

Configurer l'autorisation locale UCCE 12.0(X)

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Étape 1. Configurer les autorisations du Registre](#)

[Étape 2. Configurer les autorisations de dossier](#)

[Vérification](#)

[Dépannage](#)

Introduction

Ce document décrit les étapes nécessaires pour supprimer la dépendance de Microsoft Active Directory (AD) à gérer les autorisations dans les composants Unified Contact Center Enterprise (CCE).

Contribué par Anuj Bhatia, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Unified Contact Center Enterprise
- Microsoft Active Directory

Components Used

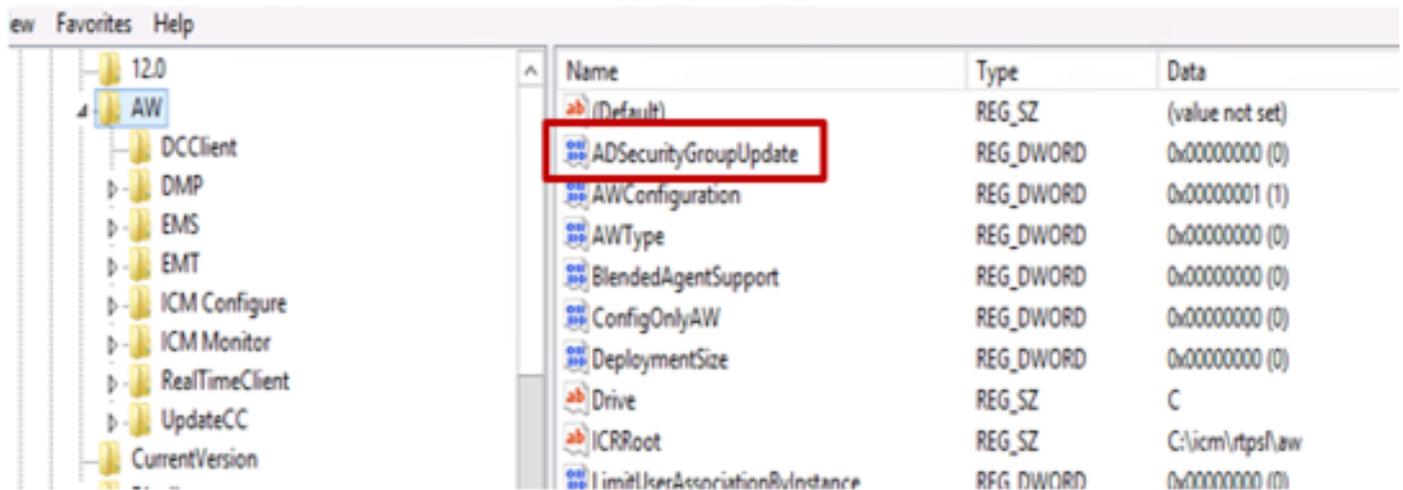
Les informations utilisées dans le document sont basées sur la version 12.0(1) de la solution UCCE.

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 actif, assurez-vous de bien comprendre l'impact potentiel de n'importe quelle étape.

Informations générales

La version UCCE 12.X fournit des privilèges d'appartenance aux utilisateurs aux groupes d'utilisateurs locaux sur le serveur d'administration local (AW), ce qui permet aux utilisateurs de

déplacer l'autorisation hors d'Active Directory (AD). Ceci est contrôlé par le Registre **ADSecSecurityGroupUpdate** qui, par défaut, est activé et évite l'utilisation des groupes de sécurité Microsoft AD pour contrôler les droits d'accès des utilisateurs pour effectuer des tâches de configuration et de configuration.



The screenshot shows the Windows Registry Editor with the following table of values:

Name	Type	Data
(Default)	REG_SZ	(value not set)
ADSecSecurityGroupUpdate	REG_DWORD	0x00000000 (0)
AWConfiguration	REG_DWORD	0x00000001 (1)
AWType	REG_DWORD	0x00000000 (0)
BlendedAgentSupport	REG_DWORD	0x00000000 (0)
ConfigOnlyAW	REG_DWORD	0x00000000 (0)
DeploymentSize	REG_DWORD	0x00000000 (0)
Drive	REG_SZ	C
ICRRoot	REG_SZ	C:\icm\rtps\aw
LimitUserAssociationByInstance	REG_DWORD	0x00000000 (0)

