Konfiguration und Fehlerbehebung für externe TACACS-Server auf der ISE

Inhalt

Einführung

In diesem Dokument wird die Funktion zur Verwendung des externen TACACS+-Servers in einer Bereitstellung mithilfe der Identity Service Engine (ISE) als Proxy beschrieben.

Voraussetzungen

Anforderungen

- Grundlegende Kenntnisse der Geräteadministration auf der ISE.
- Dieses Dokument basiert auf Identity Service Engine Version 2.0, die auf alle Versionen von Identity Service Engine Version 2.0 angewendet wird.

Verwendete Komponenten

> **Hinweis**: Jeder Verweis auf ACS in diesem Dokument kann als Verweis auf einen beliebigen externen TACACS+-Server interpretiert werden. Die Konfiguration des ACS und die Konfiguration anderer TACACS-Server können jedoch variieren.

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Identity Service Engine 2.0
- Access Control System (ACS) 5.7

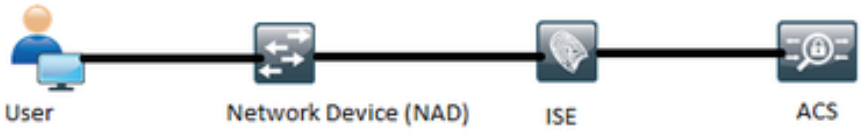
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen von Konfigurationsänderungen verstehen.

Konfigurieren

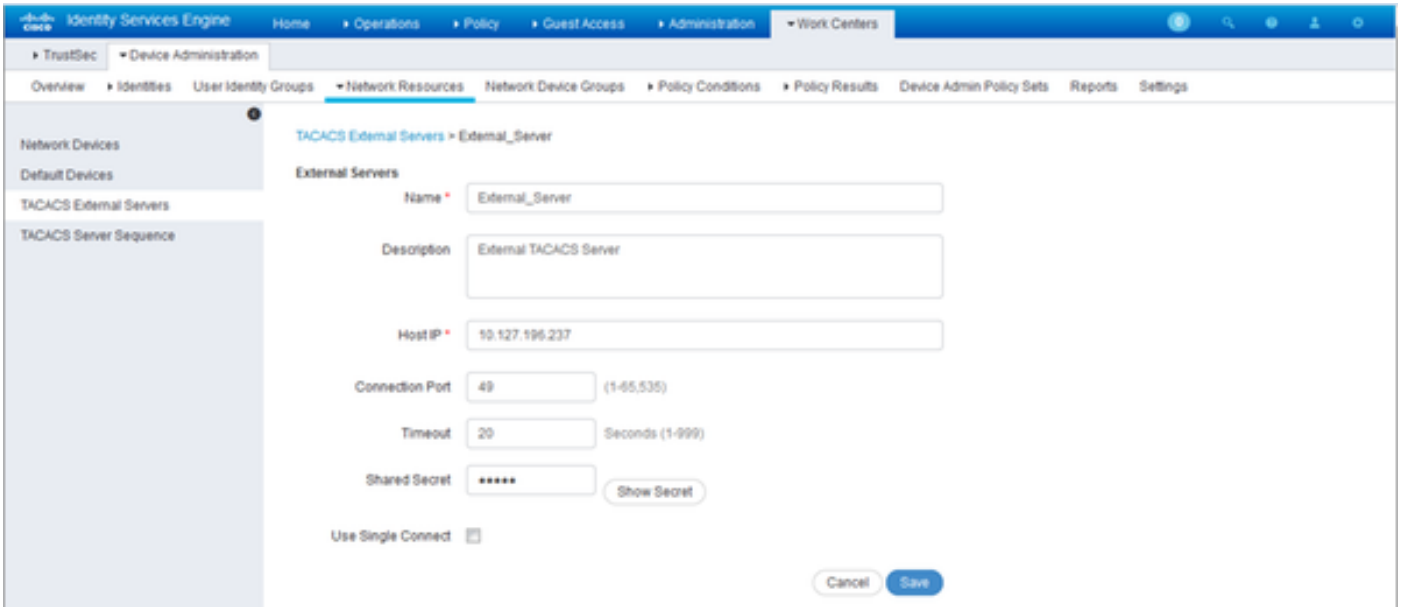
Dieser Abschnitt hilft bei der Konfiguration der ISE für die Proxy-Funktion von TACACS+-Anfragen an ACS.

