

White paper version: 13.0 Date: 24th February 2015 AUTHORS: Bhavya Natarajan Krishna Chalamasandra

A COMPLETE GUIDE FOR THE INSTALLATION, CONFIGURATION, AND INTEGRATION OF OPEN ACCESS MANAGER WITH CISCO UNIFIED COMMUNICATIONS MANAGER 8.5/8.6 AND ABOVE, CISCO UNITY CONNECTION 8.6 AND ABOVE , AND ACTIVE DIRECTORY FOR SINGLE SIGN-ON

Table of Contents

Ρ	reface	
1	Introduction	
2	Configuring Domain Controller on Windows 2003 Server	
3		
4		
5	Brief History of OpenSSO and OpenAM	
6	• · · · · · · · · · · · · · · · · · · ·	
	6.1 OpenAM Installation on Linux Platform	
	6.2 OpenAM Installation on Windows Platform	
7		
	7.1 Installation and configuration of Apache Tomcat on Linux platform	
_	7.2 Installation and Configuration of Apache Tomcat on Windows Platform	
8		
9		
	9.1 Deploying OpenSSO Enterprise War on Apache Tomcat over Linux platform	
	9.2 Deploying OpenSSO Enterprise War on Apache Tomcat over Windows Platfor	m
	27	~-
10		
	10.1 Configuring Policies on OpenSSO Server	.31
	10.1.1 Configuring Policies on OpenSSO Server for Cisco Unified Communications	
	Manager 8.5, 8.6	
	10.1.2 Configuring Policies on OpenSSO Server for Cisco Unity Connection 8.6	
	10.2 Configuring Windows Desktop SSO Authentication Module Instance	
	10.3 Configuring J2EE Agent Profile on OpenSSO Server	.46
	10.3.1 Configuring J2EE Agent Profile on OpenSSO Server for Cisco Unified Communications Manager 8.5, 8.6	10
	10.3.2 Configuring J2EE Agent Profile on OpenSSO Server for Cisco Unity Connection	
	8.6 51	ווכ
1.	1 Undeploying/Removing OpenSSO Enterprise (OpenAM)	55
•	11.1 Uninstalling OpenSSO Enterprise (OpenAM) Server Deployed on Linux Platfo	
	11.2 Uninstalling OpenSSO Enterprise (OpenAM) Server Deployed on Windows	
	Platform	.55
12	2 Configuring Browser/Registry for SSO	
	12.1 Internet Explorer	
	12.2 Mozilla Firefox	
	12.3 Configuring Windows Registry for RTMT SSO	
	12.4 SSO Configurations Test with Browser	.57
13	3 Configuring SSO on Cisco Unified Communications Manager 8.5	. 58
	13.1 Unified CM 8.5 SSO CLI Commands	. 59
	13.1.1 utils sso enable	59
	13.1.2 utils sso disable	60
	13.1.3 utils sso status	60
14	4 Configuring SSO on Cisco Unified Communications Manager 8.6	.60
	14.1 Unified CM 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	
1		
	15.1 Cisco Unity Connection 8.6 SSO CLI Commands	
	15.1.1 utils sso enable	
	15.1.2 utils sso disable	66

15.1.3 utils sso status	15
15.2 Cisco Unity Connection 8.6 SSO GUI	
OpenSSO Enterprise Session Failover	16 Op
	16.1
16.2 Configuration of AMSFO components	16.2
16.2.1 Installation and Configuration of Load Balancer	16
16.2.1.1 Installation of Load Balancer on Linux Platform	
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	16
16.2.2.1 Configuration of Session Failover Components on Linux Platform	
16.2.2.2 Configuration of Session Failover Components of Windows Platform	
16.2.3 Installation and configuration of OpenAM Enterprise Servers for Session Failover	16
98	
16.2.3.1 Installation of OpenAM Enterprise Server 1	
16.2.3.2 Installation of OpenAM Enterprise Server 2104	
16.2.3.3 Configure OpenSSO Enterprise for Session Failover	
16.3 Configuring SSO on Cisco Unified Communications Manager with AMSFO Setup	16.3
107	

Preface

This document covers the installation and configuration of all the required software that is essential for achieving a Single Sign-On solution with Cisco Unified Communications Manager 8.5/8.6 and Cisco Unity Connection 8.6. Here is a brief picture of coverage in each chapter.

Chapter 1: This chapter contains a brief introduction to the products that 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 set up 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 previously set-up domain controller. Skip this chapter if your desktop is already a domain computer of the domain controller that is under test.

Chapter 5: This chapter contains a brief introduction to 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 the Linux and Windows Platform that is set up in 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 uninstalling 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 OpenSSO Server, OpenSSO Enterprise session failover can be implemented. This chapter explains how to configure OpenSSO Enterprise session failover. Ignore this chapter if you do not wish to have OpenSSO session failover.

1 Introduction

This document covers the installation and configuration of the required software components that are essential for achieving a Single Sign-On (SSO) solution with Cisco Unified Communications Manager 8.5/8.6 and Cisco Unity Connection 8.6.

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

- Microsoft Windows 2003 server with SP2—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—For OpenAM deployment
- Microsoft Windows 2003 Server—For OpenAM deployment
- Windows XP with SP3—Client Desktop

Note: If you are planning to 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 **Run**, type **dcpromo**, and then click **Enter**.

The Active Directory Installation Wizard appears. Click Next.

Active Directory Installation	Wizard	×
	Welcome to the Active Directory Installation Wizard This wizard helps you install Active Directory services on this server, making the server a domain controller.	
	If this is the first time you have installed Active Directory, it is recommended that you first read the overview in <u>Active</u> <u>Directory Help</u> . To continue, click Next.	
	< Back Cancel	

In the following window, you get a warning about compatibility issues with other Operating Systems. Improved security settings in Windows Server 2003 affect older versions of Windows.

After reading and evaluating the consequences, click Next.

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 secure way.	more
Some older versions of Windows, including Windows 95 and Windows NT 4.0 SP3 earlier, do not meet these requirements. Similarly, some non-Windows systems, inclu 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

In the next window, you see 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 an existing domain.

Select the first option, "Domain controller for a new domain," and click Next.

Active Directory Installation Wizard
Domain Controller Type Specify the role you want this server to have.
 Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain? <u>Domain controller for a new domain</u> Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain. Additional domain controller for an existing domain Additional 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

In the next window, you get three options:

1) The first option is to set up the domain in a new forest. Select this option if this is the first domain controller in your organization, or if you want it to be totally independent of any forest.

- 2) The second option is to create a new child domain in an existing domain tree. Select this option if you want the domain to be a child domain from an existing domain.
- 3) The third option is to create a domain tree in an existing forest. If you do not want any of the above, select this option.

In our case, choose the first option, "Domain in a new forest," and click Next.

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 <u>C</u> hild 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 the next window, type the full DNS name for the new domain (for example, "vrajoli.com") and click **Next**.

Active Directory Installation Wizard		X
New Domain Name Specify a name for the new domain.		2
Type the full DNS name for the new domain (for example: headquarters.example.microsoft.co	om).	
Eull DNS name for new domain:		
vrajoli.com		
	< <u>B</u> ack <u>N</u> ext > Cancel	

In the next window, you will see the Domain NetBIOS name field. This is the name that users of earlier version of Windows will use to identify the new domain.

Choose the Domain NetBIOS name, and click Next.

Active Directory Installation Wiz	ard	×
NetBIOS Domain Name Specify a NetBIOS name for t	he new domain.	
	earlier versions of Windows will use to identify the the name shown, or type a new name.	new
Domain NetBIOS name:	VRAJOLI	
	< <u>B</u> ack <u>N</u> ext >	Cancel

In the next window, you can choose the location where you want to store the database and log files. For best performance, store them on separate disks.

Choose the location where you want to store the Active Directory database and logs, and click **Next**.

Active Directory Installation Wizard	×
Database and Log Folders Specify the folders to contain the Active Directory database and log file	s 😪
For best performance and recoverability, store the database and the log hard disks.	i on separate
Where do you want to store the Active Directory database?	
Database folder:	
C:WINDOWS/NTDS	B <u>r</u> owse
Where do you want to store the Active Directory log? Log folder:	
C:\WINDOWS\NTDS	Browse
< <u>B</u> ack	Cancel

The Shared System Volume window appears. Here, choose the location where you want to store the SYSVOL folder. This folder contains the domain public files and is 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.	X
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> Car	cel

In the next window, the DNS registration diagnostics appear. Here, you will likely see the message **Diagnostic Failed.**

You have three options.

- 1) "I have corrected the problem. Perform the DNS diagnostic test again."
- 2) "Install and Configure the DNS server on this computer..."

Allow the Active Directory wizard to install and configure DNS for you, and use this DNS as the primary DNS for this server.

3) "I will correct the problem later by configuring DNS manually"

Bypass this window if you plan to correct the problem later on.

Choose option two, "Install and configure DNS server on this computer, and set this computer to use this DNS server as its preferred DNS server," and click **Next**.

	Registration Diagnostics /erify DNS support, or install DNS on this computer.
l	Diagnostic Failed
ŀ	The registration diagnostic has been run 1 time.
1	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.
I	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.
¢	I will correct the problem later by configuring DNS manually. (Advanced)

In the next window, choose what type or permissions you want for users and group objects. Here you have two options:

1) Permissions compatible with pre-Windows 2000 server operating systems

Select this option if you run server programs with a version of Windows earlier than Windows 2000.

2) Permissions compatible only with Windows 2000 or Windows 2003 Server operating systems

Select this option if you only run Windows Servers 2000 and Windows Servers 2003 on your domain.

Select the second option, "Permissions compatible only with Windows 2000 or Windows 2003 Server operating systems," and click **Next**.

Active Directory Installation Wizard	×
Permissions Select default permissions for user and group objects.	Ş
 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 or Windows Server 2003 operating systems that are members of pre-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 Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain. 	
< <u>B</u> ack <u>N</u> ext > Cancel	

In the next window, 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.

Type your chosen password, and click Next.

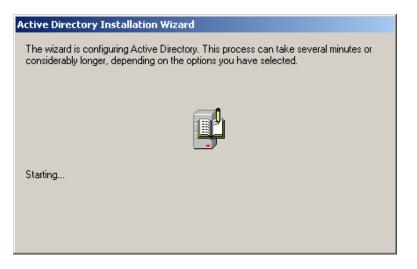
tive Directo	ry Installation Wi	zard			×
-	Directory Services Restore Mode Administrator Password This password is used when you start the computer in Directory Services Restore Mode.				
	d confirm the passwo is server is started in				unt used
	ore mode Administral The passwords for		norona nom ar	e aemann ranning	1.01.01
Restore	Mode <u>P</u> assword:	•••••	•		
<u>C</u> onfirm	password:	•••••	•		
For mor	e information about D	irectory Service	s Restore Moc	le, see <u>Active Dire</u>	ectory Help.
			< <u>B</u> ack	Next >	Cancel

Next, you see the summary of all the options you have chosen in the Active Directory wizard. Remember, the domain administrator account password is the same as the current local administrator password.

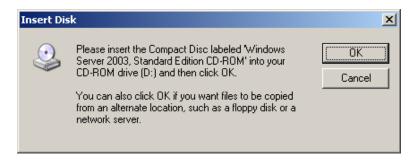
Click Next.

Active Directory Installation Wizard	×
Summary Review and confirm the options you selected.	R
You chose to:	
Configure this server as the first domain controller in a new forest of domain trees.	
The new domain name is vrajoli.com. This is also the name of the new forest.	
The NetBIOS name of the domain is VRAJOLI	
Database folder: C:\WINDOWS\NTDS Log file folder: C:\WINDOWS\NTDS SYSVOL folder: C:\WINDOWS\SYSVOL	
The DNS service will be installed and configured on this computer. This computer will be configured to use this DNS server as its preferred DNS server.	
To change an option, click Back. To begin the operation, click Next.	
< <u>B</u> ack <u>N</u> ext > Cance	;I

The Active Directory installation begins.



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



Installation of DNS server begins.

Windows Setup Installing DNS Server	×	
Configuring Components Setup is making the configuration changes you requested.		
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		
- Real Marts		
< <u>B</u> ack. <u>N</u> ext >		

Then, the wizard configures Active Directory.



The following window appears.

Click Finish.

Active Directory Installation Wizard		
	Completing the Active Directory Installation Wizard	
	< Back. Finish Cancel	

Click **Restart Now** to restart the computer.

Active Directory Installation Wi	zard	×
Windows must be restarted before t Directory Installation wizard take eff		
<u>Bestart Now</u>	Don't Restart Now	

Active Directory is now installed.

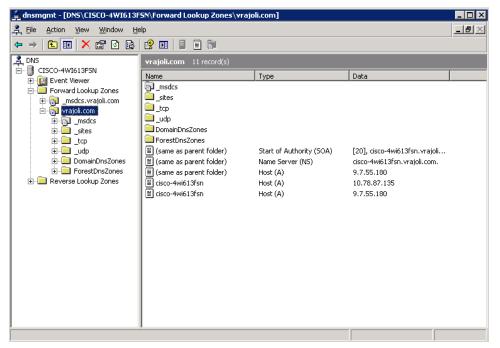
Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

3 Configuring DNS on Windows 2003 Server Domain Controller

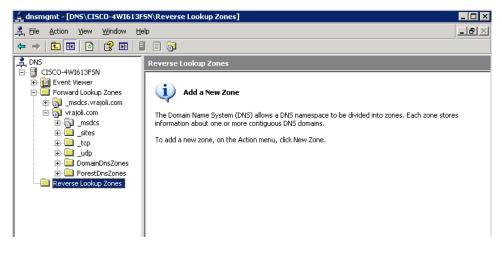
DNS is installed along with Active Directory configuration, only the configuration must be done on the DNS Server.

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

The following window appears. In the Forward Lookup Zones, you see the domain controller configured.



Now you must create the Reverse Lookup Zone. Right-click on Reverse Lookup Zones and click **New Zone**.



The following window appears. Click Next.



The Zone Type window appears. 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:
 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 <u>A</u> ctive Directory (available only if DNS server is a domain controller)
< <u>B</u> ack Next > Cancel Help

You are asked to configure a Reverse Lookup Zone name. Enter the network ID and then click **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. Ngtwork 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.
C Reverse lookup zone name: 85.78.10.in-addr.arpa For more information on creating a reverse lookup zone, click Help.
< <u>B</u> ack Cancel Help

Select the type of dynamic updates that DNS Zone accepts. Click **Allow only Secure dynamic updates** and then click **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. < Back

When the following window appears, you have successfully completed the new zone creation.

New Zone Wizard			×
	Completing the New Zone Wizard		
	You have success specified the follow	fully completed the New Zone Wizard. You wing settings:	
	Name:	85.78.10.in-addr.arpa	
	Туре:	Active Directory-Integrated Primary	
	Lookup type:	Reverse	
		now add records to the zone or ensure ipdated dynamically. You can then verify sing nslookup.	
	To close this wizar	d and create the new zone, click Finish.	
	< <u>B</u> ack	Finish Cancel Help	

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 use Windows XP desktop for joining 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**.

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

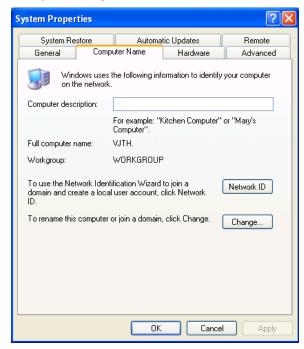
Make a DNS entry for this Client desktop. Open the DNS utility on domain controller (**Administrative Tools > DNS**), in the forward lookup zone, create a new host under the domain name (vrajoli.com). Click the check box to create associated reverse pointer. Verify that Client desktop host was added to DNS.

Vijeth	
Internet Mozilla Firefox E-mail Microsoft Office Outlook	 ➢ My Documents ☑ My Recent Documents ➢ My Pictures
C:: Command Prompt	📂 My Music
Run VNC Server	Open My Ne Explore
	Search Manage
Real-Time Monitoring Tool 8.5	Set Pr Defau Disconnect Network Drive
Microsoft Office Excel 2003	Show on Desktop Rename
Notepad	Help a Properties
All Programs 🕨	Search
	Log Off 🚺 Shut Down

Right-click **My Computer > Properties**.

Go to Computer Name tab and click on the **Change** button.

Change the computer name.



Click the **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."

Click **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

Click the Domain radio button then put in your domain name, not including the extension (in this example we use 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:
VJTH
Full computer name: VJTH.vrajoli.com
More
Member of
O Domain:
Vidui
O Workgroup:
WORKGROUP
OK Cancel

Then you will be presented with a username and password prompt. Enter the username and password of a domain administrator.

Click **OK**

Computer Name C	hanges 🛛 🛛 🔀
Enter the name and p to join the domain.	assword of an account with permission
User name:	🔮 administrator 🛛 🔽
Password:	•••••
	OK Cancel

After a minute or two, you receive a message welcoming you to the domain. Click **OK**.

Computer Name Changes 🛛 🛛 🔀						
(į)	omain.					
	ок					

Then you receive a message telling you that a restart is required; click **OK** to restart.

Computer Name Changes						
(į)	You must restart this computer for the changes to take effect.					
	ОК					

The procedure is complete. You now know 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 on to itself (which *will* use the local info) to logging on to the domain.

To change to logging on to the domain, press **Ctrl-Alt-Del**, and then click the **Options** button in the logon window. Then select the domain from the drop-down box.

