Konfigurieren der lokalen PCCE-Autorisierung

Inhalt

Einführung

In diesem Dokument werden die Schritte beschrieben, die zum Entfernen der Abhängigkeit von Microsoft Active Directory (AD) erforderlich sind, um die Autorisierung lokal in PCCE-Komponenten (Package Contact Center Enterprise) zu verwalten.

Mitarbeiter: Meenakshi Sundaram, Ramiro Amaya und Anuj Bhatia, Cisco TAC Engineers.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Paket Contact Center Enterprise
- Microsoft Active Directory

Verwendete Komponenten

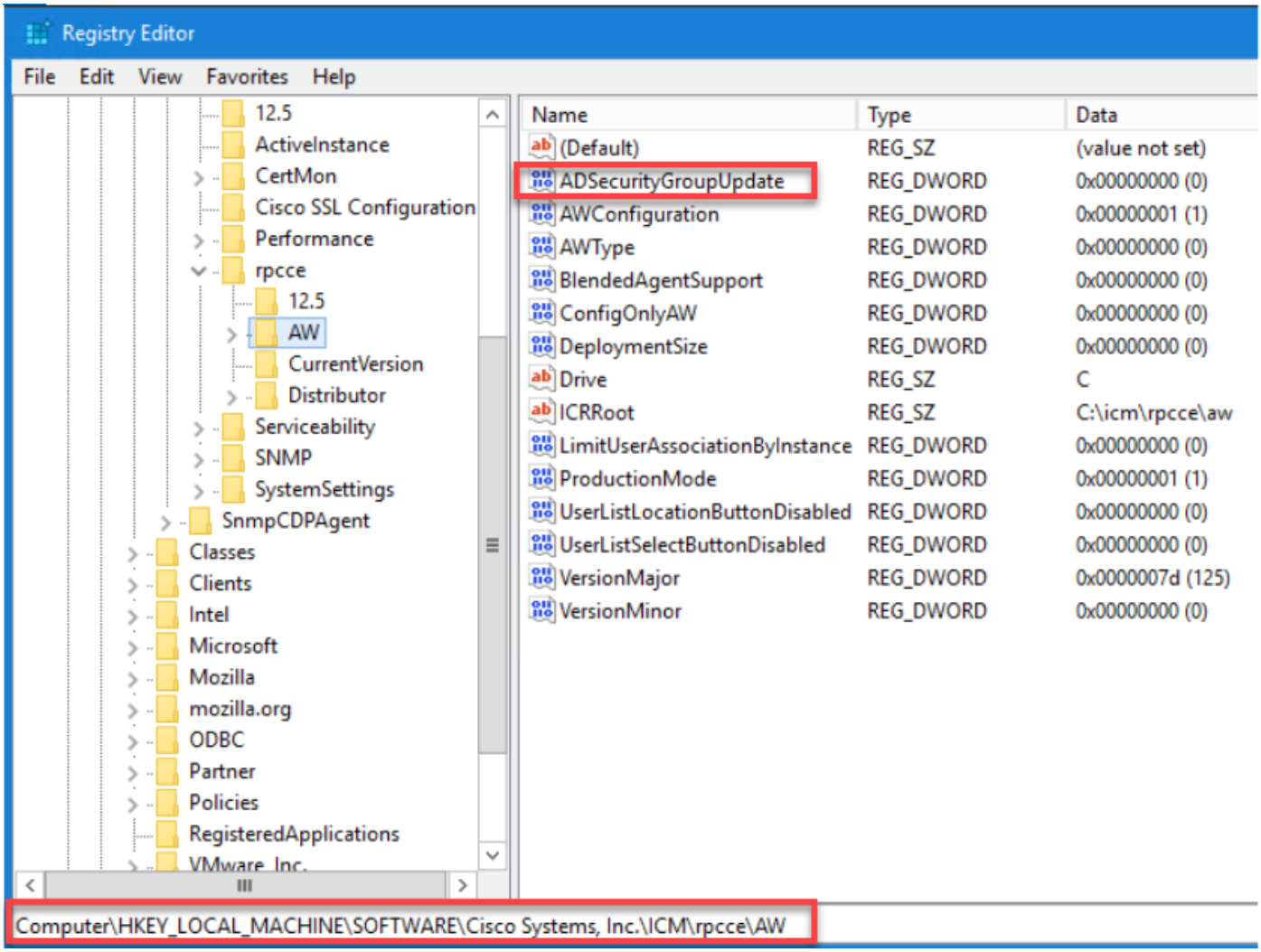
Die in diesem Dokument verwendeten Informationen basieren auf der PCCE 12.5(1)-Version.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen aller Schritte verstehen.

Hintergrundinformationen

Die PCCE 12.5-Version bietet Benutzerberechtigungen für lokale Benutzergruppen auf den Administration Servers (AW), wodurch Benutzer die Autorisierung aus Active Directory (AD) verschieben können. Dies wird von der Registrierung **ADSecurityGroupUpdate** gesteuert, die standardmäßig aktiviert ist. Dadurch wird die Verwendung von Microsoft AD Security Groups zur Kontrolle von Benutzerzugriffsrechten für Setup- und Konfigurationsaufgaben vermieden.

> **Hinweis**: Die Unterstützung für die lokale Autorisierung wurde in Unified Contact Center Enterprise (UCCE) 12.0 eingeführt und wird jetzt von PCCE 12.5 unterstützt.



> **Hinweis**: Wenn für Unternehmen das vorherige Verhalten implementiert werden muss (AD-Autorisierung), kann das ADSecurityGroupUpdate-Flag in 1 geändert werden.

