	OUT HELP	HOME REFRESH LOG					ERSION
Common Tasks Configurations Nodes Server Certificates Monitoring Common Tasks To access information about a task, select the "" info button. To understand the terminology, click here. Information about a task, select the "" info button. To understand the terminology, click here. Configuration Tasks Virtual Server Tasks Select Configuration Image: Configuration Configuration Reduct Configuration Image: Configuration Select Configuration Image: Configuration Select Configuration Image: Configuration New Instances Image: Configuration Configuration Image: Configuration New Configuration Image: Configuration <t< th=""><th>(iits)</th><th></th><th></th><th></th><th>m</th><th>ssoloadbal.vrajoli.co b Server</th><th>er: admin Server: acle iPlanet We</th></t<>	(iits)				m	ssoloadbal.vrajoli.co b Server	er: admin Server: acle iPlanet We
Common Tasks Configurations Nodes Server Certificates Monitoring Common Tasks To access information about a task, select the "I" info button. To understand the terminology, click here. Virtual Server Tasks Configuration Tasks Select Configuration is esploadibal virainit com Virtual Server Tasks Select Configuration Image: Select Server Casks Select Virtual Server Edit Configuration Image: Server Casks Select Virtual Server Edit Java Settings Image: Server Cask Select Virtual Server Add Web Application Log Preferences and Archival Image: Server Cask Select Server Cask Select Virtual Server CGi Directories URL Redirects Setup Reverse Proxy View Summary View Summary New Configuration Image: Image	Java						
Common Tasks To access information about a task, select the "I" info button. To understand the terminology, click here. Configuration Tasks Select Configuration: Select Configuration: Select Configuration: Select Configuration: Select Configuration: Select Virtual Server: Add Web Application Document Directories CG Directories URL Redirects Setup Reverse Proxy Install Server Certificate View Summary New Configuration Wigrate 6.0/6.1 Instances View Logs Documentation View Online Documentation Install Serves View Online Documentation			Monitoring	Server Certificates	Nodes	Configurations	ommon Tasks
Select Configuration: scaladdad vrainil com Edit Configuration i New Instance i Start/Stop Instances i Edit Java Settings i Log Preferences and Archival i Log Preferences and Archival i Install Server Certificate i View Summary i New Configuration i New Configuration i View Logs i Documentation i View Online Documentation i View Supplication i Product Registration i View Online Documentation i View Supplication i View Online Documentation i View Supplication i View Online Documentation i View Supplication i View Online Documentation i View Online Documentation i View Online Documentation i Stable News Updates i		gy, click here. I Server Tasks	nd the terminolo Virtua	info button. To understa	select the "i	rmation about a task, Tasks	To access info
Edit Configuration I New Instance I Start/Stop Instances I Edit Java Settings I Log Preferences and Archival I Request Server Certificate I Install Server Certificate I View Summary I New Configuration I Migrate 6.0/6.1 Instances I View Logs I Documentation I View Online Documentation I Product Registration Register with Sun Connection	v i	et Virtual Server: seoloadbal vraioli com	Sel	v (1)	l vraioli.com	iguration:	Select Confi
New Instance I Start/Stop Instances I Edit Java Settings I Log Preferences and Archival I Log Preferences and Archival I Request Server Certificate I Install Server Certificate I View Summary I New Configuration I Migrate 6.0/6.1 Instances I View Logs I Documentation I View Online Documentation I View Supdates Product Registration	i	Virtual Server	Edi	i		uration	Edit Configu
Start/Stop Instances I Edit Java Settings I Log Preferences and Archival I Request Server Certificate I Install Server Certificate I View Summary I New Configuration I Migrate 6.0/6.1 Instances I View Logs I Documentation I View Online Documentation I View Online Documentation I View Supdates I	i	Web Application	Add	1		:e	New Instand
Edit Java Settings I Log Preferences and Archival I Request Server Certificate I Install Server Certificate I View Summary I New Configuration I Migrate 6.0/6.1 Instances I View Logs I Documentation I View Online Documentation I View Online Documentation I View Supdates I	i	ument Directories	Doc	i		nstances	Start/Stop Ir
Log Preferences and Archival I Request Server Certificate I Install Server Certificate I View Summary I New Configuration I Migrate 6.0/6.1 Instances I View Logs I Documentation I View Online Documentation I View Supdates I	1	Directories	CG	1		ettings	Edit Java Se
Request Server Certificate I Install Server Certificate I View Summary I New Configuration I Migrate 6.0/6.1 Instances I View Logs I Documentation I View Online Documentation I View Supdates I	1	. Redirects	UR	1		nces and Archival	Log Prefere
Install Server Certificate Image: Certificate View Summary Image: Certificate New Configuration Image: Certificate Migrate 6.0/6.1 Instances Image: Certificate View Logs Image: Certificate Documentation Image: Certificate View Online Documentation Image: Certificate View Supdates Image: Certificate	i	up Reverse Proxy	Set	i		rver Certificate	Request Se
View Summary Image: Configuration New Configuration Image: Configuration Migrate 6.0/6.1 Instances Image: Configuration View Logs Image: Configuration Documentation Image: Configuration View Online Documentation Image: Configuration View Online Documentation Image: Configuration View Disable News Updates Image: Configuration	i	v Summary	Vie			er Certificate	Install Serve
New Configuration Image: New Virtual Server Migrate 6.0/6.1 Instances Image: New Virtual Server View Logs Image: New Virtual Server Documentation Image: New Virtual Server View Online Documentation Image: New Virtual Server View Online Documentation Image: New Virtual Server View Online Documentation Image: New Virtual Server View Disable News Updates Product Register with Sun Connection						ary	View Summ
Migrate 6.0/6.1 Instances Image: Constraint of the second secon	i	/ Virtual Server	Nev	1		uration	New Config
View Logs Image: Constraint of the second				(i)		6.1 Instances	Migrate 6.0/
Documentation Product Registration View Online Documentation Image: Connection Image: Disable News Updates Product Register with Sun Connection				(i)			View Logs
View Online Documentation Image: Connection Disable News Updates Image: Connection		ct Registration	Produ			on.	Documentatio
Disable News Updates		ister with Sun Connection	Rec	1		Documentation	View Online
		ister with Sun Connection	Reg			ws Updates	view Online
Announcing Open web Server, the open source project based on Sun Java System Web Server 7.0.	^	Veb Server 7.0.	in Java System	urce project based on Si	the open so	ng <u>Open Web Server</u>	Announcir

Click on Configurations tab, then click on the load balancer name (ssoloadbal.vrajoli.com) as shown below (Configurations \rightarrow Load Balancer Name)

🔮 Oracle iPlanet Wel	o Server Admin Cons	ole - Mozilla	Firefox				
🕢 🖓 🖓 😵	vrajol.com https://s	soloadbal.vrajol	.com:8989/admingui/admingu	i/configVirtualServers?	configVirtualServers.BreadCrumbLi	☆ - Soogle	P
🖸 1 Oracle iPlanet We	eb Serv *						
VERSION					HOI	ME REFRESH LOG	OUT HELP
User: admin Server:	ssoloadbal.vrajoli.co	m					<u>(*</u>)
Oracle iPlanet We	eb Server						Java
		-					
Common Tasks	Configurations	Nodes	Server Certificates	Monitoring			
						Migrato	View Logo
Configurations	o a set of metadata ti	nat configure	s the runtime services of	a Web Server Th	e configuration metadata is	used by the server runtin	me to load
built-in services, third	party plug-ins and se	etup other se	ver extensions such as	database drivers f	or serving web pages and dy	namic web applications	. Click on the
Migrate Configuration Web Server 6.0/6.1 in	n(s) button to migrate instance(s) to be migra	the Web Ser ated.	ver 6.0/6.1 instance(s) to	Web Server 7.0.	This action also causes all t	he deployed web applica	ations on the
Configurations (1)		_					
New Deploy	. Duplicate S	start Sto	p Restart Delete				
Configuratio	ons	_ Coi	figuration State		Instances	Instances State	
ssoloadbal.vr	ajoli.com	Dep	bloyed		1	1 Not Running	
https://ssoloadbal.vrajoli.co	m:8989/admingui/adming	jui∕serverConfigi	urationsGeneral?serverConfigu	rationsGeneral.genera	ConfigurationsTable.configHref=ss	oloadbal.vrajoli.com&toke	. 🔒 F110% 🦑

After clicking on the load balancer name, you will see below page,

🥹 Oracle iPlanet We	b Server Admin Cons	sole - Mozilla F	irefox						
🔇 🛛 • 😋 🗙 🏠	vrajol.com https://s	ssoloadbal.vrajoli.c	om:8989/admingui/a	admingui/vsGenera	?vsGeneral.BreadCrumbL	ink1=configVirtualSe	ដោ 🔹 🚮 - (Google	P
🖸 1 Oracle iPlanet W	/eb Serv *								
VERSION						НО	ME REFF	RESH LOG C	UT HELP
User: admin Server	: ssoloadbal.vrajoli.co	om					Instanc	e(s) Running 0	. (j)
Oracle Planet W	ed Server						Instanc	e(s) Stopped 🖪	1 Java"
Configurations > se	soloadbal.vrajoli.com								
Virtual Servers	HTTP Listeners	Instances	General F	erformance	Access Control	Certificates	Java	Summary]
ssoloadbal.vrajoli.d When you use virtua server. For the users create and edit virtua Virtual Servers (1	com - Configuration al servers you can offe s, it is almost as if they al servers defined for t	Virtual Serve er companies or / have their ow the selected co	rs r individuals dom n web servers, th nfiguration.	ain names, IP a nough you provi	ddresses, and some de the hardware and	server monitorir basic web serv	ng capabilitie er maintena	es with a single nce. This page	installed lets you
New Duplica	te Add Web Appl	lication De	elete						
I B Name		Lis	tener	△ Hosts		_ I	Document	Root	<u> </u>
ssoloadbal.v	rajoli.com	[*:8	443]	ssoloadb	al.vrajoli.com		./docs		
Done									🔒 F110% 🦑

Click on the Load Balancer Name (ssoloadbal.vrajoli.com) under Virtual Servers, you will see the below page.