Netzwerkdiagramm



ISE konfigurieren

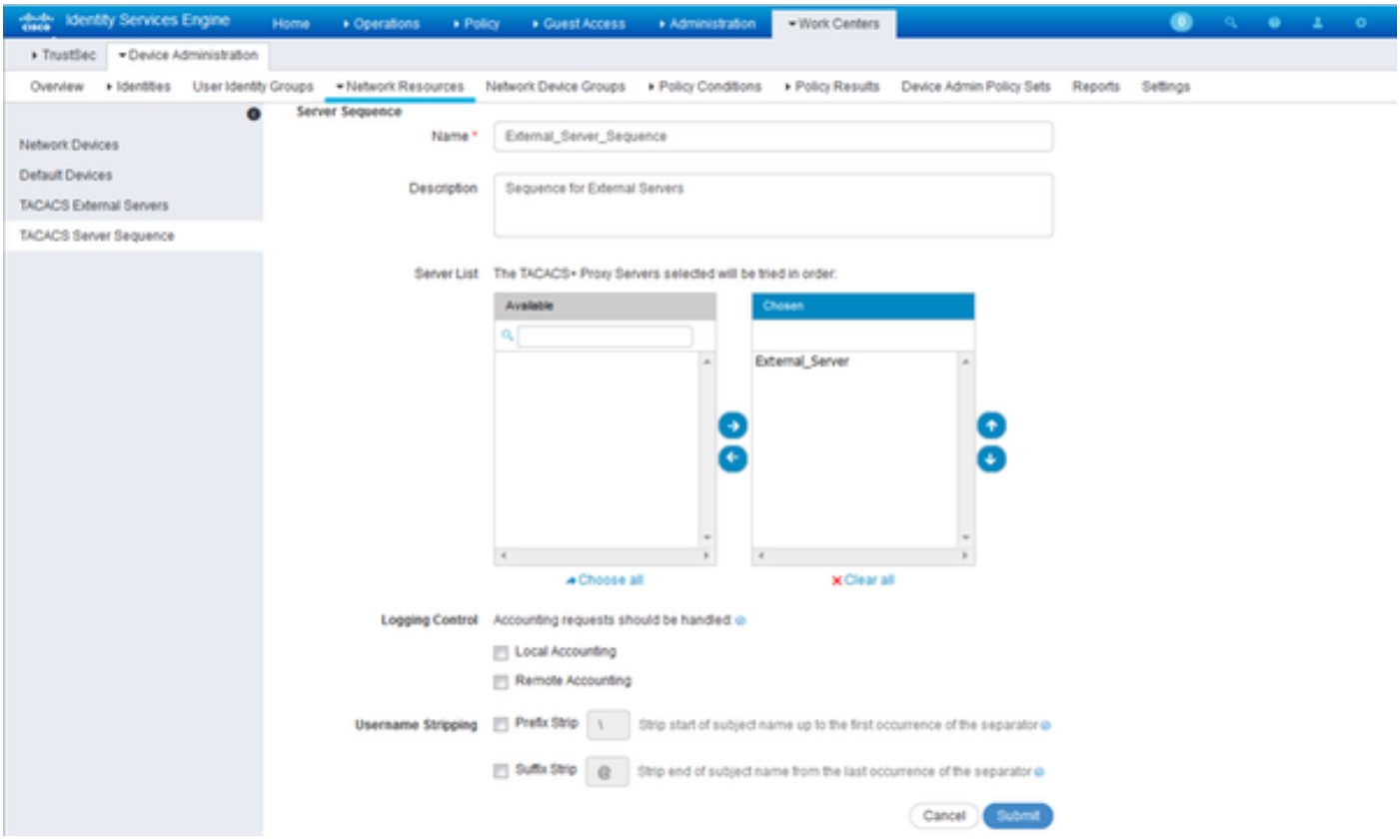
1. Auf der ISE können mehrere externe TACACS-Server konfiguriert und zur Authentifizierung der Benutzer verwendet werden. Um den externen TACACS+-Server auf der ISE zu konfigurieren, gehen Sie zu **Work Centers > Device Administration > Network Resources > TACACS External Servers.** Klicken Sie auf **Hinzufügen**, und geben Sie die Details zu den externen Serverdetails ein.



