Konfigurieren der Autorisierung für den Authentifizierungsbefehl ISE 2.0 TACACS+

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die TACACS+-Authentifizierung und die Befehlsautorisierung basierend auf der Gruppenmitgliedschaft von Microsoft Active Directory (AD) konfiguriert werden.

Hintergrundinformationen

Um die TACACS+-Authentifizierung und -Befehlsautorisierung auf der Grundlage der Gruppenmitgliedschaft von Microsoft Active Directory (AD) eines Benutzers mit Identity Service Engine (ISE) 2.0 und höher zu konfigurieren, verwendet ISE AD als externen Identitätsspeicher, um Ressourcen wie Benutzer, Computer, Gruppen und Attribute zu speichern.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco IOS Router ist voll betriebsbereit
- Verbindung zwischen Router und ISE
- ISE-Server ist bootstrapping und hat Verbindung zu Microsoft AD

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Identity Service Engine 2.0
- Cisco IOS® Softwareversion 15.4(3)M3
- Microsoft Windows Server 2012 R2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

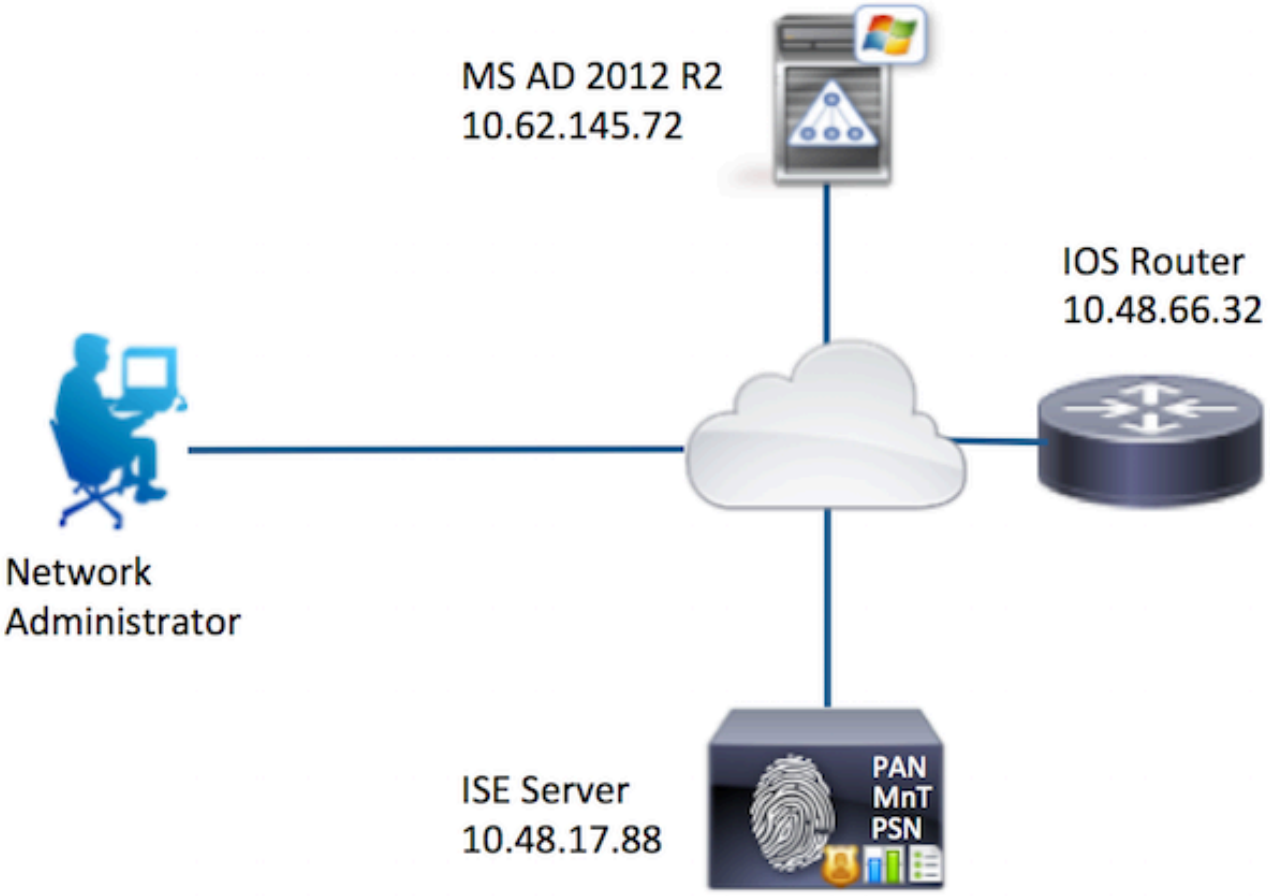
Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Konfigurieren

Ziel der Konfiguration ist es,

- Telnet-Benutzer über AD authentifizieren
- Autorisieren Sie den Telnet-Benutzer, sodass er nach der Anmeldung in den privilegierten EXEC-Modus versetzt wird.
- Überprüfen und jeden ausgeführten Befehl zur Überprüfung an die ISE senden

Netzwerkdiagramm

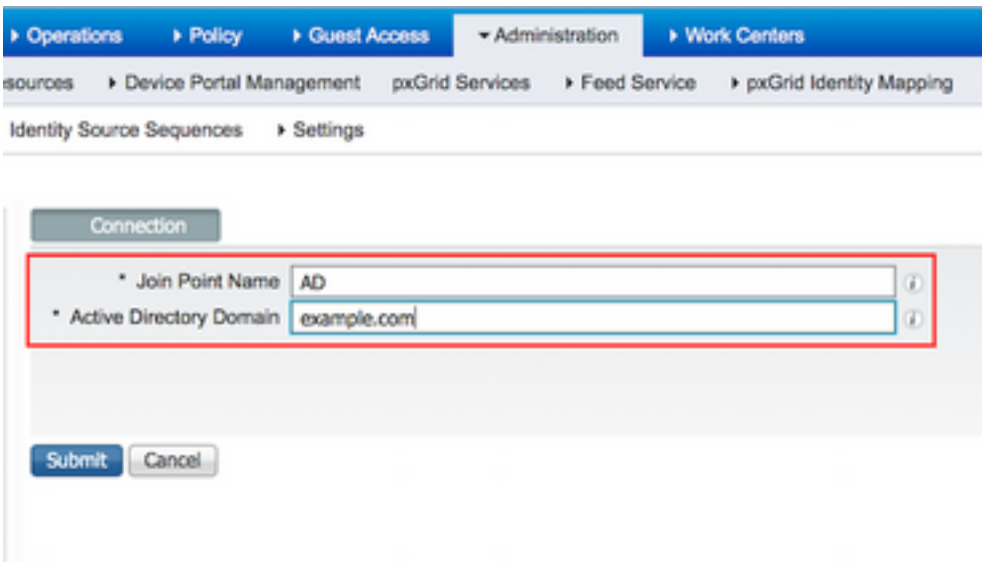


Konfigurationen

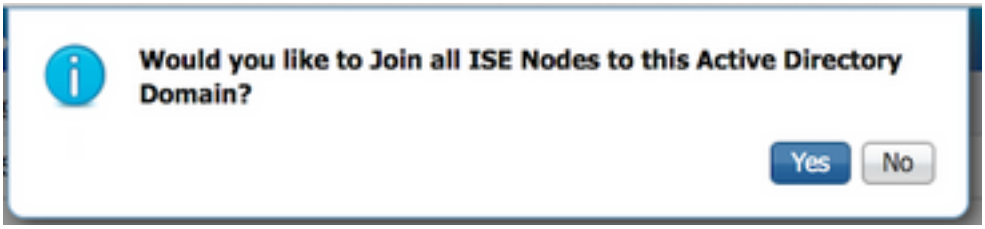
Konfigurieren der ISE für Authentifizierung und Autorisierung