🥹 Oracle iPlanet We	b Server Admin Co	nsole - Mozilla Firefo	x					
🔇 🛛 • C 🗙 🏠	🖸 vrajol.com https:	//ssoloadbal.vrajoli.com:89	89/admingui/admingui/co	onfigVirtualServers?	configVirtualServers.config	gVirtualSe 😭 🕘	Google	P
🖸 1 Oracle iPlanet W	eb Serv *							
VERSION						HOME REP	RESH LOG OUT	HELP
User: admin Server	: ssoloadbal.vrajoli.	com				Instar	ice(s) Running 0	k
Oracle iPlanet W	eb Server					Instar	ice(s) Stopped 🕡 1	E lava"
				_				java
Configurations > ss	oloadbal.vrajoli.con	n > Virtual Servers >	ssoloadbal.vrajoli.o	om				
Server Settings	Web Applicatio	ons Content Hand	lling WebDAV	Search	Access Control	Summary]	
General Log P	references Mon	itoring Settings Re	quest Limits					
ssoloadbal.vraioli.o	om - Virtual Serv	er General Propertie	s					Save
All virtual servers hav	ve one or more HTT	P Listeners specified	When a new reque	st comes in, the	Server determines v	vhich virtual se	erver to send it to ba	sed on the
configured HTTP Lis	tener. You can ass	ociate HTTP Listener	s from this page. Cor	nfigure virtual se	erver properties from	this page.		
 General 	 Quality of Serv 	vice * P3P Setting	S					
Sector Secto	 Localization 	⊭ Variables						
General								
Namo	seoloadbal vraioli	om						
Virtual Server:		tom						
Document Poot:								
bocument Root.	Document root for	the virtual server (Abs	olute nath or nath re	lative to the ser	ver's configuration di	irectory)		
Hosts'	scoloadbal vraioli		oluto putit of putitie		ver o contiguration a	needery)		
110515.	You can enter mor	e than one URL host	separated by comm	as				
Desiste text			copulated by comm					
* Back to top								
HTTP Listeners								
	(4)							_
HTTP Listeners						_		
Add Delete								
I B Name	*	IP Address	۵	Port	⇒ SSL	Desci	ription	~
http-listene	r-1	* [All IP Addresses]		8443	S Enabled			
Done								🔒 F110% 🏄

Click on HTTP Listeners, then click on http-listener-1 and set the port value to 8443 as shown below. Click on Apply button followed by Close button.

😻 Edit HTTP Listener	- General Settir	ngs - Mozilla Firefox	
🖸 vrajoli.com https://ssolo	adbal.vrajoli.com:89	989/admingui/admingui/vsGeneral?vsGeneral.	vsGeneralPropSheet 🏠
· · · ·			^
Edit HTTP Listener -	General Settin	gs	Apply Close
The Server accepts the request to the configure Listeners. HTTP Liste You can use either IPV Listener that listens or	e HTTP request red Virtual Serve ners must have a /4 or IPv6 addres n all IP addresse	s via an HTTP Listener before forwa r. This page allows you to add and co a unique combination of port number sses. Setting the IP address to "*" cre s on that port.	rding the onfigure HTTP and IP address. eates an HTTP
s General s Auva	inced	* Indicat	
General	http://stoper_1		
Name.			
* Port:	8443		
	Port on which t	o listen	
* IP Address:	*		
	IP address, or 3	to listen on all IP addresses	
* Server Name:	ssoloadbal.vra	joli.com	
	Default Server	Name	
* Default Virtual	ssoloadbal.vra	ioli.com 🗸	~
Done			🔒 F110% 🏘

Then Click in Content Handling tab under Configurations \rightarrow ssoloadbal.vrajoli.com \rightarrow Virtual Servers \rightarrow ssoloadbal.vrajoli.com.

Under Content handling tab, select Reverse Proxy tab.

🔮 Oracle i	Planet Wel	o Server Admin (Console	- Mozilla Firefox								_ 🗆 🗙
	C 🗙 🏠	🖸 vrajol.com http	os://ssolo	adbal.vrajoli.com:8989/adr	ningui/admingui/cor	ntentURLForwardir	ngs?co	ontentURLForward	ings.vsTat ☆	• 🛃 • Google	2	P
🖸 1 Oracle	e iPlanet We	eb Serv +										
VERSION	N								HOME	REFRES	LOG OUT	HELP
User: adm	in Server:	ssoloadbal.vrajo	li.com							A Deploym	ent Pending	<u>\$</u> ,
Oracle iF	vlanet We	eb Server								Instance(s)	Running 0	Java
										Instance(s)	Stopped 💿 1	
Configurat	ions > sso	oloadbal.vrajoli.co	om > V	'irtual Servers > ssol	oadbal.vrajoli.co	om						
Server	Settings	Web Applicat	ions	Content Handling	WebDAV	Search	Ac	cess Control	Summa	ry		
General	Docum	ent Directories	CGI	URL Redirects	Error Pages	Reverse Pro	oxy	FastCGI	MIME Type	S		
ssoloadba	al.vrajoli.c	om - Reverse P	roxy									
A reverse	proxy is a p	proxy that appears	s to be a	a web server (origin se	erver) to clients	but in reality fo	rward	ds the request	s it receives	to one or mo	ore origin serve	ers.
Configure	reverse pro	xy here.										
Revers	e Proxy (())	_		_	_		_	_	_		
New	Delete											
URI Pre	efix				Server Nar	nes						
No Rev	erse Proxy	URI has been ac	ded. C	lick on New button to	add a Reverse F	Proxy URI.						
-												11001 12
Done											a	-110% 🐐 🧋

Click on New button.

You will see below page.

🥹 Reverse Proxy - M	ozilla Firefox	×
vrajoli.com https://sso	loadbal.vrajoli.com:8989/admingui/admingui/vsAddReverseProxy?token=83078020-6029-41c9-8286-59cd	
Oracle iPlanet We	eb Server	
Add Reverse Proxy	r URI	
requests it receives to	o one or more origin servers.	
	* Indicates required fie	ld
* URI Prefix:		
	Enter Reverse Proxy URI here	
* Server Names:		
	Enter server names nere	
	OK Cance	
		_
Done	🔒 F110% 👹	

Under URI Prefix, enter / and under Server Names enter the OpenAM Enterprise servers hostname. In this guide, we have two OpenAM Enterprise servers namely cucmsso1.vrajoli.com and cucmsso2.vrajoli.com. Click on OK button.

URI Prefix:

/

Server Names: <u>https://cucmsso1.vrajoli.com:8443,https://cucmsso2.vrajoli.com:8443</u>

Later you see Reverse Proxy URI Created Successfully.