Der in diesem Abschnitt bereitgestellte gemeinsame geheime Schlüssel muss der gleiche geheime Schlüssel sein, der im ACS verwendet wird.

2. Um den konfigurierten externen TACACS-Server zu verwenden, muss er in einer TACACS-Serversequenz hinzugefügt werden, die in den Richtliniensätzen verwendet wird. Um die

TACACS-Serversequenz zu konfigurieren, navigieren Sie zu **Work Centers > Device Administration > Network Resources > TACACS Server Sequence.** Klicken Sie auf **Hinzufügen,** geben Sie die Details ein, und wählen Sie die Server aus, die in dieser Sequenz verwendet werden sollen.

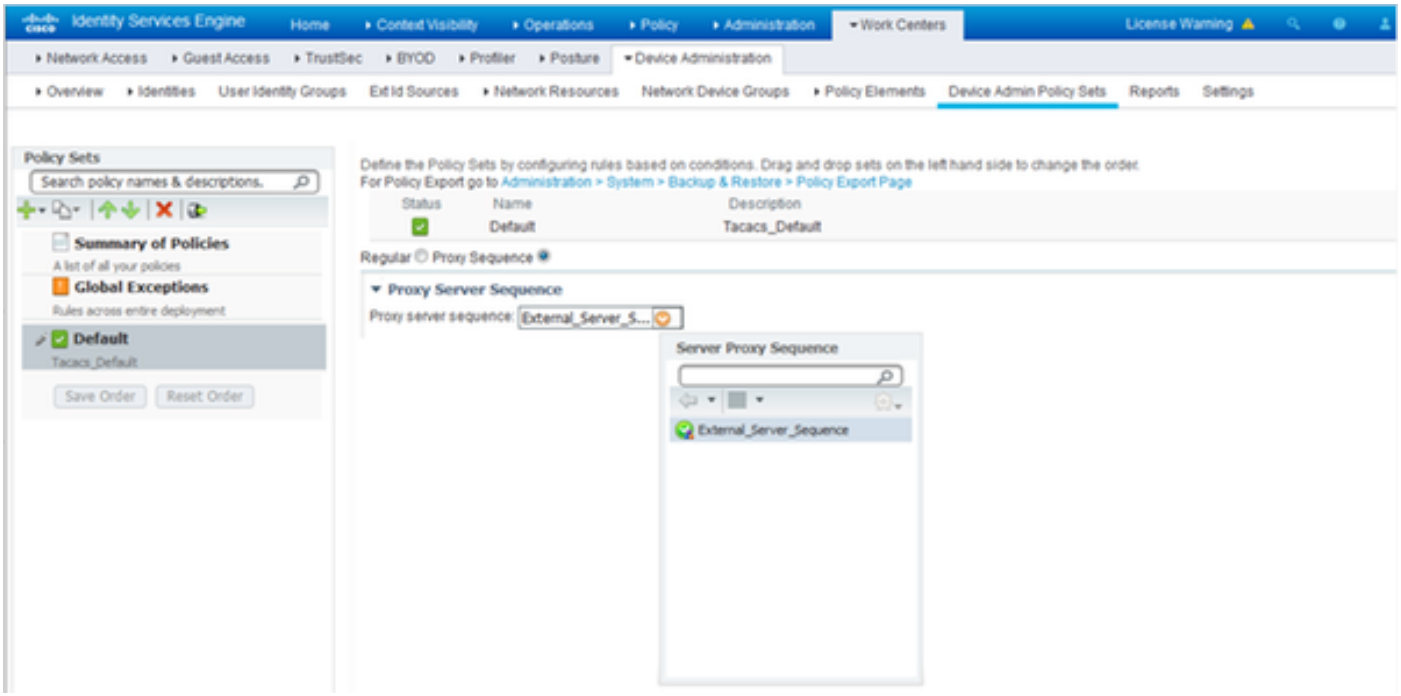


Neben der Serversequenz wurden zwei weitere Optionen bereitgestellt. Protokollierungssteuerung und BenutzernamensStripping.

Die Protokollierungskontrolle bietet die Möglichkeit, entweder die Buchhaltungsanforderungen lokal auf der ISE zu protokollieren oder die Buchhaltungsanforderungen an den externen Server zu protokollieren, der auch die Authentifizierung übernimmt.

