# Beheben Sie das Problem beim Abrufen von Active Directory-Gruppen-Fehlern (ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS) auf Identity Services Engine.

## Inhalt



## Einführung

In diesem Dokument wird beschrieben, wie Sie das Problem beim Abrufen von Active Directory-Gruppen (AD) während der Authentifizierung umgehen, während dieser Fehler in Live-Protokollen angezeigt wird:

```
ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS
```

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco Identity Services Engine
- Microsoft Active Directory

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Softwareversionen der Identity Services Engine (ISE) beschränkt.

## Problem

Das Problem besteht darin, dass das Benutzerkonto, das für den Beitritt zur ISE zu AD verwendet wird, nicht über die richtigen Berechtigungen zum Abrufen von TokenGroups verfügt. Dies ist nicht der Fall, wenn das Domänenadministratorkonto für den Beitritt zur ISE zum AD verwendet wurde. Um dieses Problem zu beheben, müssen Sie dem Benutzerkonto ISE-Knoten(s) hinzufügen und diese Berechtigungen für ISE-Knoten(s) bereitstellen:

- Inhalt auflisten
- Alle Eigenschaften lesen
- Leseberechtigungen

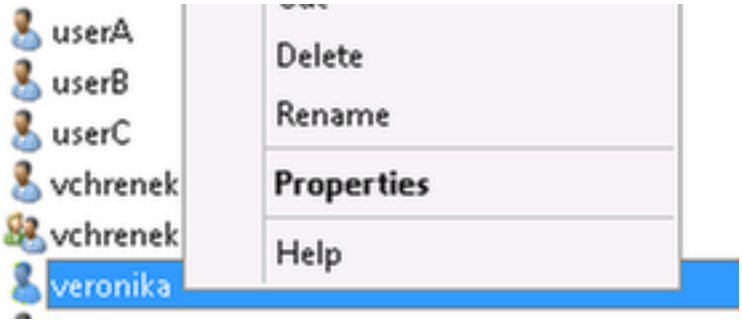
Dieses Problem tritt auf, obwohl die Berechtigungen für den Benutzer scheinbar korrekt sind (Überprüfung nach ISE 1.3 AD-Authentifizierungen fehlgeschlagen mit Fehler: "Ungenügende Berechtigung zum Abrufen von Token-Gruppen"). Diese Debuggen sind in der Datei ad-agent.log aufgeführt:

```
28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol:
LW_ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS),lsass/server/auth-providers/ad-open-
provider/provider-main.c:7409
28/08/2016 17:23:35,VERBOSE,140693934700288,Error code: 60173 (symbol:
LW_ERROR_TOKEN_GROUPS_INSUFFICIENT_PERMISSIONS),lsass/server/api/api2.c:2572
```