Konfigurieren

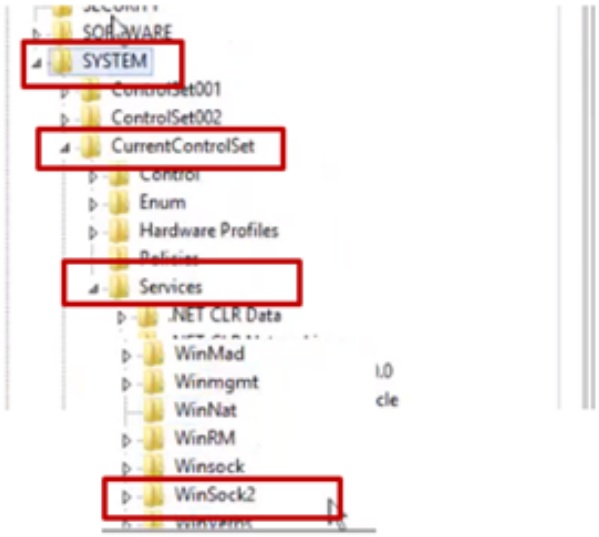
Um Berechtigungen für eine UcceConfig-Gruppe auf einem lokalen AW-Server zu erteilen, müssen zunächst Berechtigungen auf Registrierungsebene und dann auf Ordnerebene erteilt werden.

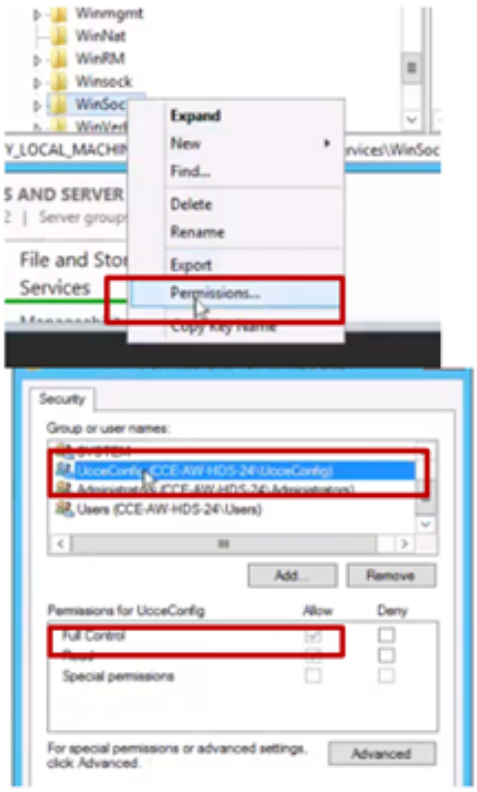
Schritt 1: Konfigurieren Sie die Registrierungsberechtigungen.

1. Führen Sie das Dienstprogramm regedit.exe aus.

2. Wählen Sie **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\WinSock2**.

3. Wählen Sie unter Berechtigungen auf der Registerkarte Sicherheit die Gruppe **UCCEConfig** aus, und aktivieren Sie **die** Option **Vollzugriff zulassen**.





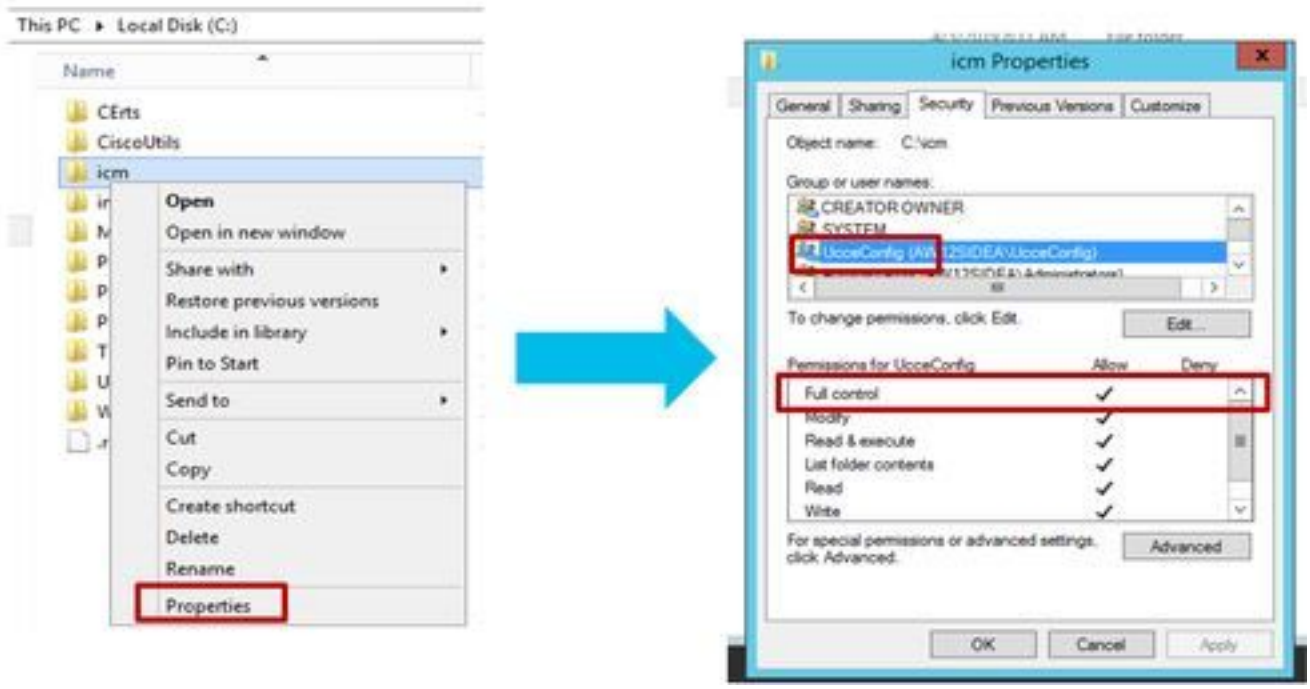
4. Wiederholen Sie die vorherigen Schritte, um der UCCEConfig-Gruppe für diese Registrierungen vollständige Kontrolle zu gewähren.