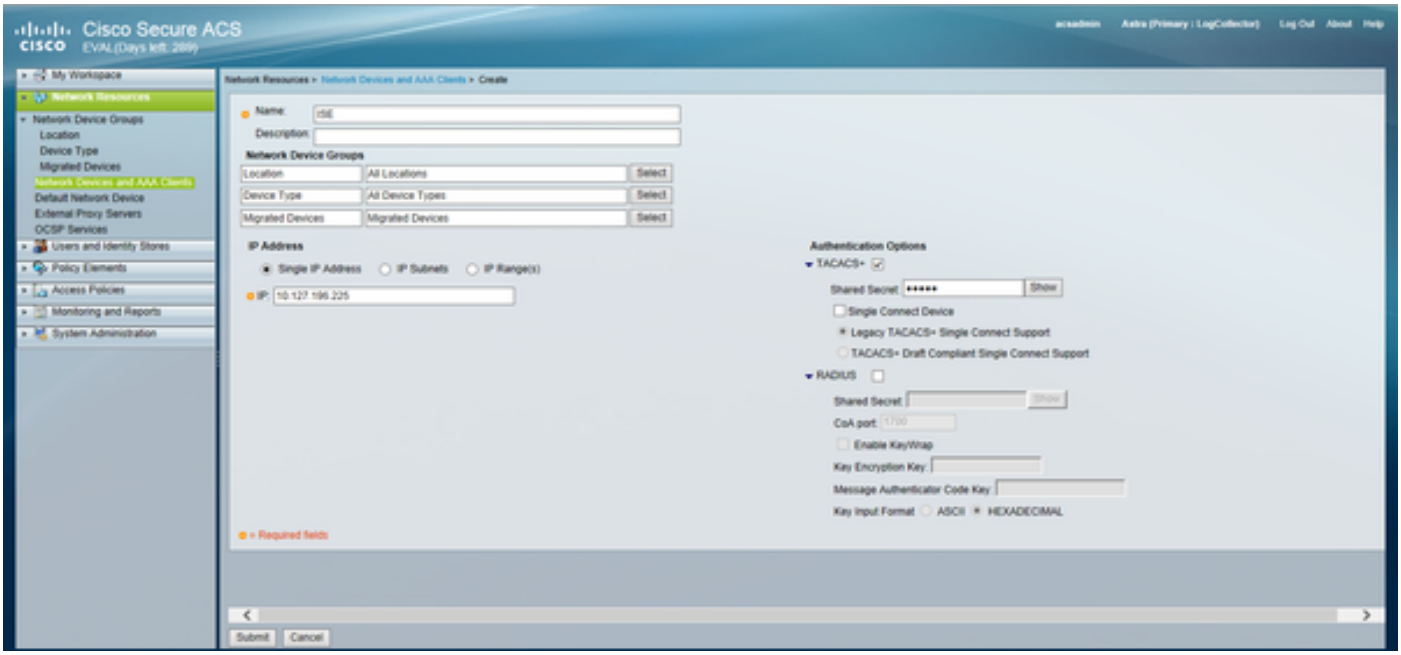
Mit der Benutzernamensabtrennung wird entweder das Präfix oder das Suffix entfernt, indem ein Trennzeichen angegeben wird, bevor die Anforderung an einen externen TACACS-Server weitergeleitet wird.

3. Um die konfigurierte externe TACACS-Serversequenz zu verwenden, müssen die Richtliniensätze für die Verwendung der erstellten Sequenz konfiguriert werden. Um die Richtliniensätze für die Verwendung der externen Serversequenz zu konfigurieren, gehen Sie zu **Work Centers > Device Administration > Device Admin Policy Sets > [den Richtliniensatz auswählen].** Aktivieren Sie das Optionsfeld **Proxy Sequence.** Wählen Sie die erstellte externe Serversequenz aus.