🥹 Oracle iP	lanet We	b Server Admin	Console	- Mozilla Firefox							
C . C	× 🏠	🖸 vrajol.com http	ps://ssoloa	dbal.vrajoli.com:8989/adr	ningui/admingui/con	tentReverseProxy			습 •	🛃 - Google	P
🖸 1 Oracle	iPlanet Wo	eb Serv +									
VERSION									HOME	REFRESH LOG C	OUT HELP
User: admin	Server:	ssoloadbal.vrajo	oli.com						4	Deployment Pendi	ng 🐇
Oracle iPl	anet We	eb Server							In	stance(s) Running 0	Java
									In:	stance(s) Stopped	p 1
Configuratio	ons > ss	oloadbal.vrajoli.c	om > Vi	rtual Servers > ssol	oadbal.vrajoli.co	m					
Server S	ettings	Web Applicat	tions	Content Handling	WebDAV	Search	Access C	ontrol	Summary		
General	Docum	ent Directories	CGI	URL Redirects	Error Pages	Reverse Prox	y Fast	CGI	MIME Types		
					hard hereined			1			
					erse Proxy URI	Created Succ	essfully				
ssoloadbal	.vrajoli.c	om - Reverse P	roxy								
A reverse pi	roxy is a p	proxy that appear	s to be a	web server (origin se	erver) to clients I	but in reality for	wards the I	request	s it receives to	one or more origin s	ervers.
Configure re	everse pro	oxy here.									
Reverse	Proxy (1)		_	_		_	-		_	
New	Delete										
⊠ 8 UF	RI Prefix		Server I	Names				_			
		_	https://cu	ucmsso1.vrajoli.com:8	3443,https://cucr	nsso2.vrajoli.co	m:8443				
□+℃											
Done											🔒 F110% 🌌
5 one											- 110/0 4

Click on / URI Prefix, modify the sticky cookie value to **amlbcookie** instead of JSESSIONID

🔮 Edit Reverse F	Proxy Uri - Mozilla Firefox	<
🖸 vrajoli.com https	://ssoloadbal.vrajoli.com:8989/admingui/admingui/contentReverseProxy?contentReverseProxy.contentReverse 🏠	2
Oracle iPlane	t Web Server	~
Edit Reverse P	roxy URI OK Cancel	
 Origin Server 	Configuration × Authentication	
HTTP Client C	Configuration * Forward Parameters	
	* Indicates required field	
Origin Server C	configuration	
URI Prefix:	7	
* Server Names:	https://cucmsso1.vrajoli.c Comma separated list of server names. The server name must be a hostname, a fully qualified domain name, an IP address, or a URL prefix without the path component (e.g. https://origin.server.com or origin.server.com). If multiple values are given, the server will distribute load among the specified servers.	
Sticky Cookie:	amlbcookie Name of a cookie that, when present in a response, will cause subsequent requests to "stick" to that origin server.	
Sticky URI	jsessionid	
Parameter:	Name of a URI parameter to inspect for route information. When the URI parameter is present in a requestURI and its value contains a colon ':' followed by a route ID, the request will "stick" to the origin server identified by that route ID.	
Route	Proxy-jroute	
Header:	Name of the HTTP request header used to communicate route IDs to origin servers. "set-origin-server" associates each origin server named by a server parameter with a unique route ID	
Route	JROUTE	
Cookie:	Name of the cookie generated by the server when it encounters a "sticky-cookie" cookie in a response. The "route-cookie" cookie stores the route ID that enables the	~
Done	🔒 F110% 🦑	

Click on OK button.

Now you need to import the OpenAM Enterprise server 1 (cucmsso1.vrajoli.com) certificate and OpenAM Enterprise server 2 (cucmsso2.vrajoli.com) certificate to the Load Balancer.

Copy OpenAM Enterprise Server 1(cucmsso1.vrajoli.com) and OpenAM Enterprise Server 2 (cucmsso2.vrajoli.com) certificate to Load Balancer box to any location.

Now on the Load Balancer, Go to Configurations \rightarrow ssoloadbal.vrajoli.com \rightarrow Certificates \rightarrow Certificate Authorities tab, you will see below page.

🔮 Orac	le iPlanet Web	Server Admin Con	sole - Mozilla	Firefox						
	• C × 🏠	🖸 vrajoli.com https://	ssoloadbal.vrajoli.	com:8989/admi	ingui/admingui/configTrus	tedCA		습 🔹 🚼 - Go	oogle	ş
010	racle iPlanet We	b Serv *								
VERS	SION						HOME	REFRES	H LOG OUT	HELP
User: a	admin Server:	ssoloadbal.vrajoli.cc	om						nent Pending	"
Oracl	e iPlanet We	b Server						Instance(s)	Running 0	E) lava
								Instance(s)	Stopped ᠾ 1	java
Canfin		leading to the leader	_	_				_	_	
Config	urations > ssc	iloadbai.vrajoli.com	1	1	1			· · · · ·		-
Virt	ual Servers	HTTP Listeners	Instances	General	Performance	Access Control	Certificates	Java	Summary	
Serv	er Certificates	Certificate Autho	rities CRL	Updates	PKCS11 Tokens					
ssoloa	dbal.vraioli.co	om - Certificate Au	thorities (CAs	5)					Set Pas	swords
The pa	ge lists the var	ious certificate autho	orities available	e in the certif	icate database. You	can install a CA cert	ificate, a Certifica	ate Revocati	on List (CRL)	or delete a
CA cer	tificate on this p	page. The filter in the	e table can be	used to view	expired certificates	or hide built-in certifi	cates.			
Corti	ficato Authori	tion (1 20 of 162)	_							
Geru		Di Doleta	Elline en All lite	100 million				_	_	
Insta		RL Delete	Filter: All ite	ms						
	Nickname					Expiration Date			CRL	
	Builtin Object	Token:ABAecom (su	ub., Am. Banke	ers Assn.) Ro	ot CA	O July 9, 2009	11:03:53 PM IST		Not Ins	stalled
	Builtin Object	Token:AC Raiz Cerl	ticámara S.A.			April 3, 2030	3:12:02 AM IST		Not Ins	talled
	Builtin Object	Token:Add Trust Ext	ternal Root	_		May 30, 2020	4:18:38 PM IST		Not Ins	stalled
	Builtin Object	Token:Add Trust Lov	w-value Servic	ces Root		May 30, 2020	4:08:31 PM IST		Not ins	stalled
	Builtin Object	Token:Add Trust Pul	blic Services F	Root		May 30, 2020	Not Ins	stalled		
	Builtin Object	Token:AddTrust Qu	alified Certifica	ates Root		May 30, 2020 4:14:50 PM IST			Not Ins	talled
	Builtin Object	Token:America Onli	ne Root Certif	ication Autho	rity 1	November 20	, 2037 2:13:00 A	MIST	Not Ins	talled
	Builtin Object	I oken:America Onli	ne Root Certif	ication Autho	rity 2	September 2	9, 2037 7:38:00 F	MIST	Not Ins	talled
	Builtin Object	Token:AOL Time W	arner Root Ce	rtification Au	thority 1	November 20	, 2037 8:33:00 P	MIST	Not Ins	talled
	Builtin Object	Token:AOL Time W	arner Root Ce	rtification Au	thority 2	September 2	9, 2037 5:13:00 /	AM IST	Not Ins	talled
	Builtin Object	Token:ApplicationC	A - Japanese (Government		December 12	, 2017 8:30:00 P	MIST	Not Ins	stalled
	Builtin Object	Token:Baltimore Cy	berTrust Root			May 13, 2025	5:29:00 AM IST		Not Ins	stalled
	Builtin Object	Token:beTRUSTed	Root CA			June 20, 201	0 6:51:04 PM IS	Ţ.	Not Ins	stalled
Done										🔒 F110% 🌾

Click on Install button, then you will be taken to Install CA Certificate wizard.

🔮 Install CA Certificate Wiz	ard - Mozilla Fir	efox	×
vrajoli.com https://ssoloadbal.v	vrajoli.com:8989/adn	$\label{eq:constraint} \end{tabular} t$	
Oracle iPlanet Web Ser	ver		
Install CA Certificate Wiza	rd		
Steps Help	Step 1:Selec	t Tokens and Passwords	^
 1. Select Tokens and Passwords 2. Enter Certificate Data 3. Certificate Type 	The page sho configuration. required. Configura	ws the list of tokens that are available for the Enter the password for the selected token if tion: ssoloadbal.vrajoli.com	Milli
4. Review 5. Results	Token: Previous	internal Select the token name from the above list. If your key is stored in the local key database maintained by Oracle iPlanet Web Server 7.0, choose internal. If your key is stored in a Smart Card or other external device or engine, choose the name of the external token from the drop down list box.	•
Done		🔒 F110% 🐐	

Click on Next,

Select 'Certificate File' radio button and specify the path where you have stored the OpenAM Enterprise Server 1 certificate,.

🥹 Install CA Certificate Wizard - Mozil	la Firefox
vrajoli.com https://ssoloadbal.vrajoli.com:898	19/admingui/admingui/WizardWindow
Oracle iPlanet Web Server	
Install CA Certificate Wizard	
Steps Help	Step 2:Enter Certificate Data
 Select Tokens and Passwords Enter Certificate Data Certificate Type Review Results 	Enter certificate data in ASCII format along with the headers in the text area provided or provide the path to a file containing the certificate data. Certificate Data Image: Certificate File /root/certs/cucmsso1.vrajoli.com.pem Path to the certificate file on the server
Dona	Previous Next Cancel

Click Next button, you will see below page.



Click on Next button.



Click in Finish button and you will see below page.



Similary, install the OpenAM Enterprise server 2 (cucmsso2.vrajoli.com) certificate.

After importing all the OpenAM Enterprise server certificates to Load Balancer, Click on Deployment Pending link on the right top corner.

