

Configurar autorização local PCCE

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

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

[Etapa 2. Configurar Permissões de Pasta.](#)

[Etapa 3. Configuração do usuário de domínio.](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve as etapas necessárias para remover a dependência do Microsoft Active Directory (AD) para gerenciar a autorização localmente nos componentes do Package Contact Center Enterprise (PCCE).

Contribuído por Meenakshi Sundaram, Ramiro Amaya e Anuj Bhatia, Engenheiros do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Package Contact Center Enterprise
- Microsoft Active Directory

Componentes Utilizados

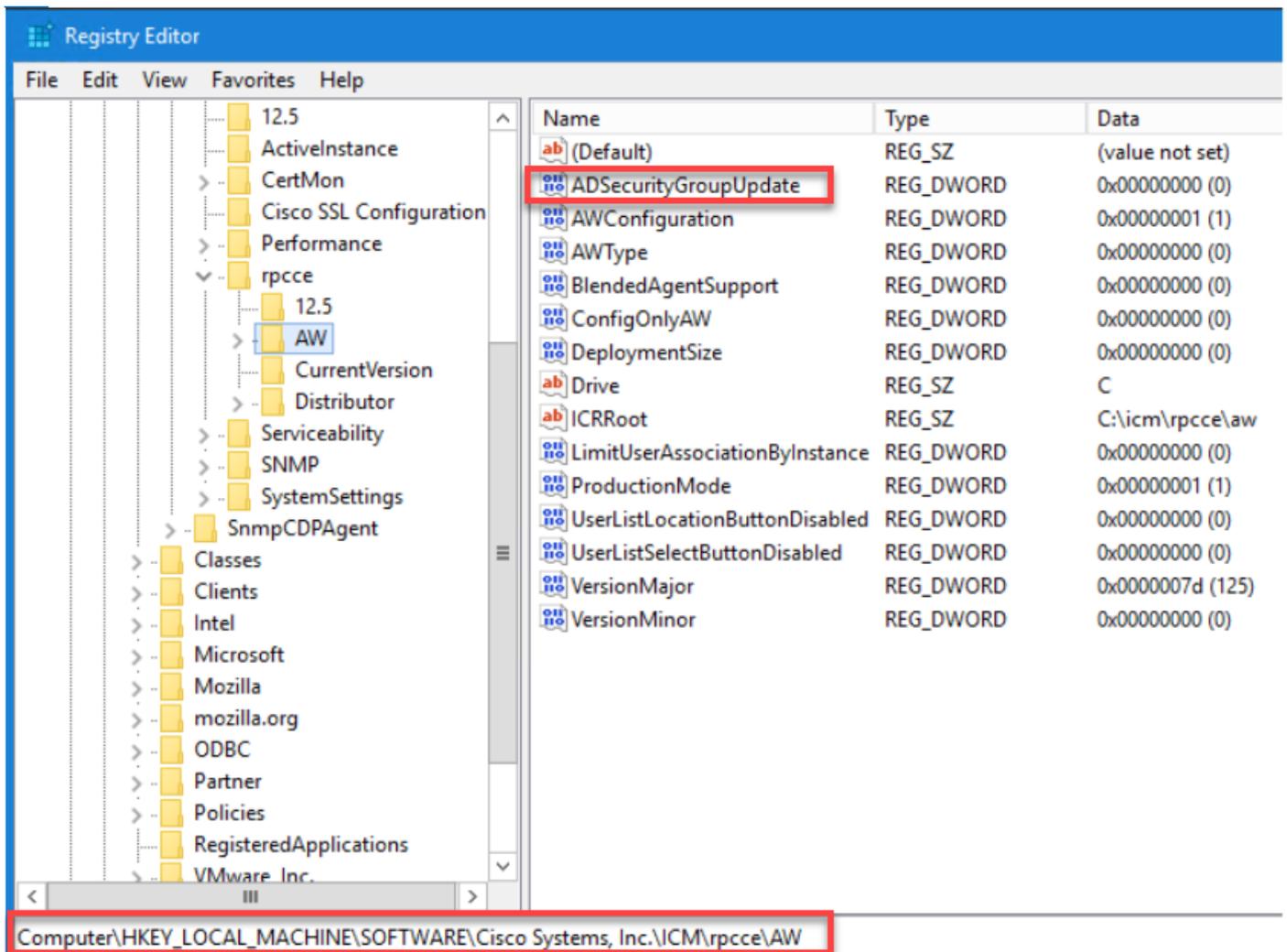
As informações usadas no documento são baseadas na versão PCCE 12.5(1).

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 PCCE 12.5 fornece privilégios de usuário para grupos de usuários locais nos Servidores de Administração (AW), que permite que os usuários retirem a autorização do Active Directory (AD). Isso é controlado pelo registro **ADSecsecurityGroupUpdate** que, por padrão, está 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.

Note: O suporte para a autorização local foi iniciado no Unified Contact Center Enterprise (UCCE) 12.0 e agora é suportado no PCCE 12.5.



Note: Se a empresa precisar ter o comportamento anterior implementado (autorização do AD), o sinalizador `ADSecsecurityGroupUpdate` pode ser alterado para 1.