Note: Si l'entreprise souhaite choisir le comportement antérieur, l'indicateur **ADSecSecurityGroupUpdate** peut être remplacé par 1 qui permet la mise à jour vers Active Directory (AD)

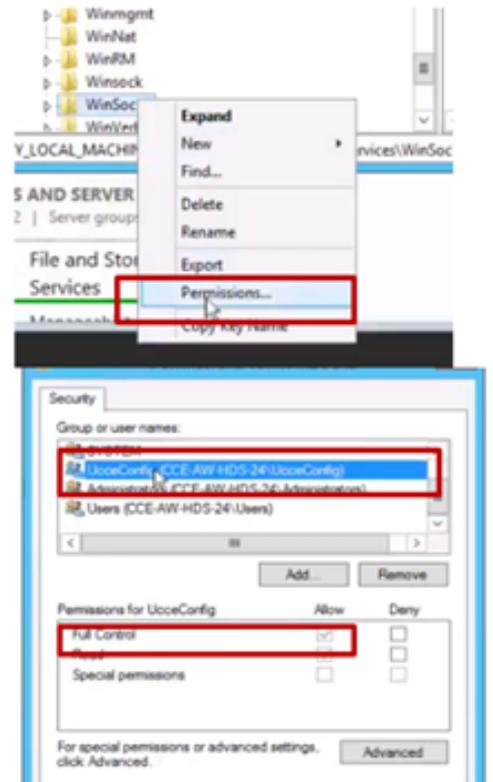
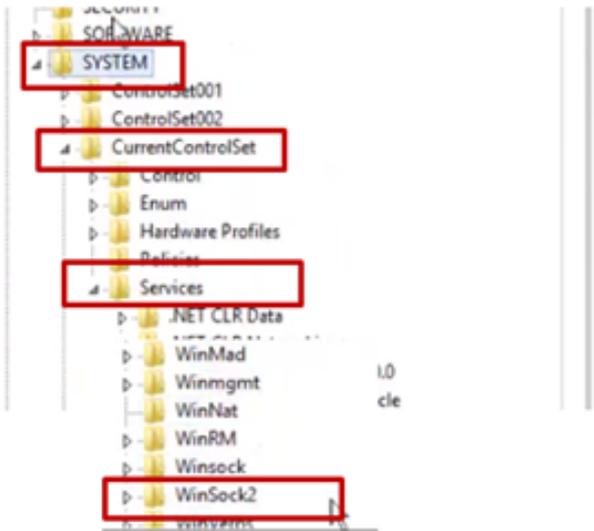
Pour déplacer l'autorisation hors d'AD, il faut effectuer une tâche unique sur chaque machine serveur AW pour accorder les autorisations requises pour le groupe **UcceConfig**. Ce document vise à présenter les étapes nécessaires à la configuration de ces autorisations, ainsi qu'un exemple de mappage d'un utilisateur de domaine dans le groupe **Configuration et configuration CCE**.

Configuration

Pour octroyer des autorisations de groupe **UcceConfig** au serveur AW local, il faut procéder en deux étapes : d'abord, les autorisations sont fournies au niveau du registre, puis transmises au niveau du dossier.

Étape 1. Configurer les autorisations du Registre

1. Exécutez l'utilitaire **regedit.exe**.
2. Sélectionnez **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2**.
3. Dans **Autorisations** sous l'onglet **Sécurité**, sélectionnez **UcceConfig group** et cochez **Autoriser** l'option **Contrôle total**.



