

UCCE 12.0(X) 로컬 권한 부여 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[1단계. 레지스트리 권한 구성](#)

[2단계. 폴더 권한 구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

소개

이 문서에서는 CCE(Unified Contact Center Enterprise) 구성 요소의 권한 부여를 관리하기 위해 microsoft AD(active directory)의 종속성을 제거하는 데 필요한 단계에 대해 설명합니다.

기고자: Anuj Bhatia, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Unified Contact Center Enterprise
- Microsoft Active Directory

사용되는 구성 요소

이 문서에 사용된 정보는 UCCE 솔루션 12.0(1) 버전을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 단계의 잠재적 영향을 이해해야 합니다.

배경 정보

UCCE 12.X 릴리스는 로컬 AW(관리 서버)의 로컬 사용자 그룹에 대한 사용자 구성원 권한을 제공하며, 이를 통해 사용자는 AD(Active Directory)에서 권한 부여를 이동할 수 있습니다. 이는 기본적으로 활성화되어 Microsoft AD 보안 그룹을 사용하여 설정 및 구성 작업을 수행하기 위한 사용자 액세스 권한을 제어하지 않는 레지스트리 ADSecurityGroupUpdate에 의해 제어됩니다.

Name	Type	Data
(Default)	REG_SZ	(value not set)
ADSecurityGroupUpdate	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\law
LimitUserAssociationByInstance	REG_DWORD	0x00000000 (0)

참고:비즈니스가 이전 동작을 선택하려는 경우 ADSecurityGroupUpdate 플래그를 1로 변경하여 AD(Active Directory)로 업데이트할 수 있습니다.

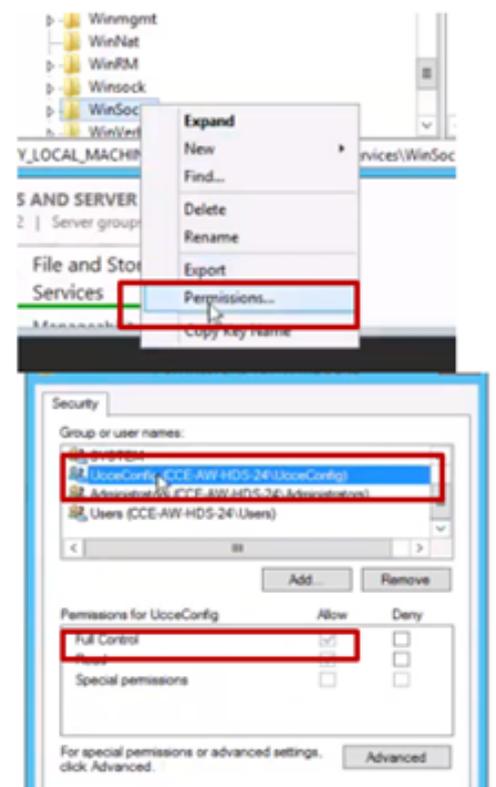
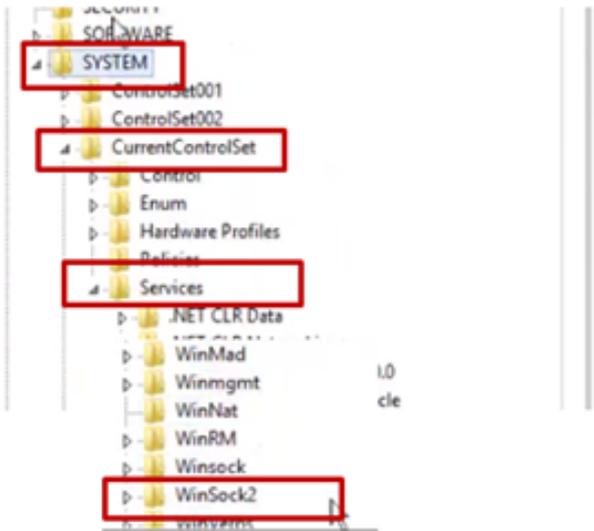
AD에서 권한 부여를 이동하려면 각 AW 서버 컴퓨터에서 UcceConfig 그룹에 필요한 권한을 부여하는 일회성 작업이 필요하며, 이 문서는 도메인 사용자를 CCE 구성 및 설정 그룹의 일부로 매핑하는 방법의 예와 함께 이러한 권한 구성에 필요한 단계를 시연하는 것을 목적으로 합니다.