Log On to Wi	ndows	
Copyright © 1985-2 Microsoft Corporatio		Microsoft
User name:	vijeth	
Password:		
Log on to:	VRAJOLI	
	ENG VJTH (this computer)	
	VRAJOLI	
	OK Cancel Shut Down	Options <<

After these steps, 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 a DNS entry for this host on the above DNS setup.

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

- Configure DNS and domain name, which should point to the above configured AD and DNS setup.
- Install JAVA on this machine. The latest version of JAVA can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html. The latest version of JAVA as of September 13, 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 <u>http://java.sun.com/products/archive/j2se/6u20/index.html</u>.
- 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 is installed and configured in 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 are prompted to input certain requests. When prompted to "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. The latest version of JAVA can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/index.html. The latest version of JAVA as of September 13, 2010 is JDK 6 Update 21.
- **Note:** The latest version of java (JDK 6 Update 21) has some issue with Kerberos; please visit http://forums.sun.com/thread.jspa?threadID=5448003 to know more.
- You can use JDK 6 Update 20, which can be downloaded from <u>http://java.sun.com/products/archive/j2se/6u20/index.html</u>.
- Create java keystore, which is required for enabling SSL on Tomcat, which is installed and configured in section 7.2.
- Open the command prompt and execute the following command. In this test setup, JAVA is 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 the OpenAM server that was set up 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 making the 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 warns you. Instruct the browser to import the

certificate and proceed. You should then see the little Tomcat logo. If you do, Tomcat is configured.

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 that was created in section 6.2, in this test it was created under C:\keystore) and **keystoreType**. Because 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 making the 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 warns you. Instruct the browser to import the certificate and proceed. You should then see the little Tomcat logo. If you do, Tomcat is configured.

8 Provisioning Active Directory for Single Sign-On

- Log on 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 hostname should not include the domain name.
- Create a keytab file on the AD server using the following 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 the keytab file, copy the keytab file to a 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

• Go to the ForgeRock site <u>http://www.forgerock.org/openam.html</u> and download the stable release of any OpenAM version supported.

Tomcat Versions supported:	TomcatV6, TomcatV7
OpenAM Versions supported:	OpenAM 9.5.4, OpenAM 10.0

- Copy the openam .war file to OpenAM server on any location and unzip it.
- Stop the Tomcat service if it is running on this OpenAM server.

- After unzipping, copy the file named opensso.war or openam.war 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

• Go to the ForgeRock site <u>http://www.forgerock.org/openam.html</u> and download the stable release of any OpenAM version supported.

Tomcat Versions supported:	TomcatV6, TomcatV7
OpenAM Versions supported:	OpenAM 9.5.4, OpenAM 10.0

- Copy the openam .war file to OpenAM server on any 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 > Services > Apache Tomcat 7 > Start

10 Configuring OpenSSO Enterprise Using the GUI Configurator

OpenAM server and policy agents require FQDNs for the hostname 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 hostnames either, because this 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 (https://vrajlnx.vrajoli.com:8443/opensso). When you access OpenSSO Enterprise for the first time, you are directed to the Configurator to perform the OpenSSO Enterprise initial configuration.

The Configuration Options window appears when you access the OpenSSO for the first time.

Select the configuration option:

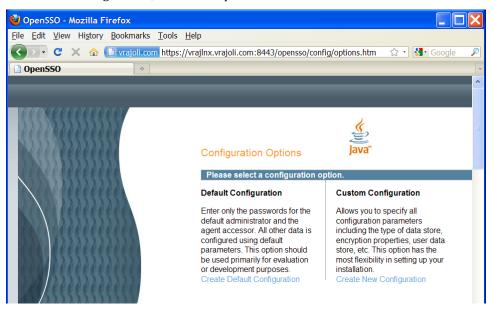
• **Default Configuration:** You specify and confirm passwords for the OpenSSO Enterprise administrator (amAdmin) and the default policy agent user (UrlAccessAgent), which is the policy agent user that connects to OpenSSO Enterprise server. The Configurator uses default values for the other configuration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

Use the 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.

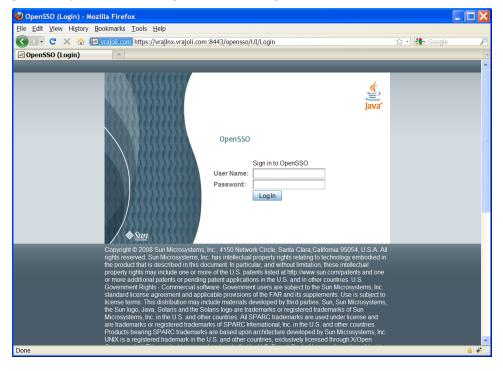
Also, check the web container log files and the install.log, which if created, will be in the configuration directory (default /opensso). These logs might contain information about the cause of a configuration problem.

By default, OpenSSO is deployed under /root/opensso directory on Linux platform; on Windows platform OpenSSO is deployed under C:\opensso.

Click **Proceed** to log in.

😡 OpenSSO - Mozilla Firefox					
File Edit View History Bookmarks Tools Help					
C X 💀 🖪 vrajol.com https://vrajinx.vrajol.co	om:8443/opensso/co	onfig/options.htm		合・ 🚮・ Google	P
C Loading +					
Configuration Options	Java"				
Default Configuration C		OpenSSO Configurator	×		
Enter only the passwords for the A	CONTRACTOR DATA AND A STREET				
default administrator and the apert accessor. All other data is configured using default parameters. This option should be be used primary for evaluation or development purposes in Create Default Configuration	Use this option fi and agent user n parameter password	or a quick setup. Only the supe ame are required. All other co Configuration Complete			
	Passw Co	onfiguration Complete!	Паок		
licrosystems, Inc., 4150 Network Circle, Santa Clara California 9505 rosystems, Inc. has intellectual property rights relating to technology e	Pito	ceed to Login			
Ibed in this document. In particular, and without limitation, these intelle de one or more of the U.S. patents listed at http://www.sun.com/paten	Default Honcy	Alleurfouwccessylleur			
ts or pending patent applications in the U.S. and in other countries. U mmercial software. Government users are subject to the Sun Microsy			BOK		
nent and applicable provisions of the FAR and its supplements. Use is button may include materials developed by third parties. Sun, Sun, Min ins and the Solaris logo are trademarks or registered trademarks of U.S. and other countries. All SPARC trademarks are used under loc ered trademarks of SPARC filtemational. Inc. in the U.S. and other of the deta data marks of SPARC filtemational. Inc. in the U.S. and other of the set of the	Confirm Pase	sword			
Tered trademarks of SHARC International, Inc. In the U.S. and other co. IC trademarks are based upon architecture developed by Sun Micros Jernark in the U.S. and other countries, exclusively licensed through X		uration	Cancel		
C Transfording data from writing writed now					>

The following window appears. Log in to the OpenSSO server with the amAdmin username and password you created during the default configuration.



Go to Access Control tab and click on / **(Top Level Realm)**, then go to the Authentication tab as shown below.

Click the **All Core Settings** button.

😢 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>H</u> el	2					
C 🗙 🏠 🐨 🕻	rajlnx.vrajoli.com:8443/op	pensso/realm/Realm	Properties?Real	mProperties.t 🏠	- 🛃 - Google	P
🖬 1 OpenSSO 🔅						-
VERSION					LOG	OUT HELP
User: amAdmin Server: vrajlnx.vrajoli.com						<u>«</u>
OpenSSO						lava"
						Sun [™] Microsystems, Inc.
General Authentication Servic	es Data Stores	Privileges	Policies	Subjects	Agents	
/ (Top Level Realm)						
(Top Level Realm) - Authentication			S	ave Reset	Back to A	ccess Control
 Core × Authentication 0 	Chaining					
Module Instances	2 Maining					
Core						
All Core Settings						
Organization Authentication Configur	ation: IdapService	e 🕶				
Administrator Authentication Configuration: IdapService V						
Default Success Login URL						
Current Values /opensso/conso	le <u> </u>	love				
•						

Set the User Profile to **Ignored**. Click the **Save** button to save the configuration.

🥹 OpenSSO - Mozilla Firefox				
<u>E</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		/		
🔇 🖸 C 🗙 🏠 🔚 vrajoi.com https://vrajlnx.vra	joli.com:8443/opensso/authentication/AuthProper	ties	☆ - Kar Google	P
5 1 OpenSSO ÷				-
VERSION			LOG OUT	HELP ^
User: amAdmin Server: vrajlnx.vrajoli.com				۵.
OpenSSO				Java
			Sun™M	icrosystems, Inc.
Core		Save Re	eset Back to Authe	ntication
Realm Attributes				
User Profile:	 ○ Dynamic ○ Dynamic with User Alias ④ Ignored ○ Required 			
Administrator Authentication Configuration:	 [empty] ● IdapService 			
User Profile Dynamic Creation Default Roles				
Current Values	Remove			•
Done			é	🔓 F110% 🛷

10.1 **Configuring Policies on OpenSSO Server**

Configuring Policies on OpenSSO Server for Cisco Unified 10.1.1 **Communications Manager 8.5, 8.6**

- Log in to OpenSSO server with amAdmin username and password
- Enable ssoadm tool from UI

Go to Configuration-> Servers and Sites -> click on the listed server name.

ser: amAdmin - Sei					
	_	_	_	_	_
Common Tasks	Access Contro	Federation	Web Services	Configuration	Sessions
Authentication	Console Sy	stem Globa	Servers and S	litee	

Servers and Sites

Default Server Settings								
Servers (1 Item(s))	Servers (1 ltem(s))							
New Delete Clone								
🗵 🗄 Server Name		۵	Site Name 🛆					
https://openaminx.cucmsso.com:8443/openam								
Sites (0 Item(s))								
New Delete								
Site Name	Primary URL	Assigned Servers						
There are no sites.								

Click on Advanced tab. Now add Advance Properties

VERSION						LOG OUT
_	_	_	_		_	
General	Security	Session	SDK	Directory Configuration	Advanced	

Edit https://openaminx.cucmsso.com:8443/openam

Edit h	ttps://openaminx.cucmsso.com:8443/openam	Save	Reset	Back to Servers and Sites					
Adva	Idvanced Properties (10 Item(s))								
Add.	Add Delete								
	Property Name		Property Value						
	com.iplanet.am.lbcookie.value		01						
	com.iplanet.security.SSLSocketFactoryImpl		com.sun.identity.shared.ldap.factory.JSSESocketFa						
	com.sun.embedded.replicationport								
	com.sun.embedded.sync.servers		on						
	com.sun.identity.common.systemtimerpool.size		3						
	com.sun.identity.sm.sms_object_class_name		com.sun.identity.sm.ldap.SMSEmbeddedLdapObje						
	com.sun.identity.urlconnection.useCache		false						
	opensso.protocol.handler.pkgs								
	org.forgerock.embedded.dsadminport		4444						

add Advance Properties ssoadm.disabled = false

VERSION						LOG OUT
Open AM	1					
General	Security	Session	SDK	Directory Configuration	Advanced	

Edit https://openamlnx.cucmsso.com:8443/openam

Save Reset Back to Servers and Sites

Adva	Advanced Properties (10 Item(s))							
Add.	Add Delete							
	Property Name	Property Value						
	com.iplanet.am.lbcookie.value	01						
	com.iplanet.security.SSLSocketFactoryImpl	com.sun.identityshared.ldap.factory.JSSESocketFa						
	com.sun.embedded.replicationport							
	com.sun.embedded.sync.servers	on						
	com.sun.identity.common.systemtimerpool.size	3						
	com.sun.identity.sm.sms_object_class_name	com.sun.identity.sm.ldap.SMSEmbeddedLdapObje						
	com.sun.identity.urlconnection.useCache	false						
	opensso.protocol.handler.pkgs							
	org.forgerock.embedded.dsadminport	4444						
	ssoadm.disabled	false						

• Browse for <u>https://<host FQDN>:8443/opensso/ssoadm.jsp</u> link

select sub-command "add-attrs"

```
add-agent-to-grp
      Add agents to a agent group.
add-amsdk-idrepo-plugin
      Create AMSDK IdRepo Plug-in
add-app-priv
      Add an application privilege to delegate resources of a given
       application.
add-attr-defs
      Add default attribute values in schema.
add-attrs
      Add attribute schema to an existing service.
add-auth-cfg-entr
      Add authentication configuration entry
add-cot-member
      Add a member to a circle of trust.
add-member
      Add an identity as member of another identity
add-plugin-interface
      Add Plug-in interface to service.
add-plugin-schema
       Add Plug-in schema to service.
```

Give value as Service Name= iPlanetAMWebAgentService , Schema Type=policy ,Attribute Schema XML =

```
<ServicesConfiguration>
<Service name="iPlanetAMWebAgentService" version="1.0">
  <Schema
   i18nFileName="amWebAgent"
   i18nKey="iplanet-am-web-agent-service-description">
    <Policy>
     <AttributeSchema name="PUT"
       type="single"
       syntax="boolean"
       uitype="radio"
       i18nKey="PUT">
       <IsResourceNameAllowed/>
       <BooleanValues>
         <BooleanTrueValue i18nKey="allow">allow</BooleanTrueValue>
         <BooleanFalseValue i18nKey="deny">deny</BooleanFalseValue>
       </BooleanValues>
     </AttributeSchema>
     <AttributeSchema name="DELETE"
       type="single"
       syntax="boolean"
       uitype="radio"
       i18nKey="DELETE">
       <IsResourceNameAllowed/>
       <BooleanValues>
         <BooleanTrueValue i18nKey="allow">allow</BooleanTrueValue>
         <BooleanFalseValue i18nKey="deny">deny</BooleanFalseValue>
```

```
</BooleanValues>
</AttributeSchema>
</Policy>
</Schema>
</Service>
</ServicesConfiguration>
```

Back to main page.	
Sub Command, add-att	trs
	a to an existing service.
Service Name*:	iPlanetAMWebAgent
Schema Type*:	
ochenna Type .	policy
Attribute Schema XML*:	
Autoute ochema Ame .	<service name="jPlanetAMWebAgentService" version="1.0"></service>
	<schema< th=""></schema<>
	i18nFileName=" <mark>amWebAgent</mark> "
	i18nKey="iplanet-am-web-agent-service-description">
	<policy> </policy>
	type="single"
	syntax="boolean"
	uitype="radio" i18nKey="PUT">
	<booleanvalues></booleanvalues>
	< <u>BooleanTrueValue</u>
	i18nKey="allow">allow"/BooleanTrueValue> <booleanfalsevalue< th=""></booleanfalsevalue<>
	i18nKey="deny">deny
	<del dtributeSchema> <attributeschema <="" name="DELETE" th=""></attributeschema>
	type="single"
	syntax="boole an"
	uitype="radio"
	i18nKey="DELETE"> sResourceNameAllowed/
	<booleanvalues></booleanvalues>
	< <u>BooleanTrueValue</u>
	i18nKey="allow">allow <booleanfalsevalue< th=""></booleanfalsevalue<>
	i18nKey="deny">deny
Name of sub schema:	
	Submit Reset

• Restart Tomcat.

Go to Access Control tab and click on / (Top Level Realm). The following window appears.

🕹 OpenSSO - Mozilla	a Firefox					
<u>File E</u> dit ⊻iew Histo	ory <u>B</u> ookmarks <u>I</u>	ools <u>H</u> elp				
🕢 🖓 - C 🗙 🍕	👌 🗷 vrajoli.com	https://vrajlnx.v	rajoli.com:8443/op	oensso/task/Home?ł	Home.tabCom	mon.TabHref=1&jato.paç 🏠 🔹 🚮 🛛 Google 🛛 🔎
OpenSSO	+					-
VERSION						LOG OUT HELP
User: amAdmin Server OpenSSO	r: vrajlnx.vrajoli.com					ر بن این Java
Common Tasks	Access Control	Federation	Web Services	Configuration	Sessions	Sun [®] Microsystems, Inc.
A realm is the unit that C defined within the realm configuration data.	OpenSSO uses to or . The top level realm	ganize configura i is created when	tion information. Au 1 you deploy OpenS	thentication properti SO. The top level re	es, authorizati 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))	ocuren					
New Delete						
🗷 🗉 Realm Name					🔺 Locati	on 🔬
/ (Top Level Rea	alm)				1	
Done						≙ *

Go to the Policies tab and add a new policy; enter the PolicyName.

🕙 OpenSSO - Mo	zilla Firefo	ĸ						
<u>F</u> ile <u>E</u> dit <u>V</u> iew ⊦	Hi <u>s</u> tory <u>B</u> ook	marks <u>T</u> ools	<u>H</u> elp					
🔇 🔊 - C 🗙	🏠 🗷 vra	ajoli.com http:	s://vrajlnx.vrajol	i.com:8443/op	ensso/policy/	PolicyNormal A	Add	😭 🔹 🚷 🖌 Google 🖉
OpenSSO		÷						-
VERSION								LOG OUT HELP
User: amAdmin Se	erver: vrajlnx.vr	ajoli.com						<u>«</u>
OpenSSO								(j) Java
			_		_			Sun [®] Microsystems, Inc.
General Auth	nentication	Services	Data Stores	Privileges	Policies	Subjects	Agents	
/ (Top Level Realm)								
(Top Level Realm)								Back to Access Control
*	Sea	rch						
Policies (0 Item(s	s))	_	_		_	_	_	
New Policy	New Referral.	Delete						
Name		Pro	tected Resourc	es				
There are no polic	ies.							
Done								🔒 🏶 g

Create a new rule from the Policy Configuration window.

In the window that appears, 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 is CUCMUser application URL (https://<CUCM FQDN>:8443/*).

Check the GET , POST , PUT and DELETE check boxes and then click Finish.