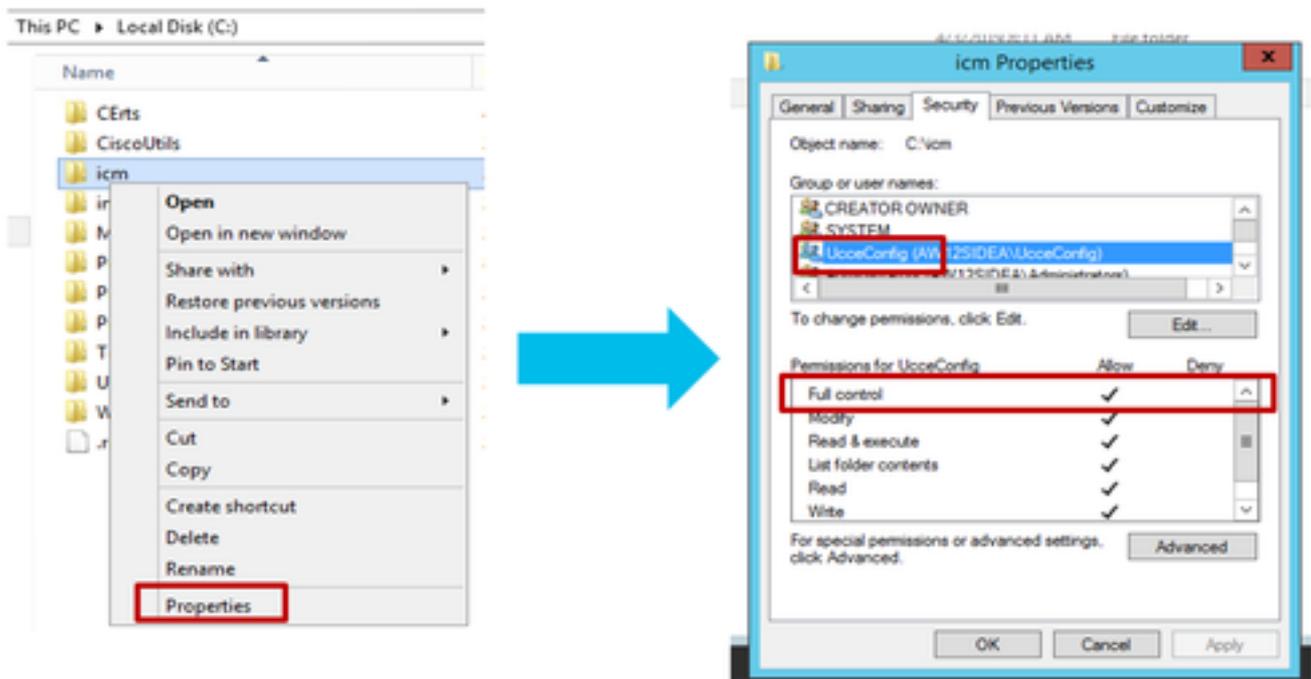
4. Répétez les étapes précédentes pour accorder le contrôle total au groupe UcceConfig pour les registres

- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, inc.\ICM
- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, inc.\ICM

Étape 2. Configurer les autorisations de dossier

1. Dans l'Explorateur Windows, sélectionnez C:\icm and go to Properties.

2. Dans l'onglet Sécurité, sélectionnez **UcceConfig** et cochez **Autoriser** l'option **Contrôle total**.



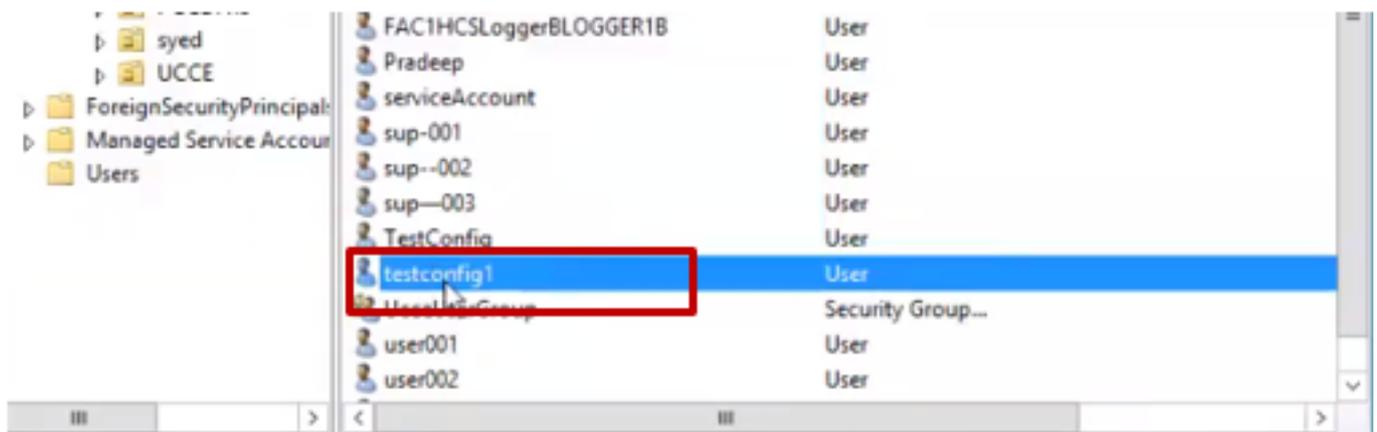
3. Cliquez sur OK pour enregistrer la modification.

