

Configurar a autorização local do UCCE 12.0(X)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Etapa 1. Configurar permissões de registro](#)

[Etapa 2. Configurar permissões de pasta](#)

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve as etapas necessárias para remover a dependência do microsoft active directory (AD) para gerenciar a autorização em componentes do Unified Contact Center Enterprise (CCE).

Contribuído por Anuj Bhatia, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Contact Center Enterprise
- Microsoft Active Directory

Componentes Utilizados

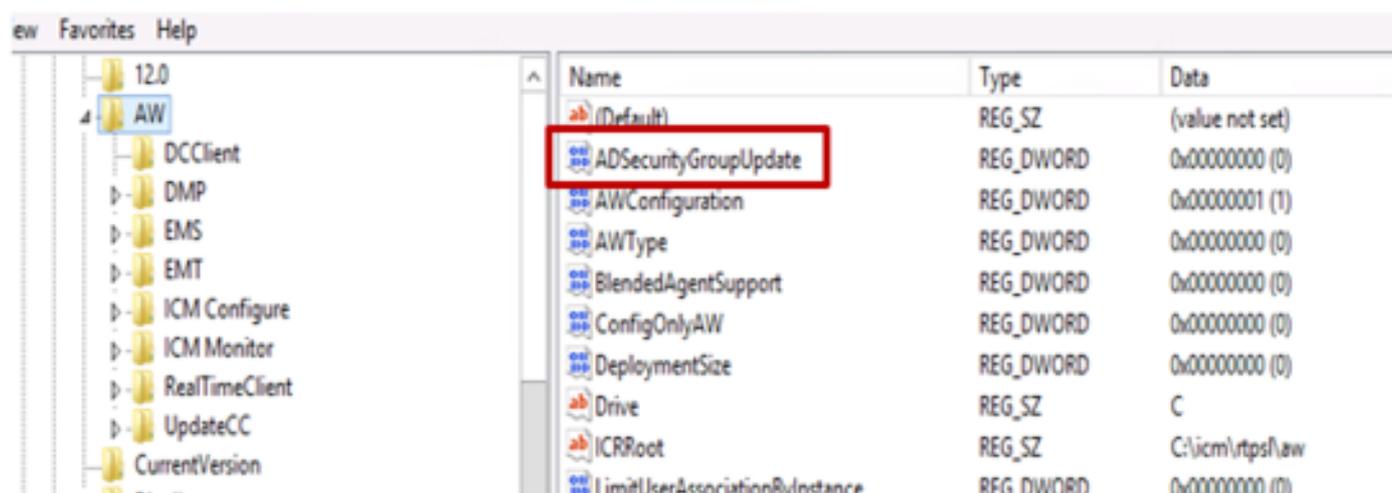
As informações usadas no documento são baseadas na versão 12.0(1) da solução UCCE.

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. Se a sua rede estiver ativa, certifique-se de que você entende o impacto potencial de qualquer etapa.

Informações de Apoio

A versão do UCCE 12.X fornece privilégios de associação de usuário para grupos de usuários locais no Servidor de Administração (AW) local, que permite que os usuários movam a autorização para fora do Active Directory (AD). Isso é controlado pelo registro

ADSecsecurityGroupUpdate que, por padrão, é ativado e evita o uso de grupos de segurança do Microsoft AD para controlar os direitos de acesso do usuário para executar tarefas de configuração e configuração.



The screenshot shows the Windows Registry Editor with the left pane displaying the tree structure under '12.0' > 'AW'. The right pane shows a list of registry values. The 'ADSecsecurityGroupUpdate' value is highlighted with a red box. The table below represents the data shown in the right pane.