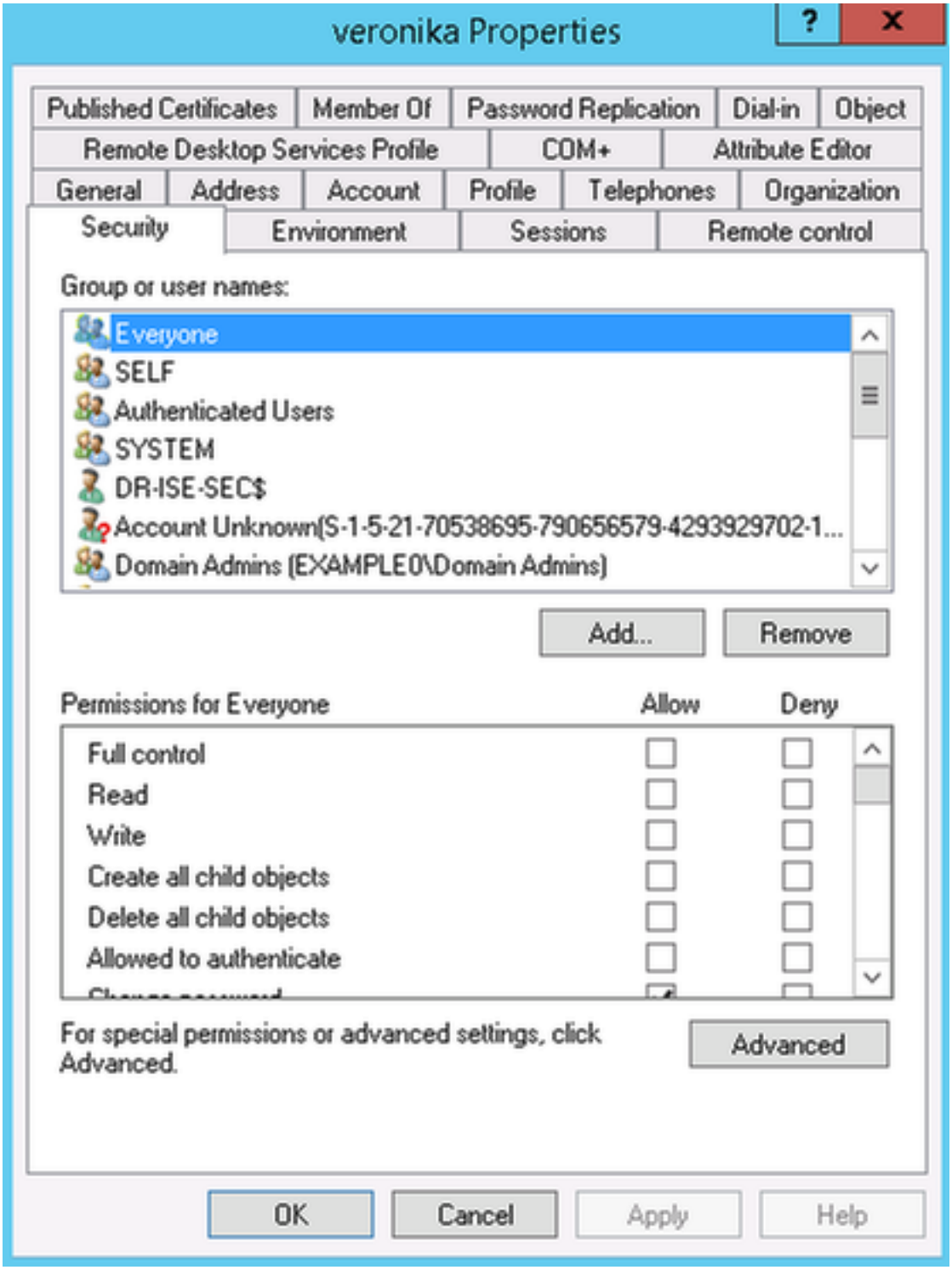
# Lösung

So erteilen Sie dem Benutzerkonto die erforderlichen Berechtigungen:

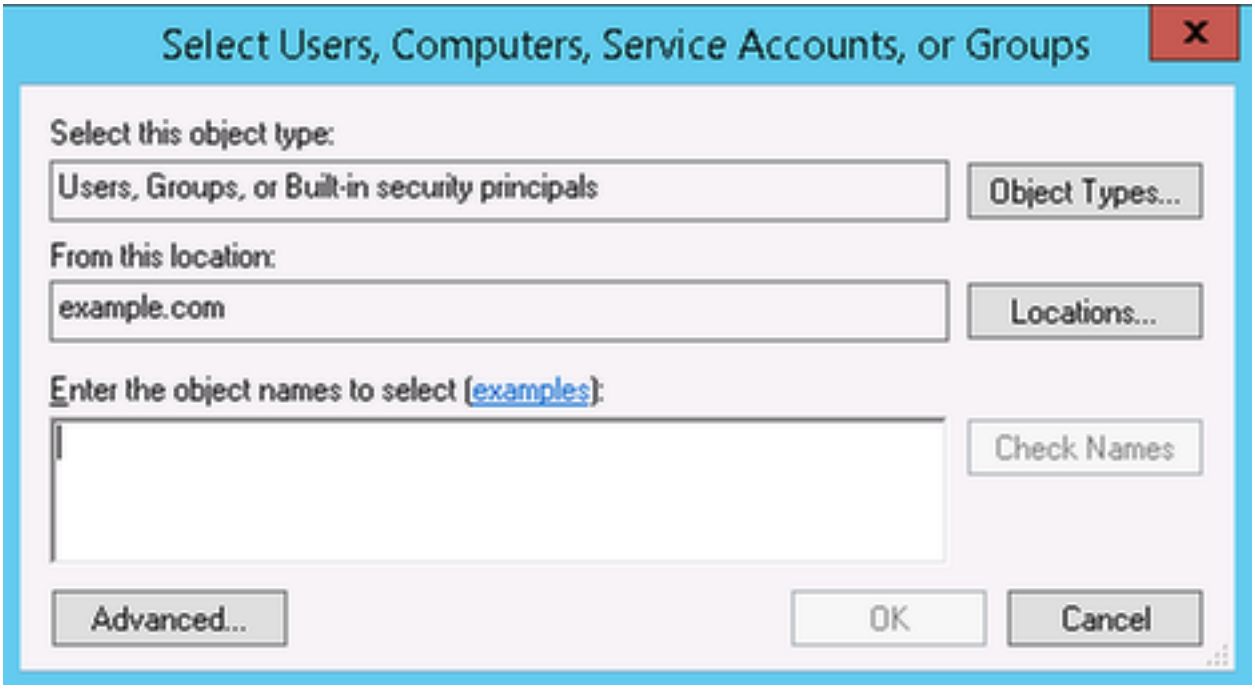
1. Navigieren Sie in AD zu **Eigenschaften** für AD-Benutzerkonto:



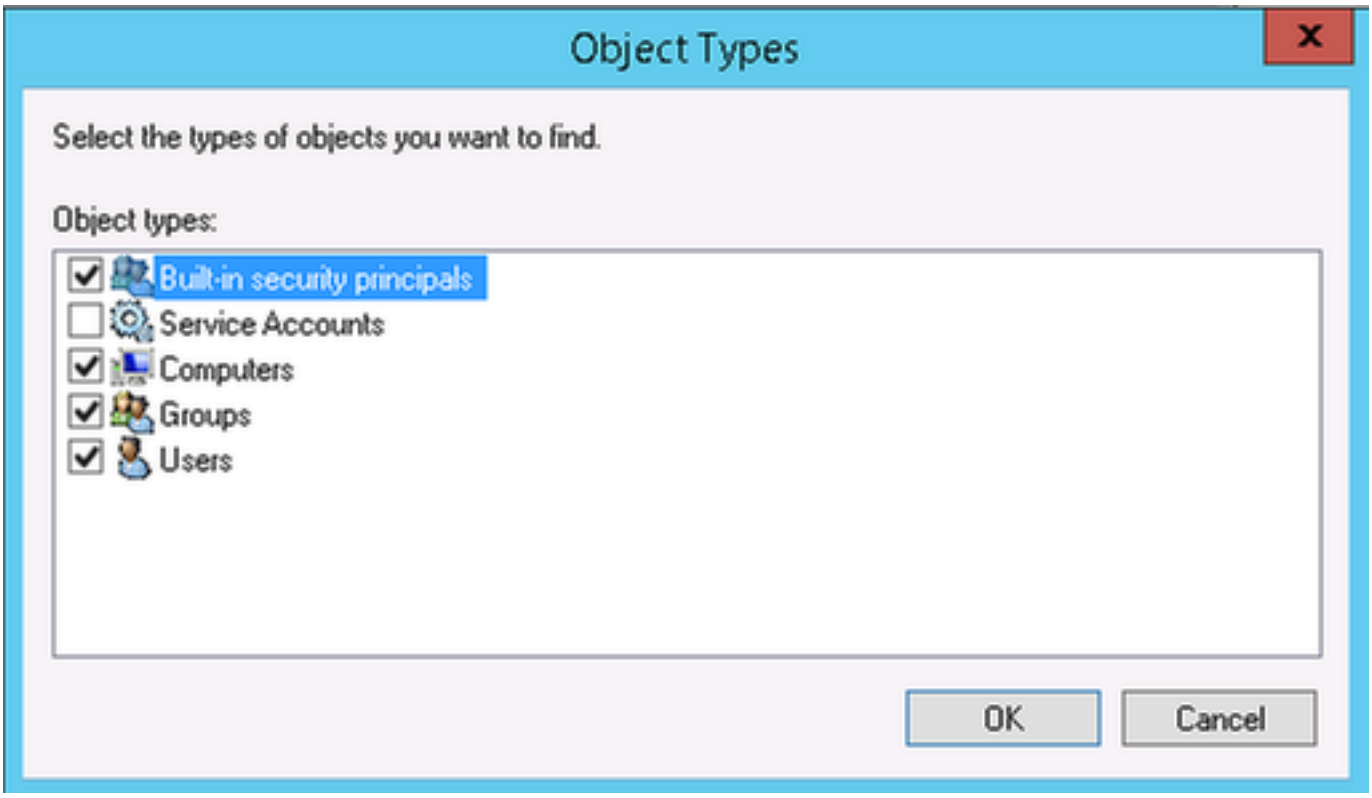

2. Wählen Sie die Registerkarte **Sicherheit**, und klicken Sie auf **Hinzufügen**:



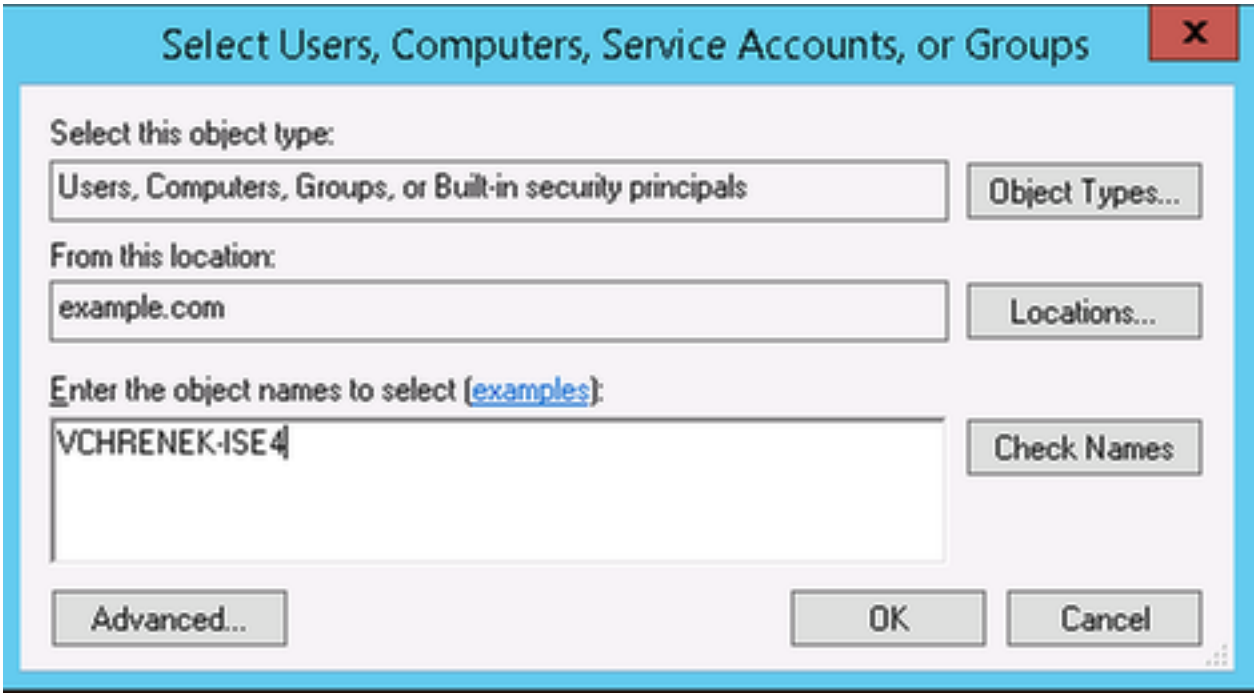

3. Wählen Sie **Objekttypen aus**:



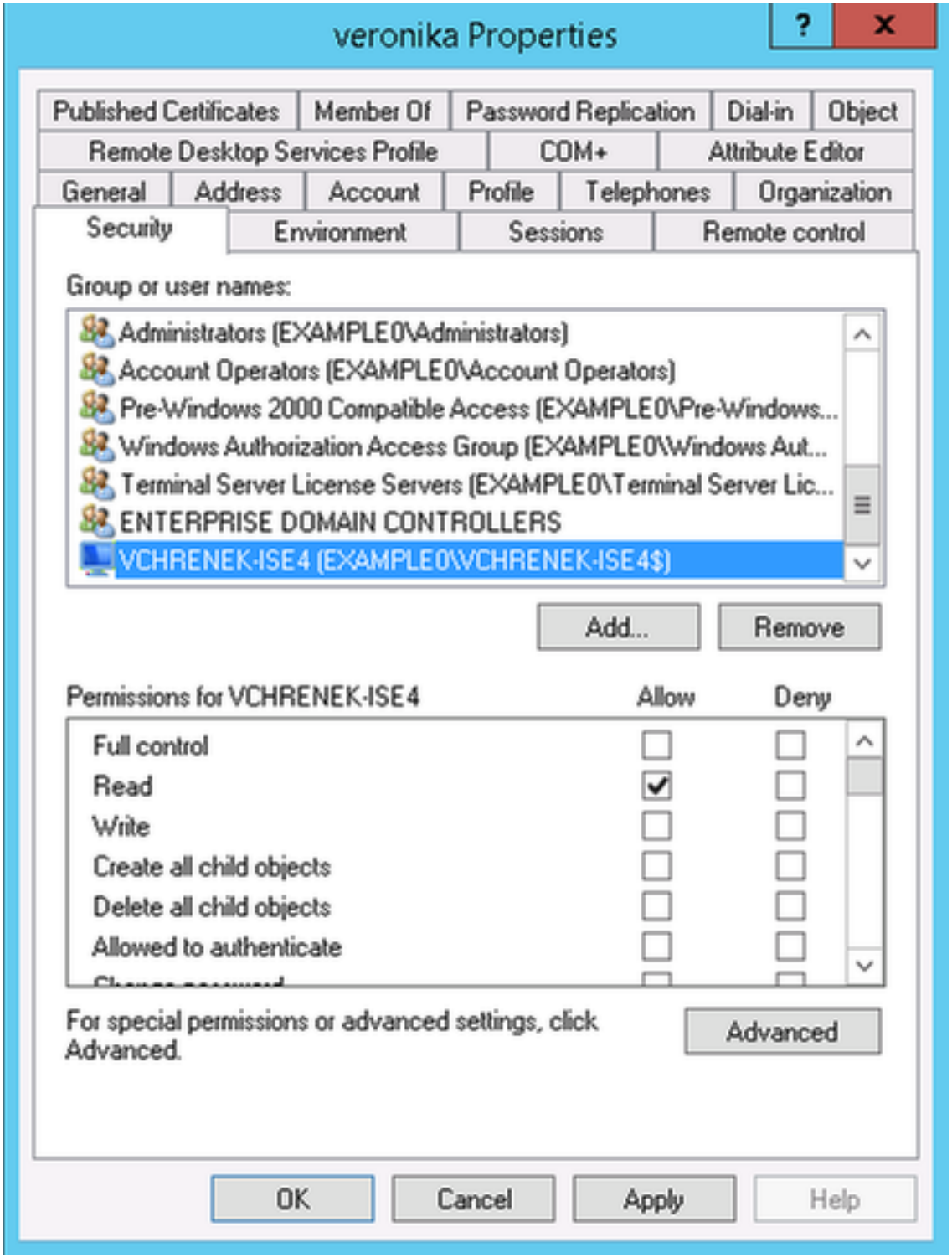

4. Wählen Sie **Computer aus**, und klicken Sie auf **OK**:



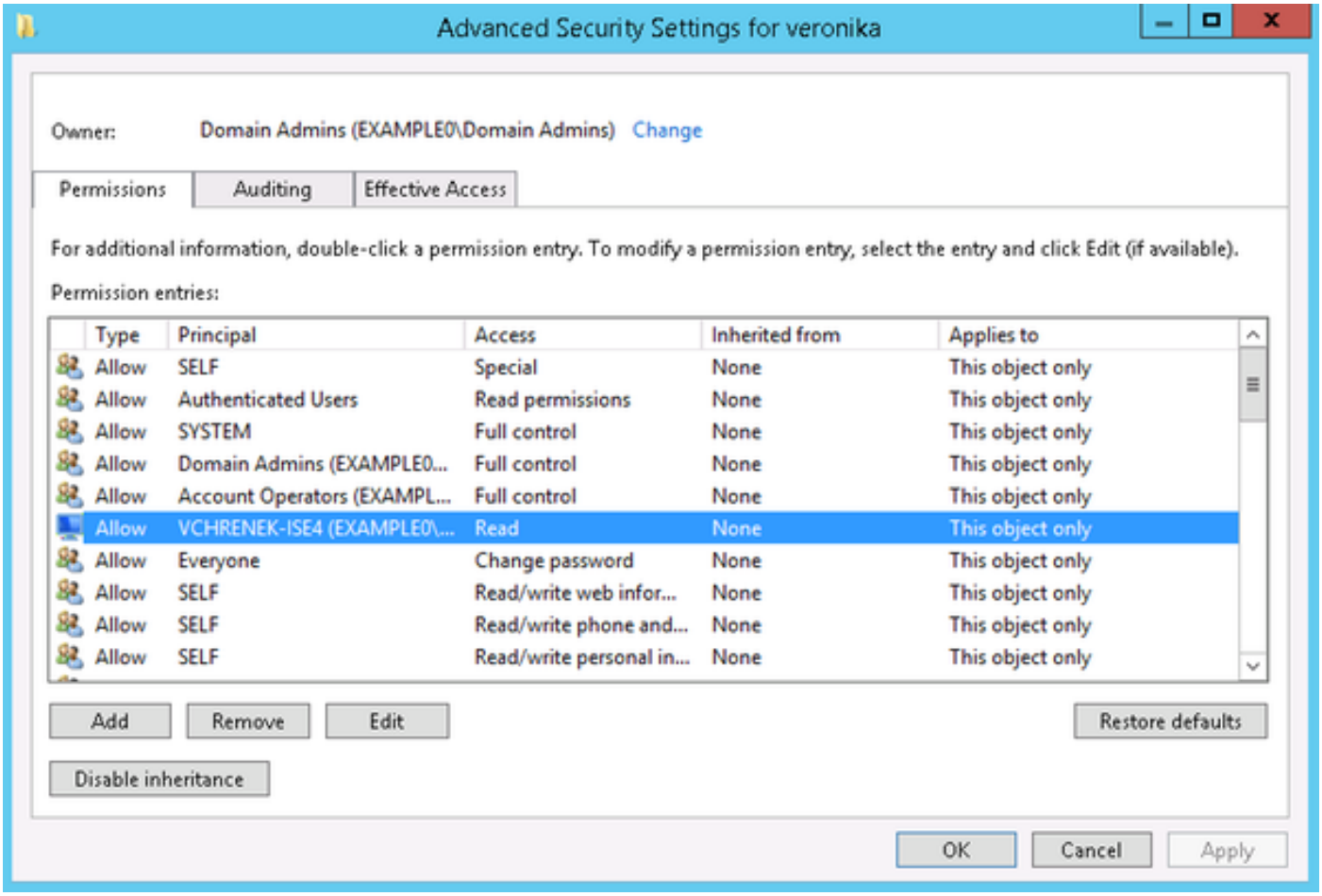

5. Legen Sie ISE-Hostnamen ein (in diesem Beispiel