4. Répétez les étapes précédentes pour accorder un contrôle total au groupe **UcceConfig** pour C:\Temp folder.

Lorsque la configuration préliminaire du jour 0 a été effectuée, examinez les étapes permettant de promouvoir un utilisateur de domaine pour qu'il dispose de droits de configuration et de configuration.

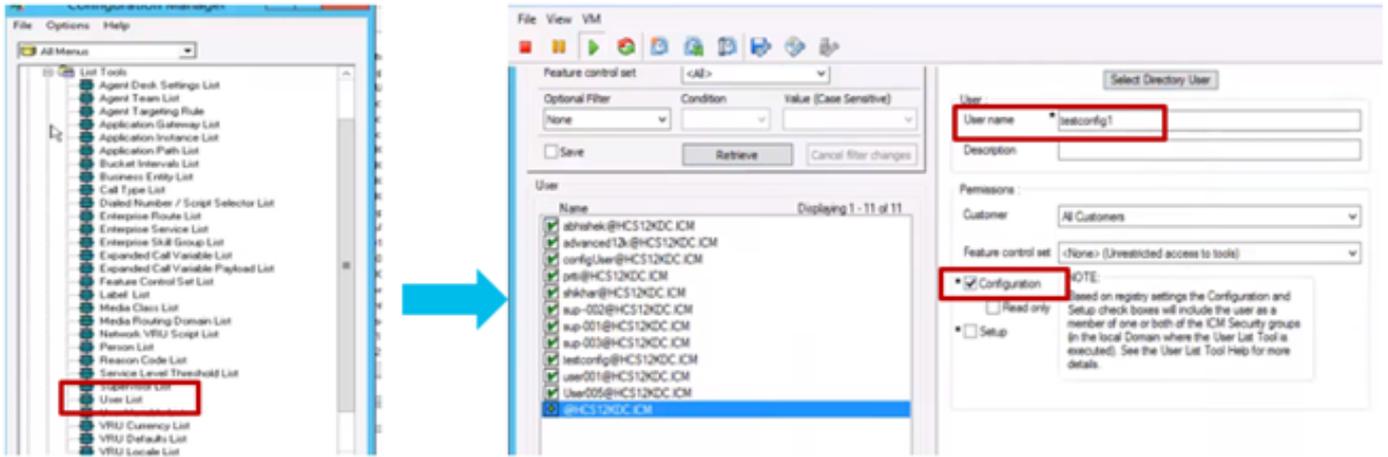
Étape 3 : Configuration de l'utilisateur du domaine