Configurar

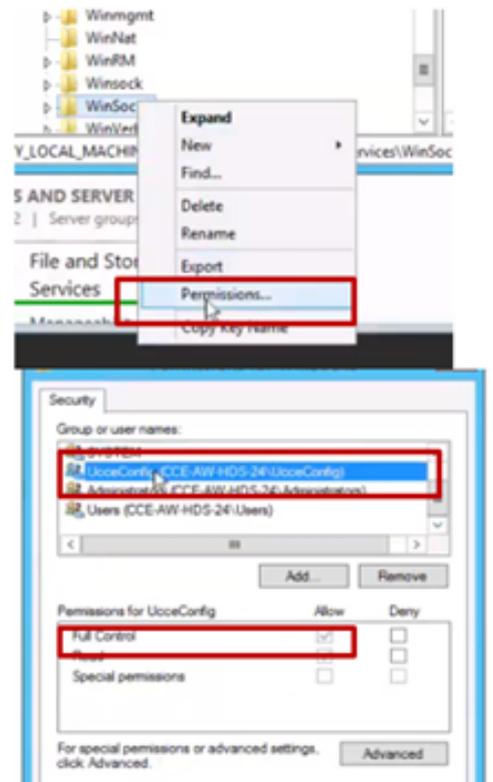
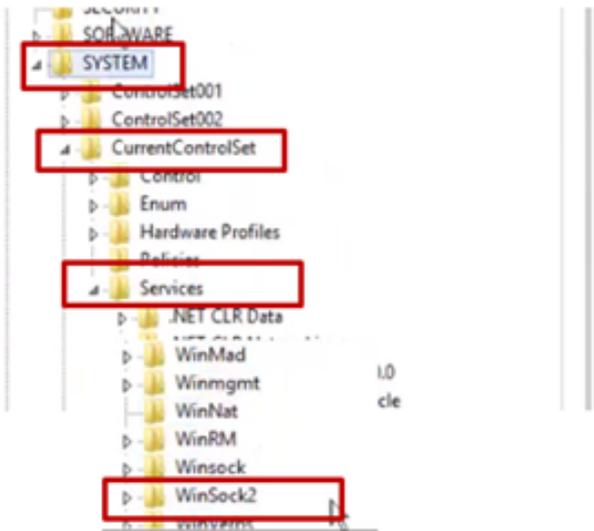
Para conceder permissões de grupo `UcceConfig` em um servidor AW local, primeiro, é necessário fornecer permissões no nível do registro e, segundo, no nível da pasta.

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**.



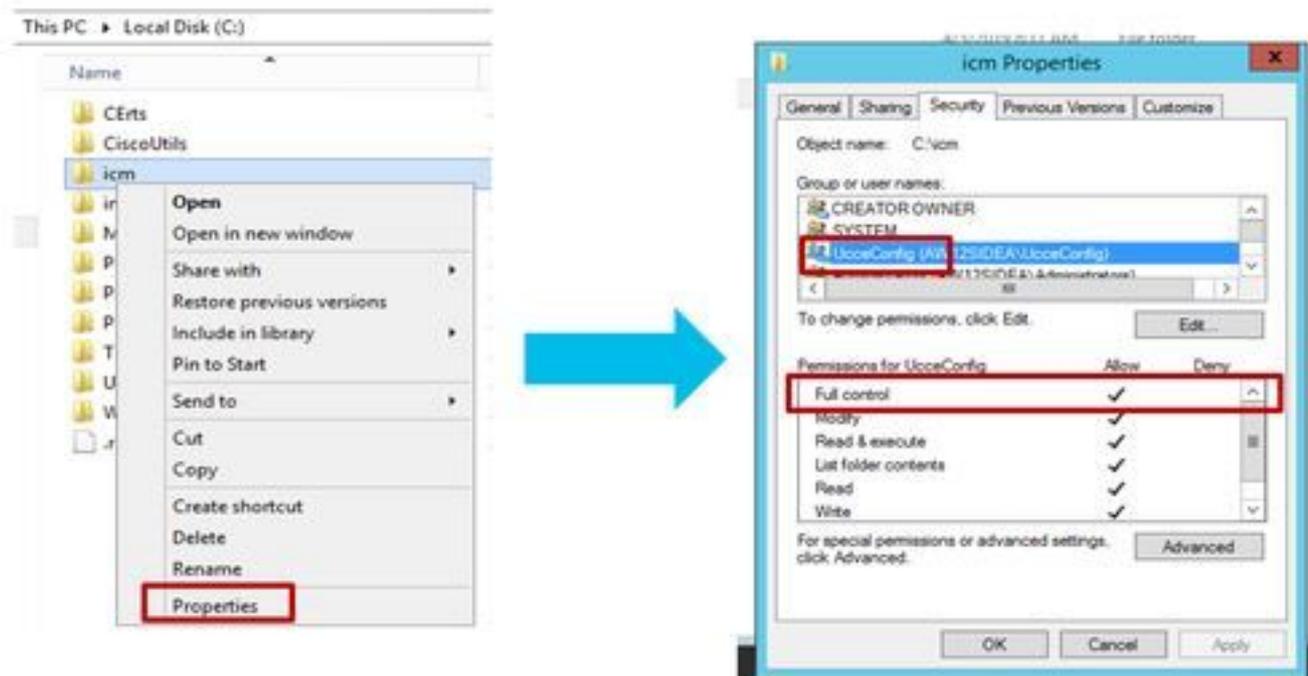
4. Repita as etapas anteriores para conceder controle total ao grupo **UcceConfig** para esses registros.