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\rtpsflaw
LimitUserAssociationInstance	REG_DWORD	0x00000000 (0)

Note: Se a empresa desejar escolher o comportamento anterior, o sinalizador **ADSecsecurityGroupUpdate** pode ser alterado para 1, o que permite a atualização para o Ativo Diretory (AD)

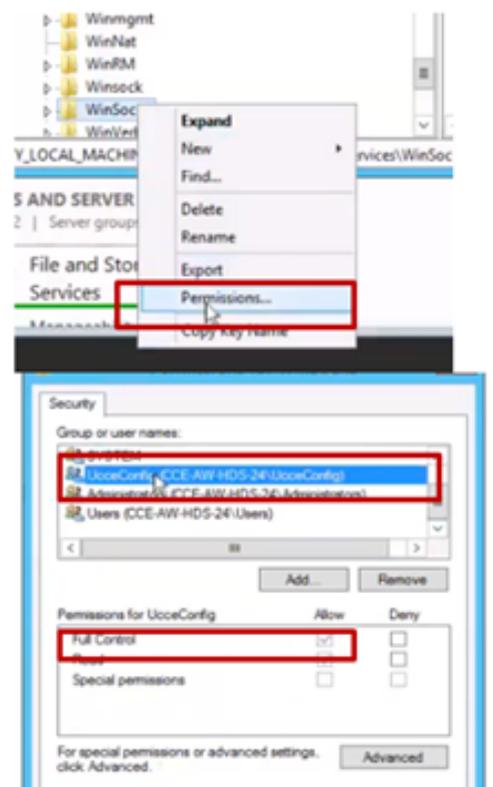
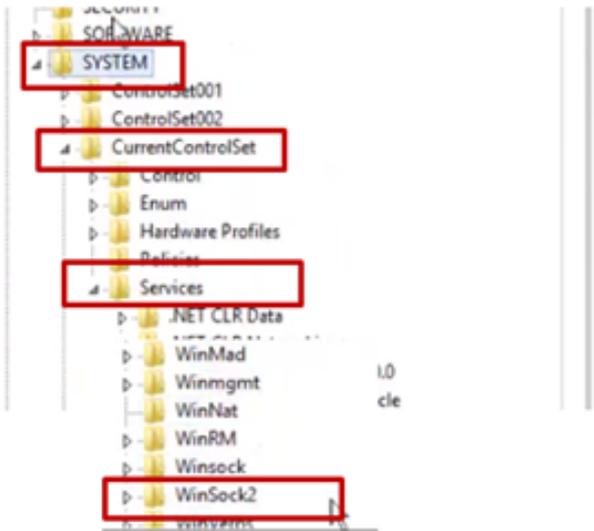
Para mover a autorização para fora do AD, é necessária uma tarefa única em cada máquina do servidor AW para conceder as permissões necessárias para o grupo **UcceConfig** e este documento tem como objetivo apresentar as etapas necessárias para configurar essas permissões, juntamente com um exemplo de como mapear um usuário de domínio como parte do grupo **Configuração e Configuração** do CCE.

Configurar

Conceder permissões de grupo **UcceConfig** no servidor AW local é um processo de duas etapas: primeiro, as permissões são fornecidas no nível do registro e, segundo, passadas para o nível da pasta.

Etapa 1. Configurar permissões de registro

1. Execute o utilitário **regedit.exe**.
2. Selecione **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2**.
3. Em **Permissões**, na guia **segurança**, selecione o grupo **UcceConfig** e marque a opção **Permitir controle total**.