1. Créez un utilisateur de domaine dans Active Directory, pour cet utilisateur Exercice testconfig1 a été créé.

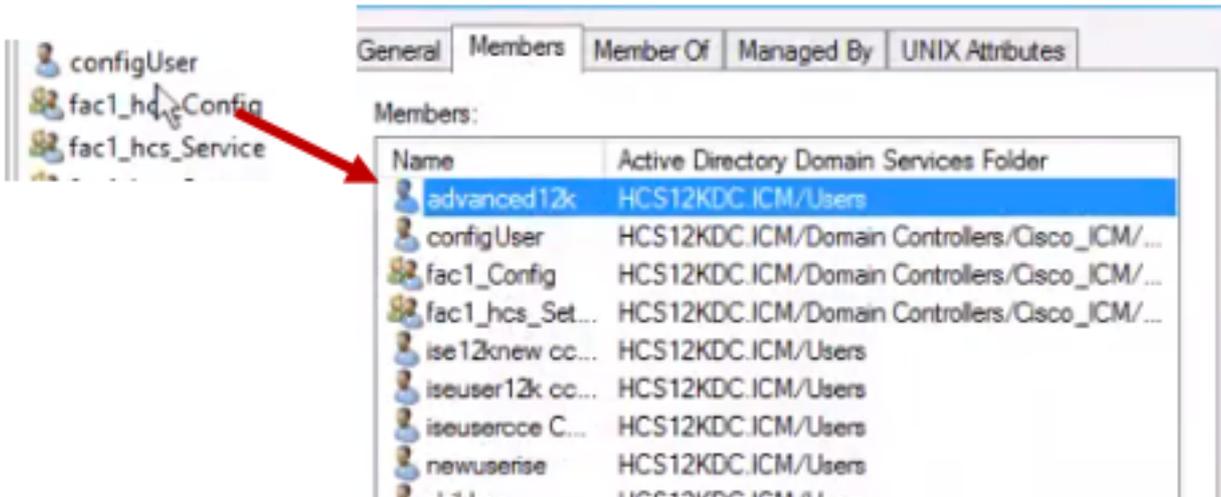


2. Connectez-vous au serveur AW à l'aide d'un admin de domaine ou d'un compte d'administrateur local.

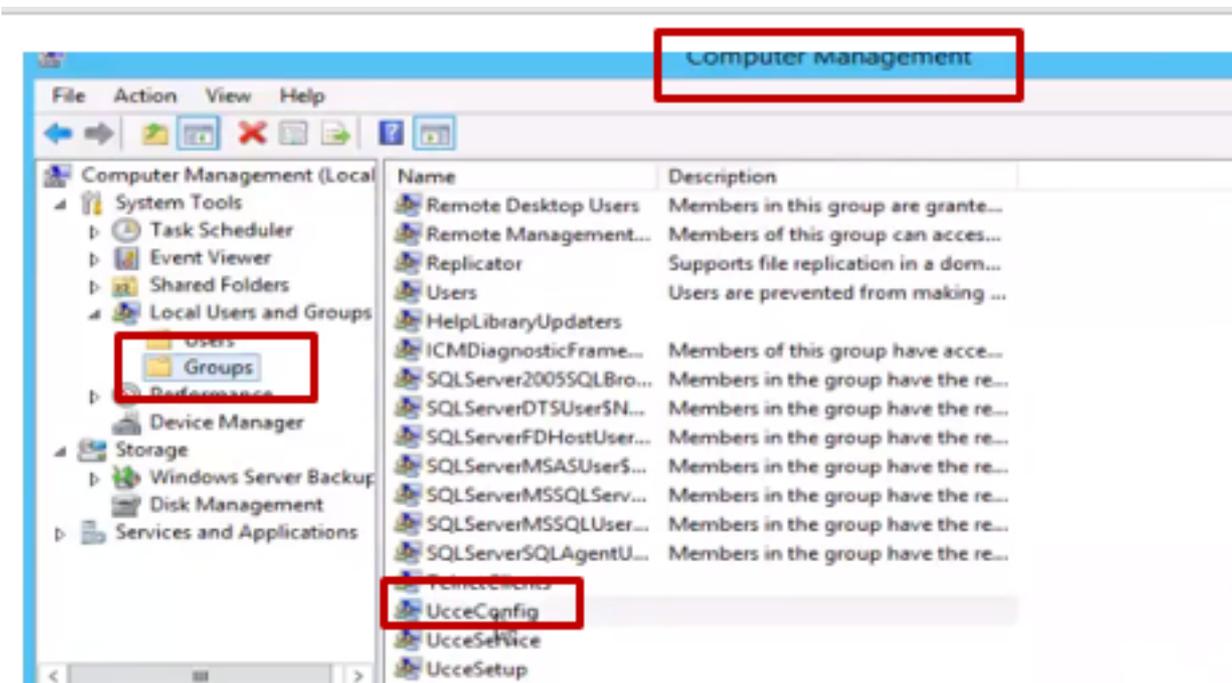
3. Dans le gestionnaire de configuration via l'outil Liste d'utilisateurs, ajoutez l'utilisateur et cochez l'option **de configuration**.



Avant la version 12.0, cette modification aurait mis à jour les groupes de sécurité Config dans le domaine sous une unité d'organisation (OU) d'instance, mais avec la version 12.0, le comportement par défaut est qu'elle n'ajoute pas cet utilisateur au groupe AD. Comme l'illustre l'image, il n'y a aucune mise à jour de cet utilisateur dans le groupe de sécurité de configuration ICM du domaine.