Beitreten zu ISE 2.0 zu Active Directory

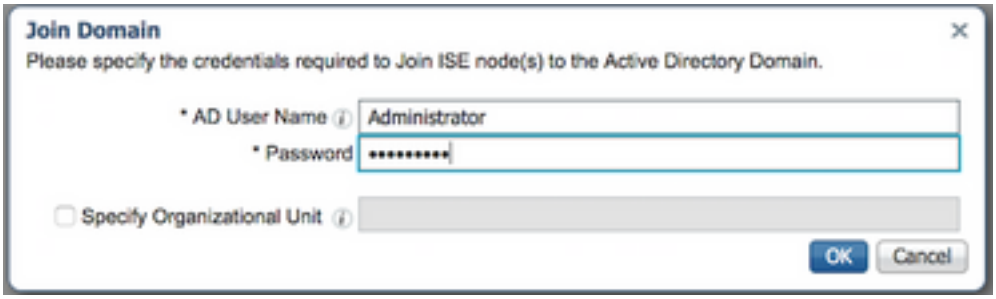
1. Navigieren Sie zu **Administration > Identity Management > External Identity Stores > Active Directory > Add**. Geben Sie den Namen des Join Points und die Active Directory-Domäne an, und klicken Sie auf **Submit (Senden).**



2. Wenn Sie aufgefordert werden, allen ISE-Knoten dieser Active Directory-Domäne beizutreten, klicken Sie auf **Ja.**



3. Geben Sie den AD-Benutzernamen und das Kennwort ein, und klicken Sie auf **OK**.

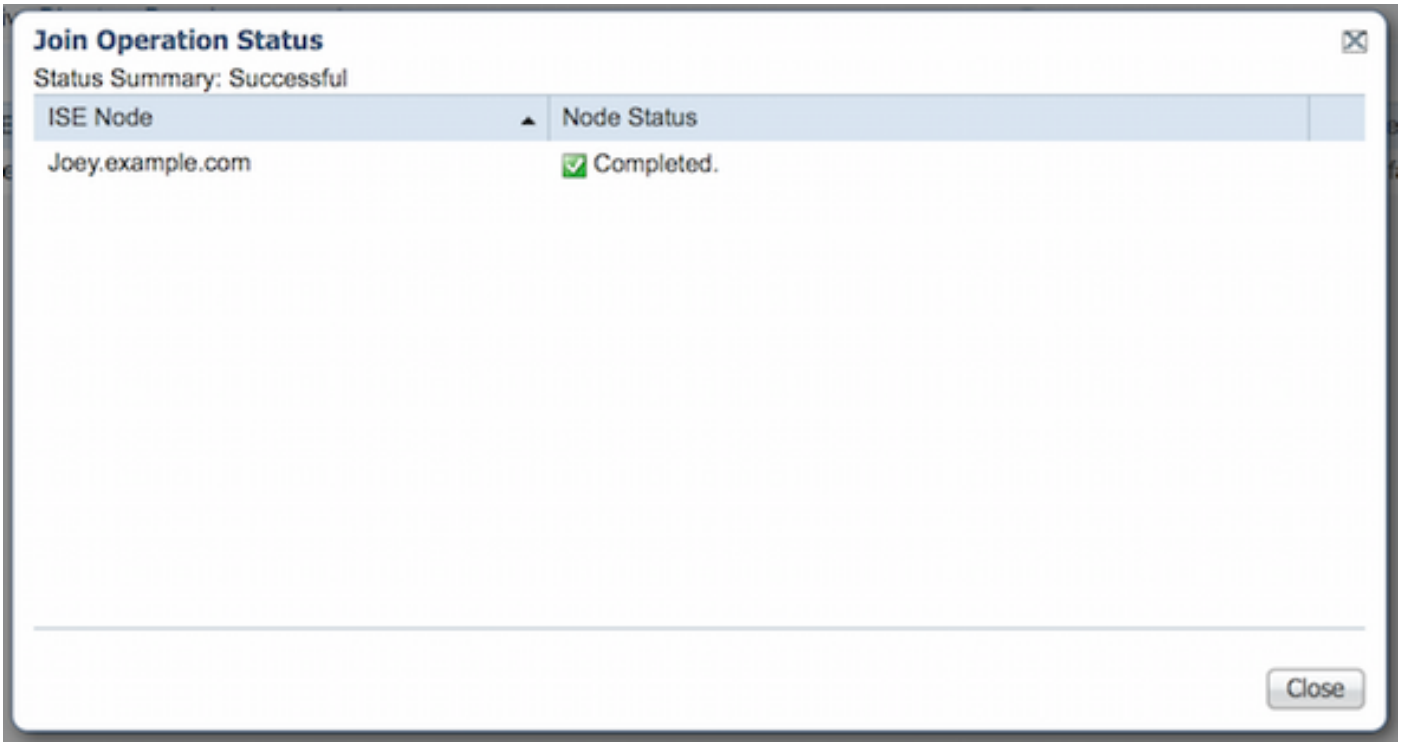


Das für den Domänenzugriff in der ISE erforderliche AD-Konto kann einen der folgenden Werte aufweisen:

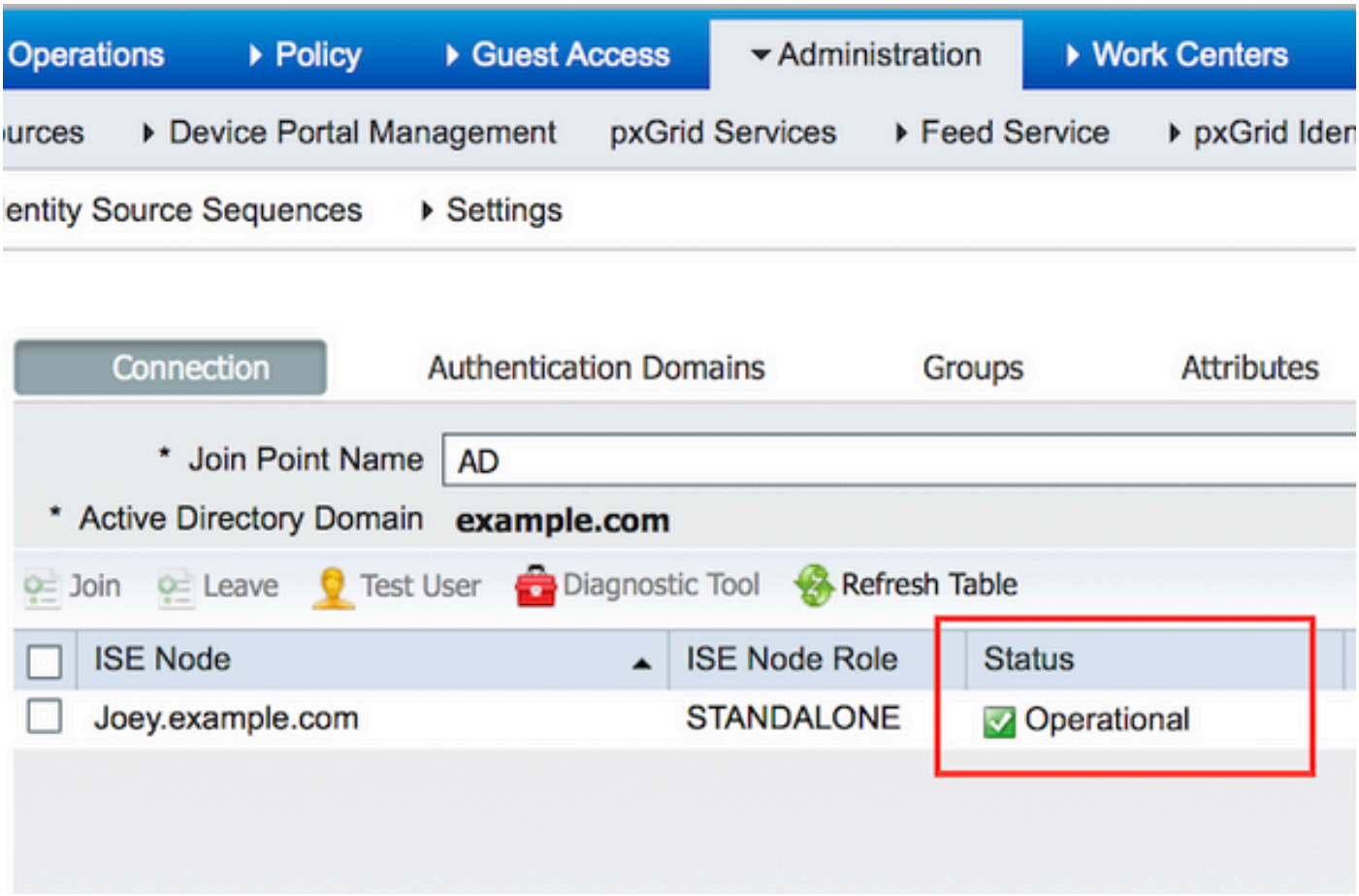
- Hinzufügen von Workstations zur Domänenbenutzerrechte in der entsprechenden Domäne
- Berechtigung "Computerobjekte erstellen" oder "Computerobjekte löschen" für den entsprechenden Computer-Container, in dem das Konto des ISE-Computers erstellt wird, bevor er dem ISE-Computer zur Domäne beitritt

  Anmerkung: Cisco empfiehlt, die Sperrrichtlinie für das ISE-Konto zu deaktivieren und die AD-Infrastruktur so zu konfigurieren, dass Warnmeldungen an den Administrator gesendet werden, wenn ein falsches Kennwort für das Konto verwendet wird. Bei Eingabe eines falschen Passworts erstellt oder ändert die ISE ihr Computerkonto nicht, wenn dies erforderlich ist, und verweigert daher möglicherweise alle Authentifizierungen.