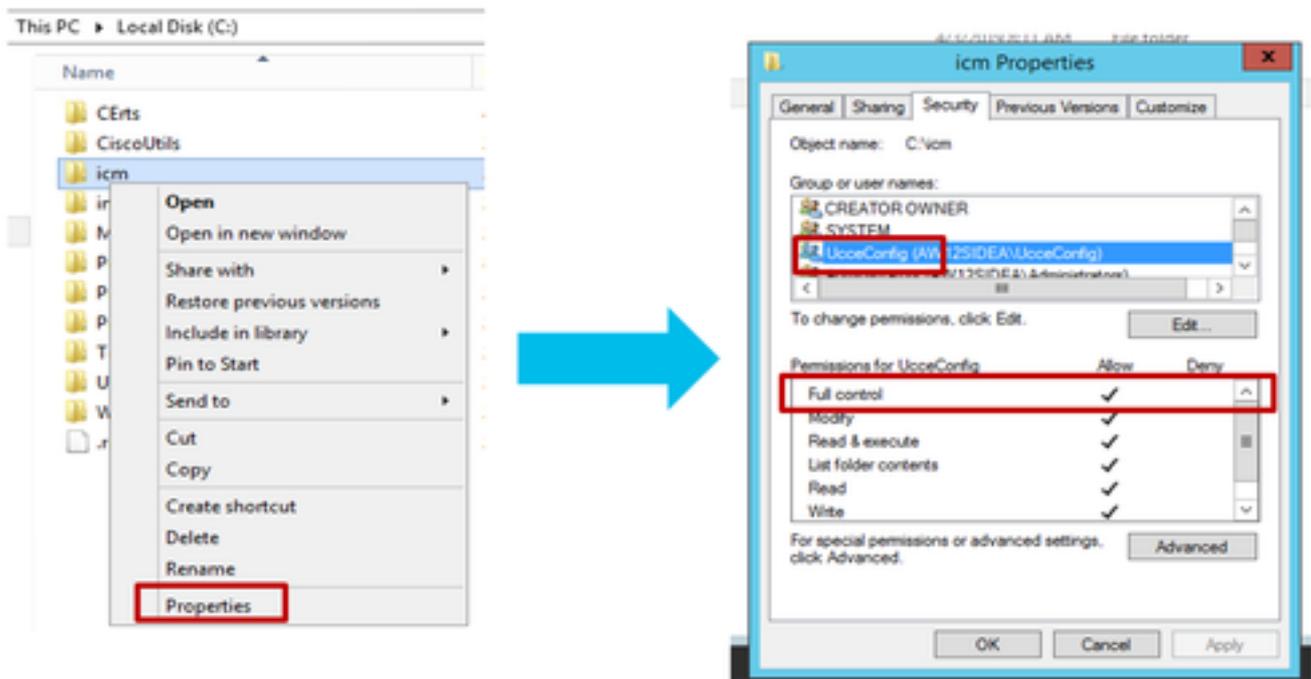
4. Repita as etapas anteriores para conceder Controle Total ao grupo UcceConfig para registros

- Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, inc.\ICM
- Computer\HKEY_LOCAL_MACHINE\SOFTWAREWow6432Node\Cisco Systems, inc.\ICM

Etapa 2. Configurar permissões de pasta

1. No Windows Explorer, selecione C:\icm and go to Properties.

2. Na guia Segurança, selecione **UcceConfig** e marque a opção **Permitir controle total**.



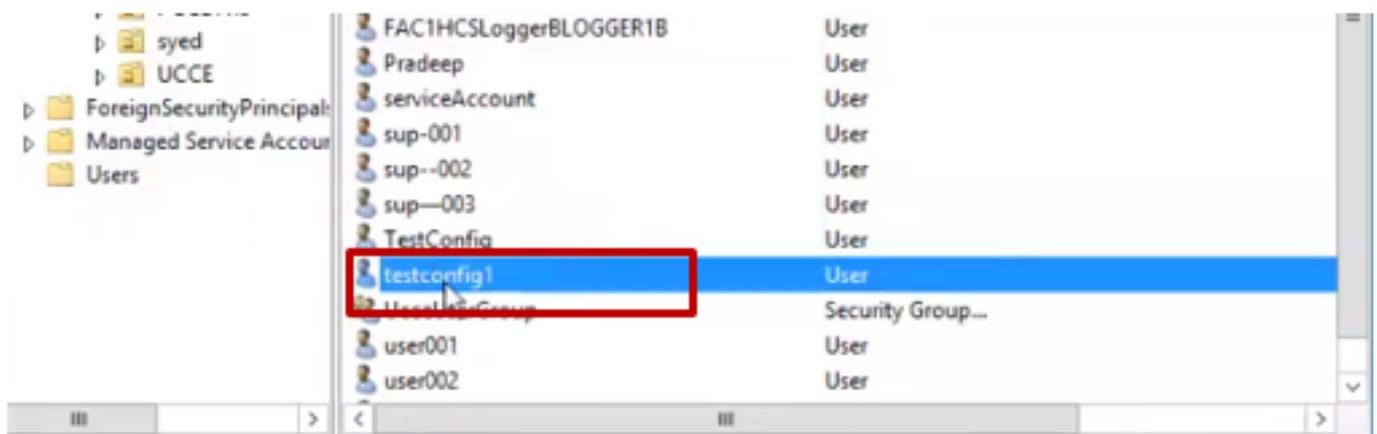
3. Selecione OK para salvar a alteração.

4. Repita as etapas anteriores para conceder controle total ao grupo **UcceConfig** para C:\Temp folder.

À medida que a configuração preliminar do Dia 0 foi alcançada, examine as etapas de como você pode promover um usuário de domínio para ter direitos de configuração e configuração.