구성

로컬 AW 서버에서 UcceConfig 그룹 권한을 부여하려면 두 단계 프로세스입니다.첫째, 사용 권한은 레지스트리 수준에서 제공되고 둘째 권한은 폴더 수준으로 전달됩니다.

1단계. 레지스트리 권한 구성

1. regedit.exe 유틸리티를 실행합니다.
2. HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2을 선택합니다.
3. Permissions(권한) 아래의 Security(보안) 탭에서 UcceConfig group(UcceConfig 그룹)을 선택하고 Allow(전체 제어 옵션 허용)을 선택합니다.



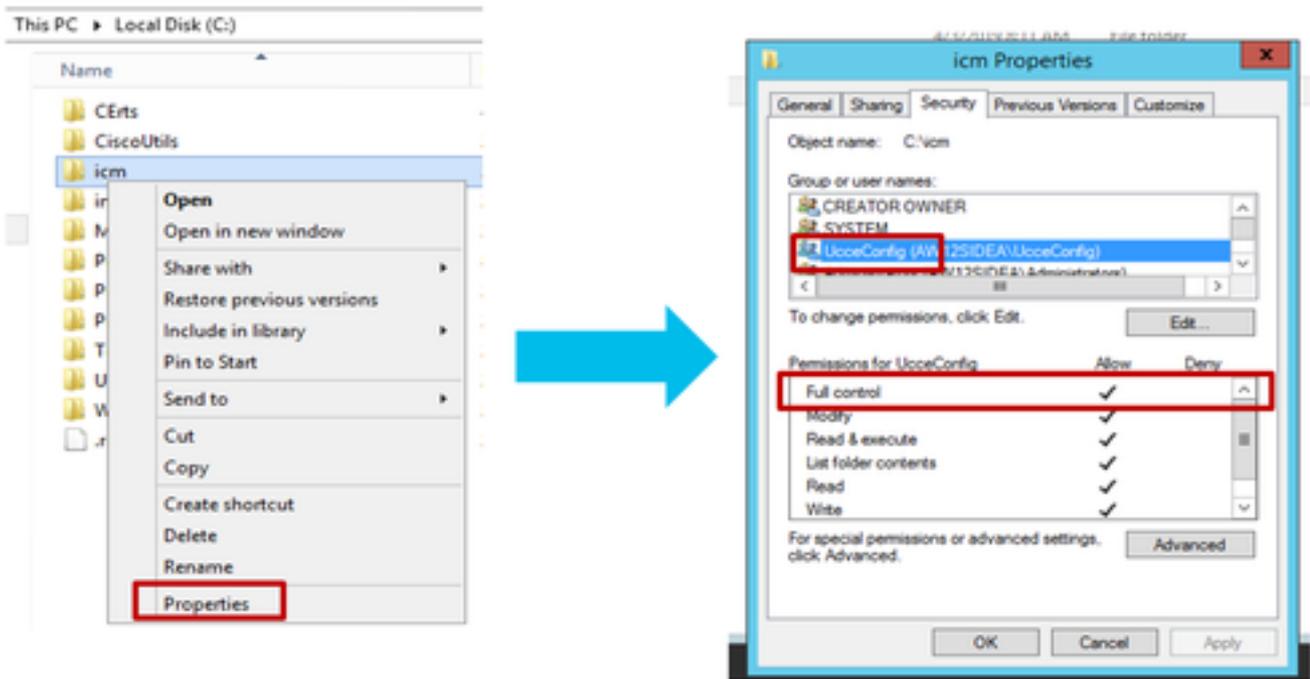
4. 이전 단계를 반복하여 레지스트리의 UcceConfig 그룹에 모든 권한을 부여합니다.