- **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, einschl.\ICM**
- **Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Cisco Systems, einschl.\ICM**

Schritt 2: Konfigurieren von Ordnerberechtigungen

1. Navigieren Sie in Windows Explorer zu <ICM Installed Directory>:\icm, und wählen Sie Eigenschaften aus.

2. Wählen Sie auf der Registerkarte Sicherheit die Option **UCCEConfig** aus, und aktivieren Sie **die Option Vollzugriff zulassen**.



3. Klicken Sie auf OK, um die Änderungen zu speichern.

4. Wiederholen Sie die vorherigen Schritte, um der **UCCEConfig-**Gruppe für C:\Temp folder volle Kontrolle zu gewähren.

5. Gehen Sie in SQL Management Studio wie folgt vor:

a) Navigieren Sie zu Sicherheit > Anmeldungen.

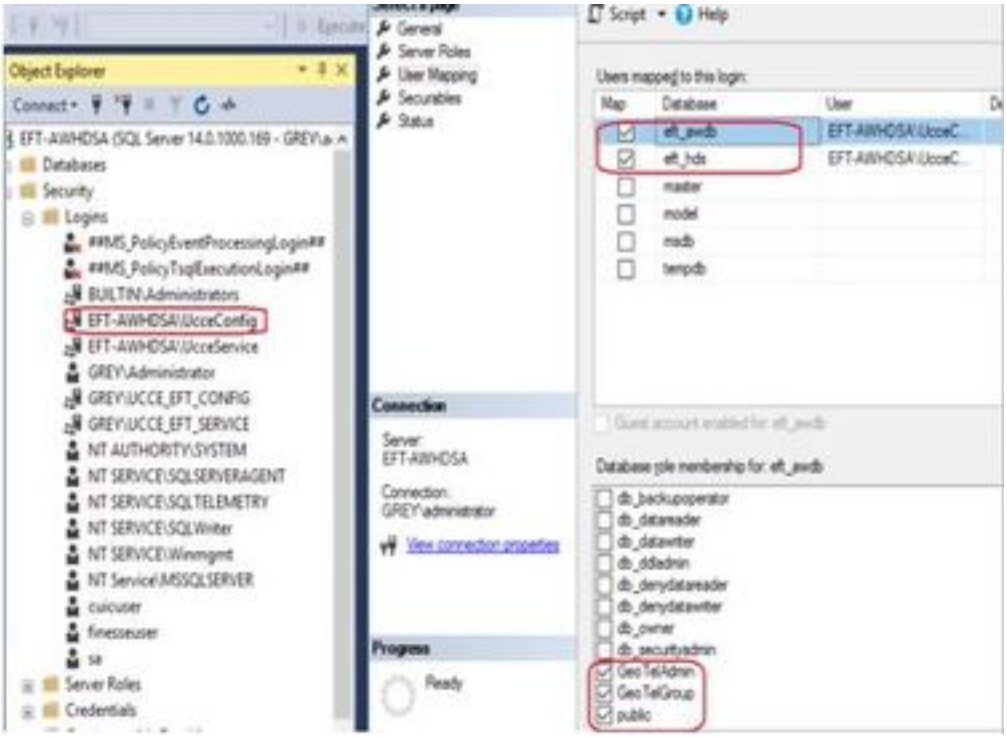
b) Suchen Sie <Gerätename>\UCCEConfig.

c) Klicken Sie mit der rechten Maustaste, und wählen Sie Eigenschaften aus.

d) Navigieren Sie zu Benutzerzuordnungen, und wählen Sie die AWDB-Datenbank aus.

e) Aktivieren Sie die Kontrollkästchen GeoTelAdmin, GeoTelGroup und public.

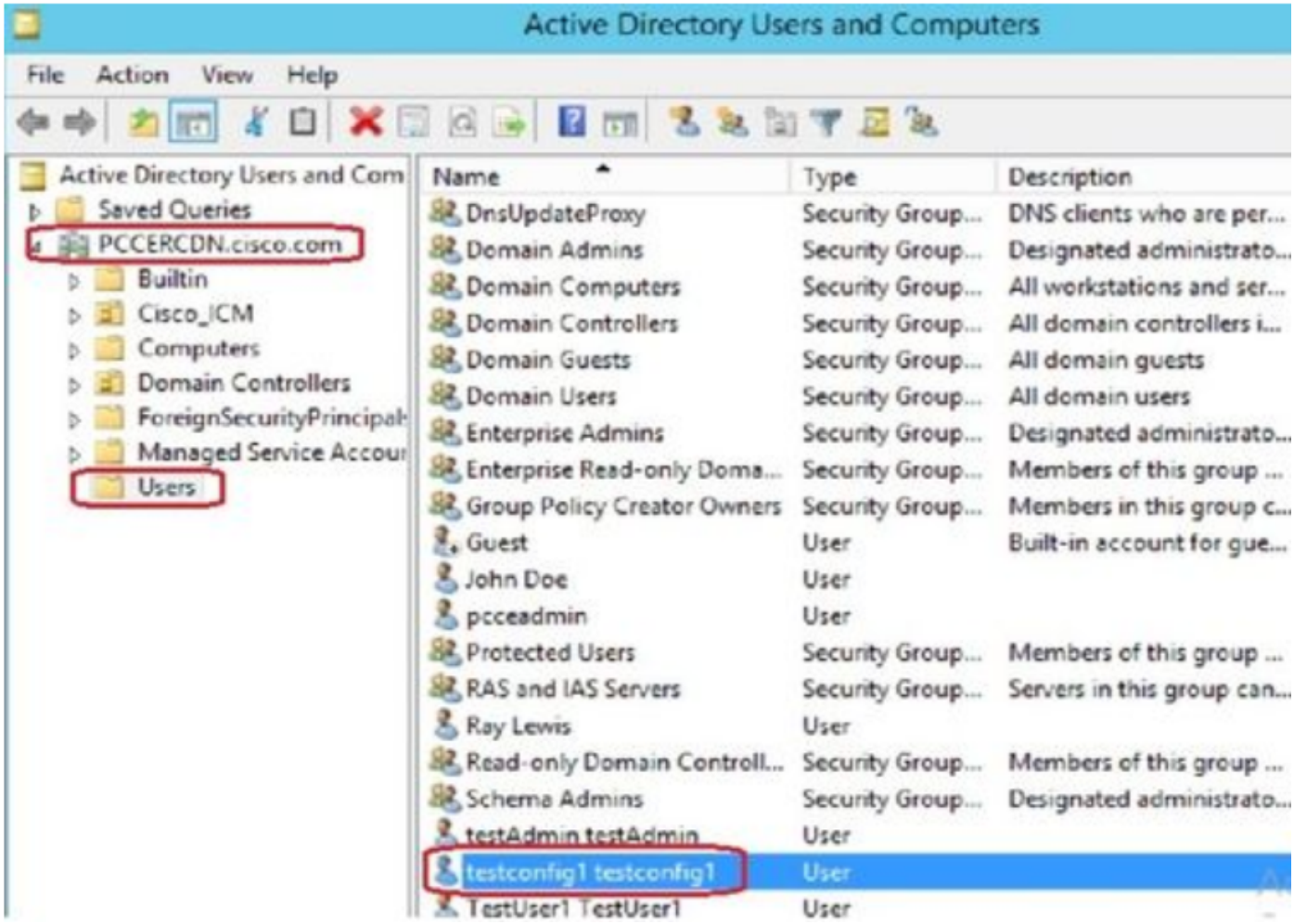
f) Schritt d) für die HDS-Datenbank wiederholen.