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

Etapa 2. Configurar Permissões de Pasta.

1. No Windows Explorer, navegue para <ICM Installed Directory>:\icm e selecione Properties.

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



3. Selecione OK para salvar as alterações.

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

5. No SQL Management Studio, faça o seguinte:

a) Navegue até Segurança > Logons.

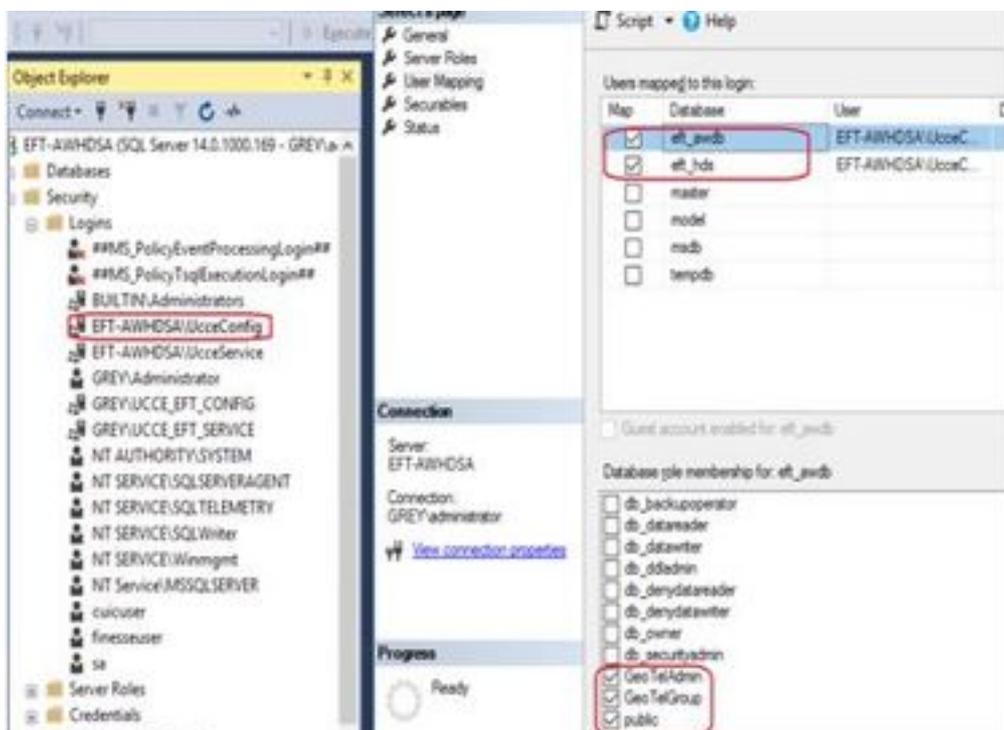
b) Localize <Machine name>\UcceConfig.

c) Clique com o botão direito do mouse e selecione propriedades.

d) Navegue pelos Mapeamentos de usuário e selecione o banco de dados AWDB.

e) Marque as caixas de seleção GeoTelAdmin, GeoTelGroup e public.

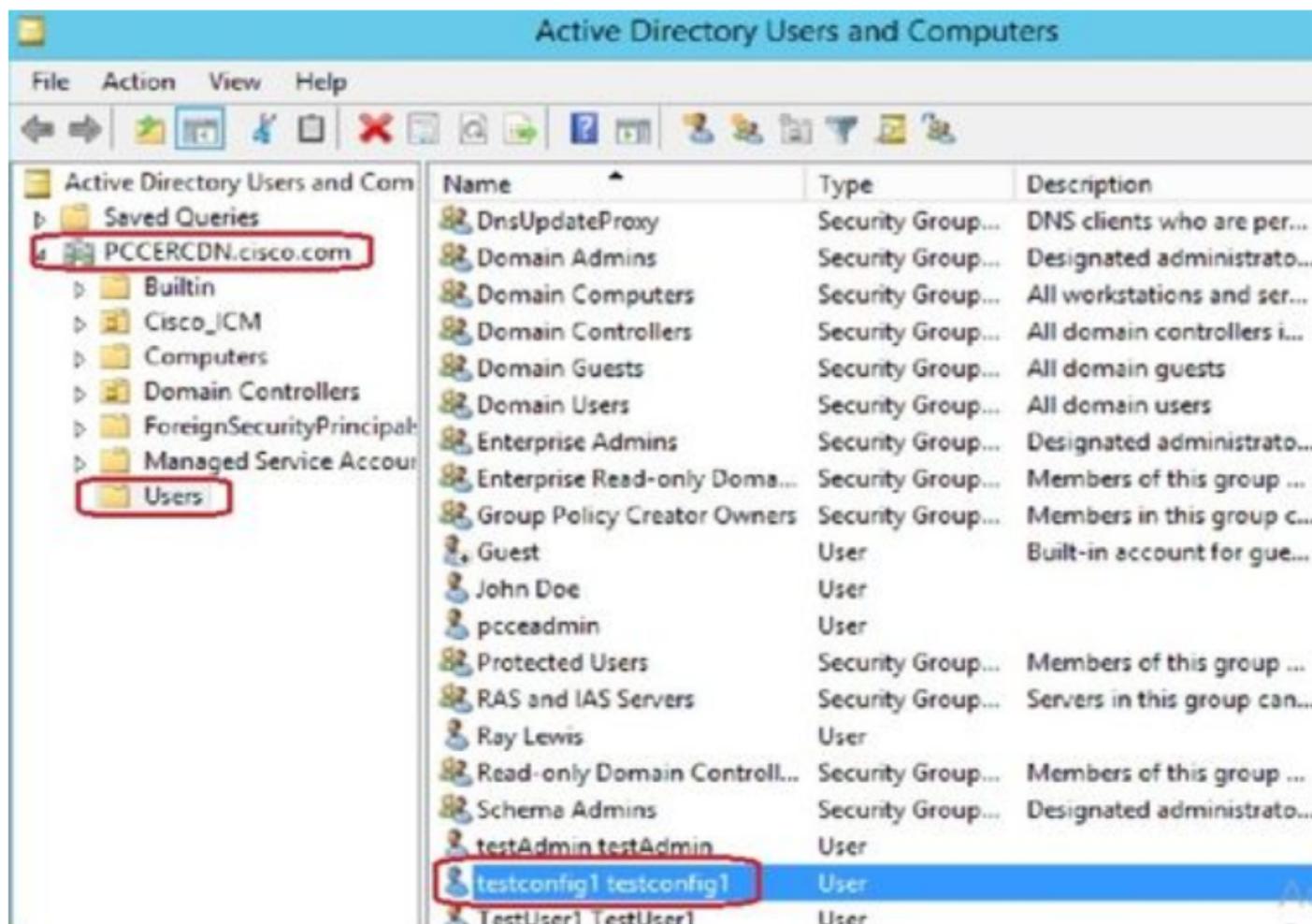
f) Repita a etapa d) para o banco de dados de dados de histórico (HDS).