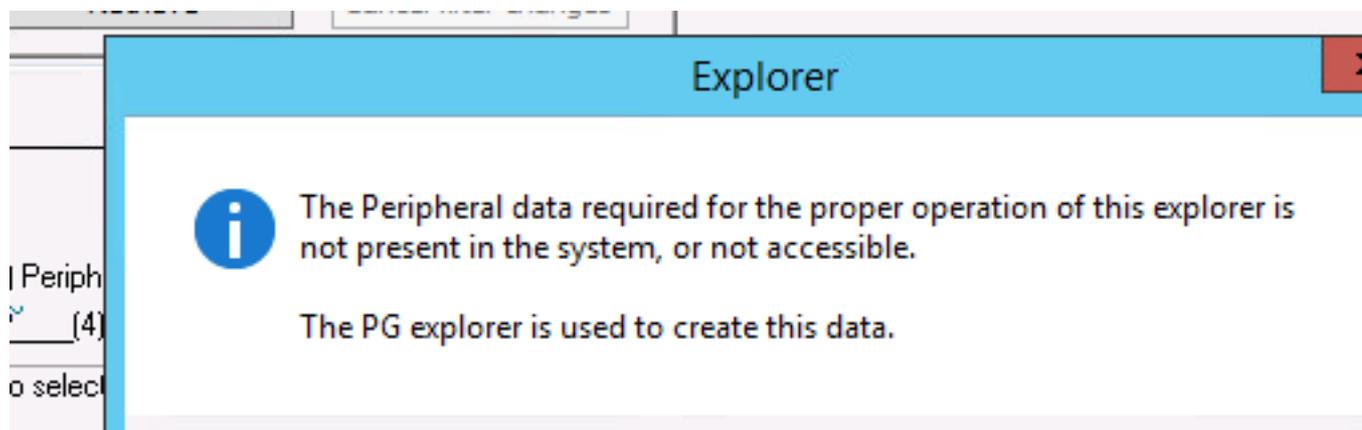
4. Dans le serveur AW sous **Gestion de l'ordinateur > Utilisateurs et groupes locaux > Groupes**, sélectionnez UcceConfig et ajoutez l'utilisateur testconfig1 à celui-ci.



5. Déconnectez-vous de l'ordinateur et connectez-vous avec les identifiants de l'utilisateur testconfig1. Comme cet utilisateur dispose de droits de configuration, il pourra exécuter des outils de configuration CCE tels que Configuration Manager, Script ou Internet Script Editor.

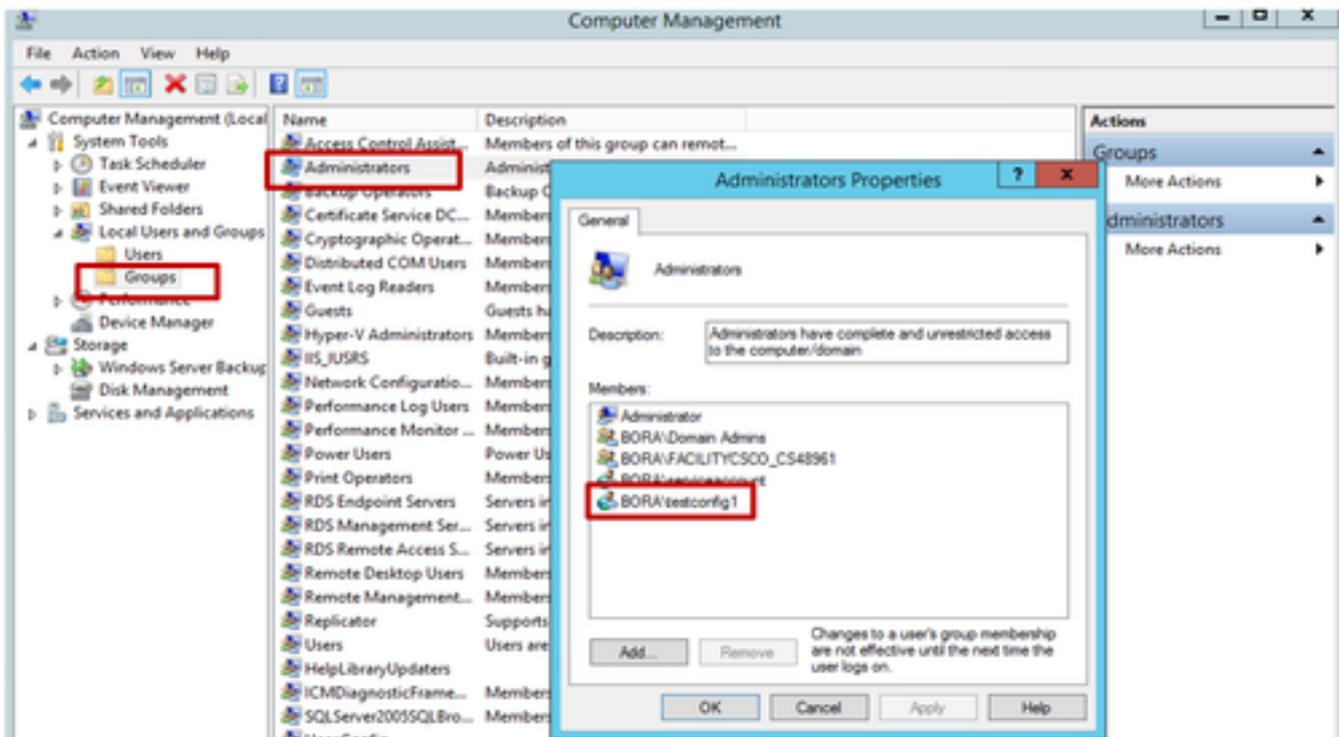
6. Cependant, si l'utilisateur tente d'exécuter une tâche nécessitant des droits de configuration, il échoue.

