

Configuration de SSO pour l'administrateur du système d'exploitation et DRS dans CUCM

Version 12.x

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Utiliser un utilisateur OS Admin existant](#)

[Utiliser un nouvel utilisateur](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit la fonctionnalité d'authentification unique (SSO) pour l'administration du système d'exploitation (OS) et le système de récupération après sinistre (DRS) qui est introduite dans Cisco Unified Communications Manager (CUCM) Version 12.0 et ultérieure.

Les versions de CUCM antérieures à la version 12.0 prennent en charge SSO pour les pages d'administration, de maintenance et de création de rapports de CM uniquement. Cette fonctionnalité permet à l'administrateur de naviguer rapidement dans les différents composants et d'améliorer l'expérience utilisateur. Il y a une option pour utiliser l'URL de récupération aussi en cas de pauses SSO pour OS Admin et DRS.

Conditions préalables

Exigences

Cisco recommande que vous connaissiez CUCM version 12.0 et ultérieure.

Composants utilisés

Les informations contenues dans ce document sont basées sur la version 12.0.1.21900-7 de Cisco Call Manager (CCM).

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configurer

Afin d'activer SSO pour OS Admin et DRS, SSO doit déjà être activé pour la connexion d'administration CM. En outre, il nécessite également un utilisateur au niveau de la plate-forme, qui peut être un nouvel utilisateur ou un utilisateur existant.

Utiliser un utilisateur OS Admin existant

L'utilisateur de la plate-forme créé au moment de l'installation peut être configuré pour la connexion SSO des composants OS Admin et DRS. La seule exigence dans ce cas est que cet utilisateur de plate-forme doit également être ajouté dans Active Directory (AD) par rapport auquel le fournisseur d'identité (IdP) est authentifié.

Utiliser un nouvel utilisateur

Complétez ces étapes afin d'activer un nouvel utilisateur pour SSO OS Admin et DRS login :

Étape 1. Créez un nouvel utilisateur avec le niveau de privilège 1/0 à partir de l'accès CLI de Publisher.

Afin de créer un nouvel utilisateur, un accès de niveau plate-forme 4 est requis, qui est possédé par l'utilisateur de la plate-forme créée au moment de l'installation.

Le privilège de niveau 0 accorde uniquement un accès en lecture à l'utilisateur, tandis que le privilège de niveau 1 accorde des autorisations en lecture et en écriture.

```
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
```

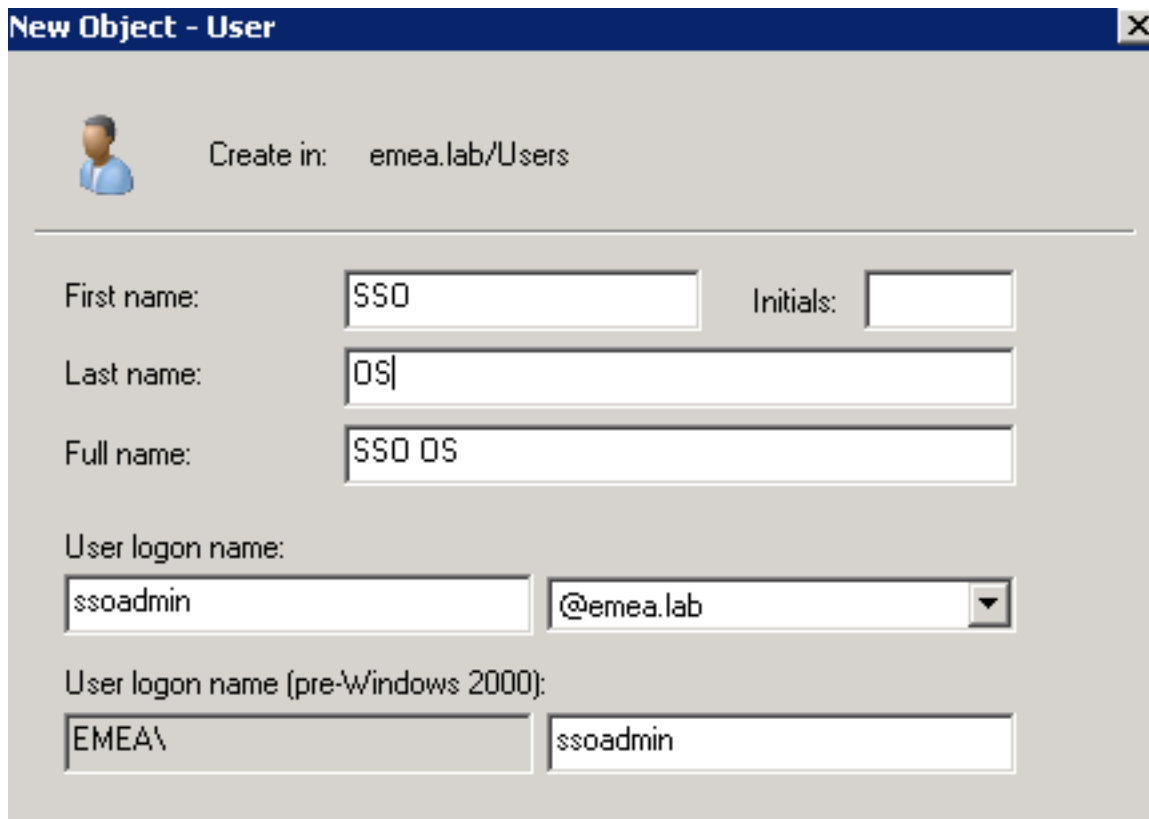
```
Please enter the password :*****
```

