

# Comment activer le code confidentiel commun pour CUCM et UCXN.

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Présentation des fonctionnalités](#)

[Configuration](#)

[Dépannage](#)

[Problème 1.](#)

[Problème 2.](#)

[Informations connexes](#)

## Introduction

Ce document décrit la procédure à suivre pour configurer la broche commune configurée pour Cisco Unified Communication Manager (CUCM) et Cisco Unity Connection (UCXN) dans la version 11.5.

## Conditions préalables

### Conditions requises

Cisco vous recommande de savoir comment créer des utilisateurs et associer des périphériques aux utilisateurs.

Avant de commencer à configurer la broche commune, vous devez intégrer CUCM à UCXN.

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes

- Cisco CallManager 11.5
- Cisco Unity 11.5

**Note:** 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.

# Informations générales

L'utilisateur doit accéder à une application de communications unifiées, telle que conférence Meet Me, mobilité des numéros de poste et messagerie vocale, lorsque vous utilisez le même code PIN, afin de ne pas avoir à gérer plusieurs informations d'identification de code PIN. L'utilisateur souhaite pouvoir définir/modifier un code PIN (commun) sur le portail d'autosoins.

L'administrateur doit être en mesure de spécifier quand un code PIN commun entre CUCM/Unity doit être utilisé, afin de choisir quand les codes PIN sont différents ou synchronisés. L'administrateur souhaite pouvoir activer le code confidentiel commun pour tous les utilisateurs affectés à Unity spécifique.

Dans CUCM version 11.5, il existe une nouvelle case à cocher **Activer la synchronisation des broches de l'utilisateur final** sous la page Serveur d'applications lorsque nous sélectionnons Type de serveur d'applications comme Cisco Unity Connection.

## Présentation des fonctionnalités

- Provisionnement permettant la synchronisation des broches des utilisateurs finaux entre CUCM et UCXN via la page Application Server à partir de l'interface utilisateur d'administration de CUCM
- Si la synchronisation des broches est activée et qu'un utilisateur met à jour la broche à partir de CUCM, BAT (Bulk Administration Tool), AXL (Administrative Extensible Markup Language), UDS (User Data Service) ou Self Care Portal, la broche doit être synchronisée avec UCXN
- Le code PIN doit être synchronisé entre CUCM et UCXN et vice versa lorsque la synchronisation du code PIN est activée dans les deux applications
- Par défaut, la synchronisation Pin doit être désactivée lorsque vous essayez de créer un nouvel enregistrement Unity Connection ou lorsque vous effectuez une mise à niveau et que vous essayez de charger un enregistrement de connexion d'unité actuel.

## Configuration

Étape 1.

Créer un utilisateur final sur CUCM et l'associer à un périphérique

Étape 2.

Importer cet utilisateur vers Unity

Étape 3.

Accédez à Administration du système d'exploitation dans CUCM

Étape 4.

Télécharger le certificat Tomcat

Étape 5.

Télécharger ceci en tant que confiance dans Unity

Étape 6.

Téléchargez maintenant le certificat Tomcat de Unity et téléchargez-le en tant que confiance tomcat dans CUCM

Étape 7.

Créer un utilisateur d'application dans CUCM avec les informations d'identification de Unity

Étape 8.

Attribuer à cet utilisateur le rôle d'AXL

**Permissions Information**

Groups: Admin-3rd Party API, Application Client Users, Standard Audit Users, Standard CAR Admin Users, Standard CCM Admin Users [View Details](#)

Roles: **Standard AXL API Access**, Standard Admin Rep Tool Admin, Standard Audit Log Administration, Standard CCM Admin Users, Standard CCM End Users [View Details](#)

**Add to Access Control Group**

**Remove from Access Control Group**

Étape 9.

Affecter également un rôle AXL à l'utilisateur de l'application CUCM

Étape 10.

Naviguez maintenant jusqu'à Cisco Unity Connection et vérifiez la commande **Enable End User Pin Synchronization**

**Cisco Unity Connection Administration**

Navigation: Cisco Unity Connection Administration

appadmin | Search Documentation | About | Sign Out

**Cisco Unity Connection**

- Video Services Accounts Status
- Dial Plan
  - Partitions
  - Search Spaces
- System Settings
  - General Configuration
  - Cluster
  - Authentication Rules
  - Roles
  - Restriction Tables
  - Licenses
  - Schedules
  - Holiday Schedules
  - Global Nicknames
  - Subject Line Formats
  - Attachment Descriptions
  - Enterprise Parameters
  - Service Parameters
  - Plugins
  - Fax Server
- LDAP
  - SAML Single Sign on
  - Cross-Origin Resource Sharing (C)
  - SMTP Configuration
  - Advanced
- Telephony Integrations
  - Phone System**
  - Port Group
  - Port
  - Speech Connect Port
  - Trunk
  - Security
- Tools
  - Task Management
  - Bulk Administration Tool

**Edit AXL Servers**

Phone System Edit Refresh Help

Save

**AXL Servers**

Delete Selected Add New

Order	IP Address	Port	Test
0	10.106.123.111	8443	Test

Delete Selected Add New

**AXL Server Settings**

Username: [cisco]

Password: [.....]

