

# Konfigurieren von SSO für OS-Admin und DRS in CUCM-Version 12.x

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Vorhandenen BS-Administrator-Benutzer verwenden](#)

[Neuen Benutzer verwenden](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einleitung

In diesem Dokument wird die Funktion Single Sign On (SSO) für das Betriebssystem Admin and Disaster Recovery System (DRS) beschrieben, die in Cisco Unified Communications Manager (CUCM) Version 12.0 und höher eingeführt wurde.

CUCM-Versionen vor 12.0 unterstützen nur SSO für die CM-Administration-, Serviceability- und Reporting-Seiten. Mit dieser Funktion kann der Administrator schnell durch verschiedene Komponenten navigieren und die Benutzerumgebung optimieren. Es gibt eine Option, die Wiederherstellungs-URL auch zu verwenden, falls SSO für OS Admin und DRS bricht.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse der CUCM-Version 12.0 und höher zu verfügen.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Call Manager (CCM) Version 12.0.1.21900-7.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

## Konfigurieren

Um SSO für OS-Admin und DRS zu aktivieren, muss SSO bereits für die CM-Administrations-

Anmeldung aktiviert sein. Darüber hinaus ist ein Benutzer auf Plattformebene erforderlich, bei dem es sich entweder um einen neuen oder um einen bestehenden Benutzer handeln kann.

## Vorhandenen BS-Administrator-Benutzer verwenden

Der bei der Installation erstellte Plattformbenutzer kann für die SSO-Anmeldung der OS-Admin- und DRS-Komponenten konfiguriert werden. In diesem Fall muss dieser Plattformbenutzer auch im Active Directory (AD) hinzugefügt werden, für das Identity Provider (IdP) authentifiziert wird.

## Neuen Benutzer verwenden

Führen Sie die folgenden Schritte aus, um einen neuen Benutzer für SSO OS Admin- und DRS-Anmeldung zu aktivieren:

Schritt 1: Erstellen Sie einen neuen Benutzer mit der Berechtigungsebene 1/0 über den CLI-Zugriff von Publisher.

Um einen neuen Benutzer zu erstellen, ist ein Zugriff auf Plattform 4-Ebene erforderlich, der vom Plattformbenutzer zum Zeitpunkt der Installation erstellt wird.

Die Berechtigungen der Ebene 0 gewähren dem Benutzer nur Lesezugriff, während die Ebene 1 sowohl Lese- als auch Schreibberechtigungen gewährt.

```
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
```

Der hier verwendeten Unique Identifier (UID) kann jeder Wert zugewiesen werden, den IdP in seiner Assertionsantwort bereitstellt, oder er bleibt leer. Wenn keine Eingabe erfolgt, verwendet CUCM die Benutzer-ID als UID.

Schritt 2: Fügen Sie einen Benutzer mit derselben Benutzer-ID wie zuvor auf dem AD-Server hinzu, über den IdP authentifiziert wird, wie im Bild gezeigt.

The screenshot shows the 'New Object - User' dialog box. At the top, it says 'Create in: emea.lab/Users'. Below this, there are several input fields: 'First name' with 'SSO', 'Last name' with 'OS', and 'Full name' with 'SSO OS'. There is also an 'Initials' field which is empty. Under 'User logon name', there is a text box with 'ssoadmin' and a dropdown menu with '@emea.lab'. Below that, 'User logon name (pre-Windows 2000)' has a text box with 'EMEA\' and another with 'ssoadmin'.

Schritt 3: Der LDAP-Server (Lightweight Directory Access Protocol) muss ebenfalls synchronisiert werden, damit neu erstellte Benutzer wie im Bild dargestellt in CUCM eingetragen werden.

<input type="checkbox"/>	ssoadmin	SSO	OS	Active Enabled LDAP Synchronized User

Buttons: Add New, Select All, Clear All, Delete Selected

Schritt 4: Für den Benutzer, der nach dem Hinzufügen zum AD erstellt wird, ist eine Kennwortzurücksetzung (wieder über die CLI) erforderlich.

```
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:
```

## Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Sobald SSO erfolgreich für OS Admin und DRS aktiviert wurde, muss die Anmeldung mit den Anmeldedaten des AD für den zuvor erstellten Benutzer funktionieren, wie im Image dargestellt.



## Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.