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

```
Account successfully created
```

L'identificateur unique (UID) utilisé ici peut recevoir n'importe quelle valeur fournie par le protocole d'identification dans sa réponse d'assertion ou la laisser vide. Si ce champ est laissé vide, CUCM utilise **userid** comme UID.

Étape 2. Ajoutez un utilisateur avec le même ID utilisateur que précédemment sur le serveur AD via lequel le fournisseur d'identité est authentifié, comme illustré dans l'image.



New Object - User

Create in: emea.lab/Users

First name: SSO Initials:

Last name: OS

Full name: SSO OS

User logon name: soadmin @emea.lab

User logon name (pre-Windows 2000): EMEA\ soadmin

Étape 3. La synchronisation du serveur LDAP (Lightweight Directory Access Protocol) est également requise pour que l'utilisateur nouvellement créé soit renseigné dans CUCM, comme illustré dans l'image.



soadmin	SSO	OS	Active Enabled LDAP Synchronized User	1
<input type="button" value="Add New"/>	<input type="button" value="Select All"/>	<input type="button" value="Clear All"/>	<input type="button" value="Delete Selected"/>	

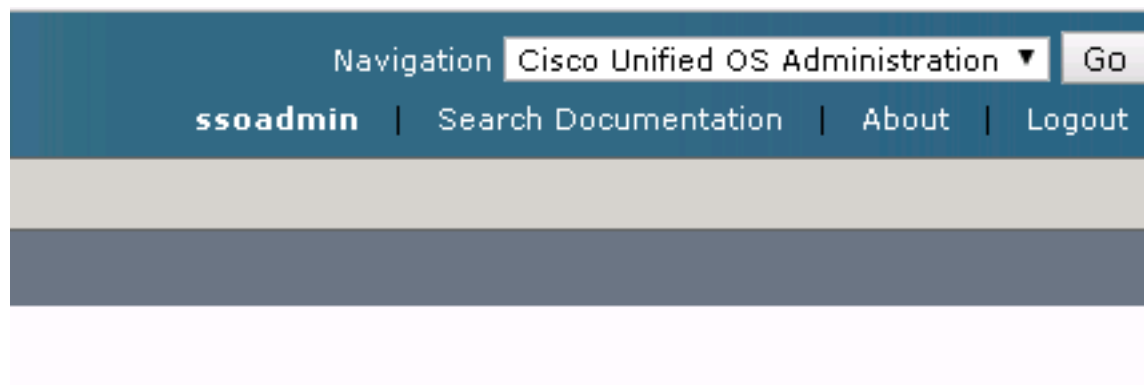
Étape 4. La réinitialisation du mot de passe (via l'interface de ligne de commande à nouveau) est requise pour l'utilisateur créé après son ajout à Active Directory.

```
login as: soadmin
soadmin@10.106.96.92's password:
WARNING: Your password has expired.
You must change your password now and login again!
Changing password for user soadmin.
Changing password for soadmin.
(current) UNIX password:
New password:
Re-enter password:
```

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

Une fois que l'authentification unique est correctement activée pour OS Admin et DRS, la connexion doit fonctionner avec les informations d'identification de l'AD pour l'utilisateur créé précédemment et comme indiqué dans l'image.



Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.