4. Überprüfen Sie den Betriebsstatus. Der Knotenstatus muss als "Abgeschlossen" angezeigt werden. Klicken Sie auf **Close** (Schließen).



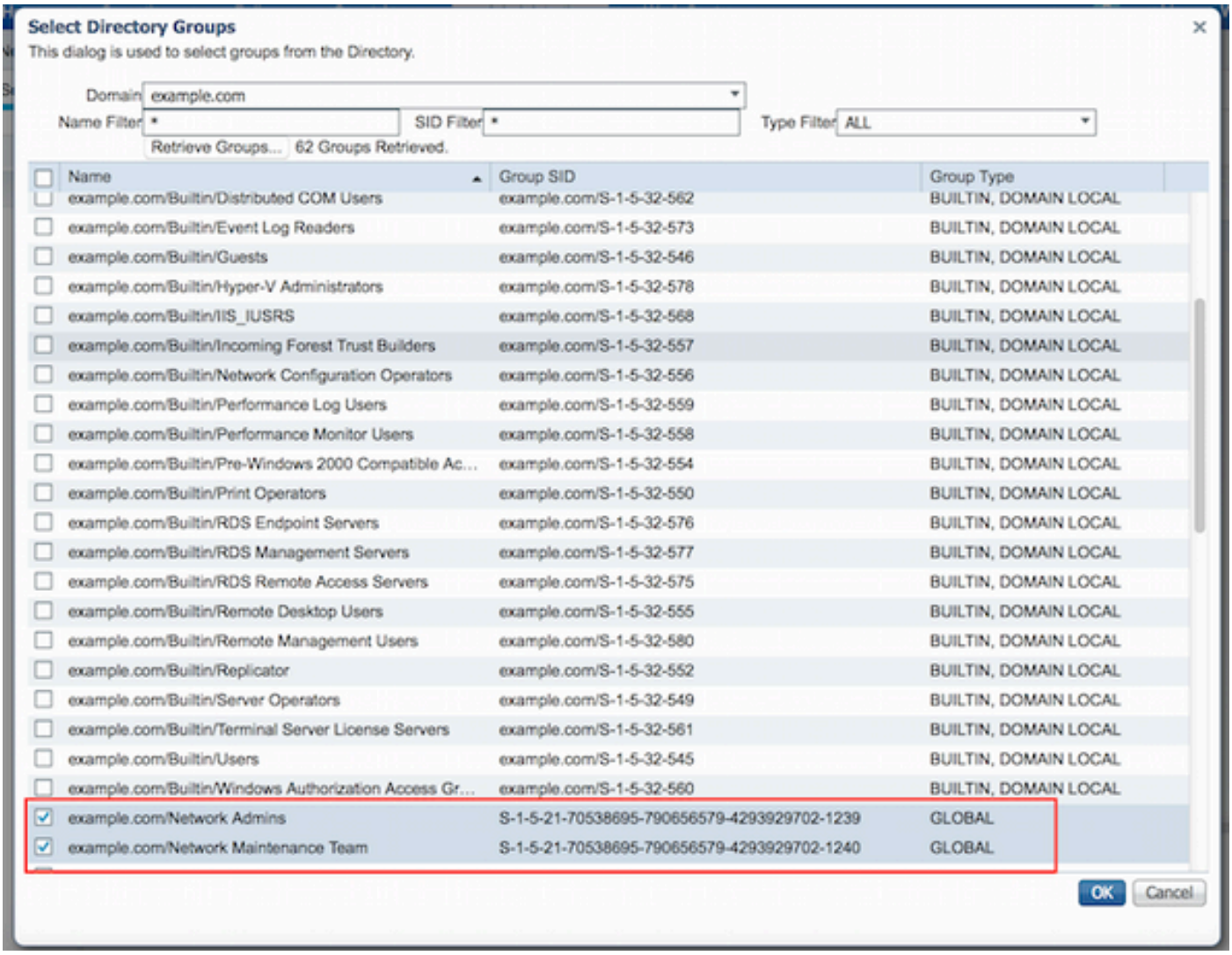
5. Der Status der AD ist operationell.



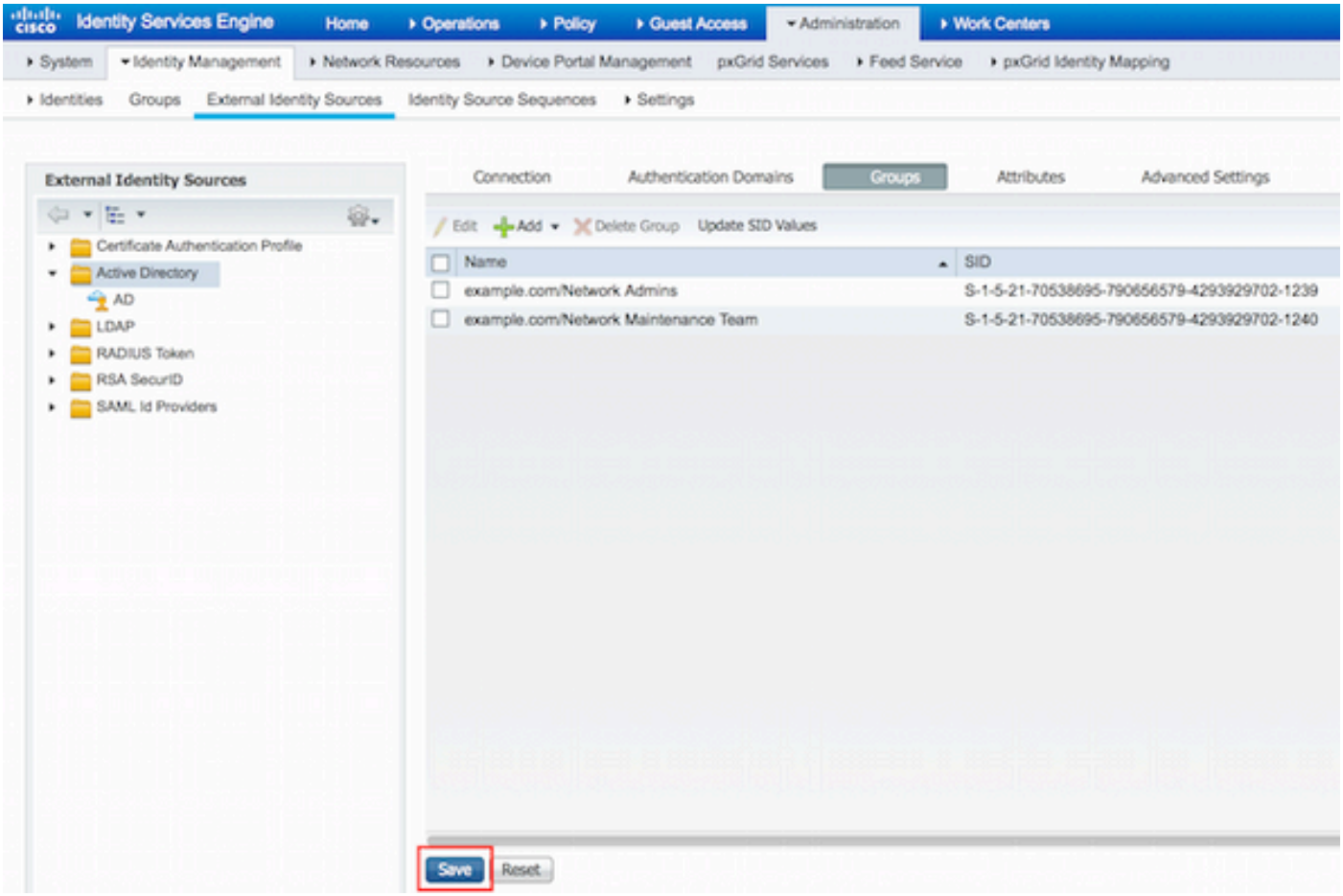
6. Navigieren Sie zu **Gruppen > Hinzufügen > Gruppen auswählen aus Verzeichnis > Gruppen abrufen.** Aktivieren Sie die Kontrollkästchen **Netzwerkadministratoren** AD-Gruppe und **Netzwerkwartungsteam** AD-Gruppe, wie in dieser Abbildung dargestellt.