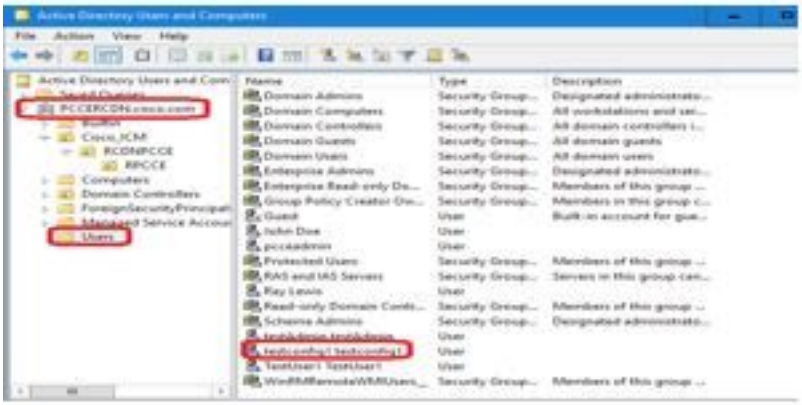


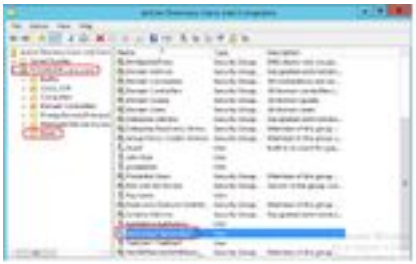
Nachdem eine vorläufige Konfiguration erreicht wurde, befolgen Sie die Schritte, wie Sie einen Domänenbenutzer bewerben können, um Konfigurations- und Einrichtungsrechte zu erhalten.

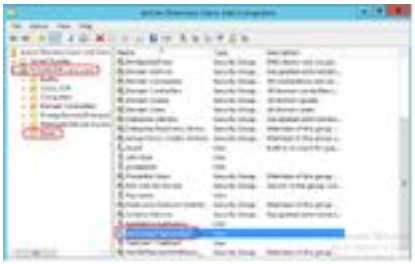
Schritt 3: Domänenbenutzerkonfiguration.

