Configure SSO for OS Admin and DRS in CUCM Version 12.x

Contents

Introduction

This document describes the Single Sign On (SSO) for Operating System (OS) Admin and Disaster Recovery System (DRS) feature which is introduced in Cisco Unified Communications Manager (CUCM) Version 12.0 and later.

CUCM versions earlier than 12.0 support SSO for CM Administration, Serviceability, and Reporting pages only. This feature helps the administrator to navigate quickly through different components and have a better user experience. There is an option to use the Recovery URL as well in case SSO breaks for OS Admin and DRS.

Prerequisites

Requirements

Cisco recommends that you have knowledge of CUCM Version 12.0 and later.

Components Used

The information in this document is based on Cisco Call Manager (CCM) Version 12.0.1.21900-7.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

In order to enable SSO for OS Admin and DRS, SSO must already be enabled for CM Administration login. In addition to this, it also requires platform level user which can be either a new user or existing user.

Use Existing OS Admin User

The platform user created at the time of installation can be configured for the SSO login of OS Admin and DRS components. The only requirement in this case is that this platform user must also be added in the Active Directory (AD) against which Identity Provider (IdP) is authenticated.

Use New User

Complete these steps in order to enable a new user for SSO OS Admin and DRS login:

Step 1. Create a new user with privilege level 1/0 from the CLI access of Publisher.

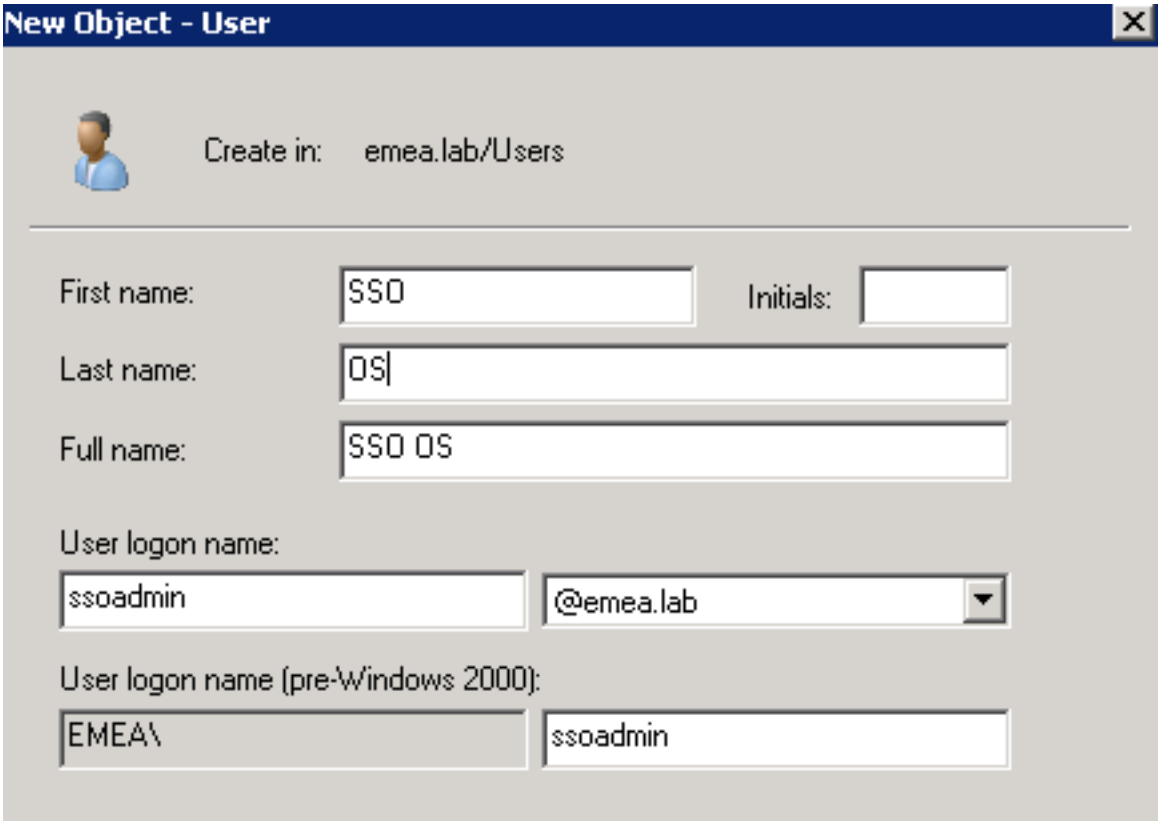
In order to create a new user, platform 4 level access is required which is possessed by the platform user created at the time of installation.