VCHRENEK-ISE4), und klicken Sie auf **OK**:



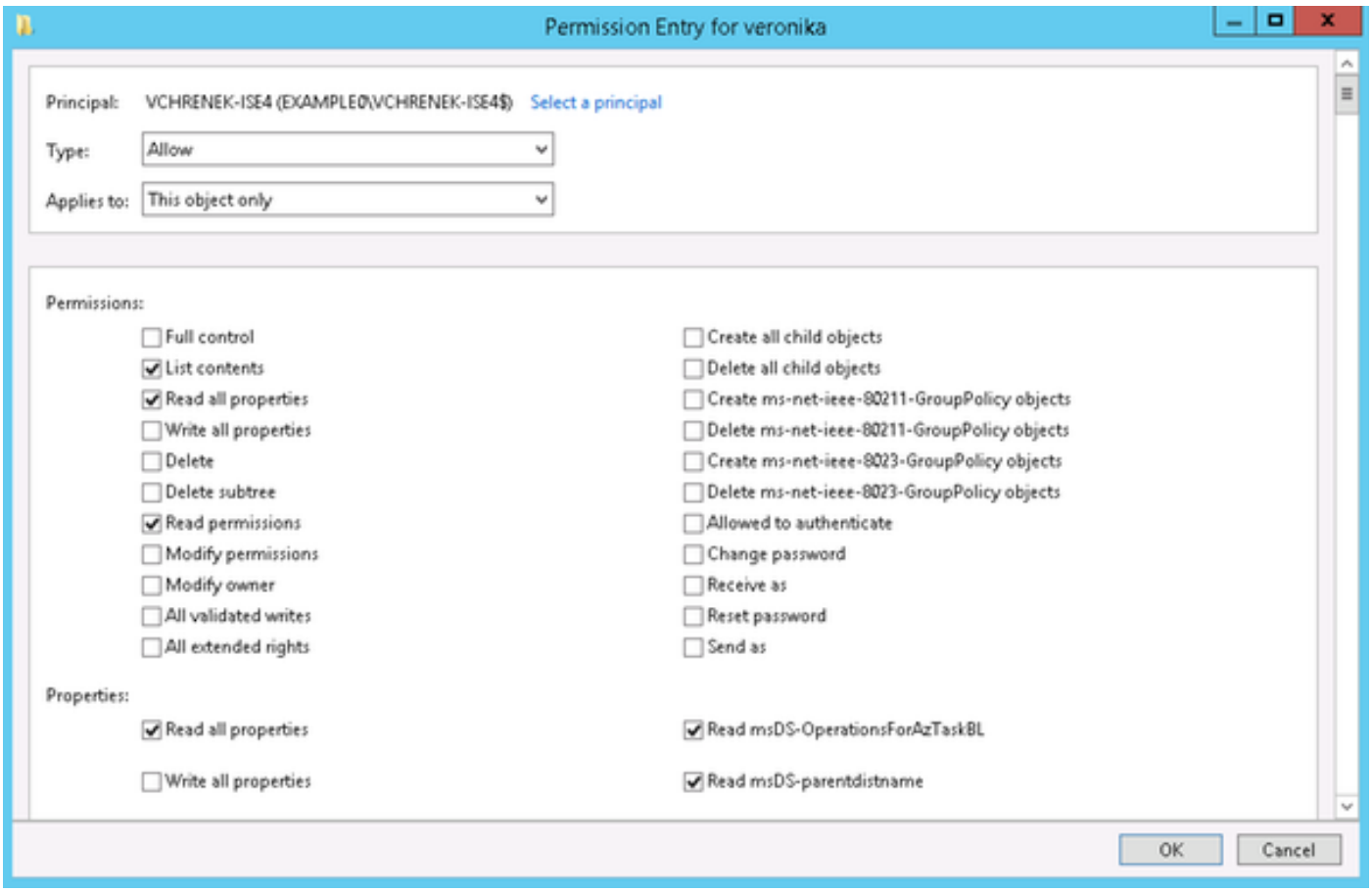

6. Wählen Sie ISE-Knoten aus, und klicken Sie auf **Erweitert**:



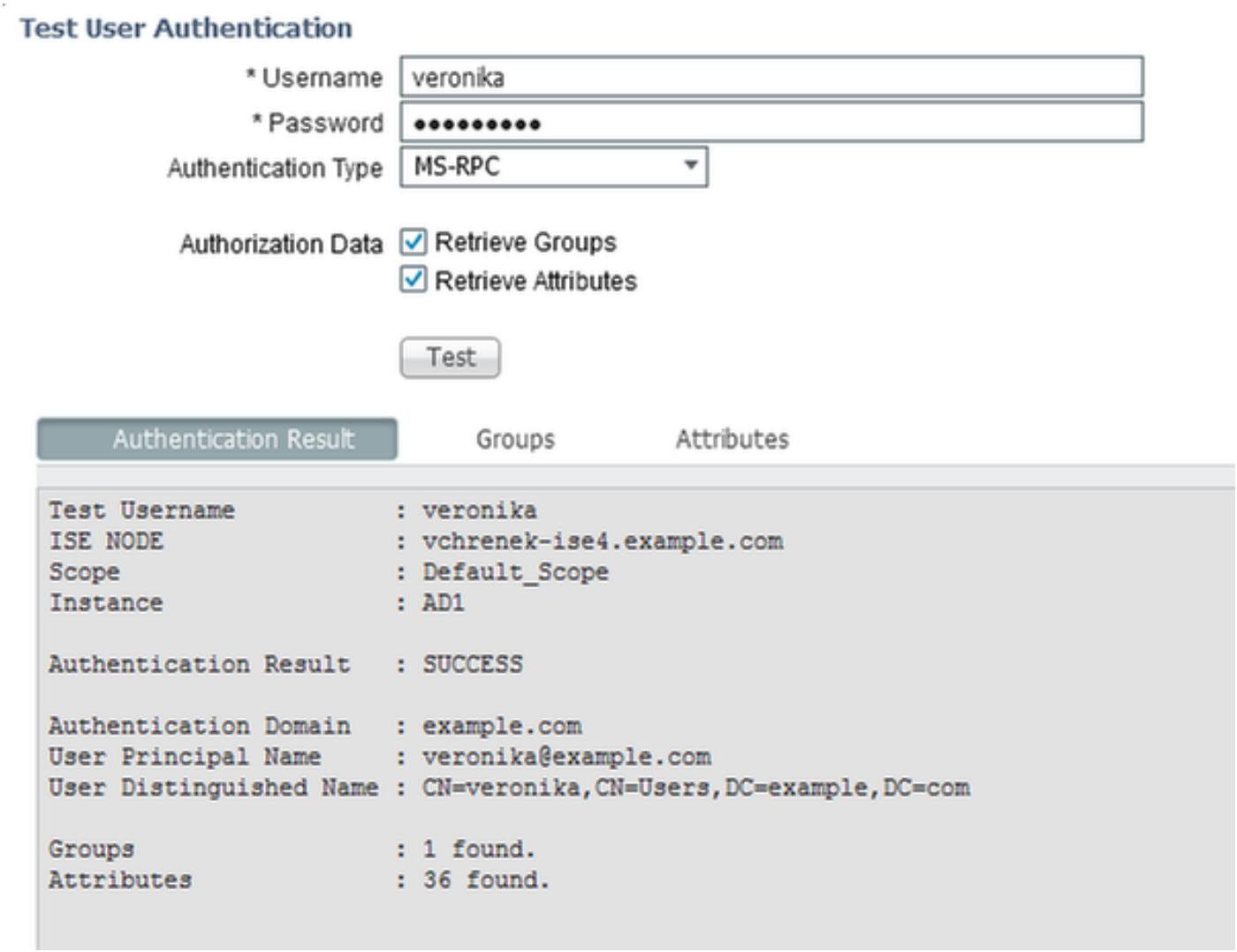

7. Wählen Sie unter Erweiterte Sicherheitseinstellungen das ISE-Systemkonto aus, und klicken Sie auf **Bearbeiten**:




8. Geben Sie diese Berechtigungen für das ISE-Systemkonto ein, und klicken Sie auf **OK**:




Nach diesen Änderungen sollten AD-Gruppen ohne Probleme abgerufen werden:




Dies muss für alle Benutzer durchgeführt werden, und die Änderungen sollten auf alle Domänencontroller in der Domäne repliziert werden.