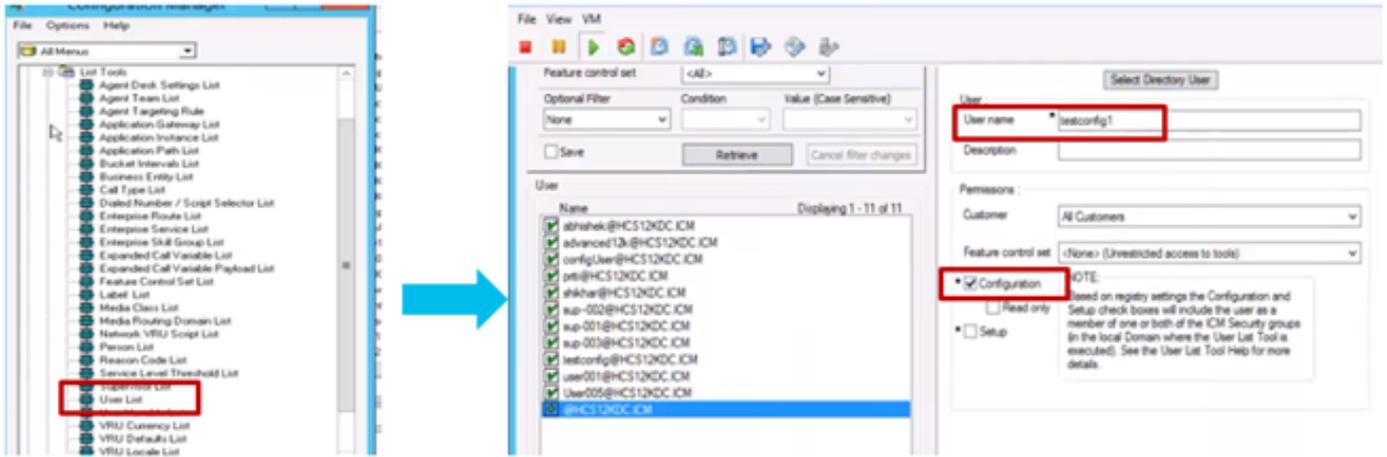
Passo 3: Configuração do usuário de domínio