🕑 OpenSSO - Moz	zilla Firefox								
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi	<u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp								
😮 🔄 C 🗙 🏠 🔚 vrajoli.com https://vrajlnx.vrajoli.com:8443/opensso/policy/SelectServiceTyr 🗘 🗉 🚺 Google 🛛 🔎									
S OpenSSO *									
VERSION LOG OUT HELF									
User: amAdmin Server: vrajlnx.vrajoli.com									
OpenSSO			iava"						
			java Sun" Microsystems, Inc.						
Step 2 of 2: New	Rule		Back Finish Cancel * Indicates required field						
* Service Type:	URL Policy Agent								
* Name:	CUCMUser								
* Resource Name:	https://vrajolicucm1.vrajoli.com	n:8443/*							
Actions									
* 0									
	actions are required.								
Actions (4 Item(s))									
Action V DELETE	A	Allow							
GET		O Deny							
		 Allow Deny 							
POST		 Allow Deny 							
PUT		 Allow Deny 							
Done			🔒 F110% 🖑						

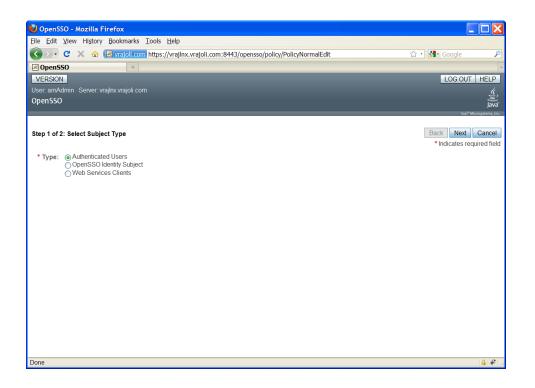
Create another rule for the requests involving query patterns (*?*) in Find and List windows of CUCMUser application.

🕑 Ope	nSSO - M	ozilla Firefox				
<u>F</u> ile <u>E</u> d	it <u>V</u> iew I	Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp				
< >	- C ×	☆ State of the	oli.com:8443/opensso/po	olicy/SelectServiceTyr 🏠 🚽	- Google	P
🐻 Ope	nSSO	÷				-
VERS	SION				LOG OUT	HELP
User: a	mAdmin	Server: vrajlnx.vrajoli.com				k
Opens	550					java"
					Sun [™] Mi	java icrosystems, Inc.
Step 2	of 2: Nev	w Rule			Back Finish * Indicates requ	Cancel uired field
* Service URL Policy Agent Type:						
* Na	me:	CUCMUser_QueryPatterns				
	source	https://vrajolicucm1.vrajoli.com:84	43/*?*			
Nam	e:					
Action	S					
* On	e or more	e actions are required.				
Acti	ons (4 Item)					
	Action DELETE	A	Allow			
			© Deny			
	GET		 Allow Deny 			
	POST		Allow			
	PUT		 Deny Allow 			
			© Deny			
Done					🔒 F1	110% 🦑 🛒

From Cisco Unified Communications Manager Release 8.6, SSO support is provided for RTMT application as well. To achieve SSO for RTMT, along with the above policy rules, you should create one more new rule for requests involving RTMT query patterns (*?*?*).

🔮 Ope	nSSO - Mo	ozilla Firefox				. 🗆 🗙		
<u>F</u> ile <u>E</u> d	lit <u>V</u> iew H	li <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp						
< >	- C X	☆ majoli.com https://vrajlnx.vraj	oli.com:8443/opensso/p	olicy/SelectServiceTyr 🏠 ·	Google	P		
🖬 Ope		*				-		
VERS	SION				LOG OUT	HELP		
User: a	User: amAdmin Server: vrajlnx.vrajoli.com							
Open	SSO					j Java		
					Sun [™] Mi	java icrosystems, Inc.		
Step 2	of 2: New	/ Rule			Back Finish * Indicates req	Cancel uired field		
* Se Type	rvice e:	URL Policy Agent						
* Na	me:	CUCMUser_QueryPatterns]				
	source	https://vrajolicucm1.vrajoli.com:84	43/*?*?*					
Nam	ie:							
Action	IS							
* On	e or more	actions are required.						
	ons (4 Item(s				_			
	Action		Value					
	DELETE		 Allow Denv 					
	GET		Allow Deny					
	POST		 Allow Deny 					
	PUT		 Allow Deny 					
Done					🔒 F1	10% 🦑 🕺		

Click the **New** button under Subjects on the Policy Configuration window. Select subject type as **Authenticated Users**.



Enter the Subject Name and Click Finish.

(Optional) If 443 re-director port is used to access CUCM web applications

Create a new rule from the Policy Configuration window.

In the window that appears, select service type as **URL Policy Agent (with resource name)**.

Enter the Rule Name and Resource URL as Web Application URL https://<CUCM:FQDN>/*.

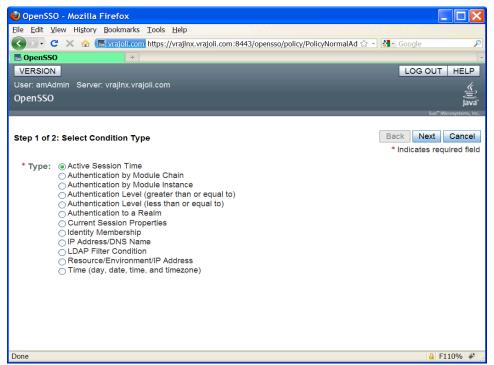
Check the **GET**, **POST**, **PUT** and **DELETE** check boxes and then click **Finish**.

Repeat the same steps for creating two more policies with Web Application URL https://<CUCM:FQDN>/*?* and https://<CUCM:FQDN>/*?*?*.

In our case, policies mentioned below needs to be created.

https://vrajolicucm1.vrajoli.com/* https://vrajolicucm1.vrajoli.com/*?* https://vrajolicucm1.vrajoli.com/*?*?* Now Policy is created with defining Rules and Subjects.

Click the **New** button under Conditions. Under select condition type, select **Active Session Time** and then click **Next**.



Configure active session timeout as 120 minutes.

🔮 OpenSSO - Mozilla Firefox		
Eile Edit View History Bookmarks Tools	Help	
🔇 🗵 - C 🗙 🏠 🜆 vrajoli.com https://	/vrajlnx.vrajoli.com:8443/opensso/policy/PMDefaultSessio 🏠 🕤	- Google 🔎
🖬 OpenSSO +		-
VERSION		LOG OUT HELP
User: amAdmin Server: vrajlnx.vrajoli.com		<i>.</i>
OpenSSO		Java"
		Sun [™] Microsystems, Inc.
		Bask Fisish Coursel
Step 2 of 2: New Condition - Active Ses	sion Time	Back Finish Cancel
		* Indicates required field
* Name:	CUCMUser	
* Maximum Session Time (minutes):	120	
* Terminate Session:	No 🛩	
Done		🔒 F110% 🖑 🚛

10.1.2 Configuring Policies on OpenSSO Server for Cisco Unity Connection 8.6

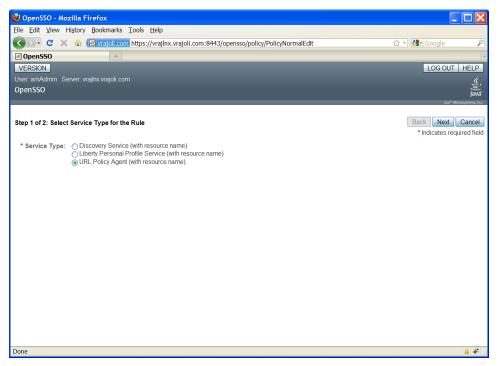
Log in to OpenSSO server with amAdmin username and password. Go to Access Control tab and click on / **(Top Level Realm)**. The following window appears.

🕹 OpenSSO - Mozilla Firefox								
Elle Edit View History Bookmarks Iools Help								
🄇 💴 C 🗙 🏠 🔄 vrajoli.com https://vrajinx.vrajoli.com:8443/opensso/task/Home?Home.tabCommon.TabHref=1&jato.paç 🏠 🕂 🚼 - Google 📃								
OpenSSO *								
VERSION		LOG OUT HELP						
User: amAdmin Server: vrajlnx.vrajoli.com		(e)						
OpenSSO		Java						
Common Tasks Access Control Federation	Web Services Configuration	Sun" Microsystems, Inc						
Common Tasks Access Control Pederation	web services Conniguration	35310113						
		erties, authorization policies, data stores, subjects and other data can be realm is the root of the OpenSSO instance and contains OpenSSO						
Realms								
* Search								
Realms (1 item(s))								
New Delete								
🗷 🗄 Realm Name		Location						
/ (Top Level Realm)		1						
Done		ê *						

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

🕘 OpenSS(🕑 OpenSSO - Mozilla Firefox 📃 🗌 🔀							
<u>F</u> ile <u>E</u> dit ⊻	/iew Hi <u>s</u> tory <u>B</u> ook	kmarks <u>T</u> ools	Help					
	3 🗙 🏡 🗷 vra	ajoli.com http:	s://vrajlnx.vrajoli	.com:8443/ope	ensso/policy/	PolicyNormalA	dd	🏠 • 🚺• Google 🔎
🗷 OpenSS	D	+						-
VERSION]							LOG OUT HELP
	min Server: vrajlnx.vi	rajoli.com						<u>(</u>)
OpenSSO								Java
								Sun" Microsystems, Inc.
General	Authentication	Services	Data Stores	Privileges	Policies	Subjects	Agents	
/ (Top Level I	Doalm)							
	Realm) - Policies							Back to Access Control
*	Sea							Dack to Access Control
		ich						
Policies (0			_	_	_	_	_	
New Polic	y New Referral.							
Name There are r		Pro	tected Resource	es				
There are r	to policies.							
Done								a * .
2 Since								🖬 🔻 🔡

Create a new Rule from the Policy Configuration window. The following window appears. Select service type **URL Policy Agent (with resource name)**.



Then create rules for Cisco Unity Connection application(s) with below resource URLs 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. The following window shows OpenSSO Policy configured for Cisco Unity Connection server.

🔮 OpenSSO -	Mozilla Firefox							
<>> · C	🗙 🏠 🖬 vrajol.co	m https://vrajlnx	.vrajoli.com:8443/op	ensso/policy/Policy?	Policy.tblSearch	☆ - 🚷 - Goo	gle	P
Some OpenSSO	÷							-
VERSION						LC		ELP
User: amAdm	nin Server: vrajlnx.v	rajoli.com						<u>«</u> ,
OpenSSO								Javaï
							Sun [™] Microsyst	ems, Inc.
General	Authentication	Services	Data Stores	Privileges	Policies	Subjects	Agents	
(Top Level F	Policies (26 - 26 of 26)							
🗵 🗄 Nam	ie 🔺	Protected R	esources					
UCSSO https://ucsso238.vrajoli.com/8443/*?* http://ucsso238.vrajoli.com/** https://ucsso238.vrajoli.com/*?* http://ucsso238.vrajoli.com/?* http://ucsso238.vrajoli.com/**								
H Pa	age: 2 of 2	Go						
	1							
Done							🔒 F1	10%

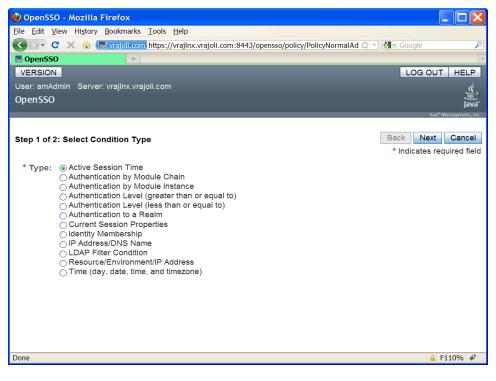
Click the **New** Button under Subjects on the Policy Configuration window. Select subject type **Authenticated Users**.

🥹 OpenSSO - Mozilla Firefox	
Elle Edit View History Bookmarks Tools Help	
🕢 🕞 🕻 🗙 🔬 🔣 vrajoli.com https://vrajlnx.vrajoli.com:8443/opensso/policy/PolicyNormalEdit	☆ • 🚷 Google 🖉
OpenSSO *	
VERSION	LOG OUT HELP
User: amAdmin Server: vrajinx.vrajoli.com	٤,
OpenSSO	Java
	Sun [™] Microsystems, Inc.
Step 1 of 2: Select Subject Type	Back Next Cancel
	* Indicates required field
* Type: Authenticated Users	
OpenSSO Identity Subject Web Services Clients	
Dana	i i i i i i i i i i i i i i i i i i i
Done	🗎 🛷 📑

Enter the Subject Name and click **Finish**. Now Policy is created with defining Rules and Subjects.

😢 OpenSSO - Mozilla Firefox	
🔇 🗁 C 🗙 🏠 🗔 vrajol.com https://vrajhx.vrajol.com:8443/opensso/policy/PMAuthenticatedUse	er 🟠 🔹 🛃 🖌 Google 🛛 🔎
s OpenSSO *	
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
Step 2 of 2. New Subject - Authenticated Users	* Indicates required field
* Name: UCSSO	
Exclusive:	
Done	∂ F110% .:
Duile	🖬 F110%

Click the **New** button under Conditions. Under select condition type, select **Active Session Time** and then click **Next**.



Configure active session timeout as 120 minutes.

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

🥹 OpenSSO - Mozilla Firefox		
🔇 🗩 C 🗙 🏠 🗔 vrajol.com https://vr	ajlnx.vrajoli.com:8443/opensso/pol	icy/PMDefaultSessionCon 😭 🕤 🚷 🖌 Google 🖉
Solution OpenSSO *		
VERSION		LOG OUT HELP
User: amAdmin Server: vrajlnx.vrajoli.com		<u>(</u>
OpenSSO		Java
		Sun [™] Microsystems, Inc.
Step 2 of 2: New Condition - Active Ses	sion Time	Back Finish Cancel
		* Indicates required field
* Name:	UCSSO	
* Maximum Session Time (minutes):	120	
* Terminate Session:	No 💌	
Done		🔒 F110% 🛒

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 Chapter 8.
- Log in to the OpenSSO Enterprise administration console as amAdmin.
- Go to Access Control > Default Realm > Authentication.
- On the Module Instances window, 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.
- On the Module Instances window, 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.
- o Return Principal with Domain Name: False
- Authentication Level: 22
- Restart the OpenSSO Enterprise server.

🥹 OpenSSO - Mozilla Firefox				
<u>File Edit View History Bookmarks Tools Help</u>				
🔇 🔍 C 🗙 🏠 🚮 vrajol.com https://v	rajlnx.vrajoli.com:8443/opensso/authentication/AuthPrope	rties?AuthPrope 🏠	- Google	P
🖬 1 OpenSSO 🔅				-
VERSION			LOG	OUT HELP
User: amAdmin Server: vrajlnx.vrajoli.com				<u>k</u> .
OpenSSO				Java
				Sun" Microsystems, Inc.
		Save Re	eset Back to A	Authentication
Windows Desktop SSO		Save Ite	Back to P	amentication
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 Re	eset Back to A	Authentication
Done				🔒 F110% 🖑 🛒

10.3 Configuring J2EE Agent Profile on OpenSSO Server

10.3.1 Configuring J2EE Agent Profile on OpenSSO Server for Cisco Unified Communications Manager 8.5, 8.6

Perform the following task 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 in to OpenSSO Enterprise. Multibyte names are not accepted.

Note: While enabling SSO on Cisco Unified Communications Manager or Cisco Unity Connection, when prompted to "Enter the name of the profile configured for this policy agent," enter the above configured agent name.

• 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 prompted to "Enter the password of the profile name," enter the above configured password.

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

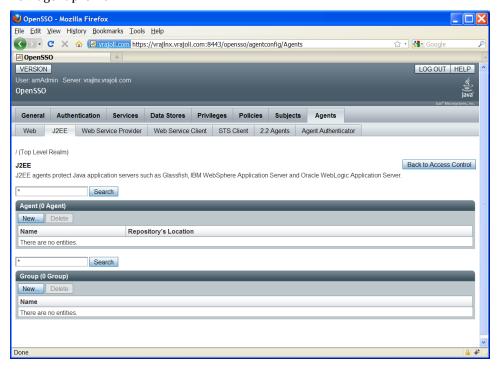
For example: https://<OpenAM FQDN>:8443/opensso

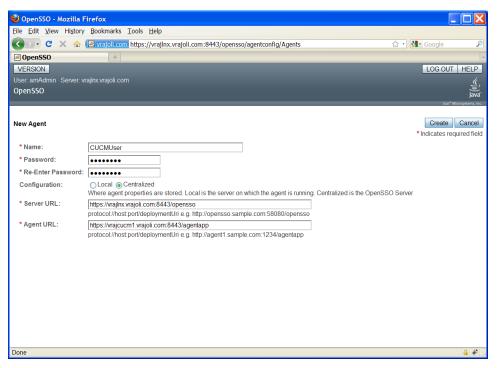
• In the Agent URL field, enter the URL for the agent application.

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

• Click Create.