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

2단계. 폴더 권한 구성

1. Windows 탐색기에서 C:\icm and go to Properties을 선택합니다.

2. 보안 탭에서 UcceConfig를 선택하고 전체 제어 옵션에 대해 허용을 선택합니다.



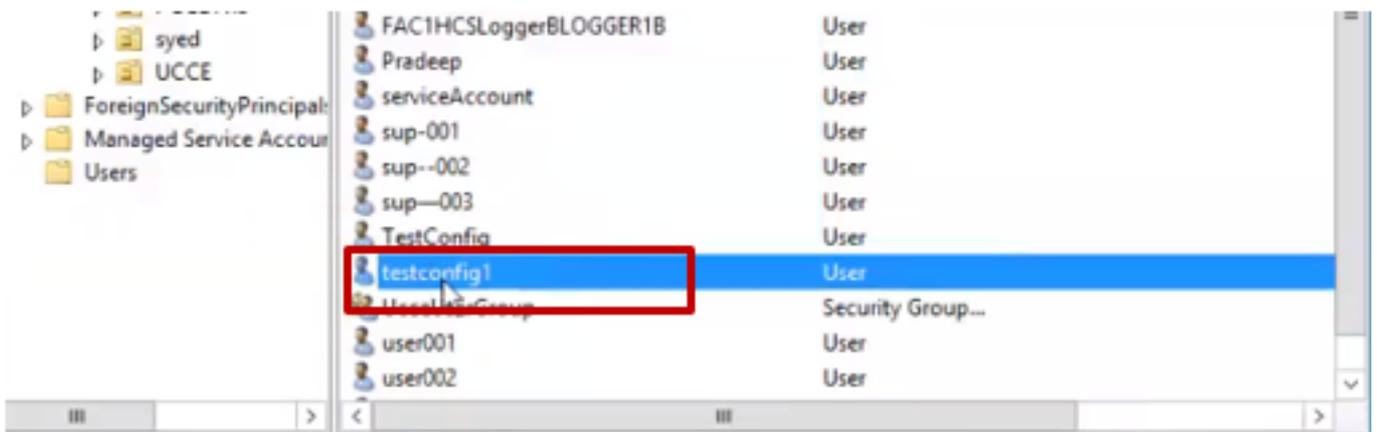
3. 확인을 선택하여 변경사항을 저장합니다.

4. 이전 단계를 반복하여 C:\Temp folder에 대한 UcceConfig 그룹에 모든 권한을 부여합니다.

Day 0 예비 컨피그레이션이 수신되었으므로 도메인 사용자를 구성 및 설정 권한을 갖도록 프로모션하는 방법에 대한 단계를 살펴봅니다.

