# Configuración de SSO para OS Admin y DRS en CUCM Versión 12.x

## Contenido



## Introducción

Este documento describe la función de inicio de sesión único (SSO) para administración del sistema operativo (SO) y sistema de recuperación ante desastres (DRS) que se introduce en Cisco Unified Communications Manager (CUCM) versión 12.0 y posteriores.

Las versiones de CUCM anteriores a la 12.0 admiten SSO solo para las páginas Administración, Mantenimiento e Informes de CM. Esta función ayuda al administrador a desplazarse rápidamente por los diferentes componentes y a tener una mejor experiencia de usuario. Existe la opción de utilizar la URL de recuperación también en caso de que se produzca un fallo de SSO para el administrador del sistema operativo y el DRS.

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento de CUCM versión 12.0 y posteriores.

### Componentes Utilizados

La información de este documento se basa en Cisco Call Manager (CCM) versión 12.0.1.21900-7.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

Para habilitar SSO para OS Admin y DRS, SSO ya debe estar habilitado para el inicio de sesión

de CM Administration. Además de esto, también requiere usuarios de nivel de plataforma que pueden ser usuarios nuevos o existentes.

## Usar usuario administrador de SO existente

El usuario de la plataforma creado en el momento de la instalación se puede configurar para el inicio de sesión de SSO de los componentes DRS y administrador del sistema operativo. El único requisito en este caso es que este usuario de plataforma también se debe agregar en Active Directory (AD) con el que se autentica el proveedor de identidad (IdP).

## Usar nuevo usuario

Complete estos pasos para habilitar un nuevo usuario para SSO OS Admin y DRS login:

Paso 1. Cree un nuevo usuario con el nivel de privilegio 1/0 a partir del acceso CLI de Publisher.

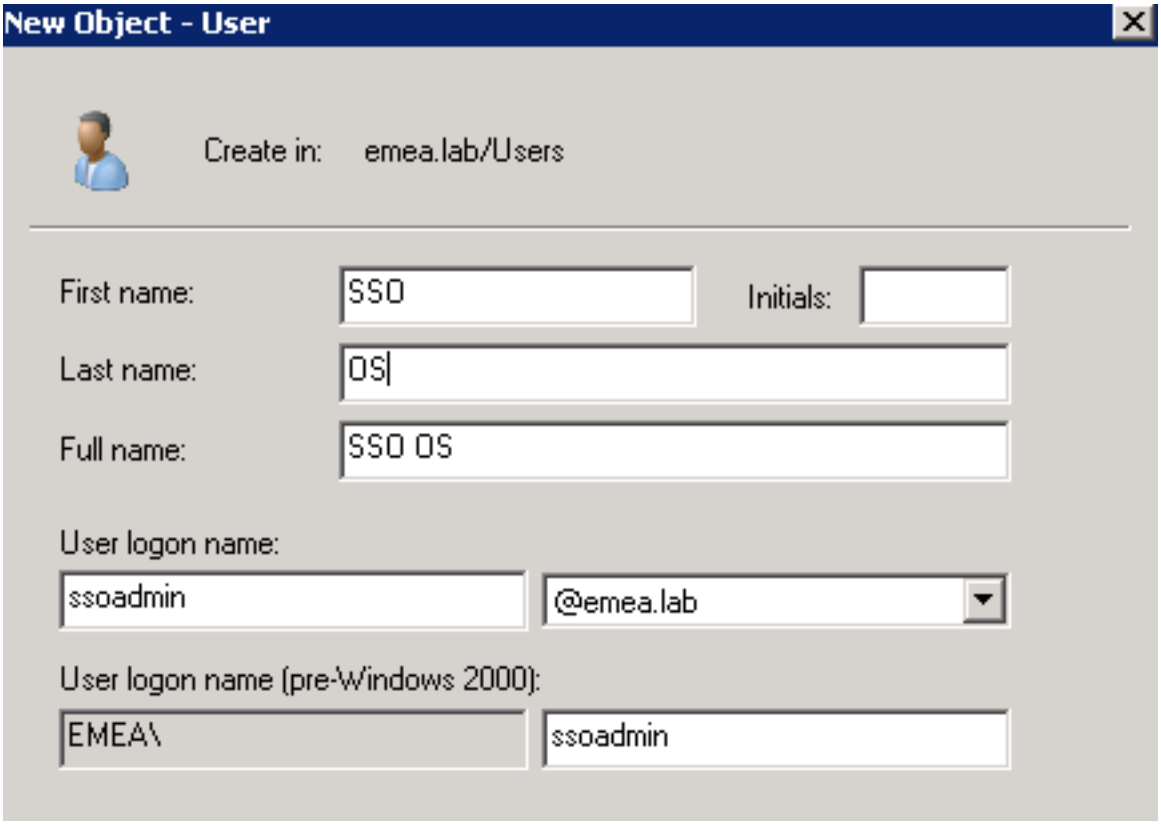
Para crear un nuevo usuario, se requiere el acceso de nivel de la plataforma 4 que posee el usuario de la plataforma creado en el momento de la instalación.

El privilegio de nivel 0 sólo otorga acceso de lectura al usuario, mientras que el nivel 1 otorga permisos de lectura y escritura.

```
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
```

El Identificador Único (UID) utilizado aquí puede recibir cualquier valor que IdP proporcione en su respuesta de aserción o lo deje en blanco. Si se deja en blanco, CUCM utiliza **userid** como UID.

Paso 2. Agregue un usuario con el mismo ID de usuario que el anterior en el servidor AD a través del cual se autentica el IdP, como se muestra en la imagen.




Paso 3. La sincronización del servidor LDAP (protocolo ligero de acceso a directorios) también es necesaria para que el usuario recién creado se rellene en CUCM, como se muestra en la imagen.


Paso 4. Se requiere el restablecimiento de la contraseña (a través de CLI de nuevo) para el usuario creado después de su adición al AD.

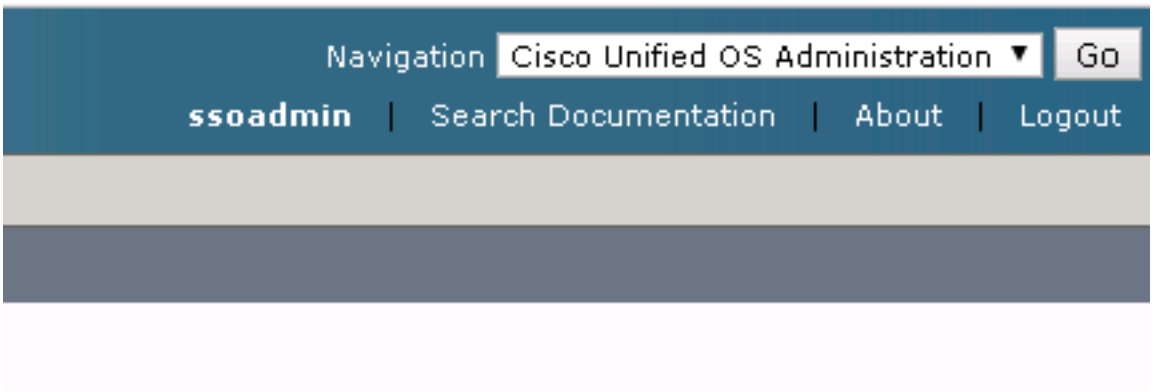
```
login as: ssoadmin

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:
```

# Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Una vez que el SSO esté habilitado correctamente para el administrador del sistema operativo y

el DRS, el inicio de sesión debe funcionar con las credenciales del AD para el usuario creado anteriormente y como se muestra en la imagen.




## Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).