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





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 Note :- For CUCM 10.0 and above, the URL is /ucmuser/dojo/entry/Login.jsp
- For Cisco UC Integration for Microsoft Office Communicator:

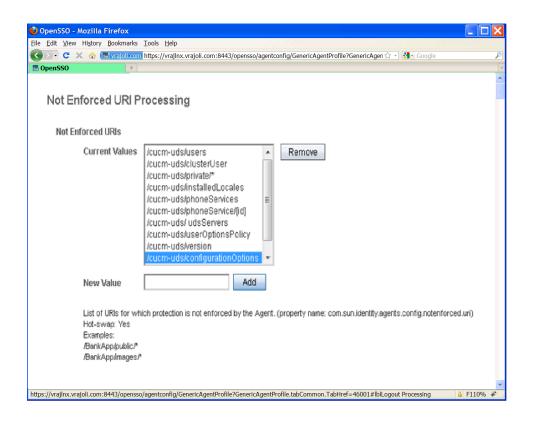
/cucm-uds/WEB-INF/pages/logon.jsp Starting from Cisco Unified Communications Manager Release 8.6, SSO support is provided for other applications like Cisco Unified CM Administration, Cisco Unified Serviceability, Cisco Unified Reporting, Cisco Unified OS Administration, Disaster Recovery System and RTMT along with Cisco Unified CM User Options and Cisco UC Integration for Microsoft Office Communicator. For these new applications, you must configure below Login Form URIs.

•	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	efox				
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u>	ookmarks <u>T</u> oo	ls <u>H</u> elp			
🔇 > - C 🗙 🏠 🌆	vrajoli.com http	s://vrajlnx.vrajoli.com:8443,	/opensso/agentconfig/	GenericAgentProfile?Ger	nericAgen 🏠 🔹 🛃 - Google 🖉
sa OpenSSO	+				
VERSION					LOG OUT HELP
User: amAdmin Server: v	rajlnx.vrajoli.c	om			ي ا
OpenSSO					Java
	_				Sun [™] Microsystems, Inc.
Global Applicatio	n SSO	OpenSSO Services	Miscellaneous	Advanced	
Edit CUCMUser					Save Reset Back to Main Page
Inheritance Settings	Export Confi	guration			
	× N	ot Enforced URI			
 Login Processing 	Pr	rocessing	 Response Att 	ributes Processing	 Privilege Attributes Processing
Logout Processing		ot Enforced IP rocessing	 Common Attri Processing 	butes Fetching	 Custom Authentication Processing
 Access Denied URI Processing 		ofile Attributes ocessing	 Session Attrib 	utes Processing	
Login Processing					
Login Form URI					
Current Values	/ccmuser/WF	B-INF/pages/logon.jsp	^ Remove		
		EB-INF/pages/logon.jsp			
			~		
New Value		Add			
https://vrajlnx.vrajoli.com:84	12/0000550/200		2Conoric A gont Drofile t	abCommon TabUrof-4	5001#lblLogout Processing 🔒 F110% 🖑

Click on **Not Enforced URI Processing** . Enter the following URI's for which authentication is not required in this section.

- /cucm-uds/users
- /cucm-uds/clusterUser
- /cucm-uds/configurationOptions
- /cucm-uds/installedLocales
- /cucm-uds/phoneServices
- /cucm-uds/phoneService/[id]
- /cucm-uds/ udsServers
- /cucm-uds/userOptionsPolicy
- /cucm-uds/version
- /cucm-uds/private/*



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								×
Eile <u>E</u> dit <u>V</u> iew	/ History <u>B</u> ookmar	ks <u>T</u> ools I	<u>1</u> elp						
🔇 > - C	🗙 🏠 🚮 vrajo	bli.com https:	//vrajlnx.vrajoli.com:8443/ope	nsso/agentconfig/Generi	AgentProfile?Generic	AgentProfile. 🕇	3 - 🚮 - G	ioogle	P
1 OpenSS	0	+							
VERSION]							LOG OUT HELP	1
User: amAdr	min Server: vrajl	nx.vrajoli.co	om						
OpenSSO								Juliana"	
								Sun [®] Microsystems, Inc.	
Global	Application	SSO	OpenSSO Services	Miscellaneous	Advanced				
									1
Edit CUCM	Jser					Save	Reset	Back to Main Page	
Inheritance	Settings	xport Confi	nuration						
	0								
	RL ≉ Policy C		e × Session Client						
		li com:8443	/opensso/UI/Login?modu			1			
_	ipolin majiniki majo		openeed, ev Legin mede		Move Up				
					Move Down]			
					Move to Top				
					Move to Bottor				
					Delete				
				*					
				Add					
Done								🔒 F110% 🐐	•
one								iii 110% 🏘	í.

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

10.3.2 Configuring J2EE Agent Profile on OpenSSO Server for Cisco Unity Connection 8.6

Perform the following task 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 in to OpenSSO Enterprise. Multibyte names are not accepted.

Note: While enabling SSO on Cisco Unified Communications Manager or Cisco Unity Connection, when prompted to "Enter the name of the profile configured for this policy agent," enter the above configured agent name.

 $\circ~$ 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.

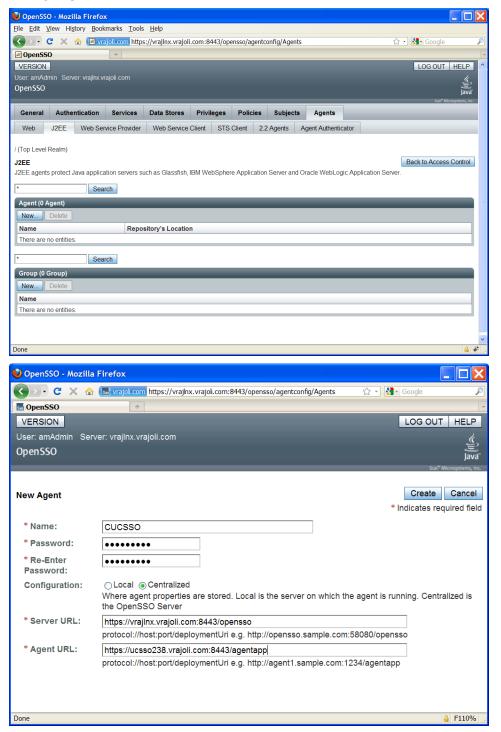
Note: While enabling SSO on Cisco Unified Communications Manager or Cisco Unity Connection, when prompted to "Enter the password of the profile name," enter the above configured.

- Reenter 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 window again with a link to the new agent profile.



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:

/cuadmin/WEB-INF/pages/logon.jsp /cuservice/WEB-INF/pages/logon.jsp

• For Cisco Unity Connection Serviceability:

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

- For Cisco Personal Communications Assistant:
- For Cisco Unity Connection Web Inbox:
- For Cisco Unified CM User option:
- For Cisco Unity Connection REST APIs:
- For Cisco UC Integration for Microsoft Office Communicator:
- 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):

/ciscopca/WEB-INF/pages/logon.jsp /inbox/WEB-INF/pages/logon.jsp

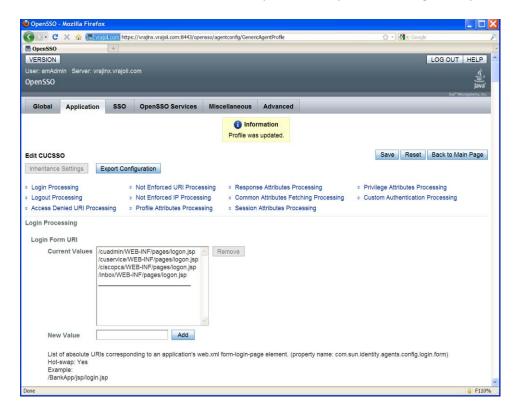
/ccmuser/WEB-INF/pages/logon.jsp

/vmrest/WEB-INF/pages/logon.jsp

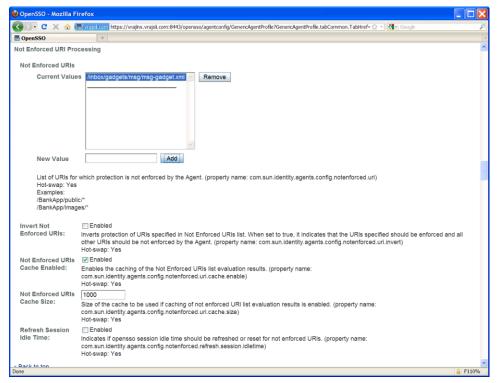
/cucm-uds/WEB-INF/pages/logon.jsp /ccmadmin/WEB-INF/pages/logon.jsp /ccmservice/WEB-INF/pages/logon.jsp /cucreports/WEB-INF/pages/logon.jsp /cmplatform/WEB-INF/pages/logon.jsp

- /drf/WEB-INF/pages/logon.jsp
- /ast/WEB-INF/pages/logon.jsp

Note :- In CUCM 10.0 and above, the URL for Cisco Unified CM User option is /ucmuser/dojo/entry/Login.jsp



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

🕢 - C X 🏤						
	🖌 🔚 vrajol.com https:	//vrajlnx.vrajol.com:8443/ope	ensso/agentconfig/GenericA	gentProfile?GenericAgentProf	le.tabCommon.TabHref= 🏠	- Google .
OpenSSO	4					
VERSION						LOG OUT HELP
	rver: vrajinx.vrajoli.co					<u>, (</u> ,
OpenSSO						Java
			I and the second se			Sun" Microsystems, Inc.
Global Appli	ication SSO	OpenSSO Services	Miscellaneous	Advanced		
dit CUCSSO					Sav	e Reset Back to Main Page
Inheritance Setting	s Export Confi	guration				
	Authentication Ser					
Logout URL =	Policy Client Service	se session Client	t Service			
ogin URL						
OpenSSO Login						
Selected:						
https://vra		/opensso/UI/Login?mod	ule=Harihara	Move Up		
https://vra		%opensso/UI/Login?mod		Move Up Nove Down		
https://vra		3/opensso/UI/Login?modi	N			
https://vra		3/opensso/UI/Login?mod	h N	Nove Down		
https://vra		i/opensso/UI/Login?modi	h N	Nove Down Nove to Top Dove to Botton		
https://vra		i/opensso/UI/Login?mod	h N	Nove Down		
https://vra		i/opensso/Ul/Login?mod	h N	Nove Down Nove to Top Dove to Botton		
https://vra		i/opensso/Ul/Login?mod		Nove Down Nove to Top Dove to Botton		
https://vra		Vopensso/UI/Login?mod	h N	Nove Down Nove to Top Dove to Botton		
	ıjinx.vrajoil.com:8443		Add	Move Down tove to Top over to Botton Delete		
OpenSSO Id Hot-swap; Y	ıjinx.vrajoil.com.8443 ogin page URL. (pro	Vopensso/UI/Login?mod	Add	Move Down tove to Top over to Botton Delete		
OpenSSO Ic Hot-swapi Y Example:	ıjinx.vrajoii.com:8443 ogin page URL. (pro fes	perty name: com.sun.ide	Add	Move Down tove to Top over to Botton Delete		
OpenSSO Ic Hot-swapi Y Example:	ıjinx.vrajoil.com.8443 ogin page URL. (pro	perty name: com.sun.ide	Add	Move Down tove to Top over to Botton Delete		
OpenSSO I: Hot-swap: Y Example: http://host.pr	ogin page URL. (pro res ort/opensso/Ul/Login	perty name: com.sun.ide	Add	Move Down tove to Top over to Botton Delete		
OpenSSO Ic Hot-swapi Y Example:	ogin page URL. (pro res ortopensso/Ul/Login [2] Enabled	perty name: com.sun.ide	Add ntity.agents.config.logi	Move Down towe to Top over to Bottor Delete	as defined in the OpenS	SO Login URL list. (property

11 Undeploying/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 configured 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/ apache-tomcat-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 > Services > Apache Tomcat 7 > Start**.

12 Configuring Browser/Registry for SSO

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

12.1 Internet Explorer

Steps to set up 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 > Internet Options > 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.
- In 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, for example, vrajoli.com.

12.3 Configuring Windows Registry for RTMT SSO

To achieve RTMT SSO, a new registry key '*allowtgtsessionkey*' of type *REG_DWORD* with value set to '*1*' should be created on desktop client (Windows XP/Windows 7) at below location corresponding the respective OS distribution.

Windows XP → HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\

Windows Vista/Windows 7 \rightarrow

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

12.4 SSO Configurations Test with Browser

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

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

• You should see the message "You're logged in" as shown in the following figure. This message indicates that the configurations you made are correct.

C OpenSSO - Windows Internet Explorer		
G S + https://vrajlnx.vrajoli.com:8443/opensso/base/A	MAdminFrame?iPl 💙 😵 Certificate Error 🛛 🗲 🗙 Live Sear	th 🛛 🔎 🔻
<u>Eile E</u> dit <u>V</u> iew F <u>a</u> vorites <u>I</u> ools <u>H</u> elp		With the second s
😪 🕸 🚮 OpenSSO		🖶 🔹 📴 Page 🔹 🎯 Tools 🔹 🎽
	Information You're logged in.	
	· · · · · · · · · · · · · · · · · · ·	

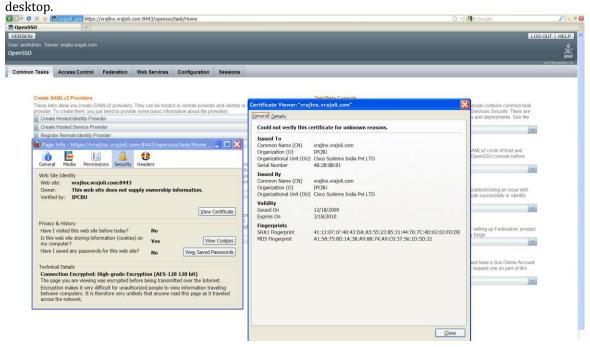
13 Configuring SSO on Cisco Unified Communications Manager 8.5

Before you enable SSO on Unified CM 8.5, you must complete the following steps:

- Log in to Cisco Unified Serviceability and activate Cisco DirSync service.
- Log in to Cisco Unified CM Administration, go to **System > LDAP > LDAP System**, check the **Enable Synchronizing from LDAP Server** check box 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 the **Perform Full Sync** button. Upon completion of directory sync, AD users are imported to Unified CM.
- On Cisco Unified CM Administration window, go to **User Management > End User**, verify all the AD users are available and LDAP Sync Status is Active.
- Associate respective User Groups to the end users and save.

Because we configure Unified CM to talk to OpenAM over HTTPS while enabling SSO, we must import OpenAM server certificate into CallManager tomcat-trust store before enabling the SSO on Unified CM.

To get the OpenAM server certificate, log in to OpenAM URL (https://<OpenAM FQDN>:8443/opensso), click the **Security** icon at the bottom right corner. Click the **Details** tab of Certificate Viewer window, click the **Export** button and save it your



After getting OpenAM server certificate, log on to Unified CM OS Administration window, go to **Security > Certificate Management**, and click the **Upload Certificate** button.

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

OpenAM server certificate has been added into the Unified CM Tomcat-trust store.

13.1 Unified CM 8.5 SSO CLI Commands

Three CLI command are available for managing SSO on Unified CM 8.5:

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

13.1.1 utils sso enable

Use this command to enable SSO-based authentication.

This command starts the wizard for enabling SSO on Unified CM. It asks for the following:

- OpenAM server URL
- Relative path for policy agent deployment
- Profile name configured for this policy agent on the AM server
- Password for the above
- 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

This command disables SSO-based authentication. No parameters are 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

This command provides the status of SSO on Unified CM 8.5. No parameters are required.

When SSO is disabled:

admin:utils sso status SSO Status: Disabled

When SSO is enabled:

```
admin:utils sso status
SSO Status: Enabled
Primary Open Access Manager (OpenAM) server URL: https://vrajlnx.vrajoli.com:8443/opensso
Profile name: CUCMUser
Login module name: CUCMUser
admin:
```

14 Configuring SSO on Cisco Unified Communications Manager 8.6

With Unified CM 8.6, SSO is extended to the following Unified CM applications along with CCMUser and Cisco UC Integration for Microsoft Office Communicator:

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

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

• RTMT

Before you enable SSO on Unified CM 8.6, you must complete the following steps:

- Log in to Cisco Unified Serviceability and activate Cisco DirSync service.
- Log in to Cisco Unified CM Administration, go to **System > LDAP > LDAP System**, check the **Enable Synchronizing from LDAP Server** check box 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 the **Perform Full Sync** button. Upon completion of directory sync, AD users are imported to Unified CM.
- On Cisco Unified CM Administration window, go to **User Management > End User**, and verify that all the AD users are available and LDAP Sync Status is Active.
- Associate respective User Groups to the end users and save. For an end user to access 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** and **Standard CCM Super Users** User Groups associated.

Because we configure Unified CM to talk to OpenAM over HTTPS while enabling SSO, we must import OpenAM server certificate into CallManager tomcat-trust store before enabling the SSO on Unified CM.

14.1 Unified CM 8.6 SSO CLI Commands

14.1.1 utils sso enable

This command enables SSO for the applications that you choose from the following list:

- 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 starts the wizard for enabling SSO on the Unified CM. It asks for the following:

- OpenAM server URL
- Relative path for policy agent deployment
- Profile name configured for this policy agent on the AM server
- Password for the above
- 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): 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.

14.1.2 utils sso disable

This command disables SSO for SSO-enabled options.

14.1.3 utils sso status

This command displays the list of SSO-enabled applications.

```
admin:utils sso status
SSO Status: Disabled
```

14.2 CUCM 8.6 SSO GUI

From Unified CM Release 8.6, SSO configurations (SSO enable/disable/status) are supported from GUI as well.

To configure SSO from GUI, log in to Cisco Unified OS Administration.