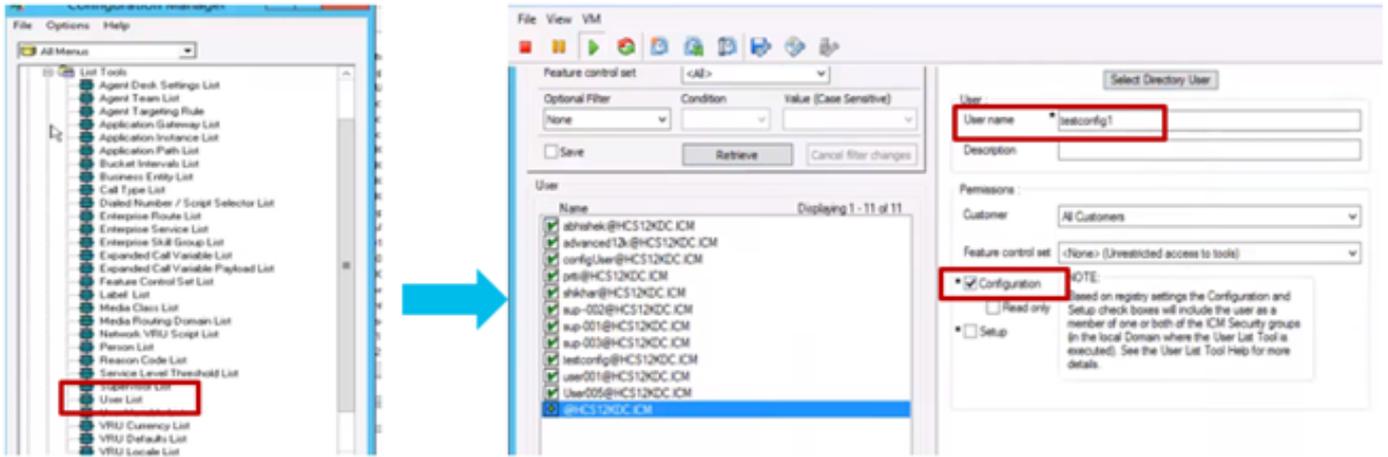
3단계:도메인 사용자 구성

1. AD에서 도메인 사용자를 생성합니다. 이 연습 testconfig1 사용자가 생성되었습니다.

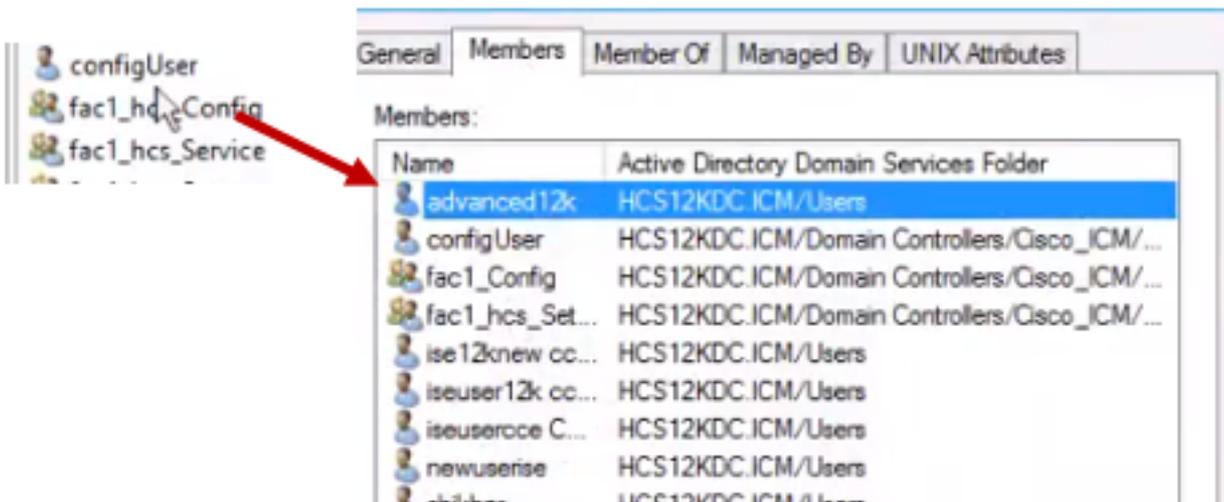


2. 도메인 도메인 또는 로컬 관리자 계정을 사용하여 AW 서버에 로그인합니다.