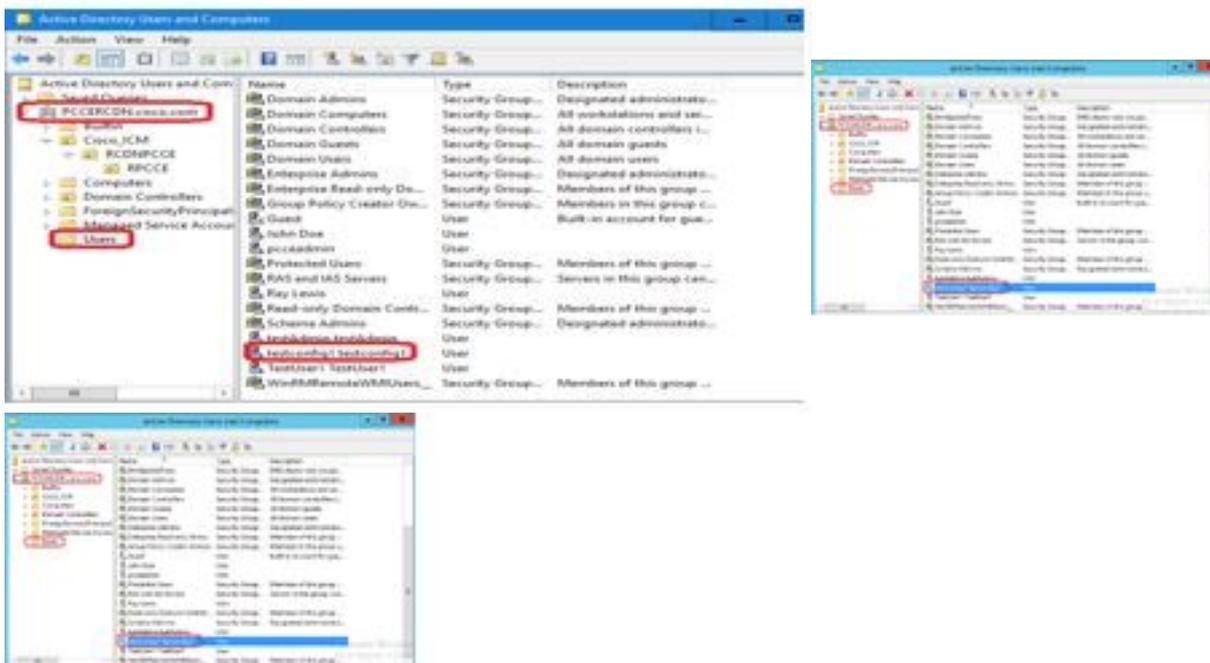


Como a configuração preliminar foi obtida, siga as etapas de como você pode promover um usuário de domínio para ter direitos de configuração e configuração.

Etapa 3. Configuração do usuário de domínio.