1. Crie um usuário de domínio no AD, pois esse usuário do testesde exercício config1 foi criado.

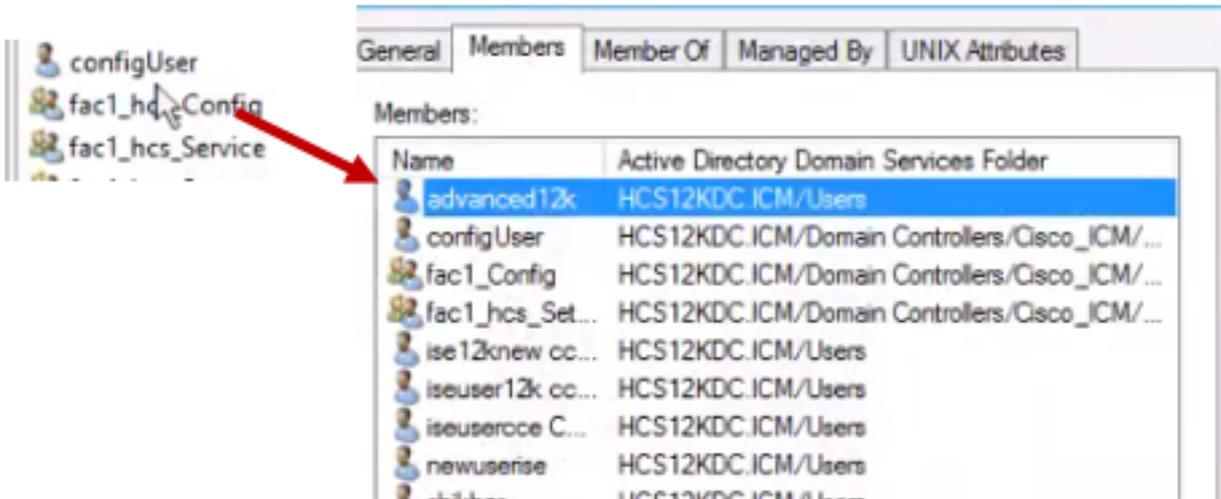


2. Efetue login no servidor AW com uma conta de administrador de domínio ou local.

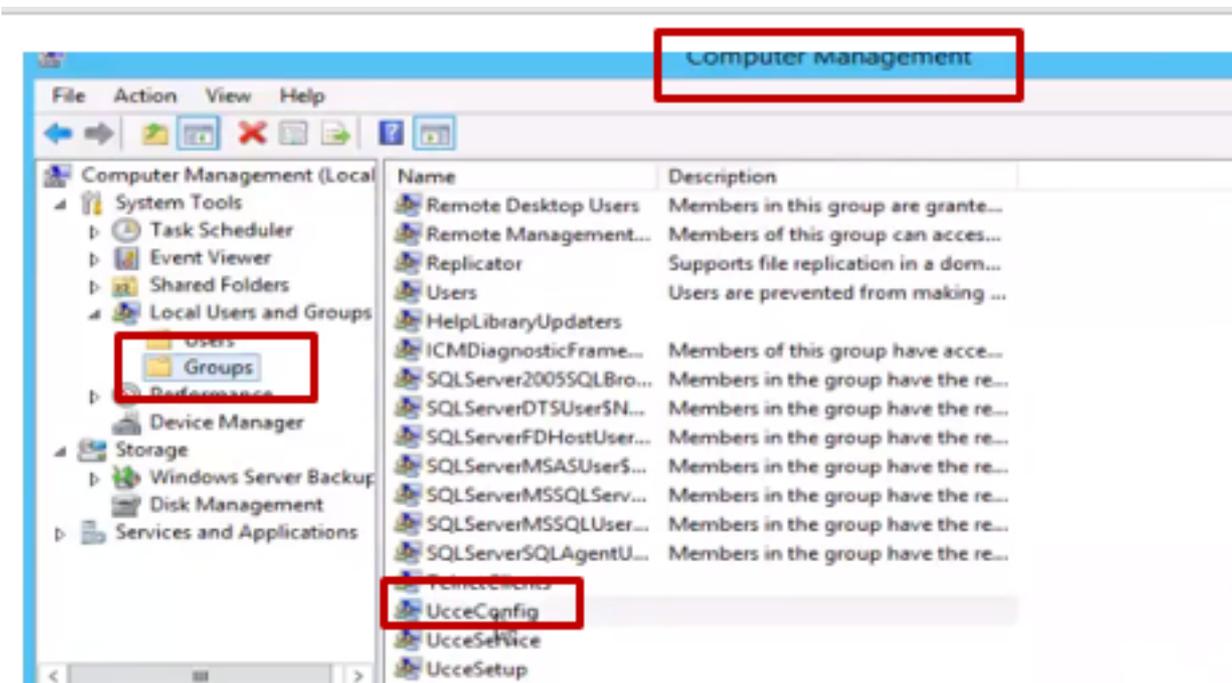
3. No gerenciador de configuração através da ferramenta Lista de usuários, adicione o usuário e marque a opção **de configuração**.



Antes da versão 12.0, esta alteração teria atualizado os grupos de segurança Config no domínio sob uma unidade organizacional (OU) de instância, mas com a versão 12.0, o comportamento padrão é que ela não adiciona esse usuário ao grupo AD. Como mostrado na imagem, não há nenhuma atualização desse usuário no grupo de segurança Config do ICM de domínio.