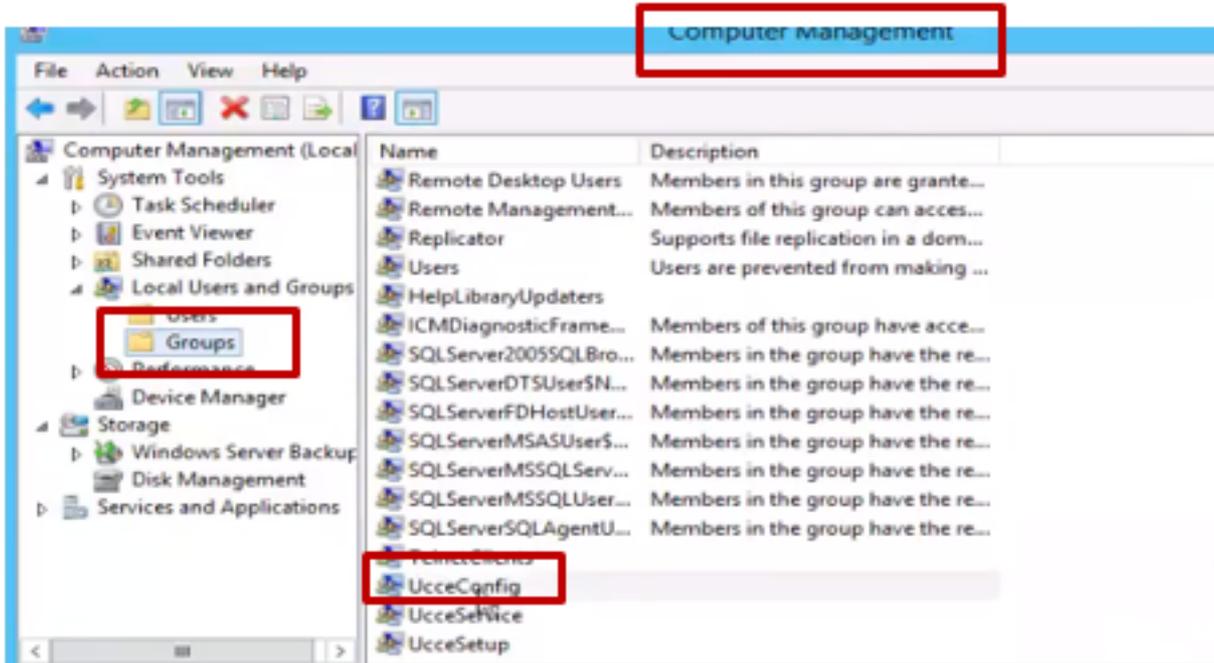
3. 사용자 목록 틀을 통한 구성 관리자에서 사용자를 추가하고 구성 옵션을 선택합니다.



12.0 버전 이전에 이 변경 사항이 인스턴스 OU(Organizational Unit)에서 도메인의 구성 보안 그룹을 업데이트했지만 12.0에서는 해당 사용자를 AD 그룹에 추가하지 않는 것이 기본 동작입니다. 이 이미지에 표시된 대로 도메인 ICM 구성 보안 그룹에 이 사용자의 업데이트가 없습니다.



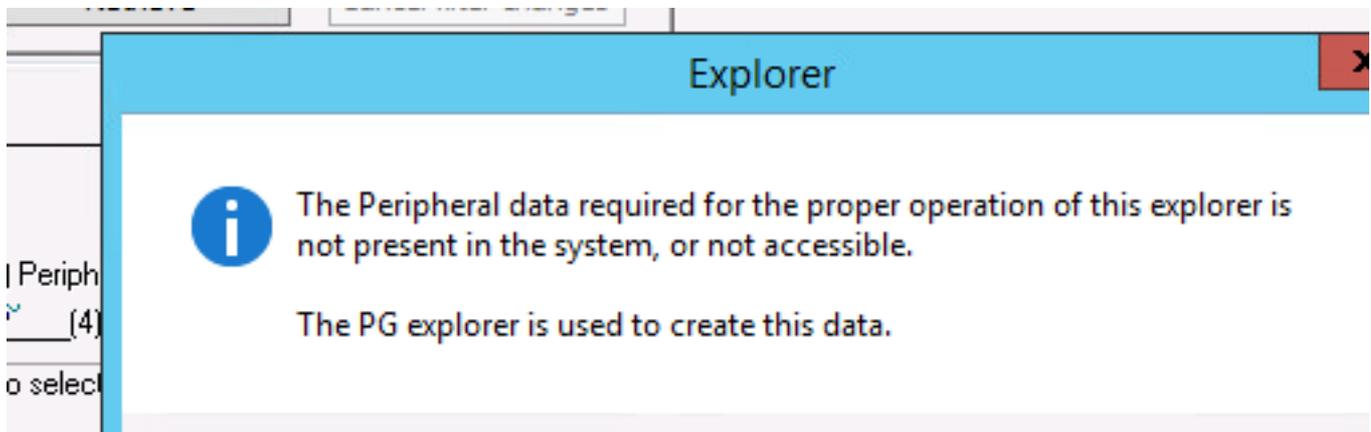
4. AW Server의 컴퓨터 관리 > 로컬 사용자 및 그룹 > 그룹에서 UcceConfig를 선택하고 testconfig1 사용자를 추가합니다.