Anmerkung: Der Benutzeradministrator ist Mitglied der AD-Gruppe "Netzwerkadministratoren". Dieser Benutzer hat volle Zugriffsberechtigungen. Dieser

Benutzer ist Mitglied der AD-Gruppe des Netzwerkwartungsteams. Dieser Benutzer kann nur show-Befehle ausführen.

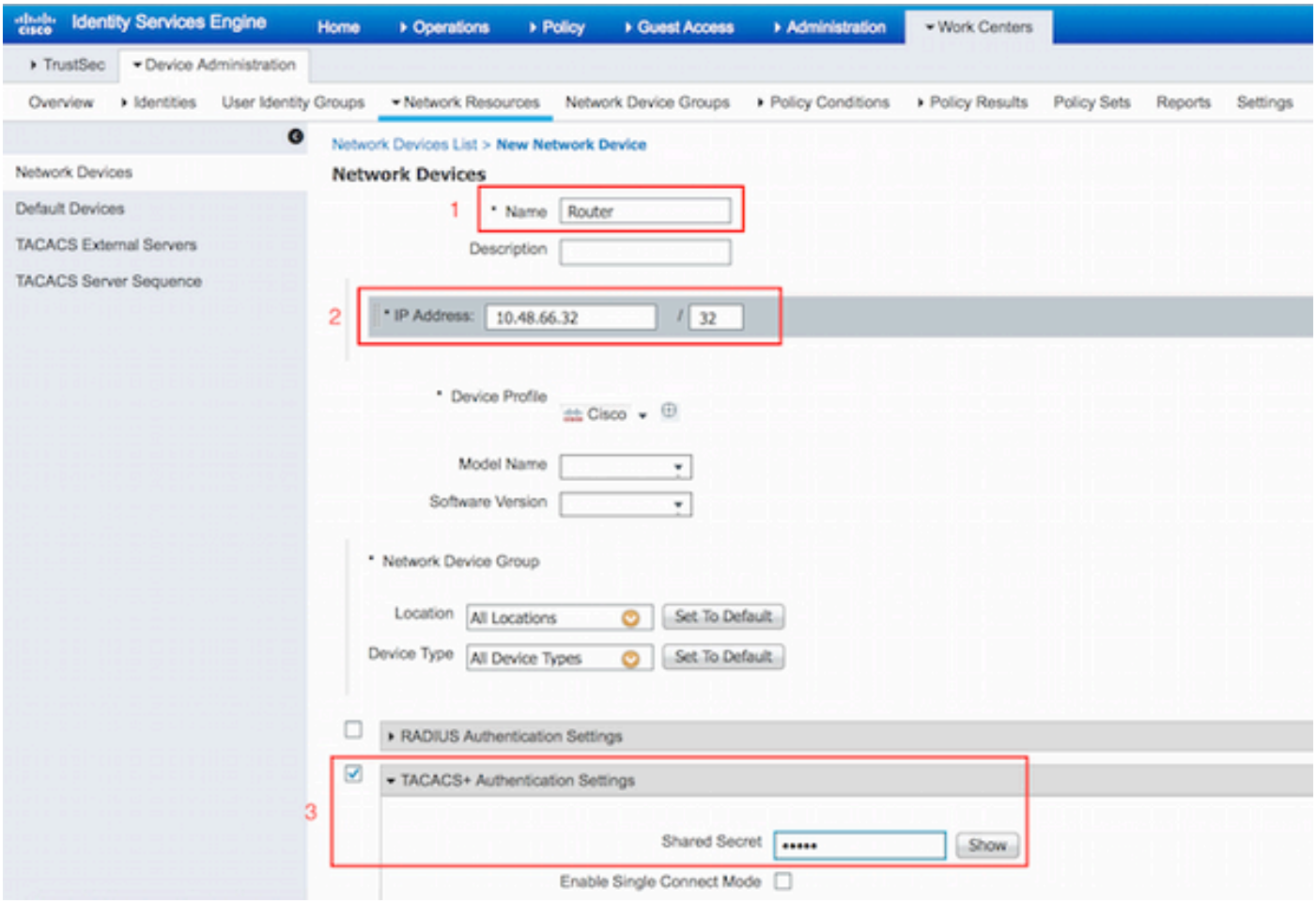


7. Klicken Sie auf **Speichern**, um abgerufene AD-Gruppen zu speichern.



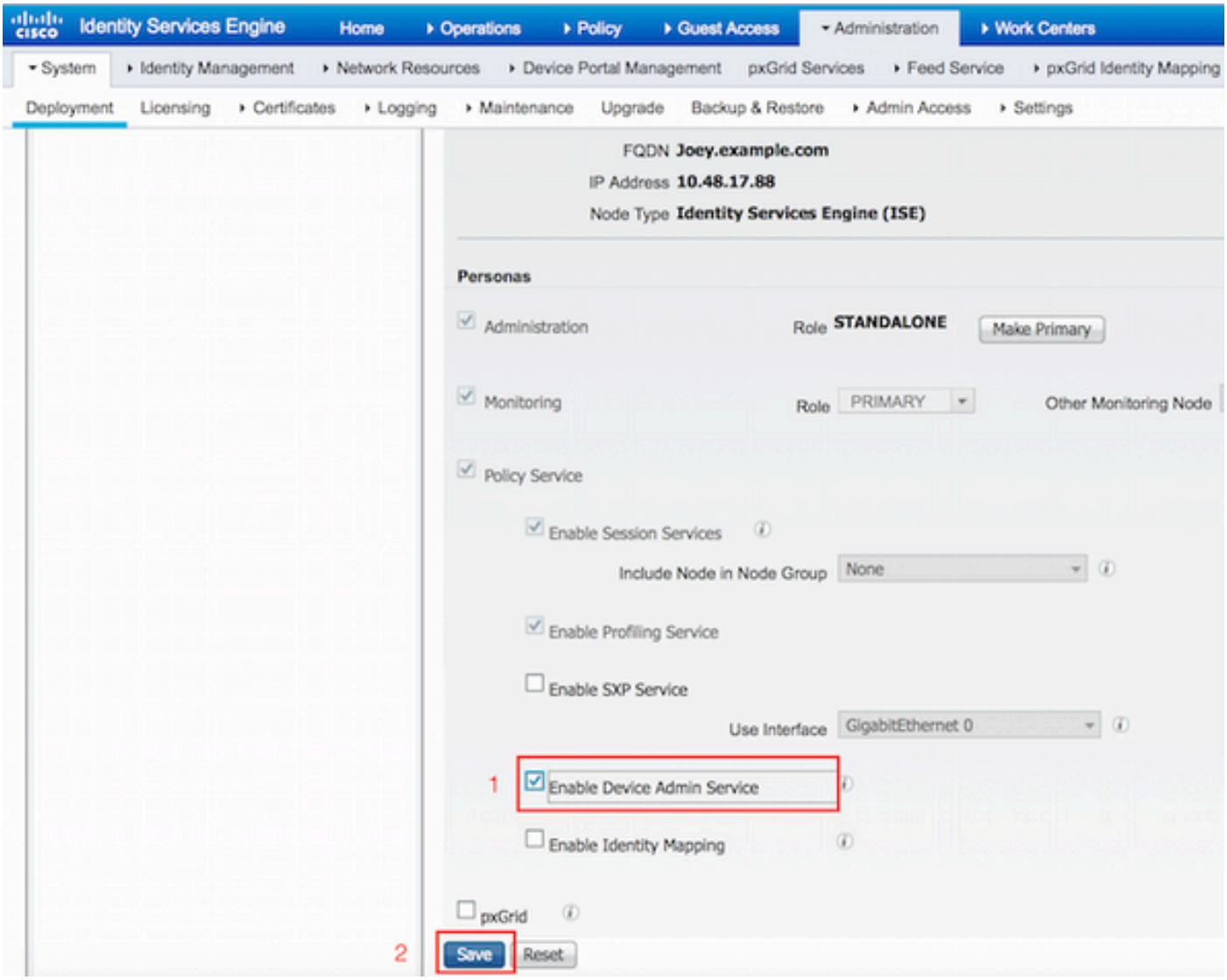
Netzwerkgerät hinzufügen

Navigieren Sie zu **Work Centers > Device Administration > Network Resources > Network Devices**. Klicken Sie auf **Hinzufügen**. Geben Sie den Namen und die IP-Adresse ein, aktivieren Sie das Kontrollkästchen **TACACS+-Authentifizierungseinstellungen**, und geben Sie den Schlüssel für den gemeinsamen geheimen Schlüssel an.