1. Erstellen Sie einen Domänenbenutzer in AD. Für diesen exakten Testconfig1-Benutzer wurde erstellt.



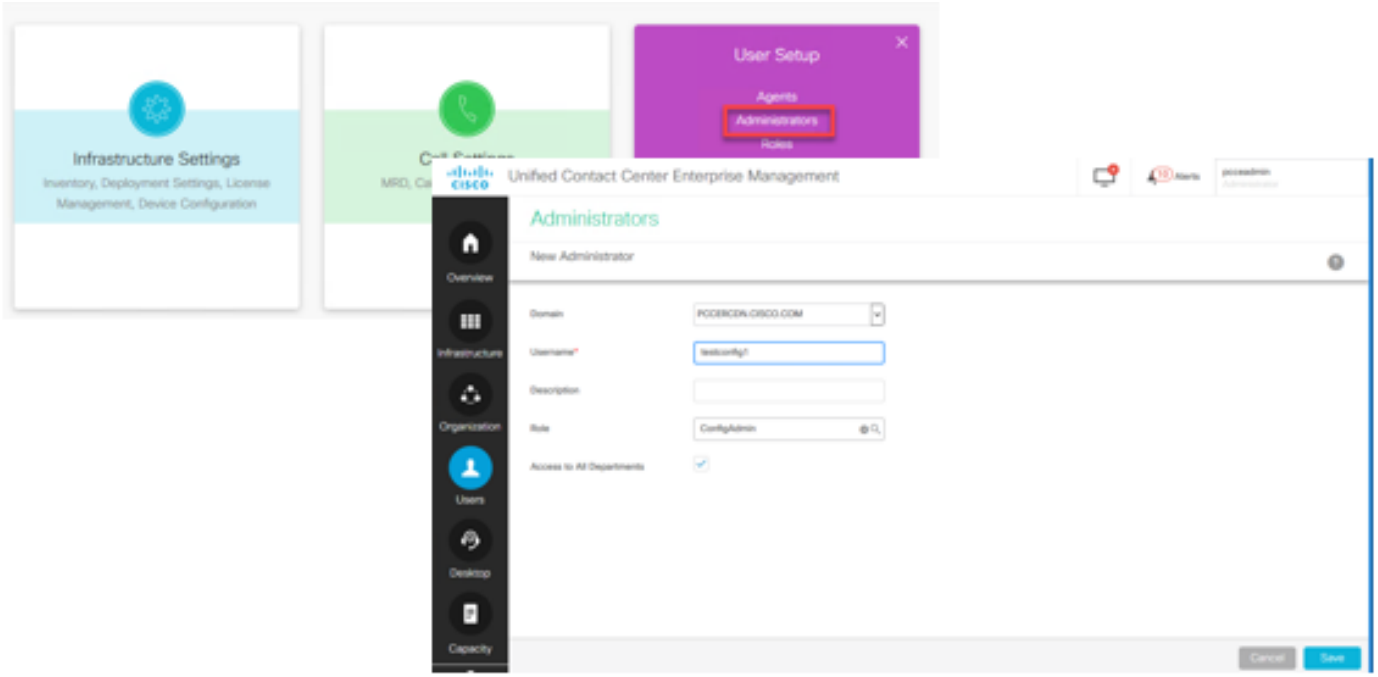




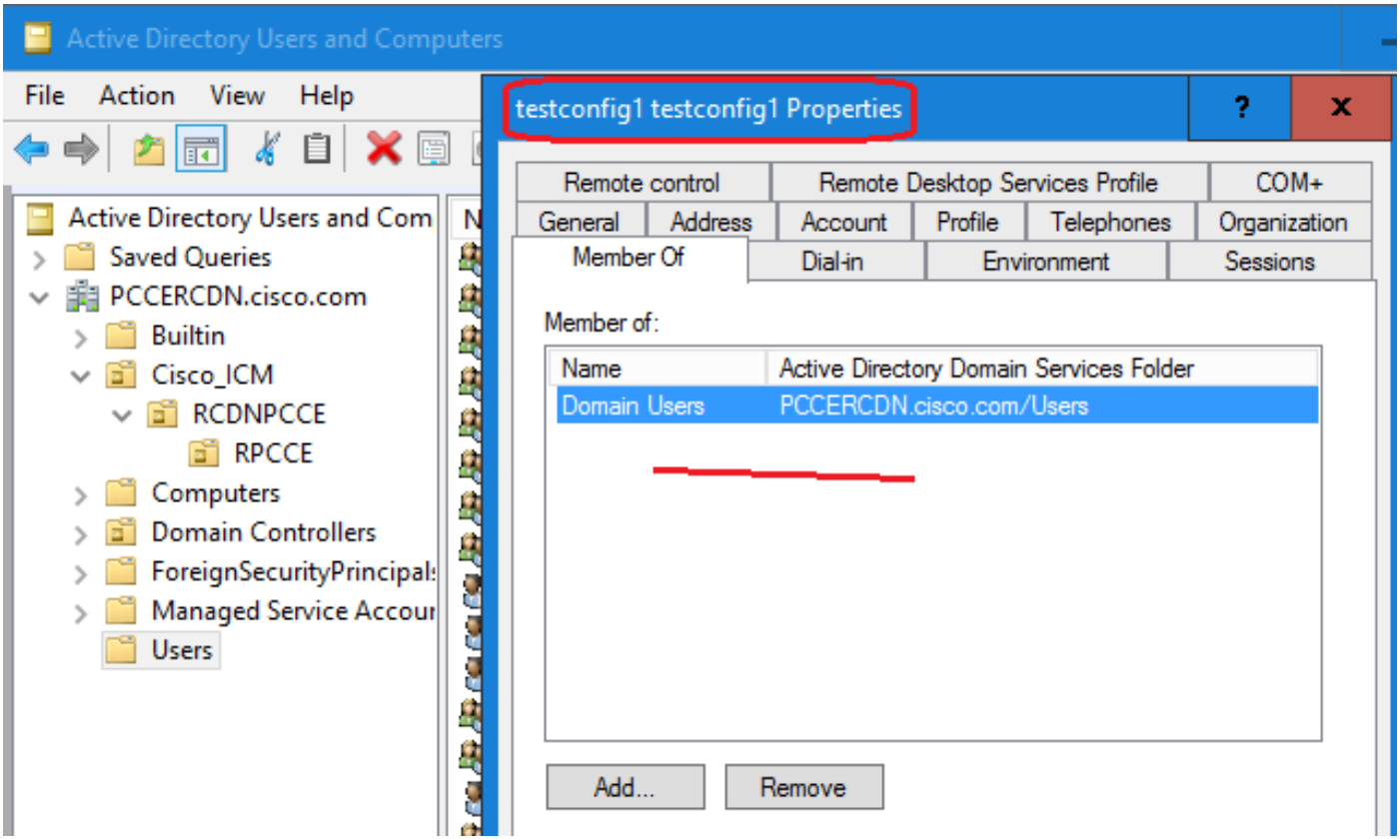


2. Melden Sie sich mit einem Domänenadmin- oder lokalen Administratorkonto beim AW-Server an.

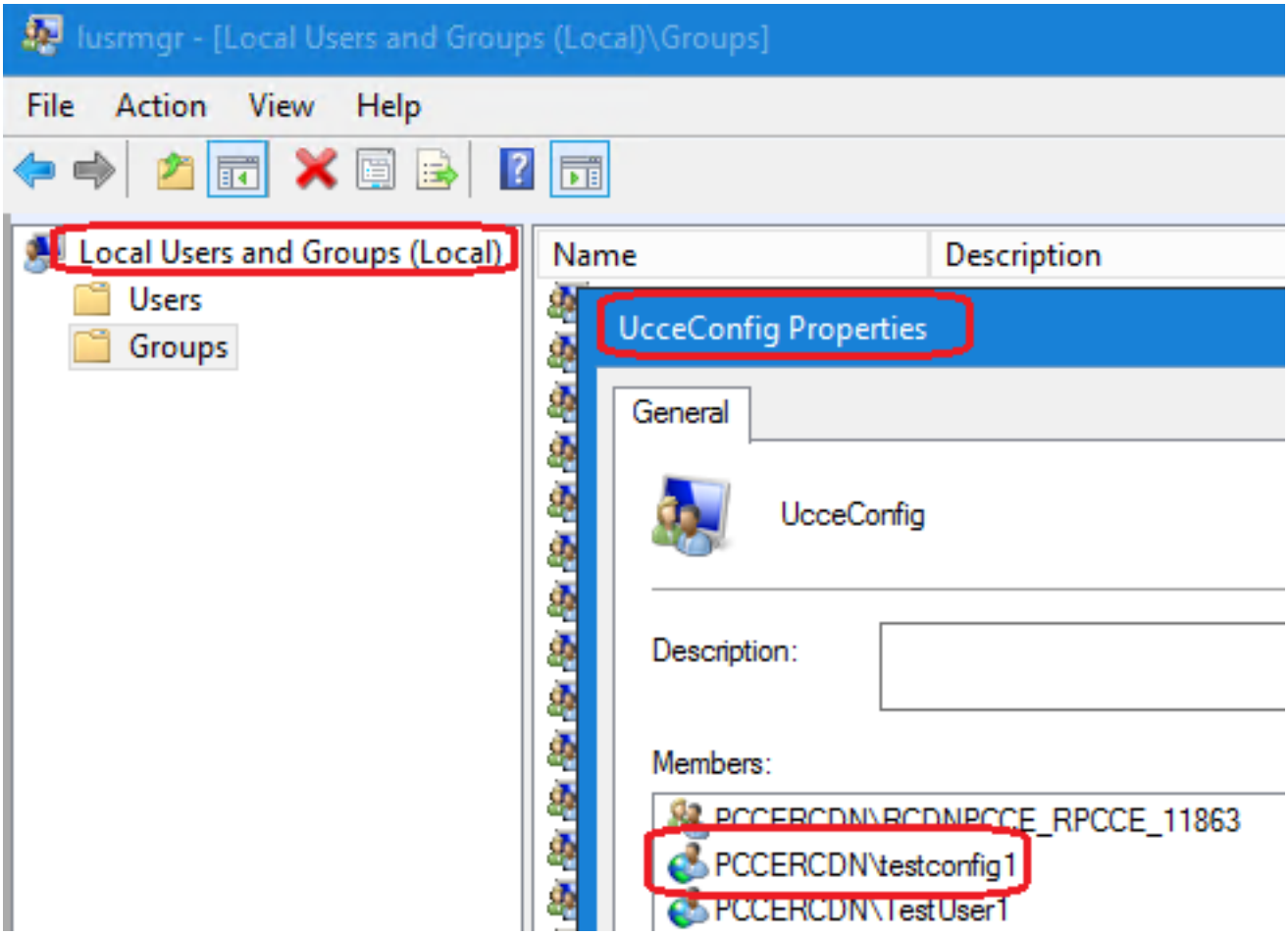
3. Öffnen Sie den CCE-Administrator auf dem AW. Navigieren Sie zur Benutzer-Setup-Karte, und wählen Sie Administratoren aus. Fügen Sie den Benutzer hinzu, und wählen Sie die Rolle **ConfigAdmin aus**.



Vor der Version 12.5 von PCCE hätte diese Änderung die Config Security Groups in der Domäne unter einer Instanz Organizational Unit (OU) aktualisiert. Mit 12.5 ist das Standardverhalten jedoch nicht, diesen Benutzer der AD-Gruppe hinzuzufügen. Wie im Bild gezeigt, gibt es in der Sicherheitsgruppe "ICM Config" der Domäne keine Aktualisierung dieses Benutzers.



4. Wählen Sie im AW-Server unter **Computerverwaltung > Lokale Benutzer und Gruppen > Gruppen** die Option UCCEConfig aus, und fügen Sie testconfig1-Benutzer hinzu.