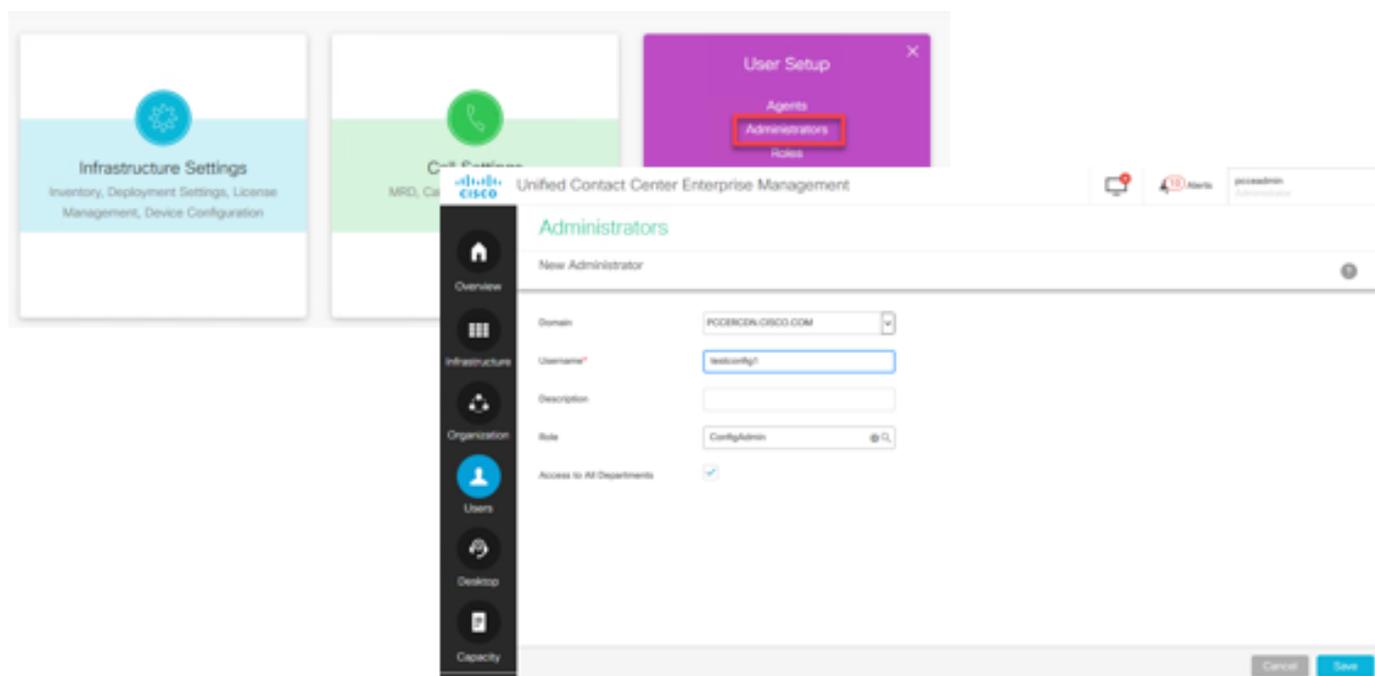
1. Crie um usuário de domínio no AD. Para este usuário do exercício testconfig1 foi criado.