Geräteverwaltungsdienst aktivieren

Navigieren Sie zu **Administration > System > Deployment.** Wählen Sie den gewünschten Knoten. Aktivieren Sie das Kontrollkästchen **"Geräte-Admin-Service aktivieren"**, und klicken Sie auf **Speichern.**

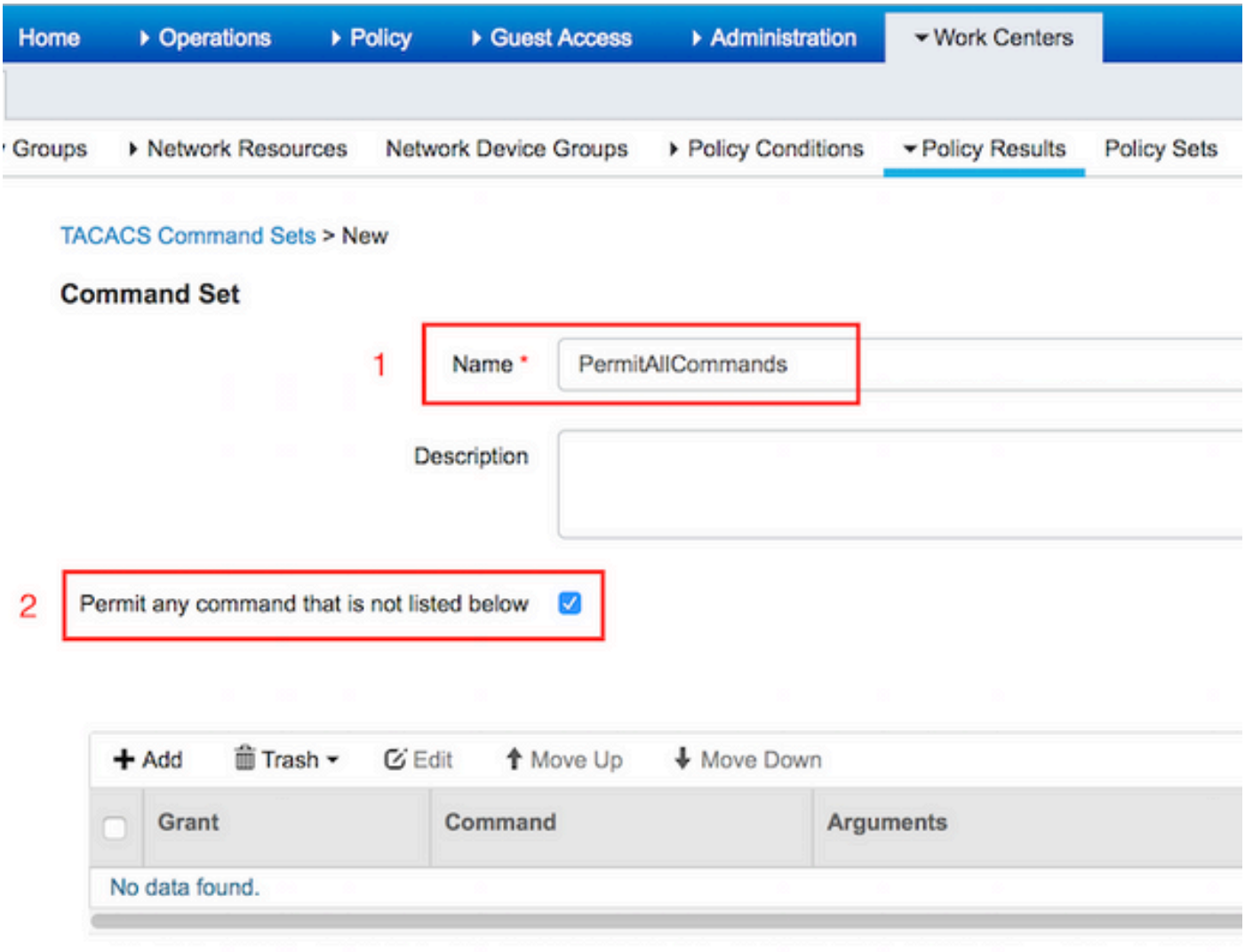


Anmerkung: Für TACACS müssen separate Lizenzen installiert sein.

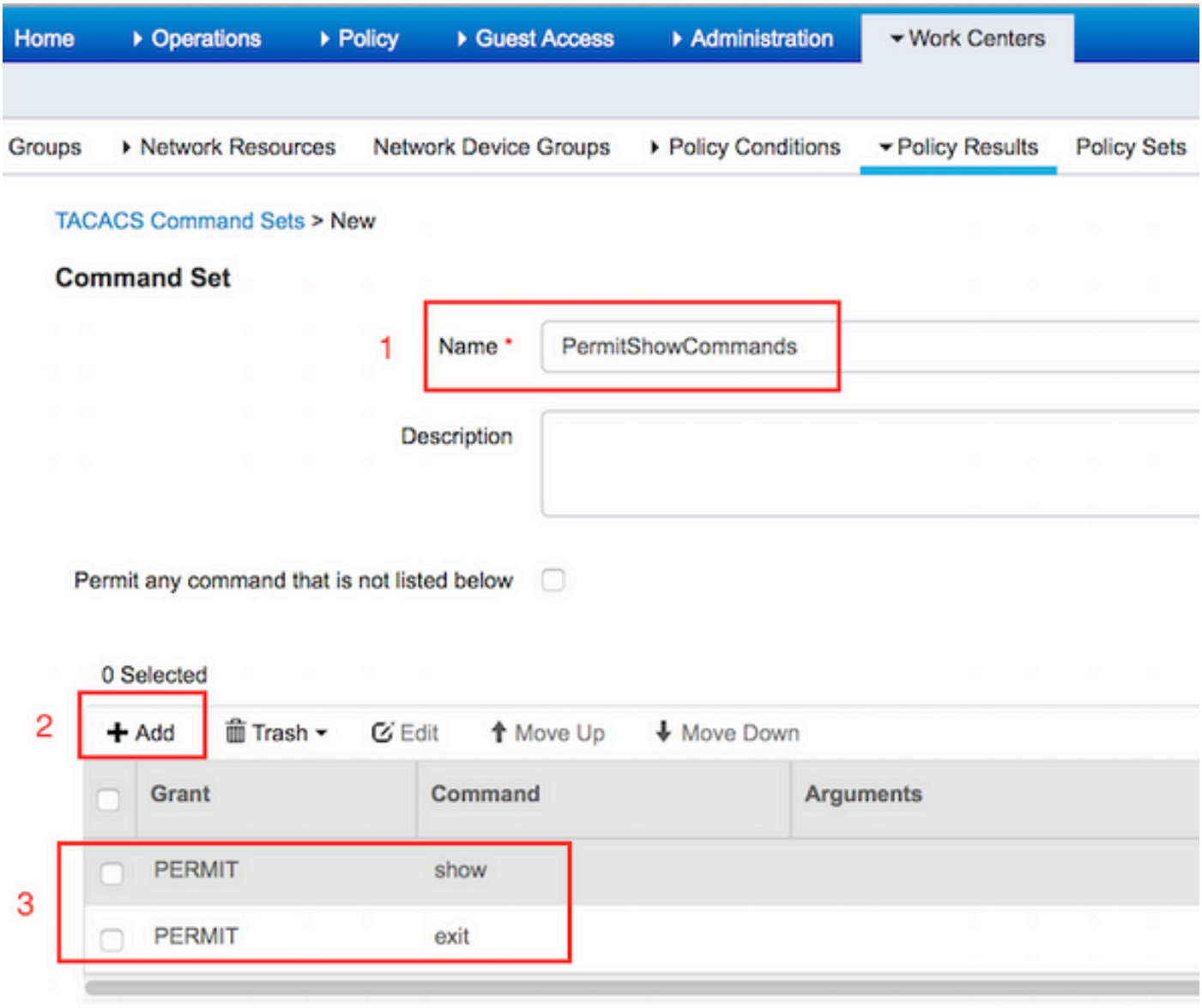
Konfigurieren von TACACS-Befehlssätzen

Es werden zwei Befehlssätze konfiguriert. Erster **PermitAllCommands** für den Benutzer admin, der alle Befehle auf dem Gerät zulässt. Zweiter **PermitShowCommands** für Benutzer, der nur show-Befehle zulässt.