Go to **Security > Single Sign on** and you will see the following configuration window.

	gs ▼ Security ▼ Software Upgrades ▼ Services ▼ Help ▼	
50 Applicat	ions Configuration	
Save		
 Status		
🔥 Warning:C	hanging the SSO settings causes an immediate Tomcat restart	
Server Setti	ngs:	
Enter URL of t	he Open Access Manager(OpenAM) server*	
	tive path where the policy agent should be deployed*	
	ne of the profile configured for this policy agent*	
	sword of the profile name*	
Enter the logi	n module instance name configured for Windows Desktop SSO*	
Select Applie	cations	
	Application name	SSO Status
Select All		Disabled
Select All	Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)	
	Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) Cisco Unified CM User Options (CUCM End User options)	Disabled
		Disabled Disabled
	Cisco Unified CM User Options (CUCM End User options)	

For enabling SSO from GUI, the same parameters are requested as requested from CLI. All the inputs are validated before enabling SSO to a selected application. A check box is provided for selecting the application(s); check the check box to select the applications on which you want to enable SSO and then click **Save**. After successful validation of all the inputs, a popup window is displayed saying "Enabling/Disabling SSO for the applications will cause Tomcat to restart. Do you want to continue?" Click **OK** if you want to proceed or click **Cancel** to cancel.

To disable SSO-enabled application(s), uncheck the check box of the SSO-enabled application(s), then click **Save**. A popup window is displayed saying "Enabling/Disabling SSO for the applications will cause Tomcat to restart. Do you want to continue?" Click **OK** if you want to proceed or click **Cancel** to cancel.

15 Configuring SSO on Cisco Unity Connection 8.6

Before you enable SSO on Cisco Unity Connection 8.6, you must complete the following steps:

- Import users to Cisco Unity Connection either directly from LDAP server **OR** from Unified CM; however, users imported from Unified CM must first be imported from LDAP to Unified CM). Users must be configured with the appropriate roles to log in to Cisco Unity Connection Administration, or Cisco Unity Connection Serviceability.
- For a coresident and standalone Cisco Unity Connection server, user 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. Select **System Administrator** from the available roles, and add it to the user's Assigned Roles.

Because we configure Cisco Unity Connection to talk to OpenAM over HTTPS while enabling SSO, we must import OpenAM server certificate into CallManager tomcat-trust store before enabling the SSO on Cisco Unity Connection.

15.1 Cisco Unity Connection 8.6 SSO CLI Commands

There are three CLI command available for managing SSO on Cisco Unity Connection 8.6:

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

15.1.1 utils sso enable

This command enables SSO-based authentication. Cisco Unity Connection offers the 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 REST APIs
- Cisco Unity Connection PCA and Web Inbox
- Cisco Unity Connection Administration
- Cisco Unified Data Service (CUCiMOC)
- RTMT

This command starts the wizard for enabling SSO on Cisco Unity Connection. It asks for the following:

- OpenAM server URL
- Relative path for policy agent deployment
- Profile name configured for this policy agent on the AM server
- Password for the above
- 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): y List of apps for which SSO can be enabled 1) Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) 2) Cisco Unified Operating System Administration (CUCM OS Admin, DRF) 3) Cisco Unity Connection Rest APIs 4) Cisco Unity Connection PCA and Web Inbox 5) Cisco Unity Connection Administration 6) Cisco Unified Data Service (CUCiMOC) 7) RTMT 8) Cisco Unified CM User Options (Cisco Unified CM User options) 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 Operating System Administration (CUCM OS Admin, DRF) (yes/no):y Do you want to enable SSO for Cisco Unity Connection Rest APIs (yes/no):y Do you want to enable SSO for Cisco Unity Connection PCA and Web Inbox (yes/no):y Do you want to enable SSO for Cisco Unity Connection Administration (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 Do you want to enable SSO for Cisco Unified CM User Options (Cisco Unified CM User options) (yes/no):y

15.1.2 utils sso disable

This command disables SSO-based authentication. No parameters are required.

```
***** U 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 Operating System Administration (CUCM OS Admin, DRF)
3) Cisco Unity Connection Rest APIs
4) Cisco Unity Connection PCA and Web Inbox
5) Cisco Unity Connection Administration
6) Cisco Unified Data Service (CUCiMOC)
7) RTMT
8) Cisco Unified CM User Options (Cisco Unified CM User options)
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 Operating System Administration (CUCM OS Admin, DRF) (yes/no):y
Do you want to disable SSO for Cisco Unity Connection Rest APIs (yes/no):y
Do you want to disable SSO for Cisco Unity Connection PCA and Web Inbox (yes/no):y
Do you want to disable SSO for Cisco Unity Connection Administration (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
Do you want to disable SSO for Cisco Unified CM User Options (Cisco Unified CM User options) (yes/no):y
```

15.1.3 utils sso status

This command provides the status of SSO on Cisco Unity Connection 8.6. No parameters are required.

admin:utils sso status SSO Status: Disabled

15.2 Cisco Unity Connection 8.6 SSO GUI

To configure SSO from GUI, log in to Cisco Unified OS Administration. Go to **Security > Single Sign on**. The following configuration window appears.

	isco Unified Operating System Administration	Navigation Cisco Unified OS Administration			
r.			admin Search Documentation		
ihow 🔻 Setting	as ▼ Security ▼ Software Upgrades ▼ Services ▼ Help ▼				
SO Applicati	ons Configuration				
📄 Save					
_					
inter URL of th	ne Open Access Manager(OpenAM) server*				
inter the relati	ive path where the policy agent should be deployed*				
Enter the name	e of the profile configured for this policy agent*				
	word of the profile name*				
Enter the pass	word of the prome fighte				
	module instance name configured for Windows Desktop SSO*				
Enter the login	module instance name configured for Windows Desktop SSO*				
Enter the login Select Applic	module instance name configured for Windows Desktop SSO*	PEA Philus			
inter the login Relect Applic	module instance name configured for Windows Desktop SSO* ations Application name	SSO Status Disabled			
inter the login elect Applic Select All	module instance name configured for Windows Desktop SSO* ations Application name Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)	Disabled			
inter the login ielect Applic Select All	module instance name configured for Windows Desktop SSO* ations Application name Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) Cisco Unified Operating System Administration (CUCM OS Admin, DRF)	Disabled Disabled			
inter the login elect Applic Select All	module instance name configured for Windows Desktop SSO* ations Application name Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting)	Disabled			
elect Applic	module instance name configured for Windows Desktop SSO* ations Application name Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) Cisco Unified Operating System Administration (CUCM OS Admin, DRF) Cisco Unity Connection Rest APIs	Disabled Disabled Disabled			
enter the login	module instance name configured for Windows Desktop SSO* ations Application name Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) Cisco Unified Operating System Administration (CUCM OS Admin, DRF) Cisco Unity Connection Rest APIs Cisco Unity Connection PCA and Web Inbox	Disabled Disabled Disabled Disabled			
Enter the login Select Applic	module instance name configured for Windows Desktop SSO* ations Application name Cisco Unified CM Administration (CUCM Admin, CU Serviceability, CU Reporting) Cisco Unified Operating System Administration (CUCM OS Admin, DRF) Cisco Unity Connection Rest APIs Cisco Unity Connection PCA and Web Inbox Cisco Unity Connection Administration	Disabled Disabled Disabled Disabled Disabled			

For enabling SSO from GUI, the same parameters are requested as requested from CLI. All the inputs are validated before enabling SSO to a selected application. A check box is provided for selecting the application(s); check the check box to select the applications on which you want to enable SSO and then click **Save**. After successful validation of all the inputs, a popup window is displayed saying "Enabling/Disabling SSO for the applications will cause Tomcat to restart. Do you want to continue?" Click **OK** if you want to proceed or click **Cancel** to cancel.

In the following figure, SSO is enabled for all applications.

	Operating System Admini mmunications Solutions	stration			Nav	-	ed OS Administration
Show - Settings - Security - So	oftware Upgrades 👻 Services 👻 Help 👻						
SSO Applications Configuration							
Save							
Warning:Changing the SSO set	ttings causes an immediate Tomcat restart						
Server Settings:							
Enter URL of the Open Access Mana							
Enter the relative path where the po	Enter the relative path where the policy agent should be deployed* agentapp						
Enter the name of the profile config	ured for this policy agent*	unityuser					
Enter the password of the profile na	me*	*****					
Enter the login module instance nan	ne configured for Windows Desktop SSO*	unitymodule					
Select Applications							
Select All Application name			SSO Statu	IS			
_	Administration (CUCM Admin, CU Service	ability, CU Reporting)	Enabled				
-	Cisco Unified Operating System Administration (CUCM OS Admin, DRF)						
Cisco Unity Conr	Cisco Unity Connection Rest APIs						
Cisco Unity Conr	Cisco Unity Connection PCA and Web Inbox						
Cisco Unity Conr	Cisco Unity Connection Administration						
Cisco Unified Dat	Cisco Unified Data Service (CUCiMOC)						
RTMT	RTMT						
Cisco Unified CM	User Options (Cisco Unified CM User optio	ons)	Enabled				
- Save							

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 user's 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 services or session data are available to the Policy Agents.

16.1 Requirements for Access Manager Session Failover (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 servers. 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). After RHEL is installed, configure network settings and create an entry in DNS servers for this RHEL host. After 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</u> URL.

On the above download window, 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 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

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

|-1%-----25%------50%-----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. After the Windows OS is installed, configure network settings and create an entry in DNS servers for this host. After 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</u> URL.

On the above download window, 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. The accompanying figures show the default settings, which you can use during installation.

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-windows-i586

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

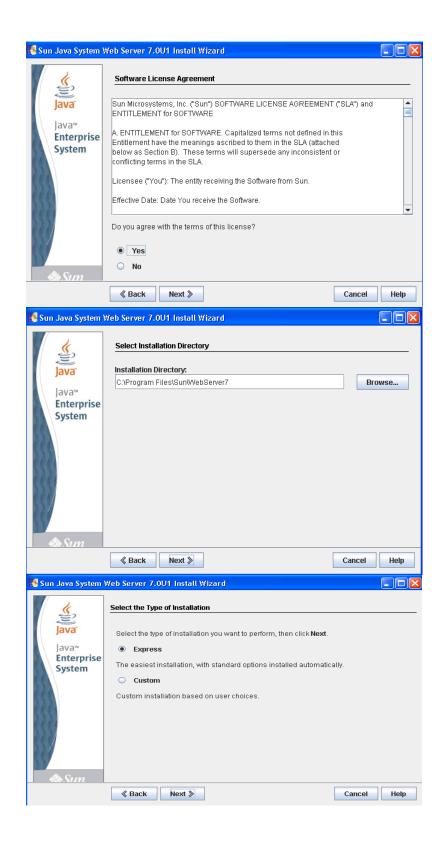
2 File(s) 21,354 bytes

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

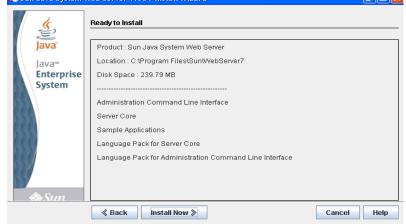
4 Dir(s) 8,806,412,288 bytes free

C:\	Documents and Settings [\]	Administrator	Desktop\sjsws-7	_0u1-windows-i58	6>setup.exe
-----	-------------------------------------	---------------	-----------------	------------------	-------------

🔣 Sun Java System N	Veb Server 7.0U1 Install Wizard
<u></u>	Welcome
Java ⁻	Welcome to the Sun Java System Web Server 7.0U1 installation wizard. This wizard is used to install the Web Server.
Java™ Enterprise System	
🐟 Sun	≪ Back Next ≫ Cancel Help
	South Next // Cancel Help



🅵 Sun Java System	Web Server 7.0U1 Install V	/izard						
<u>«</u>	Administration Server Settin	ngs						
Java	Choose a user name and password. You must remember this user name and password to administer the Web Server after installation.							
Java™ Enterprise	Administrator User Name admin							
System	Administrator Password	*****						
222	Retype Password	*****						
222								
RRRI								
559								
📣 Sun		,						
	≪ Back Next ≫		Cancel Help					
Sun Java System	Web Server 7 0111 Install W	lizard						



🕵 Sun Java System Web Server 7.0U1 Install Wizard Installation Complete Ś Java Installation Successful. Java™ Refer to the installation log file at: Enterprise C:\Program Files\Sun\WebServer7\setup\Sun_Java_System_Web_Server_install.log for System more details. Next Steps: 1. Start the Administration Server by executing: C:\Program Files\Sun\WebServer7\admin-server\bin\startserv 2. You can access the Administration Console by accessing the following URL: https://vrajoli-labxp.vrajoli.com:8989 Click Finish to exit the installation program. Finish

(al) Services (Local) Sun Java System Web Ser Administration Server				
Sun Java System Web Ser				
		Description Status	Startup Type	Log On As
Administration Server	OfficeScan NT Listener	Receives c Started	Automatic	Local System
Start the service	Service Contract Real Time Scan	Scans net Performs R Started	Manual Automatic	Local System Local System
	Performance Logs and Alerts	Collects pe	Manual	Network S
	Plug and Play	Enables a c Started	Automatic	Local System
	Portable Media Serial Number Service	Retrieves t Loads files Started	Manual Automatic	Local System Local System
	Protected Storage	Provides pr Started	Automatic	Local System
	Second Contract Contr	Provides n	Manual	Local System
	Remote Access Auto Connection Manager Remote Access Connection Manager	Creates a Creates a Started	Manual Manual	Local System Local System
	Remote Desktop Help Session Manager	Manages a	Manual	Local System
	Remote Packet Capture Protocol v.0 (experimental)	Allows to c Provides th Started	Manual	Local System
	🎭 Remote Procedure Call (RPC) 🎇 Remote Procedure Call (RPC) Locator	Manages t	Automatic Manual	Network S Network S
	Remote Registry	Enables re Started	Automatic	Local Service
	Removable Storage		Manual	Local System
	SafeNet Log Service	Offers rout Allows logg Started	Disabled Automatic	Local System Local System
	SafeNet Token Service	Token serv Started	Automatic	Local System
	SafeNet Virtual Channel Monitor	Required f Started	Automatic	Local System
	🎭 Secondary Logon 🎭 Security Accounts Manager	Enables st Started Stores sec Started	Automatic Automatic	Local System Local System
	Security Center	Monitors s	Automatic	Local System
	Server .	Supports fil Started	Automatic	Local System
	🍓 Shell Hardware Detection	Provides n Started Manages a Started	Automatic Automatic	Local System Local Service
	SolarWinds TFTP Server	SolarWinds	Manual	Local System
	SoundMAX Agent Service	Started	Automatic	Local System
	SSDP Discovery Service	Enables dis Started	Manual	Local Service
	🍓 Sun Java System Web Server 7.0 (https-vrajoli-labxp.vrajoli.com 🖏 Sun Java System Web Server 7.0 Administration Server		Manual Manual	Local System Local System
	System Event Notification	Tra Start	Automatic	Local System
	System Restore Service	Per Stop Pause	Automatic	Local System
	Task Scheduler	Ena	Automatic	Local System
	TCP/IP NetBIOS Helper	Ene Restart	Automatic Manual	Local Service Local System
	Telnet	En: All Tasks 🕨	Disabled	Local System
	Terminal Services	Alk	Manual	Local System
	🍓 Themes 🍓 Uninterruptible Power Supply	Pro	Automatic	Local System
	Supply Uninterruptible Power Supply	Ma Properties	Manual Manual	Local Service Local Service
	Who Server Version 4	Help	Automatic	Local System
	🖏 Volume Shadow Copy	Manages a	Manual	Local System
1	WebClient	Enables Wi Started	Automatic	Local Service
	min Console - Mozilla Firefox			
	//vrajoli-labxp.vrajoli.com:8989/admingui/admingui/serverTasksGeneral		☆ - 😫	 Google
iva(TM) System W * VERS	QN	_	HELP	1
660	REFERENCE			
222	000000000		<u>()</u>	
515	11111111111		Ě	
180			Java	
2.23	1888888888			
	Sun Java" System Web S	erver		
	Admin Console			
222	Server Name: vrajoli-lab	xp		
	User Name:			
100	Password:			
0.0.0		1		
	Log In			
	a a a a a a a a a a a a a a a a a a a			
	Seran			
	Sun.			
	nt © 2007 Sun Microsystems, Inc. All rights reserved. U.S.			
softwar	. Government users are subject to the Sun Microsystems,	Inc. standard license	agreement	
	licable provisions of the FAR and its supplements. Use is s			
	on may include materials developed by third parties. Sun, d Solaris are trademarks or registered trademarks of Sun №			
	untries. All SPARC trademarks or registered trademarks of Sun r			
	rks of SPARC International, Inc. in the U.S. and other cour			
	rk in the U.S. and other countries, exclusively licensed thro			

🔒 F110% 🧩 👷

Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

Done

16.2.1.3 Configuration of Load Balancer for HTTP Load Balancing

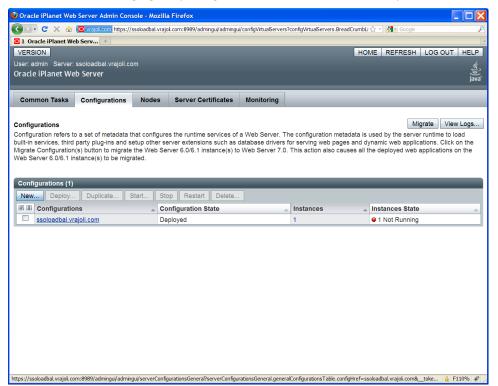
Browse the Load Balancer URL, https://ssoloadbal.vrajoli.com:8989; you will be presented with following login window. Log in to the admin console.