Cet exemple illustre la configuration de test config1 user change device gateway (pg) et le système restreint la modification par un message d'avertissement.

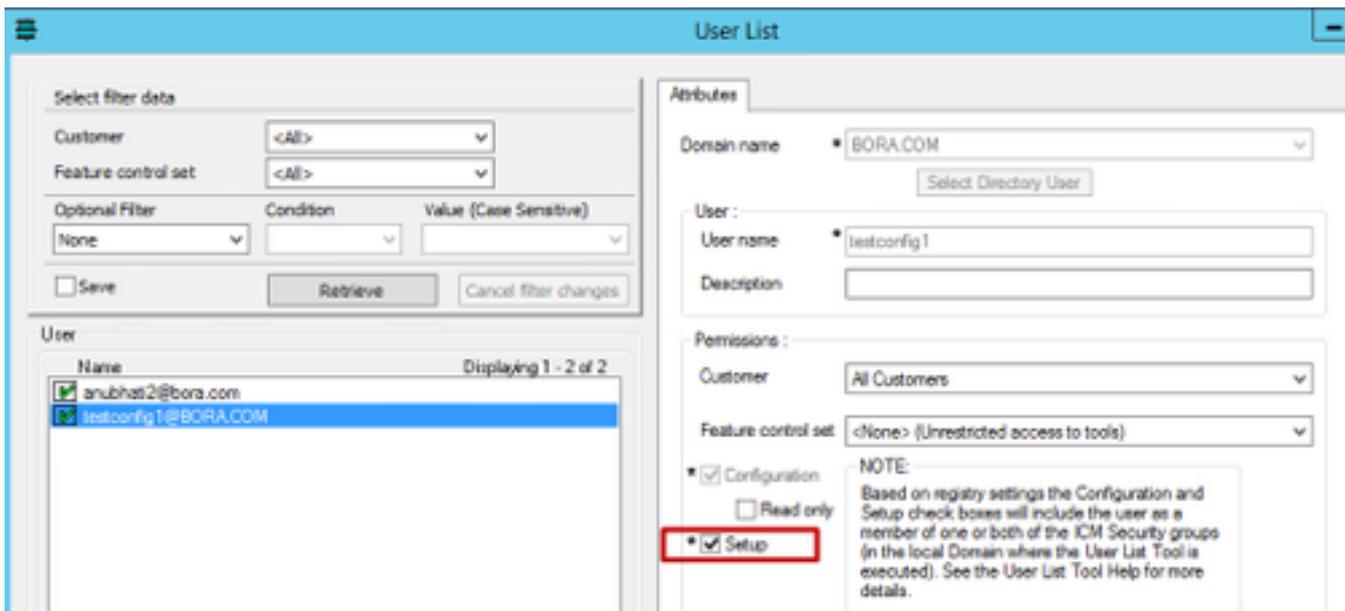


7. Si l'entreprise exige que cet utilisateur dispose de droits de configuration et de configuration, vous devez vous assurer que l'utilisateur est ajouté au groupe d'administrateurs locaux du serveur AW.

8. Afin d'atteindre, connectez-vous au serveur AW avec le compte de droits d'administration du domaine ou local et via la **gestion de l'ordinateur > Utilisateurs et groupes locaux > groupes** sélectionnez Groupes et dans Administrateurs ajoutez l'utilisateur à l'utilisateur.



9. Dans l'outil de liste Configuration Manager via User, sélectionnez l'utilisateur et activez l'option de configuration.



10. L'utilisateur peut désormais accéder à toutes les ressources de l'application CCE sur ce serveur AW et apporter les modifications souhaitées.

Vérification

La procédure de vérification fait en fait partie du processus de configuration.

Dépannage

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