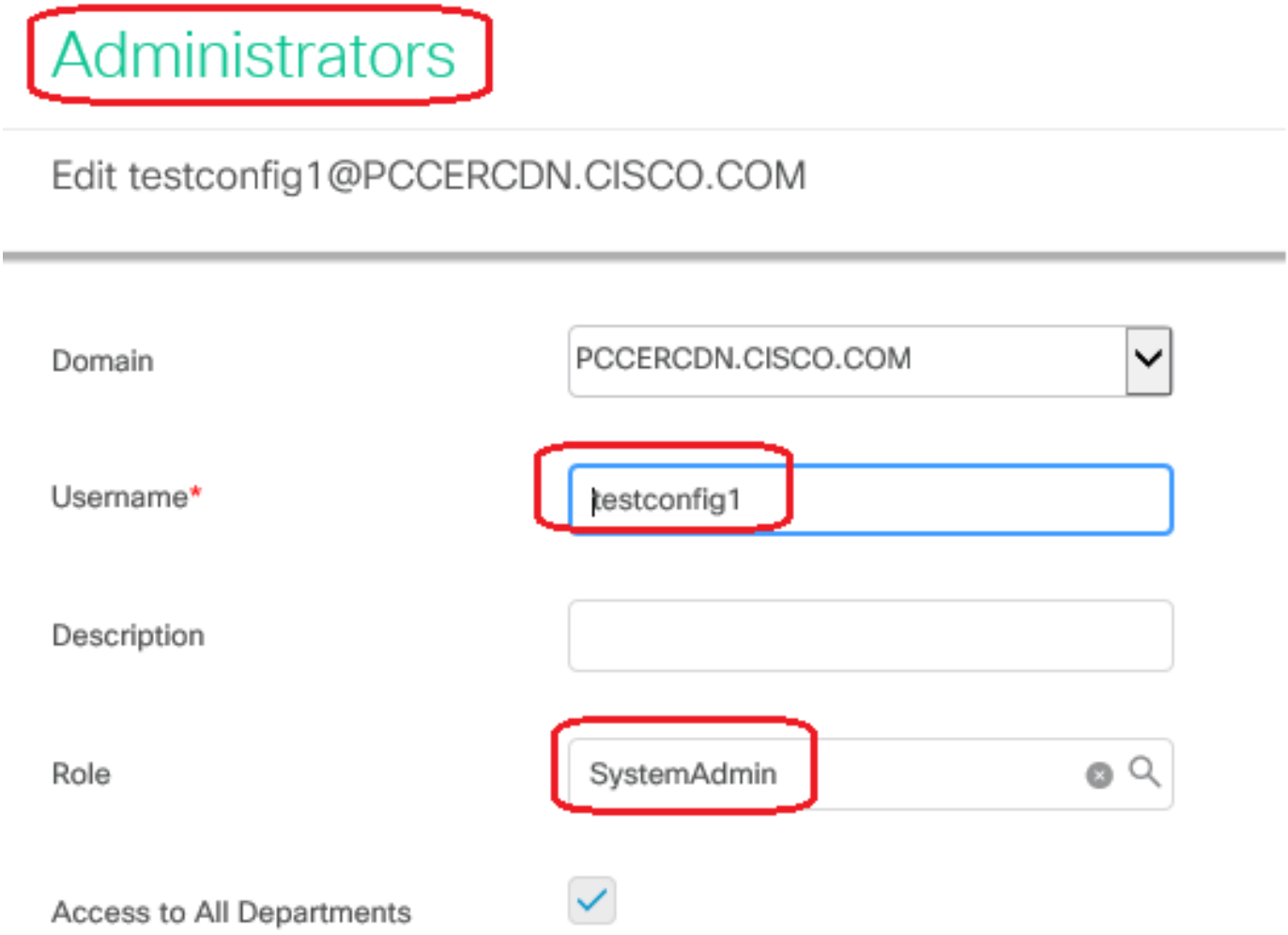


5. Melden Sie sich vom Computer ab, und melden Sie sich mit den Anmeldeinformationen des Benutzers testconfig1 an. Da dieser Benutzer über Konfigurationsrechte verfügt, kann er CCE-Konfigurationstools wie CCE Admin, Script oder Internet Script Editor ausführen.

6. Wenn der Benutzer jedoch versucht, eine Aufgabe auszuführen, die Setup-Rechte erfordert, schlägt er fehl. Dieser Benutzer hat keinen Zugriff auf alle CCE-Administrator-Ressourcen oder -Setup-Tools.

Wie im Bild gezeigt, versucht der Benutzer testconfig1 in der PCCE 4K-Bereitstellung, die Konfiguration des Peripheral Gateway (PG) auszuführen, und das System schränkt die Änderung durch eine Warnmeldung ein.

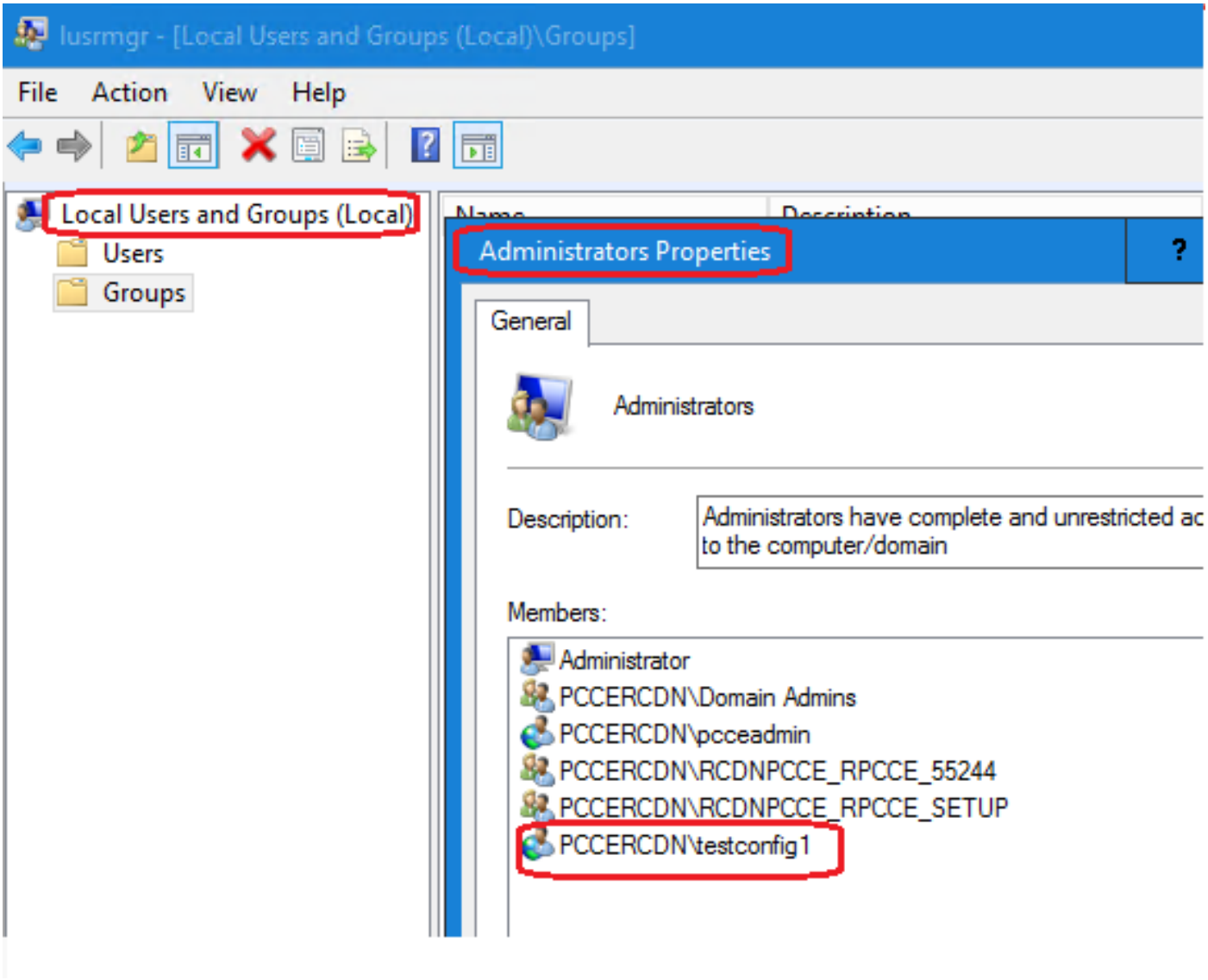
7. Wenn dieser Benutzer für eine Geschäftstätigkeit neben der Konfiguration über Setup-Rechte verfügen muss, müssen Sie sicherstellen, dass die Benutzerrolle in CCEAdmin in SystemAdmin geändert wird.