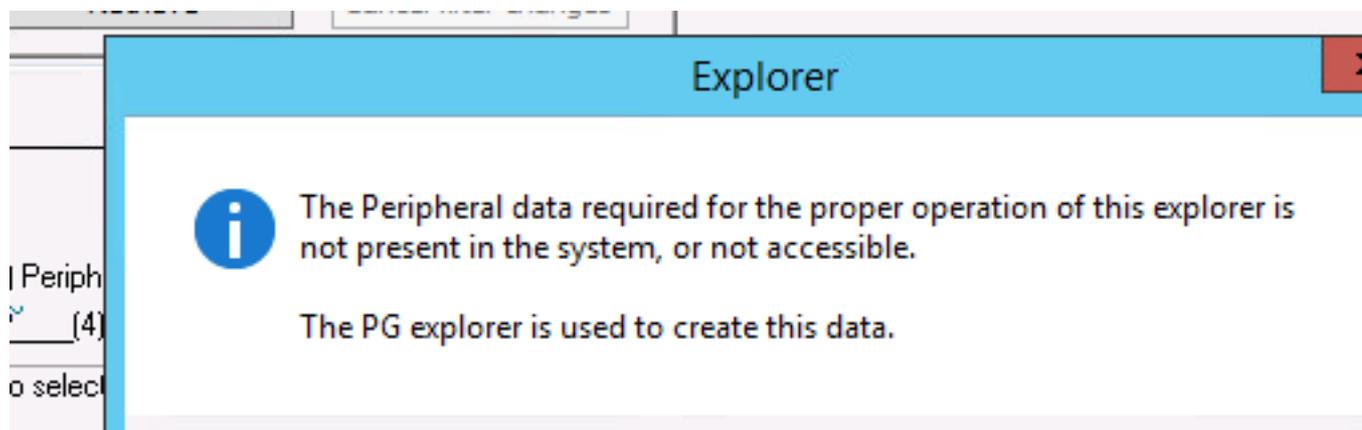
4. No AW Server em **gerenciamento de computador > Usuários e grupos locais > Grupos**, selecione UcceConfig e adicione testconfig1 usuário a ele.



5. Faça logoff da máquina e faça login com as credenciais do usuário testconfig1. Como esse usuário tem direitos de configuração, ele poderá executar ferramentas de configuração do CCE, como o Gerenciador de configuração, o Editor de scripts ou o Editor de scripts da Internet.

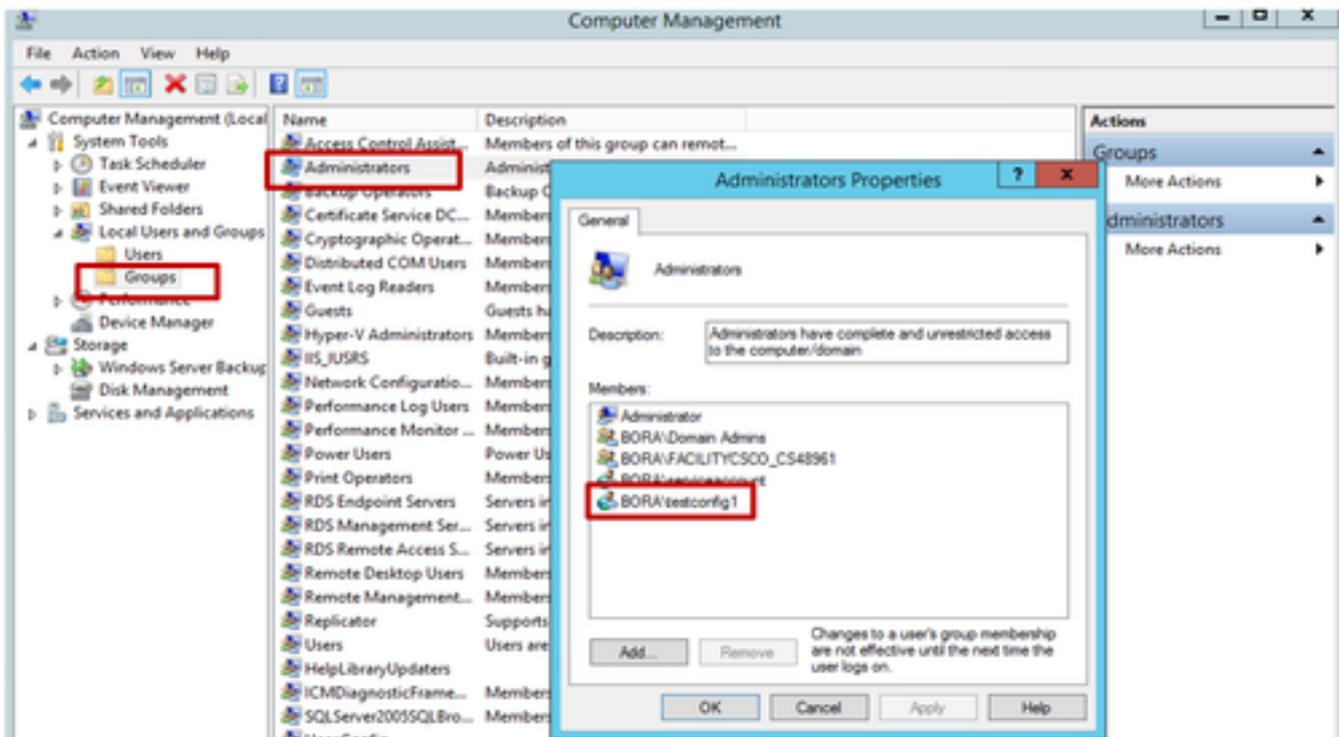
6. No entanto, se o usuário tentar executar qualquer tarefa que exija direitos de configuração, ela falhará.