After login, the following window appears:

RSION						
					HOME REFR	ESH LOG OUT HELP
	soloadbal.vrajoli.co					<u>_</u>
acle iPlanet Web	o Server					Jav
ommon Tasks	Configurations	Nodes	Server Certificates	Monitoring		
ommon tasks	configurations	Noues	Server Certificates	wontoning		
Common Tas	ks					
To access infor	mation about a task	, select the "	i" info button. To understa	and the termino	logy, click here.	
				10.4		
Configuration					al Server Tasks	
Select Config	guration: ecoloadb	al vraioli.com		Se	elect Virtual Server: ecoloadbal vraioli c	om 💌 🗓
Edit Configur	ration			Ed	dit Virtual Server	
New Instance	Э		1	Ac	dd Web Application	
Start/Stop Ins	stances		i	Do	ocument Directories	i
Edit Java Se	ttings		1	C	GI Directories	1
Log Preferen	ices and Archival		1	UF	RL Redirects	1
Request Ser	ver Certificate		1	Se	etup Reverse Proxy	
Install Server	Certificate			Vi	ew Summary	
View Summa	ry					
New Configu	ration		1	Ne	ew Virtual Server	i
Migrate 6.0/6						
View Logs						
Documentation					luct Registration	
View Online	Documentation			Re	egister with Sun Connection	

Click the **Configurations** tab, and then click on the load balancer name (ssoloadbal.vrajoli.com) as shown in the following figure (Configurations > Load Balancer Name).



After you click on the load balancer name, the following window appears.



Click on the Load Balancer Name (ssoloadbal.vrajoli.com) under Virtual Servers.

The following window appears.

Configurations > ssoloadbal.vrajol.com > Virtual Servers > ssoloadbal.vrajol.com Server Settings Web Applications Content Handling WebDAV Search Access Control Summary
VERSION HOME REFRESH LOG OUT HELP User: admin Server: ssoloadbal.vrajoil.com Instance(s) Running 0 (4) Oracle iPlanet Web Server Instance(s) Stopped (1) (4) (4) Configurations > ssoloadbal.vrajoil.com > Virtual Servers > ssoloadbal.vrajoil.com (5) (5) (5)
User: admin Server: ssoloadbal.vrajoli.com Oracle iPlanet Web Server Configurations > ssoloadbal.vrajoli.com > Virtual Servers > ssoloadbal.vrajoli.com
Oracle iPlanet Web Server Instance(s) Stopped $_{\oplus}$ 1 Java Configurations > ssoloadbal.vrajoli.com > Virtual Servers > ssoloadbal.vrajoli.com
Configurations > ssoloadbal.vrajoli.com > Virtual Servers > ssoloadbal.vrajoli.com
Configurations > ssoloadbal.vrajoli.com > Virtual Servers > ssoloadbal.vrajoli.com
Server Settingen Web Applications Content Handling WebDAV Search Access Control Summany
Server Settings Web Applications Content Handling WebbAV Search Access Control Summary
General Log Preferences Monitoring Settings Request Limits
· · · · · · · · · · · · · · · · · · ·
ssoloadbal.vrajoli.com - Virtual Server General Properties Save
All virtual servers have one or more HTTP Listeners specified. When a new request comes in, the Server determines which virtual server to send it to based on the
configured HTTP Listener. You can associate HTTP Listeners from this page. Configure virtual server properties from this page.
s General s Quality of Service s P3P Settings
s HTTP Listeners s Localization s Variables
General
Name: ssoloadbal.vrajoli.com
Virtual Server: @Enabled
Document Root:/docs
Document root for the virtual server (Absolute path or path relative to the server's configuration directory)
Hosts: ssoloadbal.vrajoli.com
You can enter more than one URL host, separated by commas
a Back to top
HTTP Listeners
HTTP Listeners (1)
Add Delete
IP Address A Port SSL Description
http-listener-1 *[All IP Addresses] 8443 © Enabled
Done A F110% a

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

🕹 Edit HTTP Listener	- General Settings - Mozilla Firefox							
vrajoli.com https://ssolo	adbal.vrajoli.com:8989/admingui/admingui/vsGeneral?vsGeneral.vsGeneral	PropSheet 😭						
Edit HTTP Listener - General Settings Apply Close								
request to the configur Listeners. HTTP Lister You can use either IPv Listener that listens on	The Server accepts the HTTP requests via an HTTP Listener before forwarding the request to the configured Virtual Server. This page allows you to add and configure HTTP Listeners. HTTP Listeners must have a unique combination of port number and IP address. You can use either IPv4 or IPv6 addresses. Setting the IP address to "*" creates an HTTP Listener that listens on all IP addresses on that port.							
∗ General v Adva		and Codel						
	* Indicates requi	red field						
General								
Name:	http-listener-1 🔽 Enabled							
* Port:	8443							
	Port on which to listen							
* IP Address:	*							
	IP address, or * to listen on all IP addresses							
* Server Name:	ssoloadbal.vrajoli.com							
	Default Server Name							
* Default Virtual	ssoloadbal.vraioli.com 🗸	*						
Done	🔒	F110% 🖑						

Then click the **Content Handling** tab under **Configurations > ssoloadbal.vrajoli.com > Virtual Servers > ssoloadbal.vrajoli.com**.

In the Content handling tab, select the **Reverse Proxy** tab.

Click New.

🔮 Oracle iPl	lanet Web	Server Admin C	onsole	- Mozilla Firefox								
🔇 🔊 - C	X 🏠	🖸 vrajol.com http	s://ssolo	adbal.vrajoli.com:8989/adr	ningui/admingui/cor	tentURLForwardin	gs?con	tentURLForward	ings.vsTat 🏠	- 🛃 - Google		P
🖸 1 Oracle	iPlanet We	b Serv +										~
VERSION									HOME	REFRESH	LOG OUT	HELP
		ssoloadbal.vrajol	li.com							<u>∧</u> Deployme	nt Pending	<u> </u>
Oracle iPl	anet We	b Server								Instance(s) R		Java
										Instance(s) S	topped ᠾ 1	
Configuratio	ins > sso	loadbal.vrajoli.co	om > ∖	/irtual Servers > ssol	oadbal.vrajoli.co	m						
Server S	ettings	Web Applicati	ions	Content Handling	WebDAV	Search	Acc	ess Control	Summa	ry		
General	Docum	ent Directories	CGI	URL Redirects	Error Pages	Reverse Pro	ху	FastCGI	MIME Type	s		
ssoloadbal	.vrajoli.co	om - Reverse Pi	roxy									
			to be	a web server (origin se	erver) to clients	but in reality fo	rward	s the request	s it receives	to one or more	e origin server	s.
Configure re	everse pro	xy here.										
Reverse	Proxy (0)	_		_	_	-	_	_	_	_	
New	Delete	, 										
URI Pref	ïx		_		Server Nar	nes						_
No Reve	rse Proxy	URI has been ad	lded. C	lick on New button to a	add a Reverse F	Proxy URI.						
Done											🔒 F:	.10% 🏶

The following window appears.

🔮 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	b Server
Add Reverse Proxy	URI
	roxy that appears to be a web server (origin server) to clients but in reality forwards the o one or more origin servers.
requests it receives to	* Indicates required field
* URI Prefix:	···············
UNIFICIA.	Enter Reverse Proxy URI here
* Server Names:	
	Enter server names here
	OK Cancel
Done	🔒 F110% 🌾

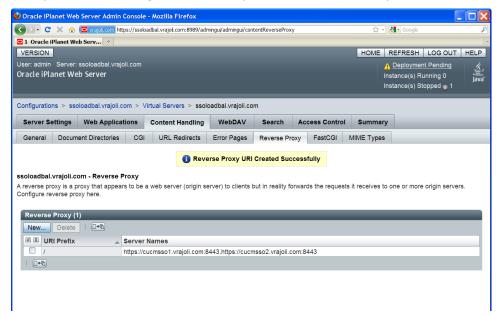
Under URI Prefix, enter / and under Server Names enter the OpenAM Enterprise server hostname. In this guide, we have two OpenAM Enterprise servers, namely cucmsso1.vrajoli.com and cucmsso2.vrajoli.com. Click **OK**.

URI Prefix:

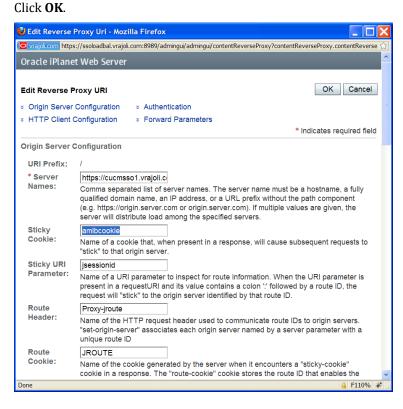
/

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

Later you see the message "Reverse Proxy URI Created Successfully."



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



Now you must 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 > ssoloadbal.vrajoli.com > Certificates > Certificate Authorities** tab. The following window appears.

) >)	• C 🗙 🏠	vrajoi.com https://	ssoloadbal.vrajol.	.com:8989/adm	inguy aurninguy cornig rifus	stedCA		☆ - 🚼 - (Google	
1 Or	racle iPlanet We	b Serv *								
/ERS	SION						HOME	REFRES	SH LOG OUT	HELP
		ssoloadbal.vrajoli.co	om					🔥 Deploy	ment Pending	(je)
racle	e iPlanet We	b Server						Instance(s) Running 0	Java
								Instance(s) Stopped ᠾ 1	
onfigu	urations > sso	loadbal.vrajoli.com								
Virtu	al Servers	HTTP Listeners	Instances	General	Performance	Access Control	Certificates	Java	Summary	
Serv	er Certificates	Certificate Autho	rities CRL	Updates	PKCS11 Tokens					
A cert	tificate on this			e in the certif		can install a CA certi or hide built-in certific		ate Revoca		swords or delete a
A cert Certii Insta	ficate on this p ficate Authori III Install C	bage. The filter in the	orities availabl	e in the certif		or hide built-in certific	ates.	ate Revoca	tion List (CRL)	
A certi Certii Insta ≶ ≣	tificate on this p ficate Authori III Install C Nickname	bage. The filter in the tites (1 - 20 of 162)	Filter: All Ite	e in the certif used to view	vexpired certificates	or hide built-in certific	ates.	-	crL	or delete a
Certif Insta	ficate on this p ficate Authori all Install C Nickname Builtin Object	ties (1 - 20 of 162) RL Delete Token:ABAecom (si	Filter: All Ite	e in the certif used to view	vexpired certificates	 a Expiration Date o July 9, 2009 1 	ates. 1:03:53 PM IST	-	CRL Not Ins	or delete a
Certif	ficate on this price of the pri	bage. The filter in the ties (1 - 20 of 162) CRL Delete I Token:ABAecom (si Token:AC Raíz Cer	Filter: All Ite ub., Am. Banke ticámara S.A.	e in the certif used to view	vexpired certificates	Expiration Date July 9, 2009 1 April 3, 2030 3	1:03:53 PM IST 3:12:02 AM IST		CRL Not Ins Not Ins	or delete a
Certif	tificate on this p ficate Authori all Install C Nickname Builtin Object Builtin Object Builtin Object	bage. The filter in th ties (1 - 20 of 162) :RL Delete I Token:ABAecom (si Token:AC Raiz Cer Token:AddTrust Ex	Filter: All Ite ub., Am. Banke ticámara S.A. ternal Root	e in the certif used to view ems ers Assn.) Ro	vexpired certificates	Expiration Date July 9, 2009 April 3, 2030 May 30, 2020	1:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST		CRL CRL CRL CRL CRL Not Ins Not Ins Not Ins	or delete a
Certif	ficate on this p ficate Authori II Install C Nickname Builtin Object Builtin Object Builtin Object Builtin Object	bage. The filter in the tites (1 - 20 of 162) ;RL Delete Token:ABAecom (si Token:AC Raíz Cer Token:AddTrust Ex Token:AddTrust Lo	Filter: All Ite ub., Am. Banko ticámara S.A. ternal Root w-Value Servio	e in the certif used to view ems ers Assn.) Ro ces Root	vexpired certificates	 Expiration Date July 9, 2009 1 April 3, 2020 May 30, 2020 May 30, 2020 	1:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST		CRL Not Ins Not Ins	Later of the second sec
A cert Certif Insta	Ificate on this p ficate Authori ill Install C Nickname Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object	bage. The filter in th ties (1 - 20 of 162) :RL Delete I Token:ABAecom (si Token:AC Raiz Cer Token:AddTrust Ex	Filter: All Ite Filter: All Ite ub., Am. Banke ticámara S.A. ternal Root w-Value Servie blic Services f	e in the certif used to view ems ers Assn.) Ro ces Root Root	vexpired certificates	 Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 May 30, 2020 May 30, 2020 	1:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST 4:01:50 PM IST		CRL Not Ins Not Ins Not Ins Not Ins Not Ins Not Ins	talled talled talled talled talled
A cert Certif	Ificate on this p ficate Authori ill Install C Nickname Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object	bage. The filter in the ties (1 - 20 of 162) (RL Delete Token:ABAecom (si Token:AC Raiz Cer Token:AddTrust Ex Token:AddTrust Lo Token:AddTrust Pu	Filter: All Ite Filter: All Ite ub., Am. Bank ticámara S.A. ternal Root w-Value Services F ialified Certific	e in the certif used to view ems ers Assn.) Ro ces Root Root ates Root	v expired certificates	Expiration Date July 9, 2009 April 3, 2030 May 30, 2020 May 30, 2020 May 30, 2020 May 30, 2020	1:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST		CRL Not Ins Not Ins Not Ins Not Ins Not Ins Not Ins Not Ins Not Ins	A constraints of the second se
A certif	tificate on this ficate Authori II Install C Nickname Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object	bage. The filter in the ties (1 - 20 of 162) IRL Delete I Token:ABAecom (si Token:AC Raiz Cer Token:AddTrust Ex Token:AddTrust Ex Token:AddTrust Pu Token:AddTrust Pu	Filter: All Ite Filter: All Ite Ub., Am. Banko ticámara S.A. ternal Root w-Value Services f ialified Certific ne Root Certifi	e in the certificused to view ems ers Assn.) Ro ces Root Root ates Root fication Autho	received certificates	 Expiration Date July 9, 2009 1 April 3, 2030 1 May 30, 2020 May 30, 2020 May 30, 2020 May 30, 2020 November 20 	1:03:53 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		CRL CRL Not Ins	A constraints of the second se
A cert Certii Insta	tificate on this ficate Authori II Install C Nickname Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object	bage. The filter in the ties (1 - 20 of 162) BR Delete I Token:ABAecom (si Token:AC Raiz Cer Token:AddTrust Ecr Token:AddTrust Pu Token:AddTrust Pu Token:AddTrust Qu	Filter: All Ite Filter: All Ite Lub., Am. Banko ticámara S.A. ternal Root w-Value Servii bilic Services f alified Certific ne Root Certifi ne Root Certifi	e in the certif used to view ams ers Assn.) Ro ces Root factor Autho fication Autho fication Autho	rity 1 rity 2	Expiration Date July 9, 2009 1 April 3, 2030 May 30, 2020 November 20 September 25	1:03:53 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 2037 2:13:00 A	· · · · MIST	CRL Ist (CRL) CRL	A stalled stal
A cert Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta	ficate on this ficate Authori all Install C Nickname Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object	bage. The filter in the ties (1 - 20 of 162) RL Delete I Token:ABAecom (sr Token:AC Raiz Cer Token:Add Trust Lo Token:Add Trust Lo Token:Add Trust Qu Token:Add Trust Qu Token:Add Trust Qu	Filter: All Itle Filter: All Itle Ub., Am. Banku ticámara S.A. ternal Root w-Value Servii blic Services fi blic Services for allfied Certific ne Root Certifi ne Root Certifi raner Root Certifi	e in the certif used to view ems ers Assn.) Ro ces Root Root ates Root fication Autho fication Autho	repried certificates	Expiration Date July 9, 2009 1 April 3, 2030 May 30, 2020 May 30, 2020 May 30, 2020 May 30, 2020 November 20 September 22 November 22	1:03:53 PM IST 3:12:02 AM IST 4:08:31 PM IST 4:08:31 PM IST 4:11:50 PM IST 2:037 2:13:00 A 0, 2037 7:38:00 F	· · · · · · · · · · · · · · · · · · ·	CRL CRL CRL Not Ins Not I	A talled
A cert Certii Insta 2 B 0 0 0 0 0 0 0	ficate on this p ficate Authori il Install C Nickname Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object	bage. The filter in the ties (1 - 20 of 152) Control (brities available table can be Filter: All Ite ub., Am. Bank ticámara S.A. ternal Root w-Value Servit bilic Services fi allified Certific ne Root Certifi ramer Root Cef (amer Root Cef (amer Root Cef	e in the certif used to view ems ers Assn.) Ro ces Root Root ates Root fication Autho fication Autho ertification Autho	repried certificates	A Expiration Date July 9, 2009 1 April 3, 2030 May 30, 2020 September 25 November 20 September 25	1:03:53 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 0; 2037 7:38:00 F 2037 8:33:00 P	- - - MIST - PMIST - MIST - AMIST	CRL CRL Not Ins Not Ins	A talled
A cert Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta Insta	ficate on this j ficate Authori al Install C Nickname Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object Builtin Object	bage. The filter in the ties (1 - 20 of 162) RL Delete I Token:ABAecom (si Token:AC Raiz Cer Token:AC Trust Ex Token:AddTrust Ex Token:AddTrust Qu Token:AddTrust Qu Token:America Onli Token:AOL Time W Token:AOL Time W	Filter: All Ite Filter: All Ite ub., Am. Bank ticàmara S.A. ternal Root w-Value Servi blic Services fi allified Certific ne Root Certifi ne Root Certifi araner Root CC araner Root CC	e in the certif used to view ers Assn.) Ro ces Root fication Autho fication Autho artification Auto artification Auto	repried certificates	A built-in certific Duly 9, 2009 April 3, 2030 May 30, 2020 May 30, 2020 May 30, 2020 May 30, 2020 May 30, 2020 November 20 September 25 November 20 September 25 December 12	1:03:53 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 2:037 2:13:00 A 2:037 7:38:00 F 2:037 5:13:00 A	- - - MIST - - MIST - - MIST - MIST	CRL CRL Not ins Not ins	A talled

Click the Install button. The Install CA Certificate Wizard appears.