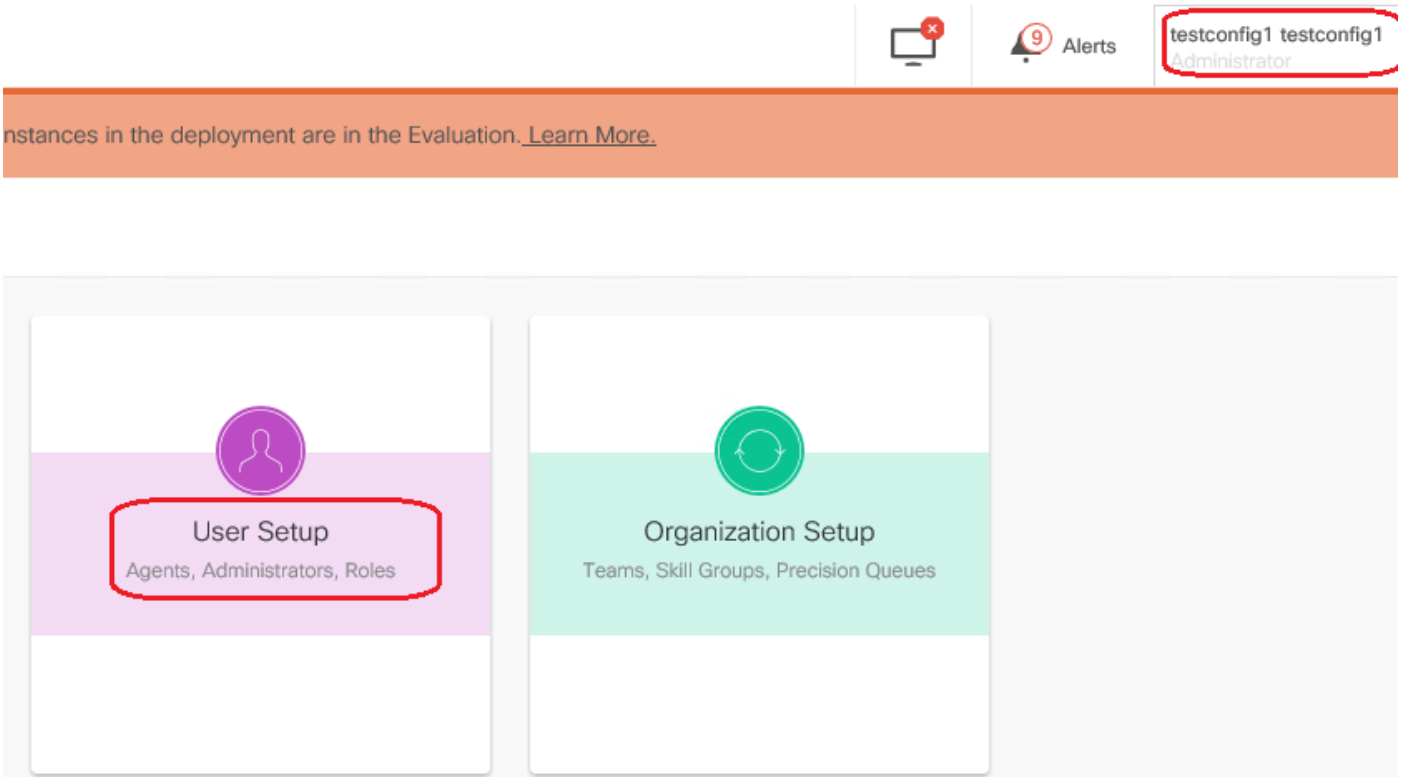
Die Benutzerrolle wurde in der Datenbank als 1 (SystemAdmin) aktualisiert:

	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. Melden Sie sich beim AW-Server mit dem Domänenkonto oder dem lokalen Administratorberechtigungskonto an, und über **Computerverwaltung > Lokale Benutzer und Gruppen > Gruppen** wählen Sie Gruppen aus, und fügen Sie den Benutzer unter "Administratoren" dem Benutzer hinzu.



10. Der Benutzer kann nun auf alle Ressourcen der CCE-Anwendung in diesem AW-Server zugreifen und die gewünschten Änderungen vornehmen.



Überprüfen

Die Überprüfung ist Teil des Konfigurationsprozesses.

Fehlerbehebung

Es sind derzeit keine spezifischen Schritte zur Fehlerbehebung für diese Konfiguration verfügbar.

Zugehörige Informationen

PCCE-Administrationsleitfaden

Technischer Support und Dokumentation - Cisco Systems