🤇 🔰 🔻 🔀 🔬 (🖸 vrajoi.com https://ssoloadbal.vrajoi.com:8989/admingui/admingui/configTi	ustedCA?serverCertificates	General.generalCert	යි 🔹 🛃 - G	oogle	
□ 1 Oracle iPlanet Web Serv *					
VERSION		HOME	REFRES	H LOG OUT	HELP
User: admin Server: ssoloadbal.vrajoli.com			A Deployn	nent Pending	k
Oracle iPlanet Web Server			Instance(s)	Running 0	E)
			Instance(s)	Stopped ᠾ 1	Java
		_	_	_	_
Configurations > ssoloadbal.vrajoli.com					
Virtual Servers HTTP Listeners Instances General Performance	Access Control	Certificates	Java	Summary	
Server Certificates Certificate Authorities CRL Updates PKCS11 Tokens					
ssoloadbal vraioli com - Certificate Authorities (CAs)				Set Pas	swords
The name lists the various certificate authorities available in the certificate database. Vo	u can install a CA cort	ificato a Cortifica	to Revocati	ion List (CRL)	or delete a
CA certificate on this page. The filter in the table can be used to view expired certificate	s or hide built-in certifi	cates.			
Certificate Authorities (1 - 20 of 162)					
Install Install CRL Delete Filter: All Items 💌 🕅+D)	_		_	
Install Install CRL Delete Filter: All Items v @+€ Ø Nickname	Expiration Date			_ CRL	<u>م</u>
Install Install CRL Delete Filter: All Items ✓ 1 %+C 図 図 Nickname Builtin Object Token:ABAecom (sub., Am. Bankers Assn.) Root CA	 Expiration Date July 9, 2009 	9 11:03:53 PM IST		CRL Not Ins	ے talled
Install CRL Delete Filter: All Items ▼ Image: Comparison of the	 Expiration Date July 9, 2009 April 3, 2030 	• 11:03:53 PM IST 3:12:02 AM IST	_	CRL Not Ins Not Ins	 talled talled
Install CRL Delete Filter: All Items ▼ Image: Comparison of the	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 	9 11:03:53 PM IST 3:12:02 AM IST 9 4:18:38 PM IST		CRL CRL Not Ins Not Ins Not Ins	talled talled talled
Install CRL Delete Filter: All Items Image: Comparison of the	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 May 30, 2020 	9 11:03:53 PM IST 3:12:02 AM IST 0 4:18:38 PM IST 0 4:08:31 PM IST		CRL Not Ins Not Ins Not Ins Not Ins	talled talled talled talled
Install CRL Delete Filter: All Items Image: Comparison of the state	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 May 30, 2020 May 30, 2020 May 30, 2020 	9 11:03:53 PM IST 3:12:02 AM IST 0 4:18:38 PM IST 0 4:08:31 PM IST 0 4:11:50 PM IST		CRL Not Ins	talled talled talled talled talled
Install CRL Delete Filter: All Items Image: Comparison of the	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020) 3:12:02 AM IST 3:12:02 AM IST 0 4:18:38 PM IST 0 4:08:31 PM IST 0 4:11:50 PM IST 0 4:11:50 PM IST		CRL Not Ins N	talled talled talled talled talled talled
Install CRL Delete Filter: All Items Image: Comparison of the	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 November 20) 3:12:02 AM IST 3:12:02 AM IST 0 4:18:38 PM IST 0 4:08:31 PM IST 0 4:11:50 PM IST 0 4:11:50 PM IST 0 4:14:50 PM IST 0 2037 2:13:00 A	MIST	CRL Not ins Not ins Not ins Not ins Not ins Not ins Not ins Not ins	talled talled talled talled talled talled talled
Install CRL Delete Filter: All Items Image: Comparison of the	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 November 20 September 23 	 11:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST 4:08:31 PM IST 4:11:50 PM IST 4:14:50 PM IST 2:037 2:13:00 A 9, 2037 7:38:00 F 	M IST PM IST	CRL Not ins Not ins Not ins Not ins Not ins Not ins Not ins Not ins Not ins	talled talled talled talled talled talled talled talled talled
Install CRL Delete Filter: All Items Image: Comparison of the	Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 November 20 September 22 November 20	 11:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST 4:11:50 PM IST 4:11:50 PM IST 4:14:50 PM IST 2:037 2:13:00 A 2:037 7:38:00 P 2:037 8:33:00 P 	M IST PM IST M IST	CRL Not ins Not ins Not ins Not ins Not ins Not ins Not ins Not ins Not ins Not ins	talled talled talled talled talled talled talled talled talled talled
Install CRL Delete Filter: All Items Items Image: State St	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 M	 3:12:02 AM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST 4:08:31 PM IST 4:11:50 PM IST 4:14:50 PM IST 2:037 2:13:00 A 9:2037 7:38:00 P 9:2037 5:13:00 A 	M IST M IST M IST M IST M IST	CRL Not ins Not ins	Lalled talled talled talled talled talled talled talled talled talled talled
Install CRL Delete Filter: All Items Image: Comparison of the state	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 M	 11:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST 4:11:50 PM IST 4:11:50 PM IST 4:14:50 PM IST 2:037 2:13:00 A 2:037 7:38:00 P 2:037 5:13:00 A 2:037 5:13:00 A 2:017 8:30:00 P 	M IST M IST M IST M IST M IST M IST	CRL Not ins Not ins	Lalled talled talled talled talled talled talled talled talled talled talled talled
Install Install CRL Delete Filter: All Items Image: Comparison of the state	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 	 a a:11:03:53 PM IST a:12:02 AM IST b 4:18:38 PM IST b 4:08:31 PM IST b 4:11:50 PM IST b 4:14:50 PM IST b 4:14:50 PM IST c) 2037 2:13:00 A c) 2037 5:13:00 P c) 2037 5:13:00 P c) 2037 5:13:00 P c) 2037 8:300 P c) 2037 5:13:00 A c) 2017 8:30:00 P c) 5:29:00 AM IST 	M IST M IST M IST M IST M IST M IST	CRL Not ins Not ins	talled
Install CRL Delete Filter: All Items Items Items Image: Strain	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 September 23 November 20 September 23 November 20 September 23 December 12 May 13, 2025 June 20, 2011 	 11:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST 4:11:50 PM IST 4:14:50 PM IST 2:037 2:13:00 A 9:2037 7:38:00 P 9:2037 5:13:00 A 9:2017 8:30:00 P 5:29:00 AM IST 0 6:51:04 PM IST 	M IST M IST M IST M IST M IST	CRL Not ins Not ins	talled talled

you will see below page, after clicking on Deployment Pending.

🥹 Configuration Deployment - Mozilla Firefox	×
Coverajoli.com https://ssoloadbal.vrajoli.com:8989/admingui/admingui/configTrustedCA?config	☆
Oracle iPlanet Web Server	
Configuration Deployment Deploying configuration to all instances.	
Deployment Pending The configuration ssoloadbal.vrajoli.com has changed locally. Click on "Deploy" to propagate the changes to all instances	
Deploy Cance	3I
Done 🔒 F110% 4	÷ .

Click on Deploy button. You will see below page after successful deployment.



Click on Close button.

16.2.2 Installation and configuration of session failover components

16.2.2.1 Configuration of session failover components on Linux Platform

Pre-Requisites: one or more OpenAM Enterprise servers (for session failover) installed and configured on Linux platform. For installing OpenAM Enterprise on Linux platform, please refer white paper of <>

In this guide, we have two OpenAM Enterprise servers for session failover.

OpenAM Enterprise server $1 \rightarrow$ cucmsso1.vrajoli.com

OpenAM Enterprise server 2 \rightarrow cucmsso2.vrajoli.com

Install the OpenSSO Enterprise session failover components on the cucmsso1.vrajoli.com host machine and thecucmsso2.vrajoli.com host machine
To Install Session Failover Components on cucmsso1.vrajoli.com OpenAM Enterprise server on Linux

- 1. As a root user, log in to the cucmsso1.vrajoli.com host machine.
- 2. Create a directory into which the MessageQueue and BerkeleyDatabase bits can be downloaded and change into it.

mkdir /export/SF0

cd /export/SFO

- 3. Copy ssoSessionTools.zip to the cucmsso1.vrajoli.com host machine, ssoSessionTools.zip is included in the openam_release9_20100207.zip file under the tools directory. (openam_release9_20100207/opensso/tools/ssoSessionTools.zip)
- 4. Unzip ssoSessionTools.zip.

cd /export/SFO

unzip ssoSessionTools.zip -d ssoSessionTools

5. Modify the permissions on the setup script and run it to initialize the session failover tools.

cd /export/SFO/ssoSessionTools

chmod +x setup

./setup

6. When prompted, enter opensso as the Directory to install the scripts (example: opensso).

Note – The directory location should be relative to the current directory.