5. 컴퓨터에서 로그아웃하고 testconfig1 사용자의 자격 증명을 사용하여 로그인합니다. 이 사용자는 구성 권한이 있으므로 Configuration Manager, 스크립트 또는 인터넷 스크립트 편집기와 같은 CCE 구성 도구를 실행할 수 있습니다.

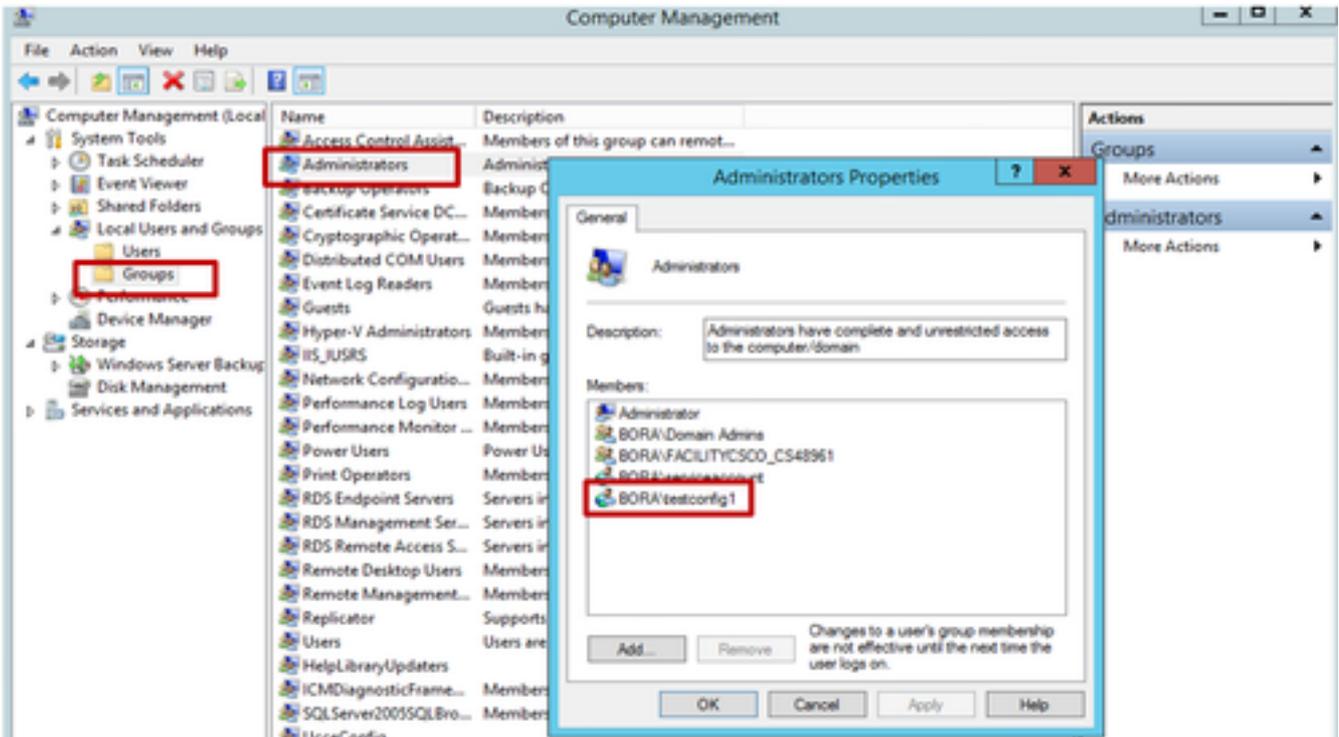
6. 그러나 사용자가 설정 권한을 필요로 하는 작업을 실행하려고 하면 실패합니다.