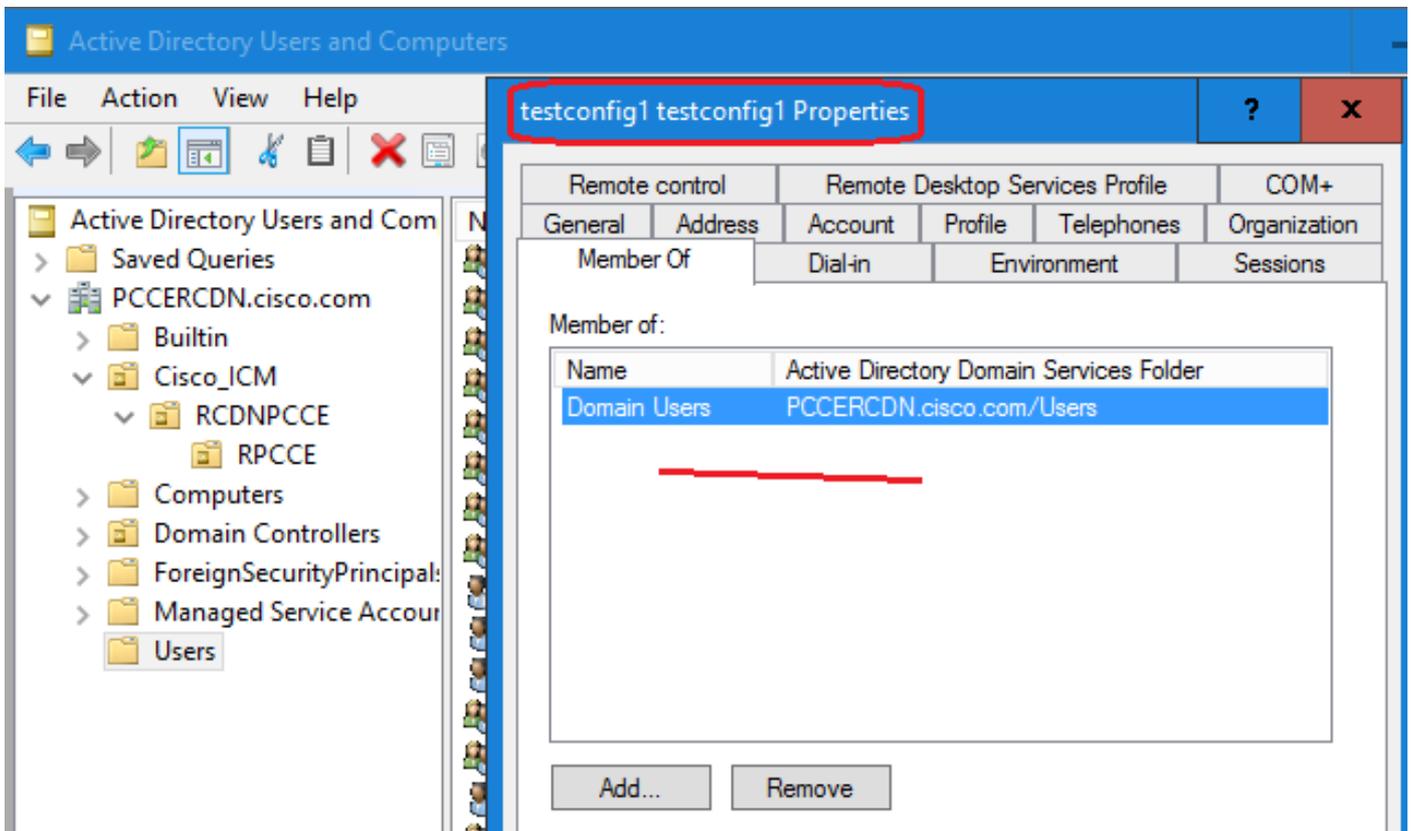


2. Faça login no servidor AW com uma conta admin de domínio ou admin local.

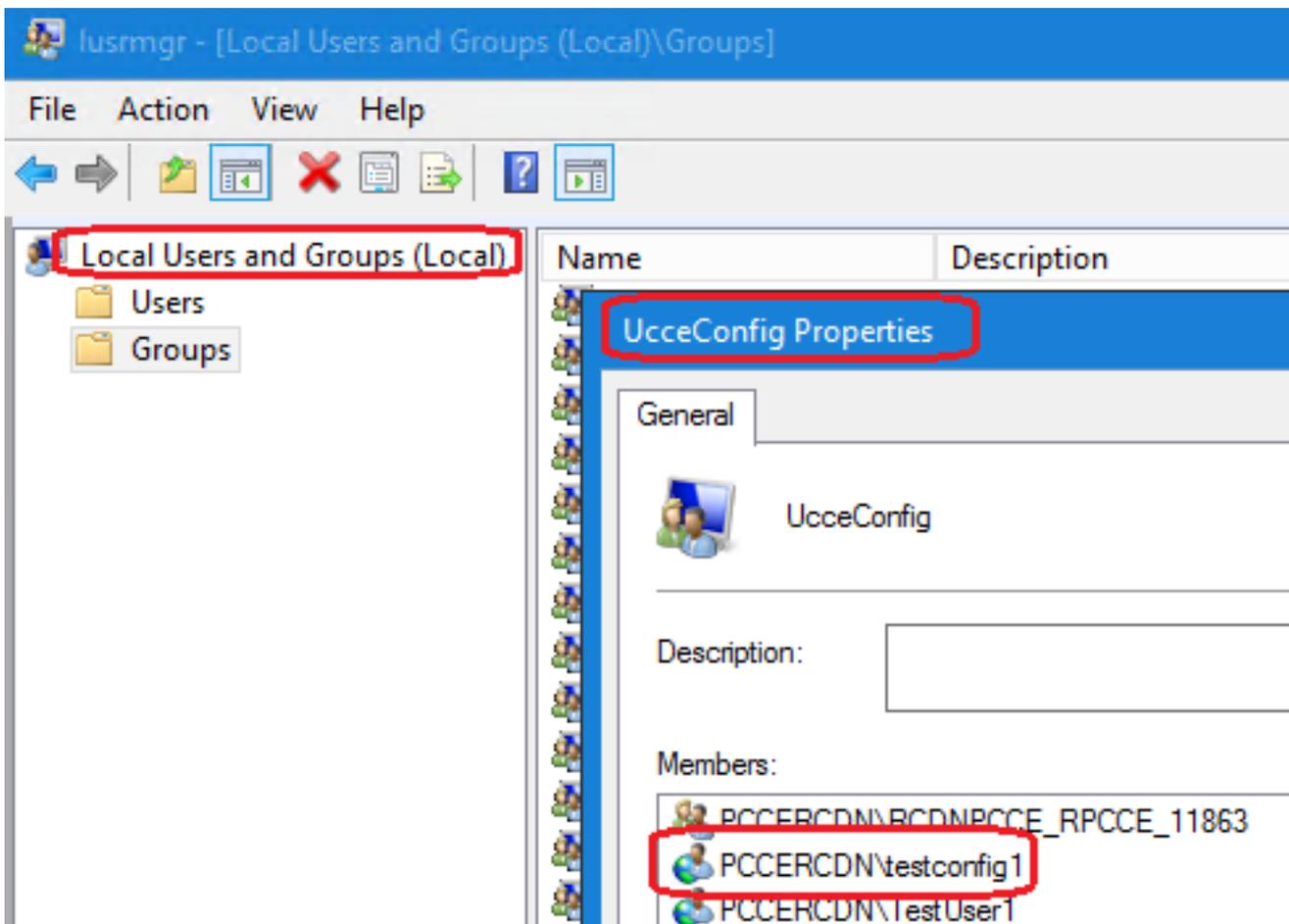
3. Abra o CCE Admin no AW. Navegue até o cartão User Setup e selecione Administrators. Adicione o usuário e selecione a função **ConfigAdmin**.