1. Navigieren Sie zu **Work Centers > Device Administration > Policy Results > TACACS Command Sets.** Klicken Sie auf **Hinzufügen.** Geben Sie den Namen **PermitAllCommands ein**, aktivieren Sie das Kontrollkästchen **Alle Befehle zulassen**, die nicht aufgeführt sind, und klicken Sie auf **Senden.**

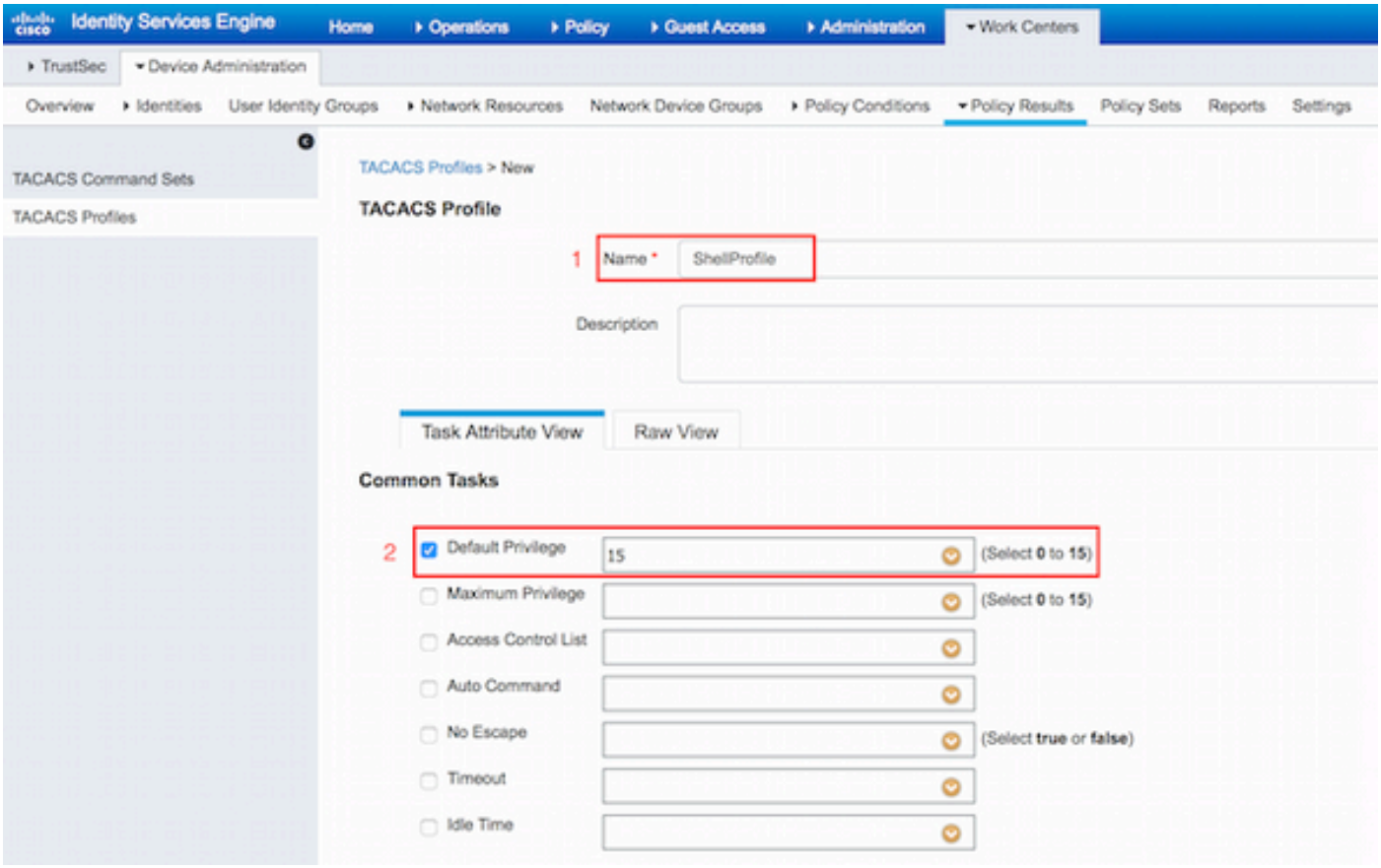


2. Navigieren Sie zu **Work Centers > Device Administration > Policy Results > TACACS Command Sets.** Klicken Sie auf **Hinzufügen.** Geben Sie den Namen **PermitShowCommands ein**, klicken Sie auf **Add**, und lassen Sie die Befehle **show** und **exit zu**. Wenn Arguments leer gelassen wird, werden standardmäßig alle Argumente eingeschlossen. Klicken Sie auf **Senden.**



Konfigurieren des TACACS-Profils

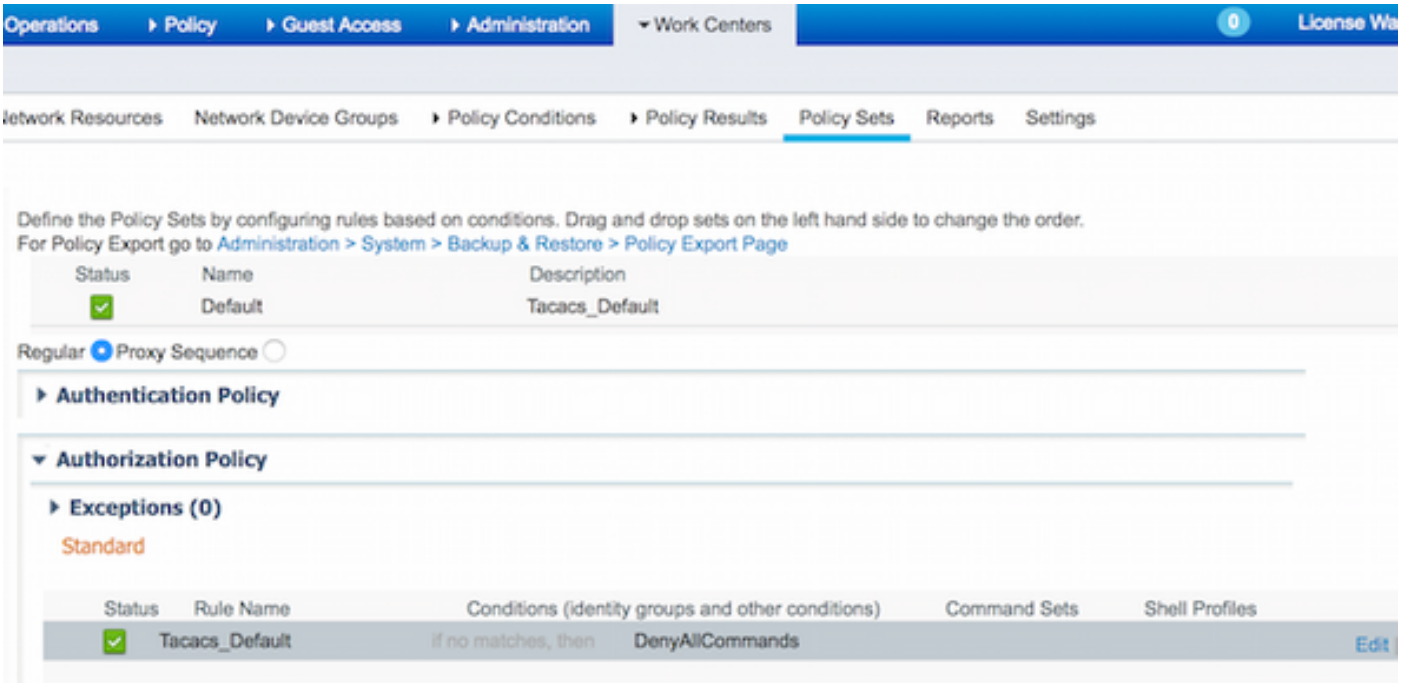
Es wird ein einzelnes TACACS-Profil konfiguriert. Das TACACS-Profil entspricht dem Shell-Profil auf dem ACS. Die eigentliche Befehlserzwingung erfolgt über Befehlssätze. Navigieren Sie zu **Work Centers > Device Administration > Policy Results > TACACS Profiles.** Klicken Sie auf **Hinzufügen.** Geben Sie den Namen ShellProfile ein, aktivieren Sie das Kontrollkästchen **Default Privilege** (Standardberechtigung), und geben Sie den Wert 15 ein. Klicken Sie auf **Submit (Senden).**