Level 0 privilege only gives read Access to the User whereas Level 1 gives both read and write permissions.

```
admin:set account name ssoadmin



Privilege Levels are:

   Ordinary - Level 0

   Advanced - Level 1



Please enter the privilege level :1

Allow this User to login to SAML SSO-enabled system through Recovery URL ? (Yes / No) :yes

To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that
identifies this user to LDAP (such as sAMAccountName or UPN).

        Please enter the appropriate LDAP Unique Identifier (UID) for this user:[ssoadmin]

Storing the default SSO UID value as username

Please enter the password :********

             re-enter to confirm :********

Account successfully created
```

The Unique Identifier (UID) used here can be given any value which IdP provides in its assertion response or leaves it blank. If it is left blank, then CUCM uses **userid** as UID.

Step 2. Add a user with the same userid as earlier in the AD server through which IdP is authenticated, as shown in the image.



Step 3. Sync of the Lightweight Directory Access Protocol (LDAP) server is also required so that newly created user gets populated in CUCM as shown in the image.

Step 4. Password Reset (through CLI again) is required for the user created after its addition to the AD.

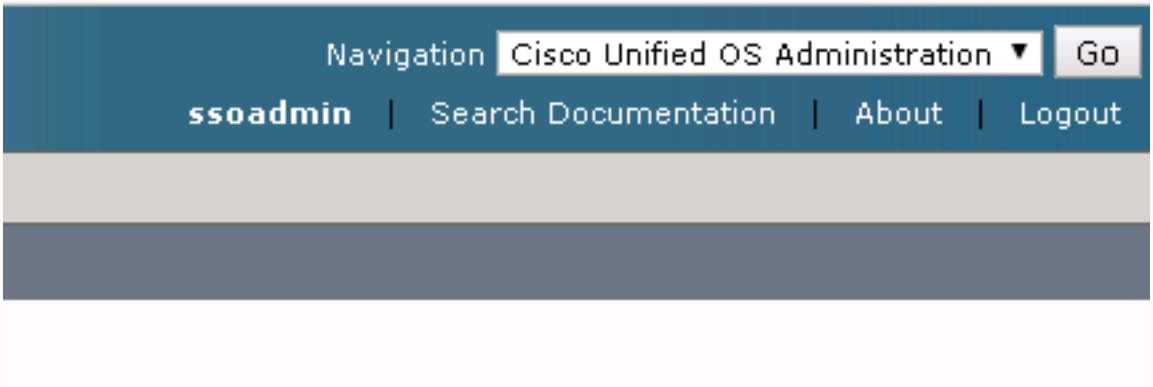
```
login as: ssoadmin

ssoadmin@10.106.96.92's password:

WARNING: Your password has expired.

You must change your password now and login again!

Changing password for user ssoadmin.

Changing password for ssoadmin.

(current) UNIX password:

New password:

Re-enter password:
```

Verify

Use this section to confirm that your configuration works properly.

Once the SSO is successfully enabled for OS Admin and DRS, the login must work with the

credentials of the AD for the user created earlier and as shown in the image.



Troubleshoot

There is currently no specific troubleshooting information available for this configuration.