이 예에서는 testconfig1 사용자가 주변 장치 게이트웨이(pg) 컨피그레이션을 변경하고 시스템은 경고 메시지와 함께 변경 사항을 제한합니다.

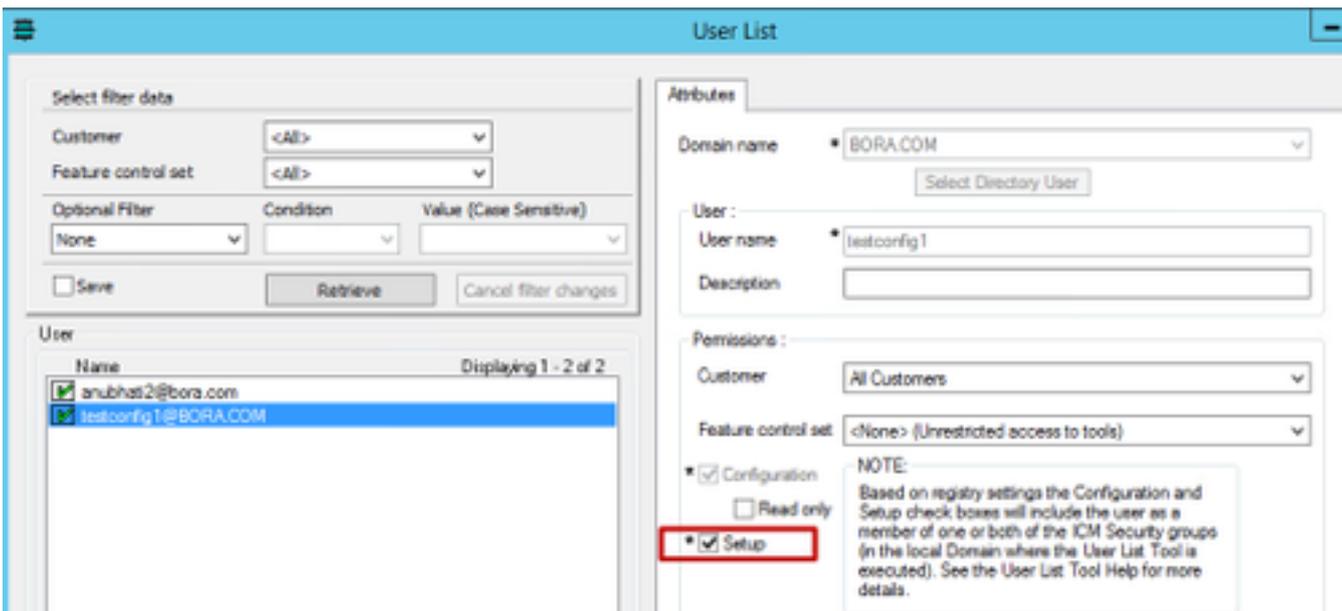


7. 비즈니스에 이 사용자에게 구성과 함께 설정 권한이 필요한 경우 사용자가 AW 서버 로컬 관리 그룹에 추가되었는지 확인해야 합니다.

8. 로그인하려면 도메인 또는 로컬 관리자 권한 계정을 사용하여 AW 서버에 로그인하고 **컴퓨터 관리 > 로컬 사용자 및 그룹 > 그룹**에서 그룹을 선택하고 관리자에서 사용자를 사용자에게 추가합니다.



9. 사용자 목록 도구를 통한 구성 관리자에서 사용자를 선택하고 설정 옵션을 선택합니다.



10. 사용자는 이제 해당 AW 서버에서 CCE 애플리케이션의 모든 리소스에 액세스하여 원하는 대로 변경할 수 있습니다.

다음을 확인합니다.

확인 절차는 실제로 구성 프로세스의 일부입니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.