Click Next.



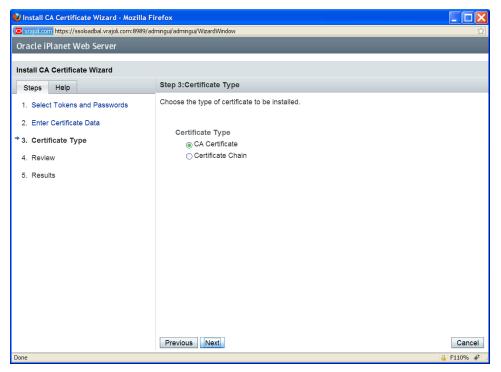
Click the **Certificate File** radio button and specify the path where you have stored the OpenAM Enterprise Server 1 certificate.

Click Next.

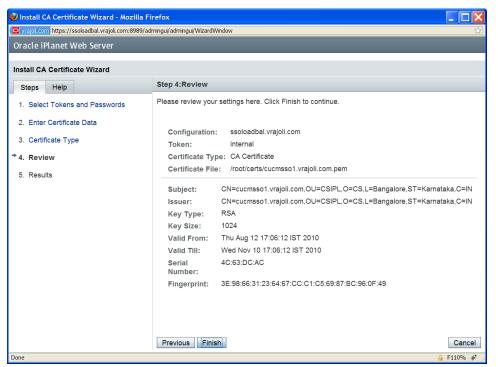
😻 Install CA Certificate Wizard - Mozilla	Dinstall CA Certificate Wizard - Mozilla Firefox								
vrajoi.com https://ssoloadbal.vrajol.com:8989	9/admingui/admingui/WizardWindow								
Oracle iPlanet Web Server									
Install CA Certificate Wizard									
Steps Help	Step 2:Enter Certificate Data								
 Select Tokens and Passwords 2. Enter Certificate Data 	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.								
3. Certificate Type	○ Certificate Data								
4. Review 5. Results	© Certificate File //root/certs/cucmsso1.vrajoli.com.pem Path to the certificate file on the server								
	Previous Next Cancel								
Done	🔒 F110% 🏶								

The following window appears.

Click Next.



Click Finish.



The following window appears, confirming you successfully installed the CA Certificate.

🕹 Install CA Certificate Wiza	ard - Mozilla Fi	refox								
vrajoi.com https://ssoloadbal.v	rajoli.com:8989/ad	mingui/admingui/WizardWindow		<u>ن</u> ک						
Oracle iPlanet Web Serv	Oracle iPlanet Web Server									
Install CA Certificate Wizard										
	lu	Step 5:Results								
Steps Help		-								
1 Select Tokens and Pas	swords	Results of Install CA Certificate	9							
2 Enter Certificate Data			CA Installation Successful							
3 Certificate Type			CA Certificate Installed Successfully.							
4 Review			,							
⇒ 5. Results										
				Close						
Done				🔒 F110% 🧩 🤢						

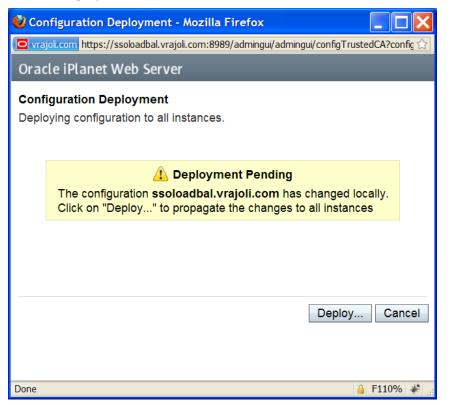
Use the same procedure to install the OpenAM Enterprise Server 2 (cucmsso2.vrajoli.com) certificate.

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

Oracle iPlanet We	o server Admin Cons	ole - mozilia	FILETOX						
🔊 · C × 🏠	vrajol.com https://s	soloadbal.vrajol	.com:8989/adm	ingui/admingui/configTru	stedCA?serverCertificatesC	General.generalCert	슈 · 🚷 · (Google	
1 Oracle iPlanet W	eb Serv *								
/ERSION						HOME	REFRES	SH LOG OU	T HELP
	: ssoloadbal.vrajoli.coi	m					A Deploy	ment Pending	\$
racle iPlanet W	eb Server						Instance(s) Running 0	Java
							Instance(s) Stopped ᠾ 1	
onfigurations > ss	oloadbal.vrajoli.com	_	_			_	_		_
	•							-	
Virtual Servers	HTTP Listeners	Instances	General	Performance	Access Control	Certificates	Java	Summary	
Server Certificates	Certificate Author	ities CRL	Updates	PKCS11 Tokens					
certificate on this	com - Certificate Auti irious certificate autho page. The filter in the ities (1 - 20 of 162)	rities availab table can be	le in the certi used to viev	v expired certificates			ate Revoca		
certificate on this certificate Author Install Install	rious certificate autho page. The filter in the ities (1 - 20 of 162)	rities availab	le in the certi used to viev		or hide built-in certific	ates.	ate Revoca	tion List (CRL)	or delete a
ertificate on this ertificate Author Install Install E Nickname	rious certificate autho page. The filter in the itites (1 - 20 of 162) CRL Delete	rities availab table can be Filter: All It	e in the certi used to view	v expired certificates	or hide built-in certific	ates.	-	tion List (CRL)	or delete :
ertificate Author nstall Install I INickname Builtin Objec	rious certificate autho page. The filter in the ities (1 - 20 of 162) CRL Delete I t Token:ABAecom (su	Filter: All It	e in the certi used to view	v expired certificates	or hide built-in certific Expiration Date July 9, 2009 1	ates. 1:03:53 PM IST	-	crection List (CRL)	or delete
certificate on this ertificate Author nstall Install Builtin Objec Builtin Objec	rious certificate autho page. The filter in the ities (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:AC Raiz Certi	rities availab table can be Filter: All It b., Am. Bank icámara S.A.	e in the certi used to view	v expired certificates	April 3, 2030 3	ates. 1:03:53 PM IST 3:12:02 AM IST		CRL Not In Not In	or delete
certificate on this ertificate Author nstall Install I Nickname Builtin Objec Builtin Objec	rious certificate autho page. The filter in the itties (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:AC Raiz Certi t Token:AddTrust Exte	rities availab table can be Filter: All It b., Am. Bank icámara S.A. ernal Root	e in the certite used to view ems ers Assn.) Ro	v expired certificates	A pril 3, 2020 May 30, 2020	1:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST		CRL Not In Not In Not In	or delete
certificate on this ertificate Author nstal Install I Nickname Builtin Objec Builtin Objec Builtin Objec	rious certificate autho page. The filter in the ities (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:AC Raiz Certi	rities availab table can be Filter: All It b., Am. Bank icámara S.A. ernal Root v-Value Servi	e in the certite used to view ems ers Assn.) Ro	v expired certificates	 Expiration Date July 9, 2009 1 April 3, 2030 3 May 30, 2020 May 30, 2020 	ates. 1:03:53 PM IST 3:12:02 AM IST		CRL CRL Not In Not In Not In Not In	or delete
certificate on this ertificate Author Install Install Builtin Objec Builtin Objec Builtin Objec	rious certificate autho page. The filter in the itites (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:ABAecom (su t Token:AddTrust Exit t Token:AddTrust Low	rities availab table can be Filter: All it b., Am. Bank icámara S.A. ernal Root <i>y</i> -Value Servi Sic Services	e in the certi e used to view ems ers Assn.) Ro ces Root Root	v expired certificates	A pril 3, 2020 May 30, 2020 May 30, 2020	1:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST		CRL CRL CRL CRL Not In	or delete
A certificate on this Certificate Author Install Install Nickname Builtin Objec Builtin Objec Builtin Objec Builtin Objec Builtin Objec	rious certificate autho page. The filter in the itties (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:AC Raiz Certi t Token:AddTrust Exte t Token:AddTrust Low t Token:AddTrust Pub	rities availab table can be Filter: All it b., Am. Bank icámara S.A. ernal Root <i>y</i> -Value Servi blic Services alified Certific	e in the certi e used to view ems ers Assn.) Ro ces Root Root ates Root	v expired certificates	 Expiration Date July 9, 2009 1 April 3, 2030 2 May 30, 2020 	1:03:53 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		CRL CRL Not In Not In Not In Not In Not In Not In Not In	or delete a
A certificate on this Certificate Author Install Install	rious certificate autho page. The filter in the itties (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:AC Raiz Certi t Token:AddTrust Exte t Token:AddTrust Low t Token:AddTrust Pub t Token:AddTrust Qua	rities availab table can be Filter: All It b., Am. Bank icámara S.A. ernal Root v-Value Servi olic Services alified Certific ne Root Certi	le in the certi e used to view ems ers Assn.) Ro ces Root Root ates Root fication Author	v expired certificates	 Expiration Date July 9, 2009 1 April 3, 2030 3 May 30, 2020 November 20, 	1:03:53 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	- - - - - -	CRL List (CRL) CRL CRL CRL Not In Not	or delete a
certificate on this ertificate Author nstall Install Nickname Builtin Objec Builtin Objec Builtin Objec Builtin Objec Builtin Objec Builtin Objec	rious certificate autho page. The filter in the itties (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:AC Raiz Certi t Token:AddTrust Exte t Token:AddTrust Exte t Token:AddTrust Qua t Token:AddTrust Qua t Token:America Onlin	rities availab table can be Filter: All it b., Am. Bank cdamara S.A. ernal Root y-Value Servi plic Services allified Certific he Root Certi he Root Certi he Root Certi	e in the certi used to viev ems ers Assn.) Ro ces Root ates Root fication Autho fication Autho	v expired certificates	A pril 3, 2030 May 30, 2020	1:03:53 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 2:037 2:13:00 A	· · · · MIST PMIST	CRL CRL Not in Not in	or delete a
certificate on this ertificate Author install Install I Nickname Builtin Objec Builtin Objec Builtin Objec Builtin Objec Builtin Objec Builtin Objec Builtin Objec	rious certificate autho page. The filter in the itties (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:AC Raiz Certi t Token:AddTrust Exte t Token:AddTrust Que t Token:AddTrust Que t Token:America Onlin t Token:America Onlin	rities availab table can be Filter: All Itt b., Am. Bank icàmara S.A. ernal Root V-Value Servi Jilc Services allified Certifica en Root Certi arner Root Certi arner Root Certi	e in the certi used to view ems ers Assn.) Ro ces Root ates Root fication Autho fication Autho ertification Autho	v expired certificates	A pril 3, 2030 May 30, 2020 November 20, September 29 November 20,	1:03:53 PM IST 3:12:02 AM IST 4:08:31 PM IST 4:08:31 PM IST 4:11:50 PM IST 4:11:50 PM IST 2037 2:13:00 A , 2037 7:38:00 I	· · · · · · · · · · · · · · · · · · ·	CRL CRL Not in	or delete a stalled stalled stalled stalled stalled stalled stalled stalled stalled
certificate on this certificate Author install Install 4 B Nickname B Builtin Objec B Builtin Objec	rious certificate autho page. The filter in the itites (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:ABAecom (su t Token:AddTrust Certi t Token:AddTrust Low t Token:AddTrust Qua t Token:America Onlin t Token:ADC Time Wa	rities availab table can be Filter: All Itt b., Am. Bank icàmara S.A. ernal Root y-Value Servi olic Services allified Certific e Root Certi arner Root Cri arner Root Cri	e in the certi used to view ems ers Assn.) Ro ces Root Root ates Root fication Author fication Author ertification Author ertification Author	v expired certificates	A Expiration Date July 9, 2009 1 April 3, 2030 3 May 30, 2020 November 20 September 29 November 20 September 29	1:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST 4:11:50 PM IST 2:037 2:13:00 A 0; 2037 7:38:00 I 2:037 8:33:00 F	- - - MIST PMIST MIST AMIST	CRL Not in Not in	cr delete a stalled stalled stalled stalled stalled stalled stalled stalled stalled stalled
A certificate on this Certificate Author Install Install Builtin Objec Builtin Objec	rious certificate autho page. The filter in the ittes (1 - 20 of 162) CRL Delete I t Token:ABAecom (su t Token:AC Raiz Certi t Token:AddTrust Low t Token:AddTrust Low t Token:AddTrust Que t Token:AddTrust Que t Token:America Onlin t Token:Anerica Onlin t Token:AOL Time Wa t Token:AOL Time Wa	rities availab table can be Filter: All itt b, Am. Bank (càmara S.A. ermal Root -Value Servi olic Services alified Certific te Root Certi ne Root Certi ne Root Certi armer Root C. A. Japanese	e in the certi used to view ems ers Assn.) Ro ces Root ates Root fication Autho fication Autho ertification Autho	v expired certificates	A pril 3, 2000 May 30, 2020 Movember 20 September 25 November 20 September 25 December 12	1:03:53 PM IST 3:12:02 AM IST 4:18:38 PM IST 4:08:31 PM IST 4:14:50 PM IST 2:037 2:13:00 A 2:037 6:33:00 F 2:037 6:13:00 /	- - - MIST - - MIST - - - MIST - - MIST	CRL CRL Not in Not	or delete a stalled stalled stalled stalled stalled stalled stalled stalled stalled stalled stalled

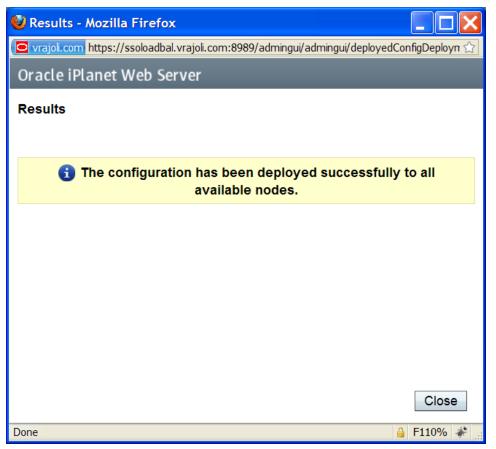
The following window appears.

Click the **Deploy** button.



The following window appears, indicating successful deployment.

Click Close.



16.2.2 Installation and Configuration of Session Failover Components

16.2.2.1 Configuration of Session Failover Components on Linux Platform

Prerequisites: one or more OpenAM Enterprise servers (for session failover) installed and configured on Linux platform. For installing OpenAM Enterprise on Linux platform, please refer to sections 6.1, 7.1 and 9.1.

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

OpenAM Enterprise Server 1 > cucmsso1.vrajoli.com

OpenAM Enterprise Server 2 > cucmsso2.vrajoli.com

Install the OpenSSO Enterprise session failover components on the cucmsso1.vrajoli.com host machine and thecucmsso2.vrajoli.com host machine.

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

As a root user, log in to the cucmsso1.vrajoli.com host machine.

1. Create a directory into which the MessageQueue and BerkeleyDatabase bits can be downloaded and change into it.

mkdir -p /export/SF0

cd /export/SF0

- 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.

cd /export/SF0

unzip ssoSessionTools.zip -d ssoSessionTools

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

cd /export/SFO/ssoSessionTools

chmod +x setup

#./setup

5. 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

6. Change to the bin directory.

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

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

#./imqbrokerd -name msgqbroker -port 7777 &

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

netstat -an | grep 7777

*.7777 *.* 0 0 49152 0 LISTEN

9. 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.

10. 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.

11. 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:7777,cucmsso2.vrajoli.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.
- 12. Generate an encrypted password in a .password file with the following subprocedure.
 - 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

- (Optional)View the encrypted password for verification.
 # more /export/SFO/ssoSessionTools/opensso/.password
 M270Gb6U4ufRu+oWAzBdWw==
- 13. (Optional) Modify the amsessiondb script if necessary.

The amsessiondb script (located in the 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: Back up amsessiondb before you modify it.

14. Restart the session failover components with the following subprocedure.

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 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

15. 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

- 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)
- 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 with the following subprocedure.

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: Back up 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: Back up 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 OpenAM</u> <u>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 set up under directory: C:\ssoSessionTools\sfoscripts.

JMQ is properly set up under directory C:\ssoSessionTools\jmq

- 5. Change to bin folder.
- 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.co m.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.
- 11. Generate an encrypted password in a .password file with the following subprocedure.

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, change the PASSWORDFILE property in amsfo.conf 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:/ss oSession

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

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

<u>To Install Session Failover Components on cucmsso2.vrajoli.com OpenAM Enterprise Server</u> <u>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 set up under directory: C:\ssoSessionTools\sfoscripts JMQ is properly set up 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.
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 subprocedure.