When the script is finished, the following messages are displayed:

The scripts are properly setup under directory

/export/SFO/ssoSessionTools/opensso

JMQ is properly setup under directory

/export/SFO/ssoSessionTools/jmq

7. Change to the bin directory.

cd /export/SFO/ssoSessionTools/jmq/imq/bin

8. Run the imqbrokerd command to create a new broker instance named msgqbroker.

./imqbrokerd -name msgqbroker -port 7777 &

9. Run netstat to verify that the newMessageQueue broker instance is up and running.

netstat -an | grep 7777

*.7777 *.* 0 0 49152 0 LISTEN

10. Add a new user named msgquser.

This user will connect to the Message Queue broker instance on servers where Message Queue is installed. This user will be used only for session failover purposes, and does not assume the privileges of the guest user. It is a good practice to create a custom user for such purposes, and not to rely on the known user accounts or default user accounts to help prevent brute force or DOS attacks.

#./imqusermgr add -u msgquser -g admin -p m5gqu5er -i msgqbroker

User repository for broker instance: msgqbroker

User msgquser successfully added.

11. Disable the guest user.

This step ensures that the guest user will not be able to access the OpenSSO Enterprise server.

#./imqusermgr update -u guest -a false -i msgqbroker

User repository for broker instance: msgqbroker

Are you sure you want to update user guest? (y/n) y

User guest successfully updated.

12. Modify the amsfo.conf file.

amsfo.conf has parameters that are consumed by the OpenSSO Enterprise session failover startup script, amsfo.

• Change to the lib directory.

cd /export/SFO/ssoSessionTools/opensso/config/lib

• Set the following properties:

CLUSTER_LIST=**cucmsso1.vrajoli.com.example.com:7777,cucmsso2.vrajoli.com** .example.com:7777

BROKER_INSTANCE_NAME=msgqbroker

USER_NAME=**msgquser**

BROKER_PORT=7777

Note – The port used for BROKER_PORT should be the same as the one used in the value of the CLUSTER_LIST.

- Save the file and close it.
- 13. Generate an encrypted password in a .password file with the following sub procedure.
 - Change to the bin directory.
 # cd /export/SFO/ssoSessionTools/opensso/bin
 - Run amsfopassword. This command generates an encrypted password, creates a new file named .password, and stores the encrypted password in the new file. Caution – amsfopassword creates the .password file in a default location based on where the scripts were installed. If a different location is used, the PASSWORDFILE property in amsfo.conf should be changed accordingly. # ./amsfopassword -e m5gqu5er -f /export/SFO/ssoSessionTools/opensso/.password os.name=SunOS SUCCESSFUL
 (0 the optimized bases and for a different if patients)
 - (Optional)View the encrypted password for verification.
 # more /export/SFO/ssoSessionTools/opensso/.password
 M270Gb6U4ufRu+oWAzBdWw==

14. (Optional) Modify the amsessiondb script if necessary.

The amsessiondb script (located in the /export/SFO/ssoSessionTools/opensso/bin directory) starts the BerkeleyDatabase client, creates the database, and sets specific database values. It is called when the amsfo script is run for the first time. The amsessiondb script contains variables that specify default paths and directories. If any of the following components are not installed in their default directories, edit the amsessiondb script to set the variables to the correct locations.

IMQ_JAR_PATH=/export/SFO/ssoSessionTools/jmq/imq/lib JMS_JAR_PATH=/export/SFO/ssoSessionTools/jmq/imq/lib AM_HOME=/export/SFO/ssoSessionTools Tip – Backup amsessiondb before you modify it.

- 15. Restart the session failover components with the following sub procedure.
 - a. Change to the bin directory.

cd /export/SFO/ssoSessionTools/jmq/imq/bin

b. Stop the MessageQueue instance using the product's command line interface. See theMessage Queue documentation for more information.

c. Run the netstat command to verify that the cucmsso1.vrajoli.com broker instance is stopped.

netstat -an | grep 7777

If netstat returns no result, the cucmsso1.vrajoli.com broker instance is stopped.

Tip – If the cucmsso1.vrajoli.com broker instance is not stopped, kill the process using the following

procedure.

a. Get the Java process IDs.

ps -ef | grep java

b. Kill the Java process IDs that were returned.

kill -9 ####

c. Run netstat again.

d. Restart the cucmsso1.vrajoli.com broker instance.

cd /export/SFO/ssoSessionTools/opensso/bin

./amfso start

e. Run the netstat command to verify that the MessageQueue port is open and listening.

netstat -an | grep 7777

*.7777 *.* 0 0 49152 0 LISTEN

16. Log out of the cucmsso1.vrajoli.com host machine.

To Install Session Failover Components on cucmsso2.vrajoli.com

- 1. As a root user, log in to the mq–2 host machine.
- 2. Create a directory into which the MessageQueue and BerkeleyDatabase bits can be downloaded and change into it.

mkdir /export/SF0

cd /export/SFO

- 3. Copy ssoSessionTools.zip to the cucmsso1.vrajoli.com host machine, ssoSessionTools.zip is included in the openam_release9_20100207.zip file under the tools directory. (openam_release9_20100207/opensso/tools/ssoSessionTools.zip)
- 4. Unzip ssoSessionTools.zip. # cd /export/SFO

unzip ssoSessionTools.zip -d ssoSessionTools

5. Modify the permissions on the setup script and run it to initialize the session failover tools.

cd /export/SFO/ssoSessionTools

chmod +x setup

./setup

6. When prompted, enter **opensso** as the *Directory to install the scripts (example: opensso)*.

Note – The directory location should be relative to the current directory.

When the script is finished, the following messages are displayed:

The scripts are properly setup under directory

/export/SFO/ssoSessionTools/opensso

JMQ is properly setup under directory

/export/SFO/ssoSessionTools/jmq

7. Change to the bin directory.

cd /export/SFO/ssoSessionTools/jmq/imq/bin

- 8. Run the impbrokerd command to create a new broker instance named msgqbroker.
- #./imqbrokerd -name msgqbroker -port 7777 &
 - 9. Run netstat to verify that the newMessageQueue broker instance is up and running.

netstat -an | grep 7777

*.7777 *.* 0 0 49152 0 LISTEN

10. Add a new user named msgquser.

This user will connect to the Message Queue broker instance on servers where Message Queue is installed. This user will be used only for session failover purposes, and does not assume the privileges of the guest user. It is a good practice to create a custom user for such purposes, and not to rely on the known user accounts or default user accounts to help prevent brute force or DOS attacks.

./imqusermgr add -u msgquser -g admin -p m5gqu5er -i msgqbroker

User repository for broker instance: msgqbroker

User msgquser successfully added.

11. Disable the guest user.

This step ensures that the guest user will not be able to access the OpenSSO Enterprise server.

./imqusermgr update -u guest -a false -i msgqbroker

User repository for broker instance: msgqbroker

Are you sure you want to update user guest? (y/n) y

User guest successfully updated.

12. Modify the amsfo.conf file with the following sub procedure.

amsfo.conf has parameters that are consumed by the OpenSSO Enterprise session failover

startup script, amsfo.

a. Change to the lib directory.

cd /export/SFO/ssoSessionTools/opensso/config/lib

Tip – Backup amsfo.conf before you modify it.

b. Set the following properties:

CLUSTER_LIST=mq-1.example.com:7777,cucmsso2.vrajoli.com.example.com:7777

BROKER_INSTANCE_NAME=msgqbroker

USER_NAME=msgquser

BROKER_PORT=7777

Note – The port used for BROKER_PORT should be the same as the one used in the value of the

CLUSTER_LIST.

c. Save the file and close it.

13. Generate an encrypted password in a .password file with the following sub procedure.

a. Change to the bin directory.

cd /export/SFO/ssoSessionTools/opensso/bin

b. Run amsfopassword.

This command generates an encrypted password, creates a new file named .password, and

stores the encrypted password in the new file.

Caution – amsfopassword creates the .password file in a default location based on where the scripts were installed. If a different location is used, the PASSWORDFILE property in amsfo.conf should be changed accordingly.

./amsfopassword -e m5gqu5er -f /export/SFO/ssoSessionTools/opensso/.password

os.name=SunOS

SUCCESSFUL

c. (Optional)View the encrypted password for verification.

more /export/SFO/ssoSessionTools/opensso/.password

M270Gb6U4ufRu+oWAzBdWw==

14. (Optional) Modify the amsessiondb script if necessary.

The amsessiondb script (located in the /export/SFO/ssoSessionTools/opensso/bin directory) starts the BerkeleyDatabase client, creates the database, and sets specific

database values. It is called when the amsfo script is run for the first time. The amsessiondb script contains variables that specify default paths and directories. If any of the following components are not installed in their default directories, edit the amsessiondb script to set the variables to the correct locations.

IMQ_JAR_PATH=/export/SFO/ssoSessionTools/jmq/imq/lib

JMS_JAR_PATH=/export/SFO/ssoSessionTools/jmq/imq/lib

AM_HOME=/export/SFO/ssoSessionTools

Tip – Backup amsessiondb before you modify it.