Antes da versão 12.5 do PCCE, essa alteração teria atualizado os grupos de segurança de configuração no domínio sob uma unidade organizacional (OU) de instância, mas com 12.5 o comportamento padrão é não adicionar esse usuário ao grupo do 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.

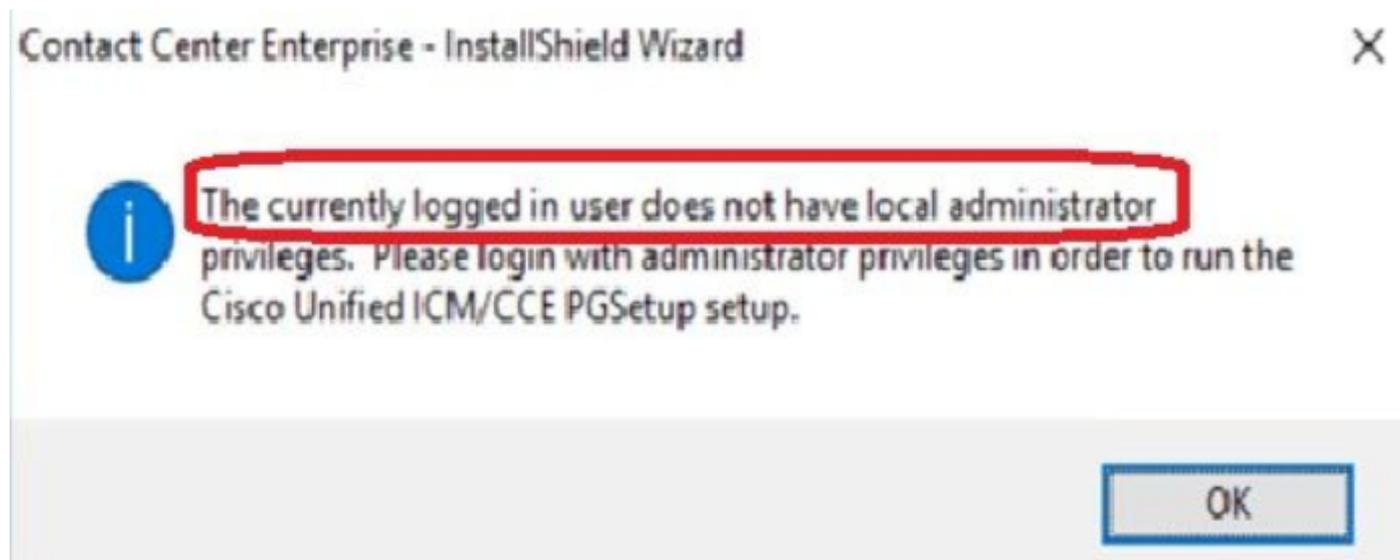


5. Faça logoff da máquina e faça logon com as credenciais do usuário testconfig1. Como esse usuário tem direitos de configuração, ele pode executar ferramentas de configuração do CCE,

como o CCE Admin, Script ou Internet Script Editor.

6. No entanto, se o usuário tentar executar qualquer tarefa que exija direitos de configuração, ela falhará. Este usuário não tem acesso a todos os recursos do CCE Admin ou ferramentas de configuração.

Como mostrado na imagem, o usuário testconfig1 na implantação do PCCE 4K tenta executar a configuração do Gateway Periférico (PG) e o sistema 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 a função de usuário seja alterada para SystemAdmin em CCEAdmin.