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:/ss oSession

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	LISTENING
--	-----	--------------	-----------	-----------

TCP 10.78.85.131:60787 10.78.85.131:7777 TIME_WAIT

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

16.2.3 Installation and configuration of OpenAM Enterprise Servers for Session Failover

16.2.3.1 Installation of OpenAM Enterprise Server 1

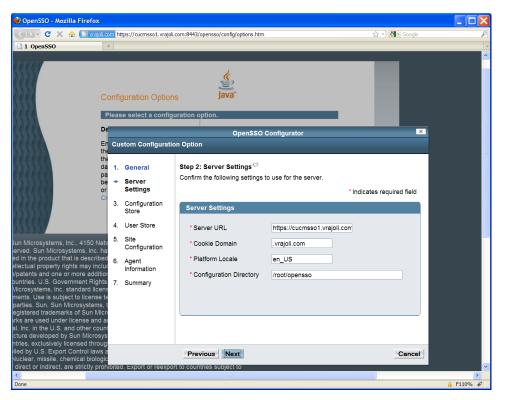
Browse the OpenAM URL: <u>https://cucmsso1.vrajoli.com:8443/opensso</u>, you will see the following Configurator. Click on **Create New Configuration** under Custom Configuration.



Create a new password for default user [amAdmin]. Click Next.

😂 OpenSSO - Mozilla Firefox				_ 🗆 🔀
C X 🏠 🖿 vrajol.c	om ht	ttps://cucmsso1.vrajoli	.com:8443/opensso/config/options.htm 🖒 - 🛃 - Google	P
1 OpenSSO	4			-
2222	Pleas	guration Option		
		stom Configuration		
th th da	e	General	Step 1: General 🛱	3
pa be or	2.	Server Settings	Enter the password for the default user, amAdmin. The password must be at least 8 characters in length. If this configuration will be part of an existing deployment, the password you enter must match that of the original deployment.	
KKKKK	3.	Configuration Store	* Indicates required field	
55555	4.	User Store	Default User Password	
Bun Microsystems, Inc., 4150 Networks and Automatic Sun Microsystems, Inc. ha		Site Configuration	Default User [amAdmin]	
ed in the product that is described ellectual property rights may inclu patents and one or more additio	¢ 0.	Agent Information	* Password VCA	
vipatents and one of more addition ountries. U.S. Government Rights Microsystems, Inc. standard licen- ments. Use is subject to license to	s 7.	Summary		
parties. Sun, Sun Microsystems, egistered trademarks of Sun Micr	t			
irks are used under license and a al, Inc. in the U.S. and other coun				
cture developed by Sun Microsys ntries, exclusively licensed throug	в			
lled by U.S. Export Control laws a Nuclear, missile, chemical biologic	a		Previous Next Cancel	
direct or indirect, are strictly prof		d. Export or reexpo	rt to countries subject to	~
Done				🔒 F110% 🗚

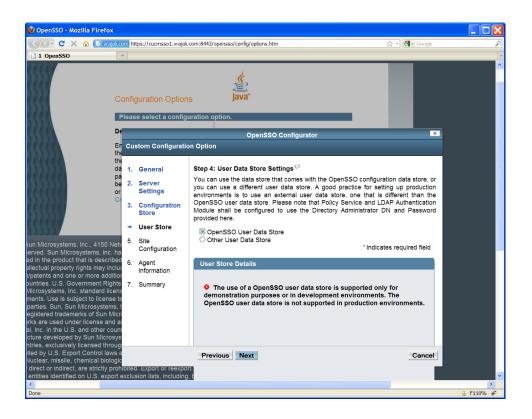
Click Next.



Click Next.

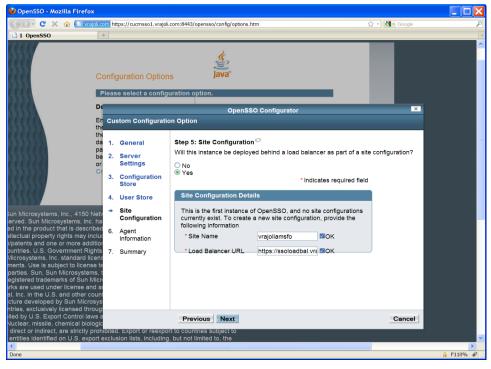
🥹 OpenSSO - Mozilla Firefox				
🔇 🖸 🗸 🏠 🗋 vrajol.co	m ht	tps://cucmsso1.vrajol.o	om:8443/opensso/config/options.htm 🖧 🕤 🛃 🗸 Google	P
1 OpenSSO				-
		guration Option		
	leas	e select a configu	ration option.	
De	_		OpenSSO Configurator	
En the	Cu	stom Configuratio	n Option	
the da	1.	General	Step 3: Configuration Data Store Settings 💬	
pa be or Cr	2.	Server Settings	If no other OpenSSO instance already exists in the environment, then choose First Instance. If one or more OpenSSO instances already exist in the environment, choose Add to Existing Deployment.	
	+	Configuration Store	First Instance Add to Existing Deployment? Indicates required field	=
1111	4.	User Store	Configuration Store Details	
un Microsystems, Inc., 4150 Netv erved. Sun Microsystems, Inc. ha	5.	Site Configuration	Configuration Data Store OpenSSO Sun Java System Directory	
ed in the product that is described ellectual property rights may includ //patents and one or more additior	6.	Agent Information	- Server	
ountries. U.S. Government Rights	7.	Summary	* SSL/TLS Enabled	
Microsystems, Inc. standard licens ments. Use is subject to license te			* Host Name localhost	
parties. Sun, Sun Microsystems, t egistered trademarks of Sun Micro			* Port 50389	
irks are used under license and ai al, Inc. in the U.S. and other count			* Encryption Key 9IBAZkZt6fCuJYzbE+cwOV	
cture developed by Sun Microsys ntries, exclusively licensed throug			* Root Suffix dc=opensso,dc=java,dc=ne	
lled by U.S. Export Control laws a Nuclear, missile, chemical biologic			Previous Next Cancel	
direct or indirect, are strictly prohi				
entities identified on U.S. export e specially designated nationals lis			but not limited to, the	
un Microsystems, Inc., 4150 Netw	ork	Circle, Santa Clara,	California 95054,	v
<	_			>
Done				🔒 F110% 🦑

Select the **OpenSSO User Data Store** radio button and click **Next**.

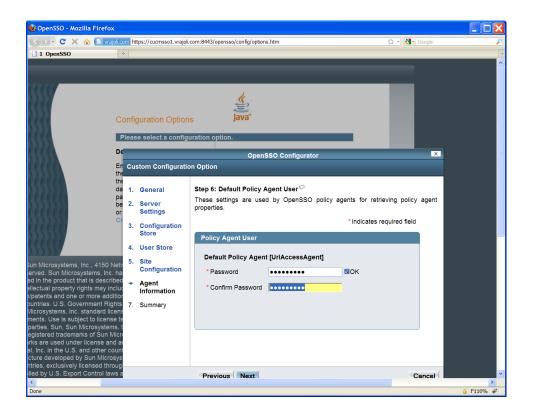


Under Site Configuration, click the **Yes** radio button and enter a site name and provide the Load Balancer URL (which was set up in section 3.1). Click **Next**.

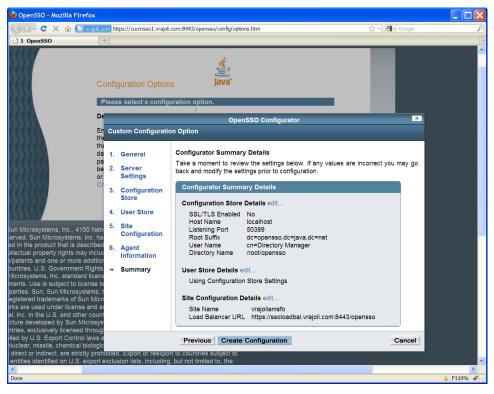
Example for Load Balancer URL: https://ssoloadbal.vrajoli.com:8443/opensso



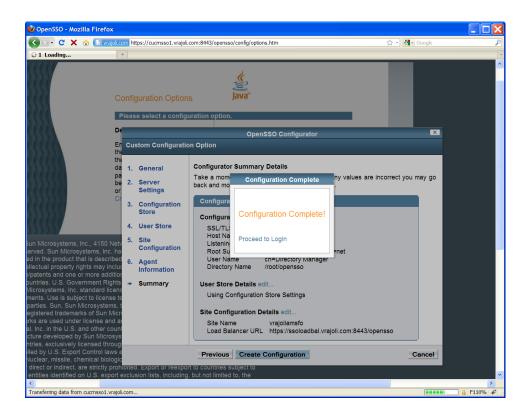
Create a password for Default Policy Agent and click Next.



Click the **Create Configuration** button.



Click on **Proceed to Login** link.



The OpenAM login window appears.

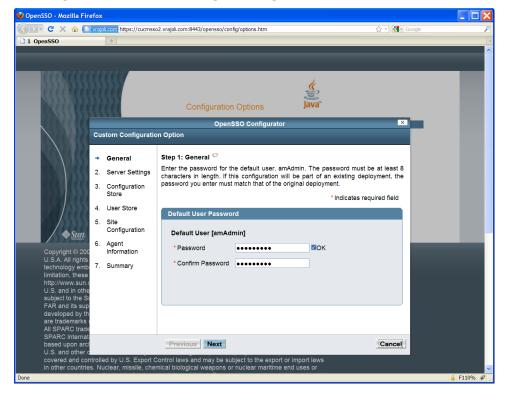
🔮 OpenSSO (Login) - Mozilla Firefox	
😮 🗸 C 🔀 🕼 vrajoi.com https://cucmsso1.vrajoi.com:8443/opensso/UI/Login	☆ - 🛃 - Google 🔎
1 OpenSSO (Login)	•
OpenSSO User Name: Password:	Sign in to OpenSSO
Copyright © 2008 Sun Microsystems, Inc. 4150 Netw U.S.A. All rights reserved. Sun Microsystems, Inc. has technology embodied in the product that is described limitation, these intellectual property rights may includ http://www.sun.com/patents and one or more addition U.S. and in other countries. U.S. Government Rights subject to the Sun Microsystems, Inc. Standard license FAR and its supplements. Use is subject to license te developed by third parties. Sun Sun Microsystems, Inc. All SPARC trademarks are used under license and ar SPARC International, Inc. In the U.S. and other count based upon architecture developed by Sun Microsyst U.S. and other countries, exclusively licensed through covered and controlled by U.S. Export Control laws a in other countries, microlar missing, chemical biologic U.S. embargo or to entities identified on U.S. export e	s intellectual property rights relating to In this document. In particular, and without le one or more of the U.S. patents listed at all patents or pending patent applications in the - Commercial software. Government users are e agreement and applicable provisions of the rms. This distribution may include materials he Sun logo. Java, Solaris and the Solaris logo paystems, Inc. in the U.S. and other countries. e trademarks or registered trademarks of rise. Products bearing SPARC trademarks are lems, Inc. UNIX is a registered trademark in the h X/lopen Company. Lut. This product is nd may be subject to the export or import laws all weapons or nuclear maritime end uses or bled. Export or reexport to countries subject to

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 following Configurator. Click on **Create New Configuration** under Custom Configuration.



Create a password for default user [amAdmin] and click Next.



Click Next.

🔮 OpenSSO - Mozilla Fire	fox				
🔇 🖻 - C 🗙 🏠 🚺	vrajol.com https://cucmss	o2.vrajoli.com:8443/opensso/config/opt	ions.htm	☆ - Google	P
1 OpenSSO	+				
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- All SPARC trade SPARC Internet	Custom Configuration 1. General * Server Settings 3. Configuration Store 4. User Store 5. Site Configuration 6. Agent Information 7. Summary	on Option Step 2: Server Settings ^{CP} Confirm the following settings I Server Settings • Server URL • Cookie Domain • Platform Locale • Configuration Directory	Configurator	s required field	
based upon arch U.S. and other o		Previous Next		Cancel	
		Control laws and may be subject mical biological weapons or nucl			
Done	s. Nuclear, missile, che				🔒 F110% 🦑

Click **Add to Existing Deployment** radio button and enter the OpenAM Enterprise Server 1 URL in the Server URL text box. Click **Next**.

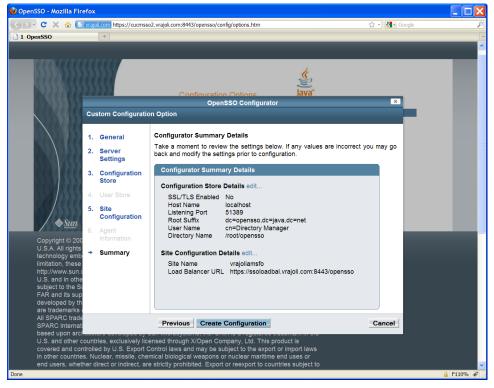
Note: Before you complete this step you must import the OpenAM Enterprise Server 1 certificate to the OpenAM Enterprise Server 2 trust store.

Copyright © Configuration Image: Configuration Options Image: Configuration Options Image: Configuration Options 1. OpenSSO Image: Configuration Options Image: Configuration Options Image: Configuration Options Image: Configuration Options 1. General 1. General Step 3: Configuration Data Store Settings If no other OpenSSO Instance already exists in the environment, then choose First Instance. If one or more OpenSSO Instances already exists in the environment, then choose First Instance. If one or more OpenSSO Instances already exists in the environment, choose Add to Existing Deployment? Image: Configuration Store Details Copyright © COL Step Store Image: Configuration Store Details Image: Configuration Store Details Copyright © COL Server URL https://cucmsso1.vrajoli.com:8443/opensso Image: Configuration Details Server URL https://cucmsso1.vrajoli.com:8443/opensso Image: Configuration Details Image: Configuration Details Server URL https://cucmsso1.vrajoli.com:8443/opensso Image: Configuration Details Image: Configuration Details Server URL https://cucmsso1.vrajoli.com:8443/opensso Image: Configuration Details Image: Configuration Details
Configuration Onlines
Custom Configuration Option Image: Custom Configuration Option 1. General Step 3: Configuration Data Store Settings (*) 2. Server Settings If no other OpenSSO instance already exists in the environment, then choose First Instance. If one or more OpenSSO instances already exist in the environment, then choose First Instance. If one or more OpenSSO instances already exist in the environment, choose Add to Existing Deployment. * Configuration Store • First Instance (*) Add to Existing Deployment? * User Store • First Instance (*) Add to Existing Deployment? * Site Configuration Store Details • Site • Server URL * Server URL https://cucmsso1.vrajoil.com/8443/opensso • OK URL of the existing OpenSSO server. ex: * URL https://cucmsso1.vrajoil.com/808/0nemsro.
limitation, these http://www.sun c 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 architectures, exclusively licensed through X/Open SSO instance is not set up for replication. The following ports Will be used SPARC Internat based upon architectures, exclusively licensed through X/Open Company, Ltd. This product is covered and controlled by U.S. Export Control Reserved Through X/Open Company, Ltd. This product is covered and controlled by U.S. Export Control Reserved Through X/Open Company, Ltd. This product is covered and controlled by U.S. Export Control Reserved Through X/Open Company to the export or import to for ther countries, Nuclear, missile, chemical biological weapons or nuclear maritime end uses or end users, whether direct or inducer, are strictly prohibited. Export to countries subject to

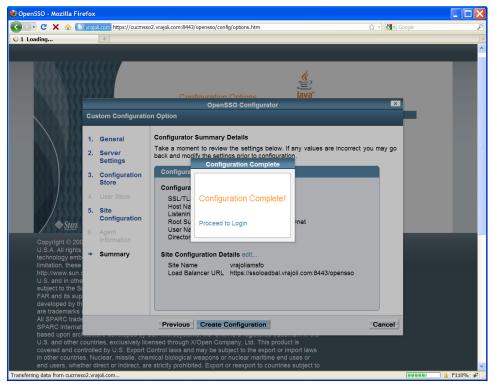
Under Site Configuration, click the **Yes** radio button and enter the same site name that was used in OpenAM Enterprise Server 1. Click **Next**.

Enter the Load Balancer URL that was set up in section 3.1, for example: https://ssoloadbal.vrajoli.com:8443/opensso.

Click the Create Configuration button.



Click the **Proceed to Login** link.



Copyright © 2010-2011 Cisco Systems, Inc. All rights reserved.

16.2.3.3 Configure OpenSSO Enterprise for Session Failover

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

Log in to OpenAM Enterprise console.

Click the **Configuration** tab.

Under Global properties, click Session.

Under Secondary Configuration Instance, click **New**.

In the Add Sub Configuration window, 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 the Message 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 (https://ssoloadbal.vrajoli.com:8989) from the web browser. Click the **Lock** icon on the right bottom corner, and click the **View Certificate** button. Go to the **Details** tab and export the certificate to your local machine from where you are browsing.

Because a replication setup is running on all the OpenSSO Enterprise servers in AMSFO environment, Policies, Authentication Module instances, and J2EE Agents that are created on one OpenSSO Enterprise server get replicated on the rest of the OpenSSO Enterprise servers.

For the Authentication Module instance, you must create a keytab for the Load Balancer host and not for the OpenSSO Enterprise server hosts. Place the Load Balancer keytab file on both the OpenSSO Enterprise host file systems.

Create OpenAM Policies, Authentication Module instance, and J2EE agent profile on any one of the OpenSSO Enterprise servers. For creating Policies, Authentication Module instances, and J2EE agent profile, refer to sections 10.1, 10.2 and 10.3.

Log in to Unified CM OS Administration; go to **Security > Certificate Management > Upload Certificate**.

Select certificate type as tomcat-trust, and browse for the above Load Balancer certificate that you saved in the previous step. When you find the certificate, click the **Upload** button.

Now log in to the CLI of Unified CM 8.5, and execute the command **utils sso enable** with OpenSSO URL as your Load Balancer host (https://ssoloadbal.vrajoli.com:8443/opensso).