15. Restart the session failover components.

a. Change to the bin directory.

cd /export/SFO/ssoSessionTools/jmq/imq/bin

b. Stop the MessageQueue instance using the product's command line interface.

See the Message Queue documentation for more information.

c. Run the netstat command to verify that the cucmsso2.vrajoli.com broker instance is stopped.

netstat -an | grep 7777

If netstat returns no result, the cucmsso2.vrajoli.com broker instance is stopped.

Tip – If the cucmsso2.vrajoli.com broker instance is not stopped, kill the process using the following

procedure.

a. Get the Java process IDs.

ps -ef | grep java

b. Kill the Java process IDs that were returned.

kill -9 ####

c. Run netstat again.

d. Restart the cucmsso2.vrajoli.com broker instance.

cd /export/SFO/ssoSessionTools/opensso/bin

./amfso start

e. Run the netstat command to verify that the MessageQueue port is open and listening.

netstat -an | grep 7777

*.7777 *.* 0 0 49152 0 LISTEN 16. Log out of the cucmsso2.vrajoli.com host machine.

16.2.2.2 Configuration of session failover components of windows platform

<u>To Install Session Failover Components on cucmsso1.vrajoli.com</u> <u>OpenAM Enterprise server on Windows</u>

- 1. Log in to the server where you want to install and configure the session failover components (cucmsso1.vrajoli.com)
- Copy ssoSessionTools.zip to the cucmsso1.vrajoli.com host machine, ssoSessionTools.zip is included in the openam_release9_20100207.zip file under the tools directory. (openam_release9_20100207/opensso/tools/ssoSessionTools.zip)
- 3. Unzip ssoSessionTools.zip to ssoSessionTools folder and cd to ssoSessionTools folder

C:\>cd ssoSessionTools

4. Run the setup.bat script to install the session tools on Windows systems.

C:\ssoSessionTools>setup.bat

Name of the directory to install the scripts (example: sfoscripts):sfoscripts The scripts are properly setup under directory: C:\ssoSessionTools\sfoscripts JMQ is properly setup under directory C:\ssoSessionTools\jmq

- 5. Change to bin folder.
- 6. Run the imqbrokerd command to create a new broker instance named msgqbroker.

C:\ssoSessionTools\jmq\imq\bin>imqbrokerd.exe -name msgqbroker -port 7777 &

[25/Sep/2010:23:38:40 IST]

=======

Sun GlassFish(tm) Message Queue 4.4

Sun Microsystems, Inc.

Version: 4.4 (Build 16-a)

Compile: Thu 08/27/2009

Copyright (c) 2009 Sun Microsystems, Inc. All rights reserved. Use is subject to license terms.

Java Runtime: 1.6.0_21 Sun Microsystems Inc. c:\Program Files\Java\jdk1.6.0_21\jre [25/Sep/2010:23:38:40 IST] IMQ_HOME=C:\ssoSessionTools\jmq\imq [25/Sep/2010:23:38:40 IST] IMQ_VARHOME=C:\ssoSessionTools\jmq\imq\var [25/Sep/2010:23:38:40 IST] Windows Server 2008 6.0 x86 cucmsso1.vrajoli.com (1 cp

u) Administrator

[25/Sep/2010:23:38:40 IST] Java Heap Size: max=190080k, current=15872k

[25/Sep/2010:23:38:40 IST] Arguments: -name msgqbroker -port 7777

[25/Sep/2010:23:38:40 IST] [B1060]: Loading persistent data...

[25/Sep/2010:23:38:40 IST] Using built-in file-based persistent store: C:\ssoSes

sionTools\jmq\imq\var\instances\msgqbroker\

[25/Sep/2010:23:38:40 IST] [B1039]: Broker "msgqbroker@cucmsso1.vrajoli.com:7777" ready.

7. Run netstat to verify that the newMessageQueue broker instance is up and running.

C:\ssoSessionTools\jmq\imq\bin>netstat -an | findstr 7777 TCP 0.0.0.0:7777 0.0.0.0:0 LISTENING TCP 10.78.85.131:60787 10.78.85.131:7777 TIME_WAIT TCP [::]:7777 [::]:0 LISTENING

8. Add a new user named msgquser.

This user will connect to the Message Queue broker instance on servers where Message Queue is installed. This user will be used only for session failover purposes, and does not assume the privileges of the guest user. It is a good practice to create a custom user for such purposes, and not to rely on the known user accounts or default user accounts to help prevent brute force or DOS attacks.

C:\ssoSessionTools\jmq\imq\bin>imqusermgr.exe add -u msgquser -g admin -p m5gqu5er -i msgqbroker

User repository for broker instance: msgqbroker

User msgquser successfully added.

9. Disable the guest user. This step ensures that the guest user will not be able to access the OpenSSO Enterprise server.

C:\ssoSessionTools\jmq\imq\bin>imqusermgr.exe update -u guest -a false -i msgqbroker

User repository for broker instance: msgqbroker

Are you sure you want to update user guest? (y/n)[n] y

User guest successfully updated.

10. Modify the amsfo.conf file.

amsfo.conf has parameters that are consumed by the OpenSSO Enterprise session failover startup script, amsfo.

• Change to the lib directory.

cd C:\ssoSessionTools\sfoscripts\config\lib

• Set the following properties:

CLUSTER_LIST=cucmsso1.vrajoli.com.example.com:7777,cucmsso2.vrajoli.com.exa mple.com:7777

BROKER_INSTANCE_NAME=msgqbroker

USER_NAME=msgquser

BROKER_PORT=7777

Note – The port used for BROKER_PORT should be the same as the one used in the value of the

CLUSTER_LIST.

- Save the file and close it.
- 11. Generate an encrypted password in a .password file with the following sub procedure.

Change to the bin directory.

cd C:\ssoSessionTools\sfoscripts\bin

• Run amsfopassword.bat

This command generates an encrypted password, creates a new file named .password, and stores the encrypted password in the new file.

Caution – amsfopassword creates the .password file in a default location based on where the scripts were installed. If a different location is used, the PASSWORDFILE property in amsfo.conf should be changed accordingly.

C:\SSOSES~1\SFOSCR~1\bin>amsfopassword.bat -e m5gqu5er -f c:\ssoSessionTools\sfoscripts\.password

os.name=Windows Server 2008 SUCCESSFUL 12. start the cucmsso1.vrajoli.com broker instance. To start the amsfo.pl you need to have Perl installed on OpenAM host. In this guide ActivePerl 5.12.2 Build 1202 has been installed on Windows machine where OpenAM is installed.

C:\ssoSessionTools\sfoscripts\bin>amsfo.pl c:\ssoSessionTools\sfoscripts\config\lib\amsfo.conf start

starting JMQ Broker

C:/ssoSessionTools/jmq/imq/bin/imqbrokerd.exe -bgnd -silent -vmargs "-Xms256m -Xmx512m" -name msgqbroker -port 7777 -cluster cucmsso1.vrajoli.com:7777,cucmsso2.vrajoli.com:7777

starting amsessiondb client

c:/Program Files/Java/jdk1.6.0_21/jre/bin/java.exe -classpath "C:/ssoSessionTools/jmq/imq/lib/imq.jar;C:/ssoSessionTools/jmq/imq/lib/jms.jar;C:/ ssoSession

Tools/ext/je.jar;C:/ssoSessionTools/locale;C:/ssoSessionTools/lib/am_sessiondb.jar;." com.sun.identity.ha.jmqdb.client.FAMHaDB -a cucmsso1.vrajoli.com:7777,

cucmsso2.vrajoli.com:7777 -u msgquser -f C:/ssoSessionTools/sfoscripts/.password -b /tmp/amsession/amsessiondb -m c:\ssoSessionTools\sfoscripts\config\l

ib\amsfo.conf

Initializing and connecting to the Message Queue server ...

Successfully started.

13. Run the netstat command to verify that the MessageQueue port is open and listening.

C:\ssoSessionTools\sfoscripts\bin>netstat -an | findstr 7777

ТСР	0.0.0.0:7777	0.0.	0.0:0 LISTENIN	G
ТСР	10.78.85.131:6	50787	10.78.85.131:7777	TIME_WAIT
ТСР	[::]:7777	[::]:0	LISTENING	

<u>To Install Session Failover Components on cucmsso2.vrajoli.com OpenAM Enterprise</u> <u>server on Windows</u>

- 1. Log in to the server where you want to install and configure the session failover components (cucmsso1.vrajoli.com)
- Copy ssoSessionTools.zip to the cucmsso1.vrajoli.com host machine, ssoSessionTools.zip is included in the openam_release9_20100207.zip file under the tools directory. (openam_release9_20100207/opensso/tools/ssoSessionTools.zip)
- 3. Unzip ssoSessionTools.zip to ssoSessionTools folder and cd to ssoSessionTools folder

C:\>cd ssoSessionTools

4. Run the setup.bat script to install the session tools on Windows systems.

C:\ssoSessionTools>setup.bat

Name of the directory to install the scripts (example: sfoscripts):sfoscripts The scripts are properly setup under directory: C:\ssoSessionTools\sfoscripts JMQ is properly setup under directory C:\ssoSessionTools\jmq

- 5. Change to bin folder.
- 6. Run the imqbrokerd command to create a new broker instance named msgqbroker.