Administrators

Edit testconfig1@PCCERCDN.CISCO.COM

Domain

PCCERCDN.CISCO.COM

Username*

testconfig1

Description

Role

SystemAdmin

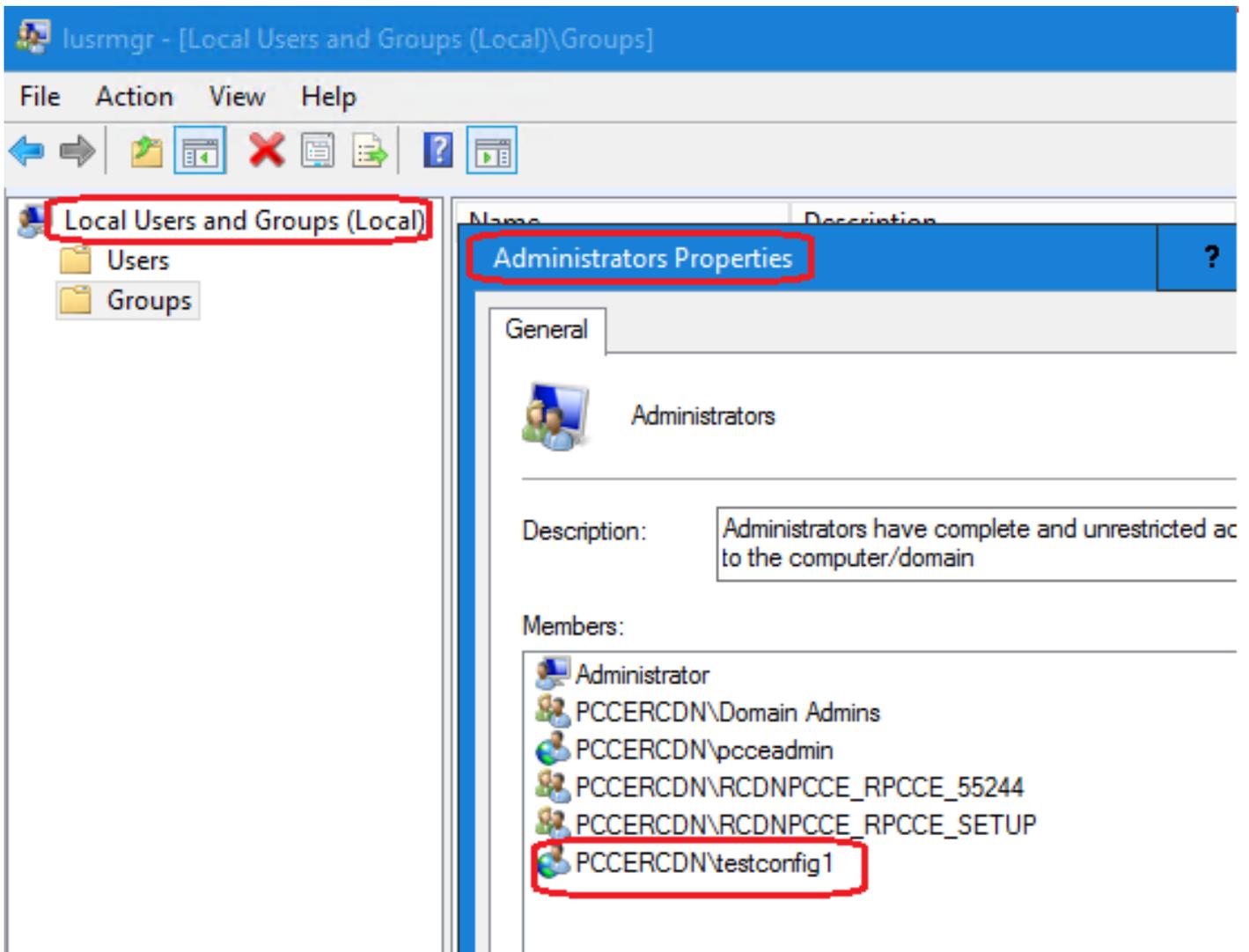
Access to All Departments



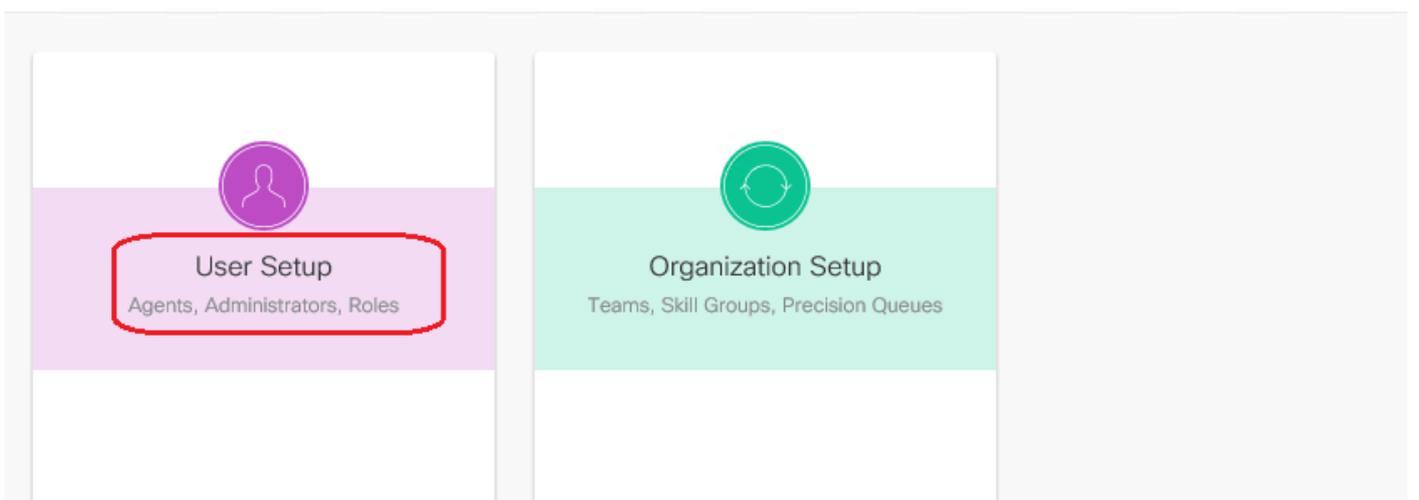
A função de usuário foi atualizada como 1 (SystemAdmin) no banco de dados:

	UserRole	UserGroupID	CustomerDefinitionID	UserGroupName	UserGroupType	Description	ServiceProvider	ReadOnly	FeatureSetID
1	0	1	NULL	DBO	U	The ICM System Administrator	Y	N	NULL
2	0	5000	NULL	PCCERCDN\RLEWIS	U	NULL	N	N	NULL
3	1	5002	NULL	PCCERCDN\TESTCONFIG1	U	NULL	N	N	5000
4	2	5001	NULL	PCCERCDN\TESTUSER1	U	NULL	N	N	5001

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



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 há etapas específicas disponíveis para solucionar problemas dessa configuração.

Informações Relacionadas

[guia de administração de PCCE](#)

[Suporte Técnico e Documentação - Cisco Systems](#)