Cisco Unified Communications Manager Version: 5.0 or Greater (SSL)

Enable End User PIN Synchronization for Primary AXL Server

Ignore Certificate Errors

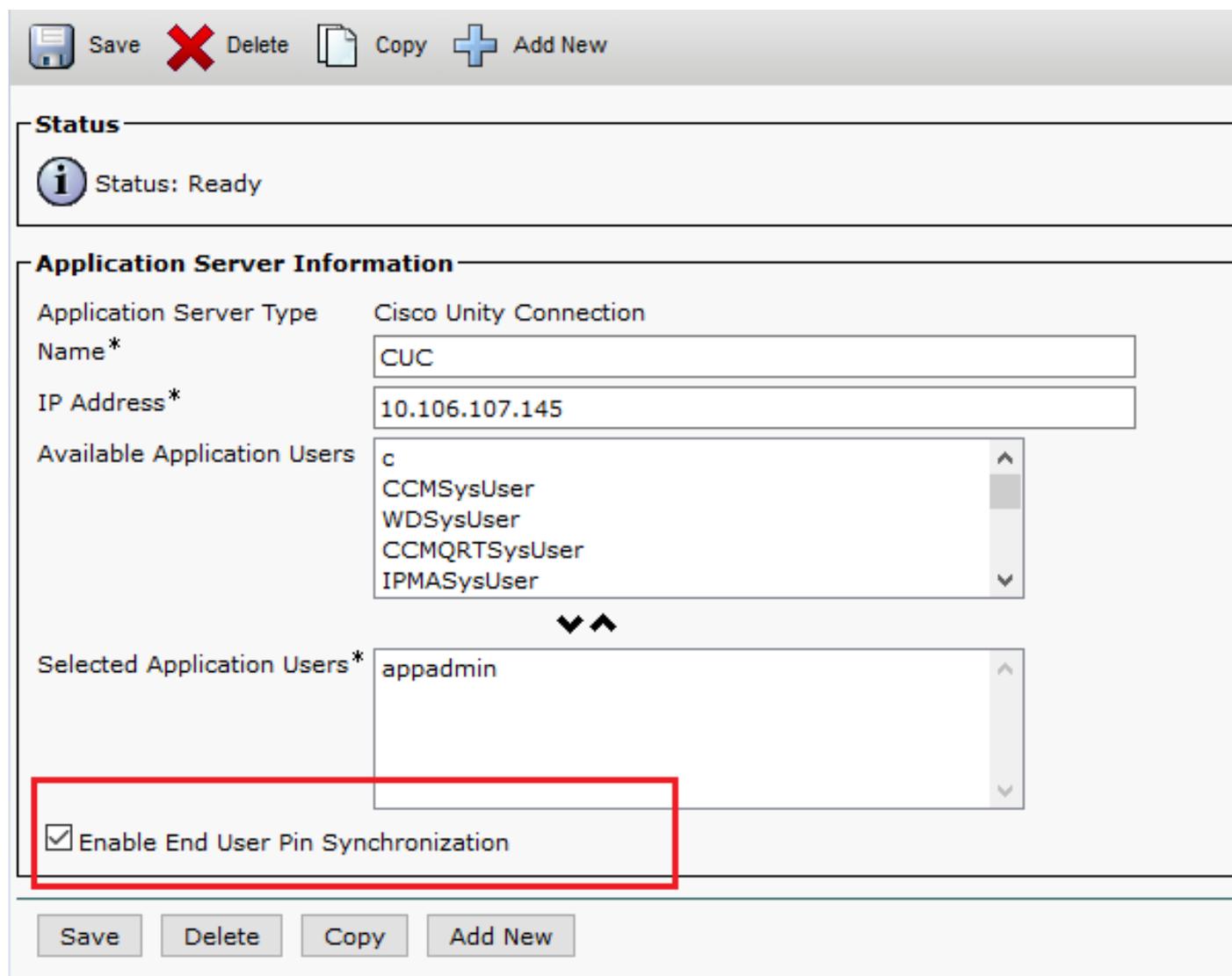
Save

Étape 11.

À partir de CUCM, accédez à **System>Application server>Add the new application server as Cisco Unity Connection** (si ce n'est déjà fait).

Étape 12.

Cochez la case **Activer la synchronisation des broches de l'utilisateur final**



The screenshot shows the configuration page for a new application server. At the top, there are navigation buttons: Save, Delete, Copy, and Add New. Below this is a 'Status' section with an information icon and the text 'Status: Ready'. The main section is 'Application Server Information', which includes:

- Application Server Type: Cisco Unity Connection
- Name\*: CUC
- IP Address\*: 10.106.107.145
- Available Application Users: A list box containing 'c', 'CCMSysUser', 'WDSysUser', 'CCMQRTSysUser', and 'IPMASysUser'.
- Selected Application Users\*: A list box containing 'appadmin'.
- At the bottom of the form, a checkbox labeled 'Enable End User Pin Synchronization' is checked and highlighted with a red rectangle.

At the bottom of the page, there are buttons for Save, Delete, Copy, and Add New.

Étape 13.

Cliquez sur **Enregistrer**

Le message Pin Synchronization a réussi est reçu.

## Dépannage

### Problème 1.

Message d'erreur " la synchronisation Pin n'est pas activée en raison de l'absence de vérification du certificat. "

Dépannage des étapes

- Vérifiez que les certificats sont chargés correctement.
- Vérifiez que Unity Connection est accessible et que nous sommes en mesure de nous connecter correctement.

## Problème 2.

Message d'erreur " la synchronisation Pin n'est pas activée en raison du code de réponse  
HttpsURLConnection : 401: Non autorisé »

Dépannage des étapes

- Vérifiez que vous avez vérifié l'**activation de la synchronisation des broches de l'utilisateur final** sur
- Vérifiez que vous avez attribué le rôle AXL aux utilisateurs d'applications.

## Informations connexes

[https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/11x/administration/guide/b\\_cuc\\_sag/b\\_cucsag\\_appendix\\_01111.html#id\\_16699](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/11x/administration/guide/b_cuc_sag/b_cucsag_appendix_01111.html#id_16699)