C:\ssoSessionTools\jmq\imq\bin>imqbrokerd.exe -name msgqbroker -port 7777 &

[25/Sep/2010:23:38:40 IST]

Sun GlassFish(tm) Message Queue 4.4

Sun Microsystems, Inc.

Version: 4.4 (Build 16-a)

Compile: Thu 08/27/2009

Copyright (c) 2009 Sun Microsystems, Inc. All rights reserved. Use is subject to license terms.

Java Runtime: 1.6.0_21 Sun Microsystems Inc. c:\Program Files\Java\jdk1.6.0_21\jre

[25/Sep/2010:23:38:40 IST] IMQ_HOME=C:\ssoSessionTools\jmq\imq

[25/Sep/2010:23:38:40 IST] IMQ_VARHOME=C:\ssoSessionTools\jmq\imq\var

[25/Sep/2010:23:38:40 IST] Windows Server 2008 6.0 x86 cucmsso1.vrajoli.com (1 cp

u) Administrator

[25/Sep/2010:23:38:40 IST] Java Heap Size: max=190080k, current=15872k

[25/Sep/2010:23:38:40 IST] Arguments: -name msgqbroker -port 7777

[25/Sep/2010:23:38:40 IST] [B1060]: Loading persistent data...

[25/Sep/2010:23:38:40 IST] Using built-in file-based persistent store: C:\ssoSes

sionTools\jmq\imq\var\instances\msgqbroker\

[25/Sep/2010:23:38:40 IST] [B1039]: Broker "msgqbroker@cucmsso1.vrajoli.com:7777" ready.

7. Run netstat to verify that the newMessageQueue broker instance is up and running.

C:\ssoSessionTools\jmq\imq\bin>netstat -an | findstr 7777

 TCP
 0.0.0.0:7777
 0.0.0.0:0
 LISTENING

 TCP
 10.78.85.131:60787
 10.78.85.131:7777
 TIME_WAIT

 TCP
 [::]:7777
 [::]:0
 LISTENING

8. Add a new user named msgquser.

This user will connect to the Message Queue broker instance on servers where Message Queue is installed. This user will be used only for session failover purposes, and does not assume the privileges of the guest user. It is a good practice to create a custom user for such purposes, and not to rely on the known user accounts or default user accounts to help prevent brute force or DOS attacks.

C:\ssoSessionTools\jmq\imq\bin>imqusermgr.exe add -u msgquser -g admin -p m5gqu5er -i msgqbroker

User repository for broker instance: msgqbroker

User msgquser successfully added.

9. Disable the guest user. This step ensures that the guest user will not be able to access the OpenSSO Enterprise server.

C:\ssoSessionTools\jmq\imq\bin>imqusermgr.exe update -u guest -a false -i msgqbroker

User repository for broker instance: msgqbroker

Are you sure you want to update user guest? (y/n)[n] y

User guest successfully updated.

10. Modify the amsfo.conf file.

amsfo.conf has parameters that are consumed by the OpenSSO Enterprise session failover startup script, amsfo.

• Change to the lib directory.

cd C:\ssoSessionTools\sfoscripts\config\lib

• Set the following properties:

CLUSTER_LIST=cucmsso1.vrajoli.com.example.com:7777,cucmsso2.vrajoli.com.exa mple.com:7777

BROKER_INSTANCE_NAME=msgqbroker

USER_NAME=msgquser

BROKER_PORT=7777

Note – The port used for BROKER_PORT should be the same as the one used in the value of the

CLUSTER_LIST.

• Save the file and close it.

11. Generate an encrypted password in a .password file with the following sub procedure.

Change to the bin directory.

cd C:\ssoSessionTools\sfoscripts\bin

• Run amsfopassword.bat

This command generates an encrypted password, creates a new file named .password, and stores the encrypted password in the new file.

Caution – amsfopassword creates the .password file in a default location based on where the scripts were installed. If a different location is used, the PASSWORDFILE property in amsfo.conf should be changed accordingly.

C:*SSOSES*~1*SFOSCR*~1*bin*>*amsfopassword.bat* -*e m5gqu5er* -*f c*:*ssoSessionTools**sfoscripts*\.*password*

os.name=Windows Server 2008

SUCCESSFUL

12. Start the cucmsso2.vrajoli.com broker instance. To start the amsfo.pl you need to have Perl installed on OpenAM host. In this guide ActivePerl 5.12.2 Build 1202 has been installed on Windows machine where OpenAM is installed.

C:\ssoSessionTools\sfoscripts\bin>amsfo.pl c:\ssoSessionTools\sfoscripts\config\lib\amsfo.conf start

starting JMQ Broker

C:/ssoSessionTools/jmq/imq/bin/imqbrokerd.exe -bgnd -silent -vmargs "-Xms256m -Xmx512m" -name msgqbroker -port 7777 -cluster cucmsso1.vrajoli.com:7777,cucmsso2.vrajoli.com:7777

starting amsessiondb client

c:/Program Files/Java/jdk1.6.0_21/jre/bin/java.exe -classpath "C:/ssoSessionTools/jmq/imq/lib/imq.jar;C:/ssoSessionTools/jmq/imq/lib/jms.jar ;C:/ssoSession

Tools/ext/je.jar;C:/ssoSessionTools/locale;C:/ssoSessionTools/lib/am_sessiondb.ja r;." com.sun.identity.ha.jmqdb.client.FAMHaDB -a cucmsso1.vrajoli.com:7777,

cucmsso2.vrajoli.com:7777 -u msgquser -f C:/ssoSessionTools/sfoscripts/.password -b /tmp/amsession/amsessiondb -m c:\ssoSessionTools\sfoscripts\config\l ib\amsfo.conf

Initializing and connecting to the Message Queue server ...

Successfully started.

13. Run the netstat command to verify that the MessageQueue port is open and listening.

C:\ss	oSessionTools	sfoscri	ots\bin>i	netstat -an f	ändstr 7777
ТСР	0.0.0.0:7777	0,0,	0.0:0	LISTENIN	G
ТСР	10.78.85.131:	60787	10.78.8	5.131:7777	TIME_WAIT
ТСР	[::]:7777	[::]:0	L	ISTENING	

16.2.3 Installation and configuration of OpenAM Enterprise servers for session failover.

16.2.3.1 Installation of OpenAM Enterprise server 1

Browse the OpenAM URL: <u>https://cucmsso1.vrajoli.com:8443/opensso</u>, you will see the below Configurator. Click on Create New Configuration under Custom Configuration.



🥹 OpenSSO - Mozilla Firefox				
🔇 🗩 - C 🗙 🏠 🗋 vrajoli.c	om ht	ttps://cucmsso1.vrajoli	.com:8443/opensso/config/options.htm 😭 🚽 🚼 - Google	P
1 OpenSSO	÷			
	onfi Pleas	guration Optior	IS Java" uration option.	
2020A		atom Configurati	OpenSSO Configurator	
Sun Microsystems, Inc., 4150 Nett erved. Sun Microsystems, Inc., 4150 Nett erved. Sun Microsystems, Inc. ha ed in the product that is described blectual property rights may inclu /patents and one or more additio puntries. U.S. Government Rights	 4. 5. 6. 7. 	General Server Settings Configuration Store User Store Site Configuration Agent Information Summary	Step 1: General	
Microsystems, Inc. standard licen- ments. Use is subject to license to parties. Sun, Sun Microsystems, i egistered trademarks of Sun Micr riks are used under license and a al, Inc. in the U.S. and other coun cture developed by Sun Microsys ntries, exclusively licensed throug liled by U.S. Export Control laws a Nuclear, missile, chemical biologic direct or indirect, are strictly proh		a. Export or reexpo	Previous Next Cancel rt to countries subject to	► F110% *

Create a new password for default user [amAdmin]

Click on Next button,

🔮 OpenSSO - Mozilla Firefox					
C X 🏠 🗋 vrajol.c	om ht	ttps://cucmsso1.vrajoli	:om:8443/opensso/config/options.htm	☆ - 🛃 - Google	Q
1 OpenSSO	÷				
Sun Microsystems, Inc., 4150 Netw Err thm da pa be or Cr Sun Microsystems, Inc., 4150 Netw erved. Sun Microsystems, Inc. ha ed in the product that is described ellectual property rights may inclut /patents and one or more addition puntries. U.S. Government Rights Microsystems, Inc. standard licens ments. Use is subject to license to parties. Sun, Sun Microsystems, i egistered trademarks of Sun Micr riks are used under license and a al, Inc. in the U.S. and other coun cture developed by Sun Microsys ntries, exclusively licensed throug lied by U.S. Export Control laws a Nuclear, missile, chemical biologic direct or indirect, are strictly profi	onfi Pleas 1. 3. 4. 5. 6. 7.	guration Option se select a config stom Configuratio General Server Settings Configuration Store User Store Site Configuration Agent Information Summary	ration option. OpenSSO Configurator n Option Step 2: Server Settings Confirm the following settings to use for the server. Server Settings Server URL https://cucmsso1.vrajo Cookie Domain Platform Locale en_US Configuration Directory /root/opensso Previous Next Cto countries subject to	Indicates required field	
Done					🔒 F110% 🦑

Click on next button,





Select OpenSSO User Data Store radio button and click Next,

Under Site Configuration, check the Yes radio button and enter a name for sitename and provide the loadbalancer URL (which was setup in section 3.1) and click on Next button.