Este exemplo mostra o testcase config1 user change peripheral gateway (pg) configuration and system restringe a alteração com uma mensagem de aviso.

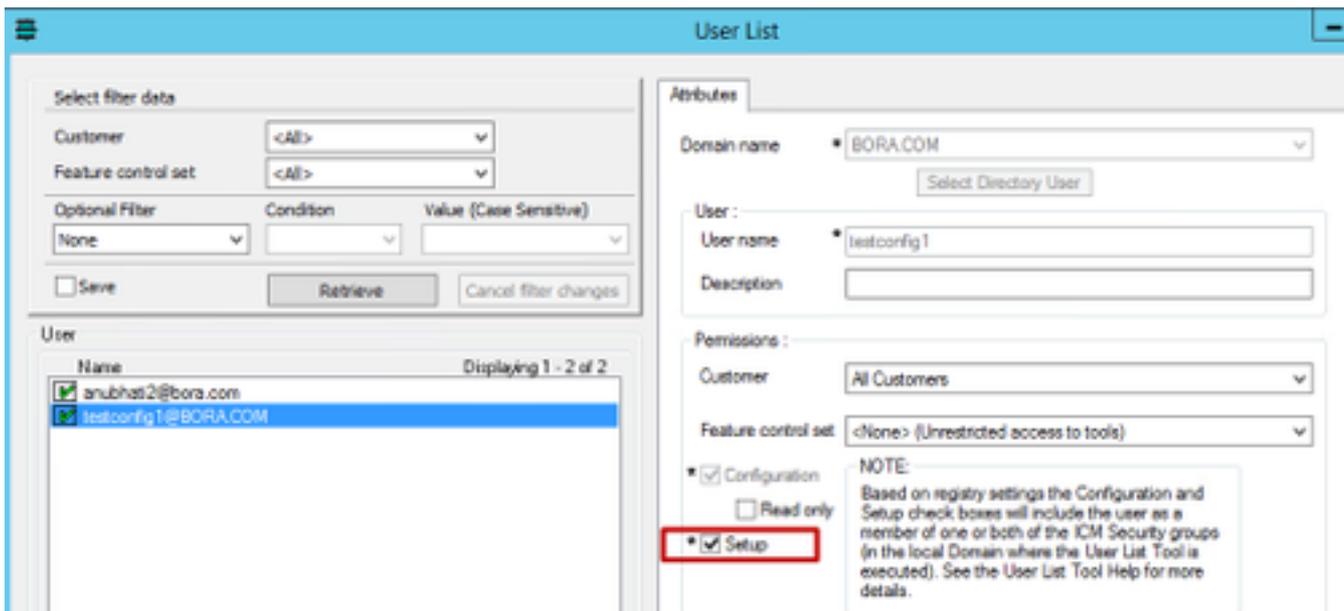


7. Se a empresa exigir que esse usuário tenha direitos de configuração junto com a configuração, você deverá garantir que o usuário seja adicionado ao grupo AW server Local Admin.

8. Para obter êxito, faça login no servidor AW com a conta de direitos de administrador de domínio ou local e por meio de **gerenciamento de computador > Usuários e grupos locais > grupos** selecione Grupos e, em Administradores, adicione o usuário ao usuário.



9. No Gerenciador de configurações através da ferramenta de lista Usuário, selecione o usuário e marque a opção de configuração.



10. O usuário agora pode acessar todos os recursos do aplicativo CCE nesse servidor AW e fazer as alterações desejadas.

Verificar

O procedimento de verificação faz parte do processo de configuração.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.