Konfigurieren der TACACS-Autorisierungsrichtlinie

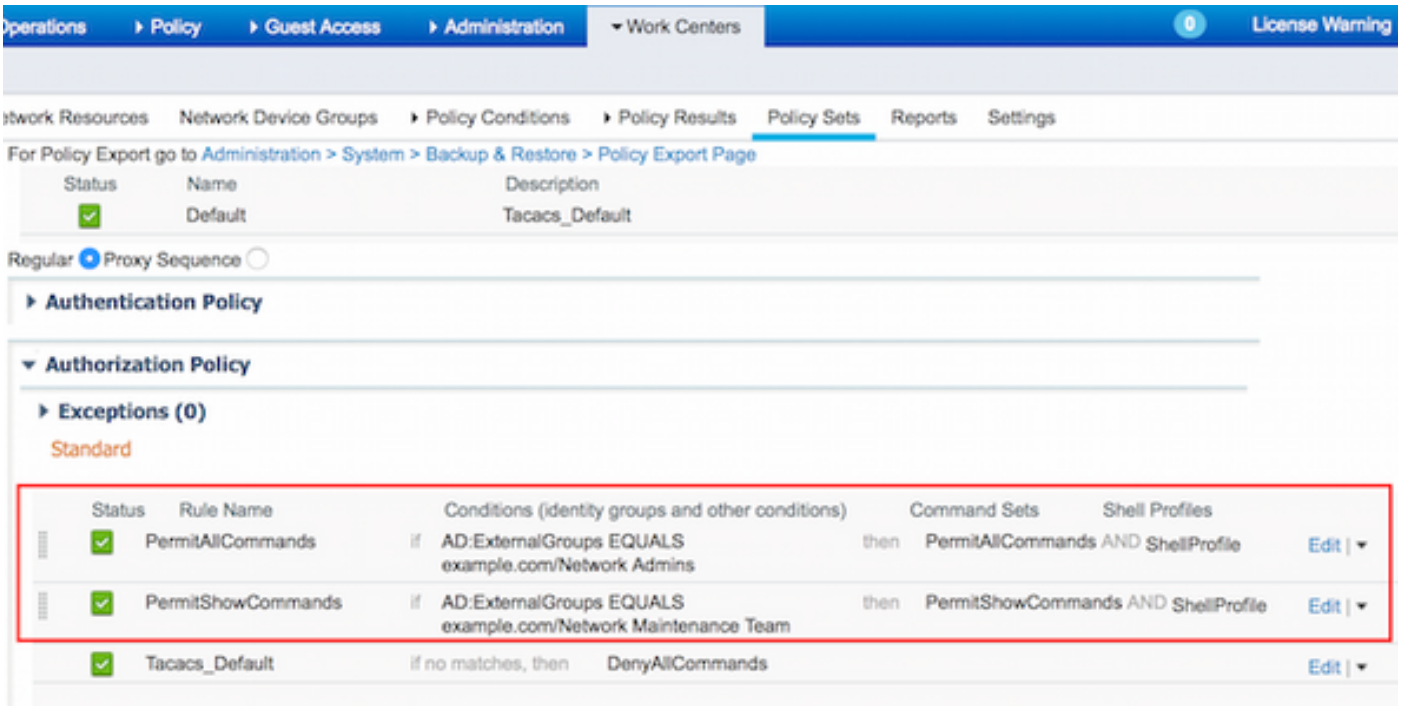
Die Authentifizierungsrichtlinie verweist standardmäßig auf All_User_ID_Stores, das AD enthält, sodass sie unverändert bleibt.

Navigieren Sie zu **Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule oben.**



Es werden zwei Autorisierungsregeln konfiguriert: Die erste Regel weist dem TACACS-Profil ShellProfile und dem Befehl Set PermitAllCommands basierend auf der AD-Gruppenmitgliedschaft

von Netzwerkadministratoren zu. Die zweite Regel weist dem TACACS-Profil ShellProfile und dem Befehl Set PermitShowCommands basierend auf der AD-Gruppenmitgliedschaft des Netzwerkwartungsteams zu.



Konfigurieren des Cisco IOS-Routers für Authentifizierung und Autorisierung

Führen Sie diese Schritte aus, um den Cisco IOS-Router für die Authentifizierung und Autorisierung zu konfigurieren.

1. Erstellen Sie mit dem Befehl **username** einen lokalen Benutzer mit voller Berechtigung für den Fallback, wie hier gezeigt.

```
username cisco privilege 15 password cisco
```

2. Aktivieren Sie ein neues Modell. Definieren Sie den TACACS-Server ISE, und platzieren Sie ihn in der Gruppe ISE_GROUP.

```
aaa new-model

tacacs server ISE
 address ipv4 10.48.17.88
 key cisco
aaa group server tacacs+ ISE_GROUP
 server name ISE
```

> **Anmerkung:** Der Serverschlüssel entspricht dem auf dem ISE-Server zuvor definierten Schlüssel.

3. Testen Sie die Erreichbarkeit des TACACS-Servers mit dem Befehl test **aaa** wie dargestellt.

```
Router#test aaa group tacacs+ admin Krakow123 legacy
Attempting authentication test to server-group tacacs+ using tacacs+
User was successfully authenticated.
```

Die Ausgabe des vorherigen Befehls zeigt an, dass der TACACS-Server erreichbar ist und der Benutzer erfolgreich authentifiziert wurde.

4. Konfigurieren Sie die Anmeldung, aktivieren Sie die Authentifizierungen, und verwenden Sie dann die exec- und Command-Autorisierungen wie dargestellt.

```
aaa authentication login AAA group ISE_GROUP local
aaa authentication enable default group ISE_GROUP enable
aaa authorization exec AAA group ISE_GROUP local
aaa authorization commands 0 AAA group ISE_GROUP local
aaa authorization commands 1 AAA group ISE_GROUP local
aaa authorization commands 15 AAA group ISE_GROUP local
aaa authorization config-commands
```

> **Anmerkung:** Die erstellte Methodenliste erhält den Namen AAA und wird später verwendet, wenn sie Zeile vty zugewiesen wird.

5. Zuordnen von Methodenlisten zu Zeile vty 0 4.

```
line vty 0 4
 authorization commands 0 AAA
 authorization commands 1 AAA
 authorization commands 15 AAA
 authorization exec AAA
 login authentication AAA
```

Überprüfung

Cisco IOS Router-Verifizierung

1. Telnet zum Cisco IOS-Router als Administrator, der zur Gruppe mit vollem Zugriff in AD gehört. Die Gruppe Netzwerkadministratoren ist die Gruppe in AD, die dem Befehlssatz ShellProfile und PermitAllCommands auf der ISE zugeordnet ist. Versuchen Sie, einen beliebigen Befehl auszuführen, um vollständigen Zugriff zu gewährleisten.

```
Username:admin
Password:

Router#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#encryption aes
Router(config-isakmp)#exit
Router(config)#exit
Router#
```