Example for Loadbalancer URL: https://ssoloadbal.vrajoli.com:8443/opensso

🔮 OpenSSO - Mozilla Firefox				
C X 🏠 🖓 C	m ht	tps://cucmsso1.vrajoli.	.com:8443/opensso/config/options.htm 🖧 🚽 🚼 – Google	P
1 OpenSSO *				
Co	onfiç leas	guration Option	IS Java	*
De			OpenSSO Configurator	
En the the	Cus	stom Configuratio	on Option	
da	1.	General	Step 5: Site Configuration 🕫	
pa be or	2.	2. Server Settings O No	Will this instance be deployed behind a load balancer as part of a site configuration?	
Cr	3.	Configuration Store	Yes Indicates required field	
	4.	User Store	Site Configuration Details	
Sun Microsystems, Inc., 4150 Netv erved. Sun Microsystems, Inc. ha	+	Site Configuration	This is the first instance of OpenSSO, and no site configurations currently exist. To create a new site configuration, provide the following information	
ed in the product that is described ellectual property rights may includ l/patents and one or more additior	6.	Agent Information	* Site Name vrajoliamsfo ZOK	
puntries. U.S. Government Rights Microsystems, Inc. standard licens ments. Use is subject to license te parties. Sun, Sun Microsystems, t egistered trademarks of Sun Micro rks are used under license and a al, Inc. in the U.S. and other count cture developed by Sun Microsys ntries, exclusively licensed throug-	7.	Summary	* Load Balancer URL https://ssoloadbal.vra	
lled by U.S. Export Control laws a Nuclear, missile, chemical biologic direct or indirect, are strictly prohi	oitec	d. Export or reexport	Previous Next Cancel	
entities identified on U.S. export e	xclus	sion lists, including	, but not limited to, the	▼
< Dono	_			A E1100/ 48
Done				1110.40 - 46

🔮 OpenSSO - Mozilla Firefox			
🕢 🕞 C 🗙 🏠 🗋 vrajol.com https://d	/cucmsso1.vrajoli.com:8443/opensso/config/options.htm	ය - 👪 -	Google 🔎
1 OpenSSO *			
La Configura Please se De En Custom the da 1. Ger pa be 2. Ser or Set or 3. Cor Set or 3. Cor Set or 3. Cor Set 5. Site Cor 4. Use 5. Site Cor 5. Site Sun Microsystems, Inc. standard licens T. Sun Site Other Cor Site Other Cor Site Site Site Other Cor Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Site Si	ation Options elect a configuration option. OpenSSO n Configuration Option neral rver titings nfiguration ore enfiguration ent ormation mmary ent confirm Password • • • •	Configurator It User PopenSSO policy agents for retrieving policy * Indicates required field IAccessAgent] ••••••••••••••••••••••••••••••••••••	/ agent
cture developed by Sun Microsys htries, exclusively licensed throug- iled by U.S. Export Control laws a	Previous Next		Cancel

Create password for Default Policy Agent and click Next button,



Click on Create Configuration button.

Click on Proceed to Login link.





You will be presented with OpenAM login page.

16.2.3.2 Installation of OpenAM Enterprise server 2

Browse the OpenAM URL: <u>https://cucmsso2.vrajoli.com:8443/opensso</u>, you will see the below Configurator. Click on Create New Configuration under Custom Configuration.



🥹 OpenSSO - Mozilla Firefox			
C X 🏠 🗋 vrajol.com https://cucms	so2.vrajoli.com:8443/opensso/config/options.htm	값 + 🛂 - G	oogle 🔎
1 OpenSSO *			
Custom Configurat General Server Settings Configuration Store	Configuration Options OpenSSO Configurator ion Option Step 1: General ^C Enter the password for the default user, an characters in length. If this configuration w password you enter must match that of the o		
4. User Store 5. Site Copyright © 200 U.S.A. All rights technology emb limitation, these http://www.sun.d U.S. and in othe subject to the Si FAR and its sup developed by th are trademarks All SPARC trade SPARC Internat based upon arct U.S. and other d covered and controlled by U.S. Export in other countries. Nuclear, missile, ch	Default User Password Default User [amAdmin] * Password * Confirm Password • Confirm Password Previous Next Control laws and may be subject to the export emical biological weapons or nuclear maritime	Cancel or import laws end uses or	
Done			🔒 F110% 🛷

Create a password for default user [amAdmin] and click on Next button,

Click on Next button,

🥹 OpenSSO - Mozilla Firefox				
C X 🏠 🗋 vrajol.com https://cucmsso	o2.vrajoli.com:8443/opensso/config/opti	ons.htm	☆ → 🛃 – Google	P
1 OpenSSO *				
Custom Configuration Custom Configuration Custom Configuration Server Settings Copyright © 200 U.S.A. All rights technology emb limitation, these http://www.sunc U.S. and in othe Subject to the Si FAR and its sup developed by th are trademarks of All SPARC trade SPARC Internat	Configuration Op OpenSSO (on Option Step 2: Server Settings Confirm the following settings to Server Settings * Server URL * Cookie Domain * Platform Locale * Configuration Directory	tions Configurator o use for the server. * Indi https://cucmsso2.vrajoli.com en_US /root/opensso	icates required field	
based upon arcl U.S. and other c	Previous Next		Cancel	
covered and controlled by U.S. Export C	Control laws and may be subject t	to the export or import laws		
Done				🔒 F110% 🛷

Check 'Add to Existing Deployment' radio button and enter the OpenAM Enterprise server 1 URL under Server URL text box and click on Next button.

NOTE: Before this, you need to import the OpenAM Enterprise server 1 certificate to the OpenAM Enterprise Server 2's trust store.



Under Site Configuration, check the 'Yes' radio button and enter a site name which should be same as the one which was used in OpenAM Enterprise server 1. Click Next button.

Enter the Load Balancer URL which was setup in section 3.1, example: https://ssoloadbal.vrajoli.com:8443/opensso

Click on Create Configuration button.



Click on Proceed to Login link.



16.2.3.3 Configure OpenSSO Enterprise for Session Failover

Access <u>https://cucmsso1.vrajoli.com:8443/opensso</u> from a web browser.

Login to OpenAM Enterprise console.

Click the Configuration tab.

Under Global properties, click Session.

Under Secondary Configuration Instance, click New.

In the Add Sub Configuration page, provide the following information. Name Select External Session Store User Enter **msgquser** Session Store Password Enter **m5gqu5er** Session Store Password (confirm) Enter **m5gqu5er** Maximum Wait Time Keep the default value of 5000. Database URL Enter **cucmsso1.vrajoli.com:7777,cucmsso2.vrajoli.com:7777**. This is theMessage Queue broker address list. Enter multiple values using a comma and no space. Click Add. Click Save.

Log out of the OpenSSO Enterprise console.

16.3 Configuring SSO on Cisco Unified Communications Manager with AMSFO setup

Access Load Balancer URL (<u>https://ssoloadbal.vrajoli.com:8989</u>) from the web browser, Click the Lock icon on the right bottom corner, click on view certificate button. Go to Details tab and export the certificate to your local machine from where you are browsing.

Since there is a replication setup running on all the OpenSSO Enterprise servers in AMSFO environment, Policies, Authentication Module instances and J2EE Agents created on one OpenSSO Enterprise server, gets replicated on rest OpenSSO Enterprise servers.

For the Authentication module instance, you need to create a keytab for load balancer host and not for the OpenSSO Enterprise server hosts. Place the load balancer keytab file on both the OpenSSO Enterprise host filesystem.

Create OpenAM Policies, Authentication Module instance and J2EE agent profile on any one of the OpenSSO Enterprise server, for creating policies, Authentication module instance and J2EE agent profile refer to section 10.1, 10.2 and 10.3

Logon to CUCM OS Administration page; go to Security \rightarrow Certificate Management \rightarrow Upload certificate.

Select certificate type as tomcat-trust, and browse for the above load balancer certificate which you saved in the above step, after browsing click on upload button.

Now Logon to command line interface of CUCM 8.5, and execute the command 'utils sso enable' with OpenSSO URL as your Load Balancer host (<u>https://ssoloadbal.vrajoli.com:8443/opensso</u>).