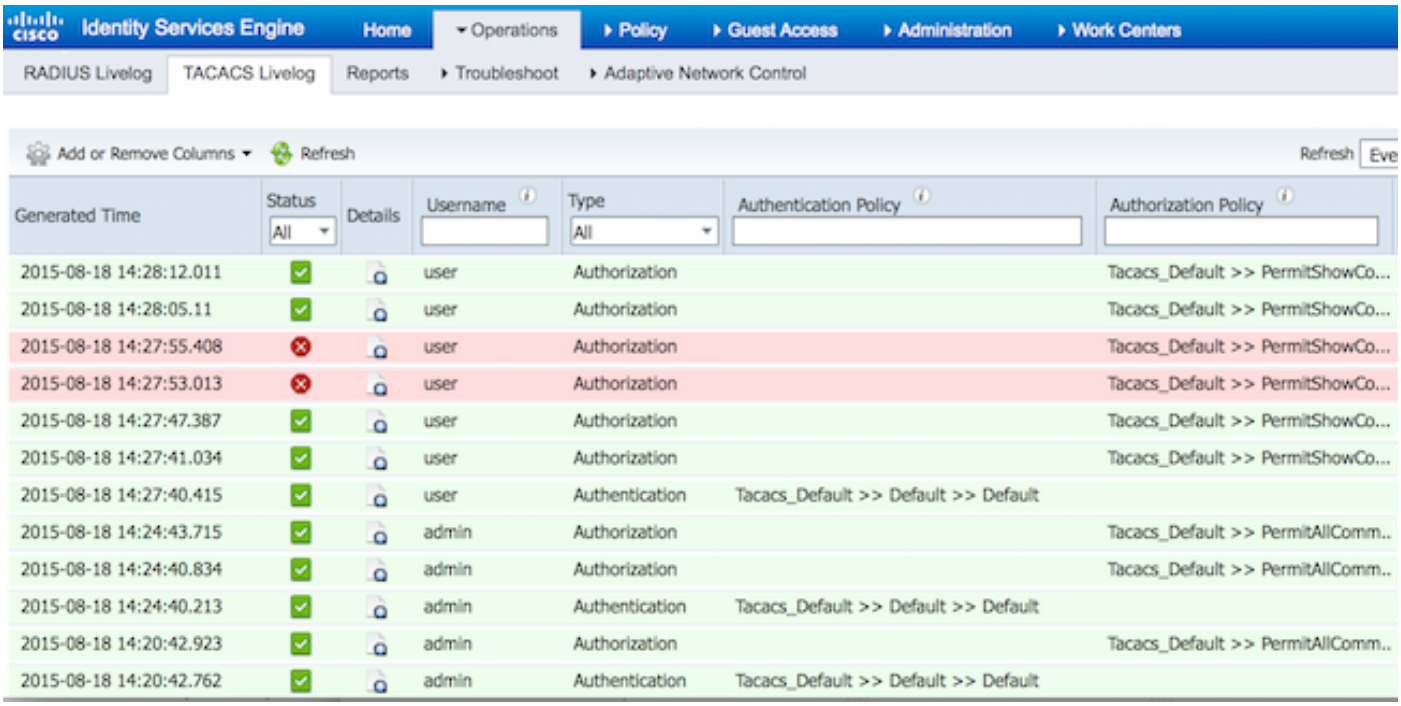
2. Telnet zum Cisco IOS-Router als Benutzer, der zur Gruppe mit beschränktem Zugriff in AD gehört. Die Gruppe "Netzwerkwartungsteam" ist die Gruppe in AD, die dem Befehlssatz ShellProfile und PermitShowCommands auf der ISE zugeordnet ist. Versuchen Sie, einen beliebigen Befehl auszuführen, um sicherzustellen, dass nur show-Befehle ausgegeben werden können.

```
Username:user
```

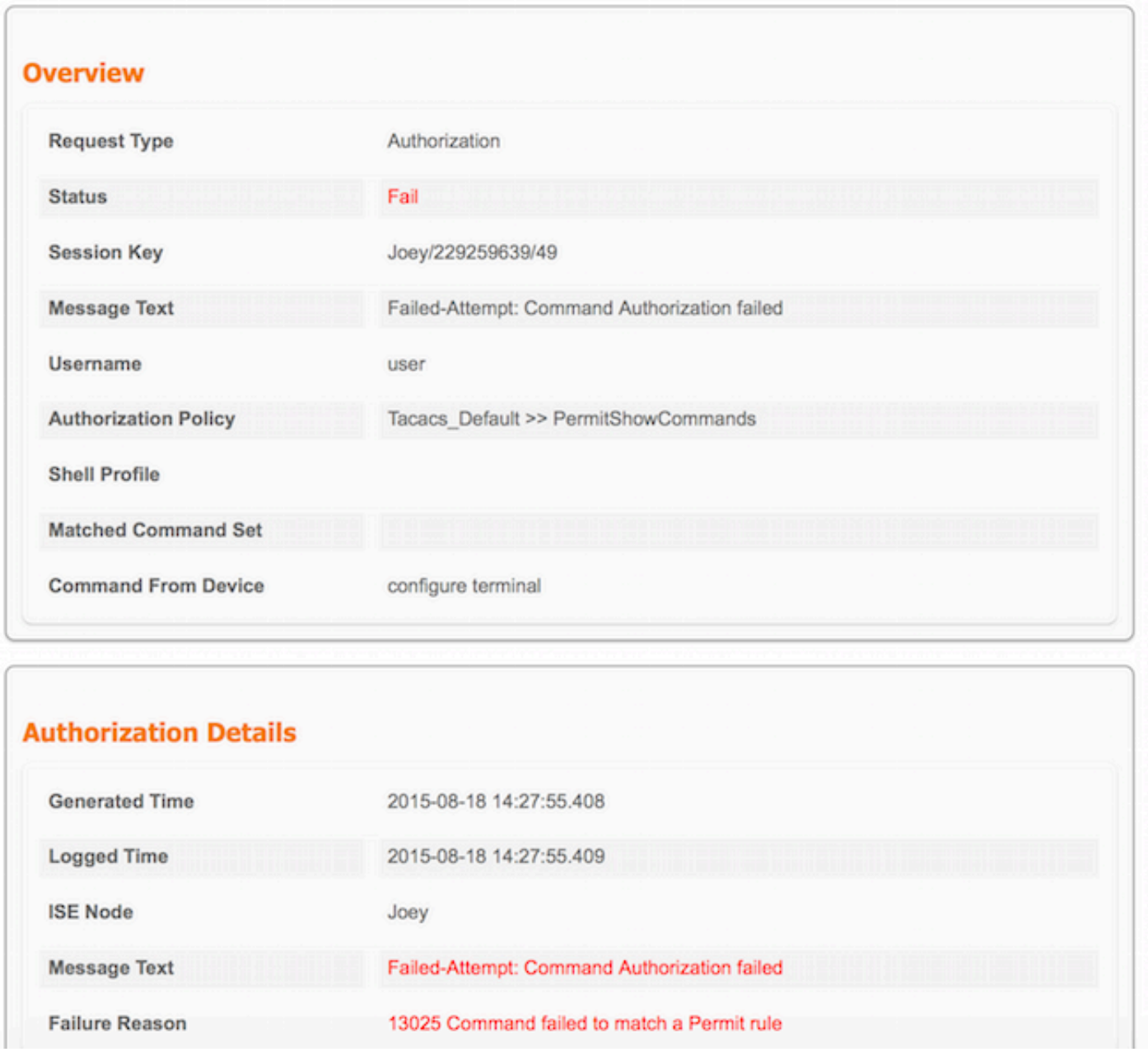
```
Password:

Router#show ip interface brief | exclude unassigned
Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         10.48.66.32     YES NVRAM  up                    up

Router#ping 8.8.8.8
Command authorization failed.

Router#configure terminal
Command authorization failed.

Router#show running-config | include hostname
hostname Router
Router#
```

ISE 2.0-Verifizierung

1. Navigieren Sie zu **Operationen > TACACS-Livelog.** Stellen Sie sicher, dass die durchgeführten Versuche erkannt werden.



2. Klicken Sie auf die Details eines der roten Berichte. Fehlgeschlagener Befehl, der früher ausgeführt wurde, wird angezeigt.



Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229259639/49
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> PermitShowCommands
Shell Profile	
Matched Command Set	
Command From Device	configure terminal

Authorization Details

Generated Time	2015-08-18 14:27:55.408
Logged Time	2015-08-18 14:27:55.409
ISE Node	Joey
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

Fehlerbehebung

Fehler: 13025 Befehl konnte nicht mit einer Zulässigkeitsregel übereinstimmen

Überprüfen Sie die SelectedCommandSet-Attribute, um zu überprüfen, ob die erwarteten Befehlssätze von der Autorisierungsrichtlinie ausgewählt wurden.

Zugehörige Informationen

Technischer Support und Dokumentation für Cisco Systeme

ISE 2.0 - Versionshinweise

ISE 2.0 Hardware-Installationshandbuch

ISE 2.0 Upgrade-Leitfaden

ACS auf ISE Migration - Tool-Leitfaden

ISE 2.0 Active Directory Integration Guide

ISE 2.0 Engine - Administratorhandbuch

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.