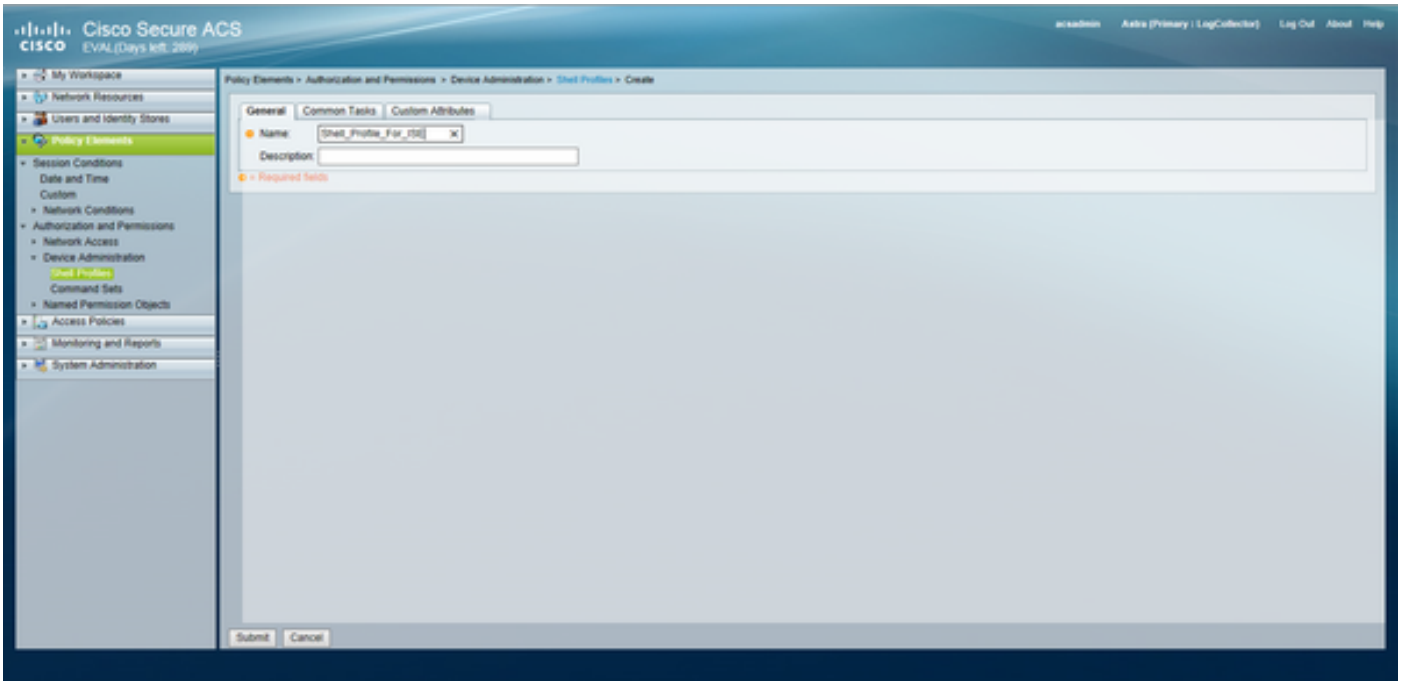


ACS konfigurieren

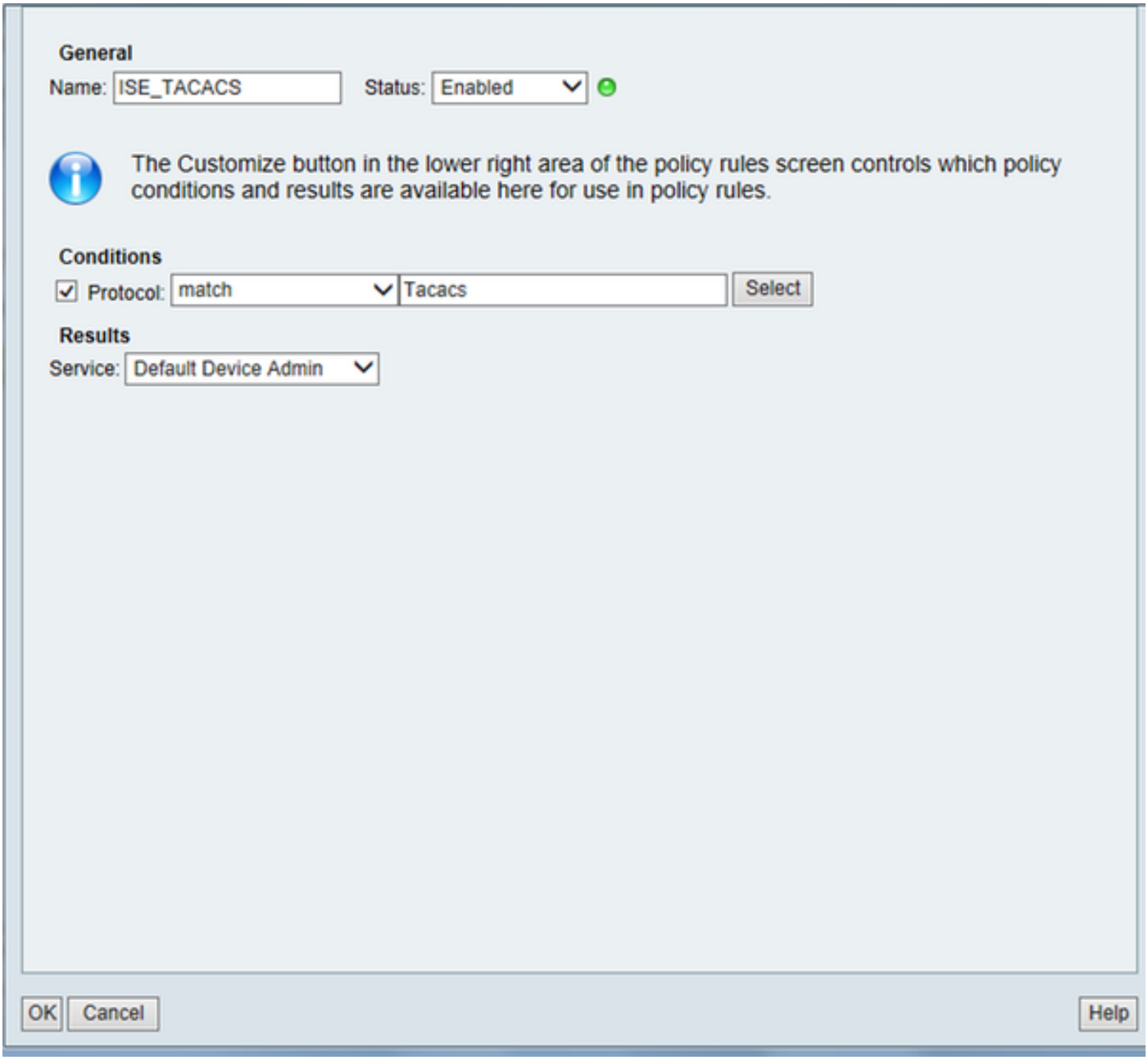
Für den ACS ist die ISE nur ein weiteres Netzwerkgerät, das eine TACACS-Anforderung sendet. Um die ISE in ACS als Netzwerkgerät zu konfigurieren, navigieren Sie zu **Netzwerkressourcen > Netzwerkgeräte und AAA-Clients.** Klicken Sie auf **Erstellen,** und geben Sie die Details des ISE-Servers unter Verwendung des auf der ISE konfigurierten gemeinsamen geheimen Codes ein.



Konfigurieren Sie die Geräteverwaltungsparameter für den ACS, die Shell-Profile und die Befehlssätze. Navigieren Sie zum Konfigurieren von Shell-Profilen zu **Richtlinienelementen > Autorisierung und Berechtigungen > Geräteverwaltung > Shell-Profile.** Klicken Sie auf **Erstellen** und konfigurieren Sie den Namen, die allgemeinen Aufgaben und die benutzerdefinierten Attribute entsprechend der Anforderungen.



Navigieren Sie zum Konfigurieren von Befehlssätzen zu **Richtlinienelementen > Autorisierung und Berechtigungen > Geräteverwaltung > Befehlsgruppen.** Klicken Sie auf **Erstellen** und füllen Sie die Details entsprechend den Anforderungen aus.



Konfigurieren Sie den in der Dienstauswahl-Regel ausgewählten Zugriffsdienst entsprechend der Anforderung.Um Zugriffsdienstregeln zu konfigurieren, navigieren Sie zu **Zugriffsrichtlinien > Zugriffsdienste > Standardgeräteadministrator > Identität,** wo der zu verwendende Identitätsspeicher für die Authentifizierung ausgewählt werden kann. Sie können die Autorisierungsregeln konfigurieren, indem Sie zu **Access Policies > Access Services > Default Device Admin > Authorization** (**Zugriffsrichtlinien > Zugriffsdienste > Standardgeräteadministrator > Autorisierung)** navigieren**.**

> **Hinweis**: Die Konfiguration der Autorisierungsrichtlinien und Shell-Profile für bestimmte Geräte kann variieren. Dies wird in diesem Dokument nicht behandelt.

Überprüfen

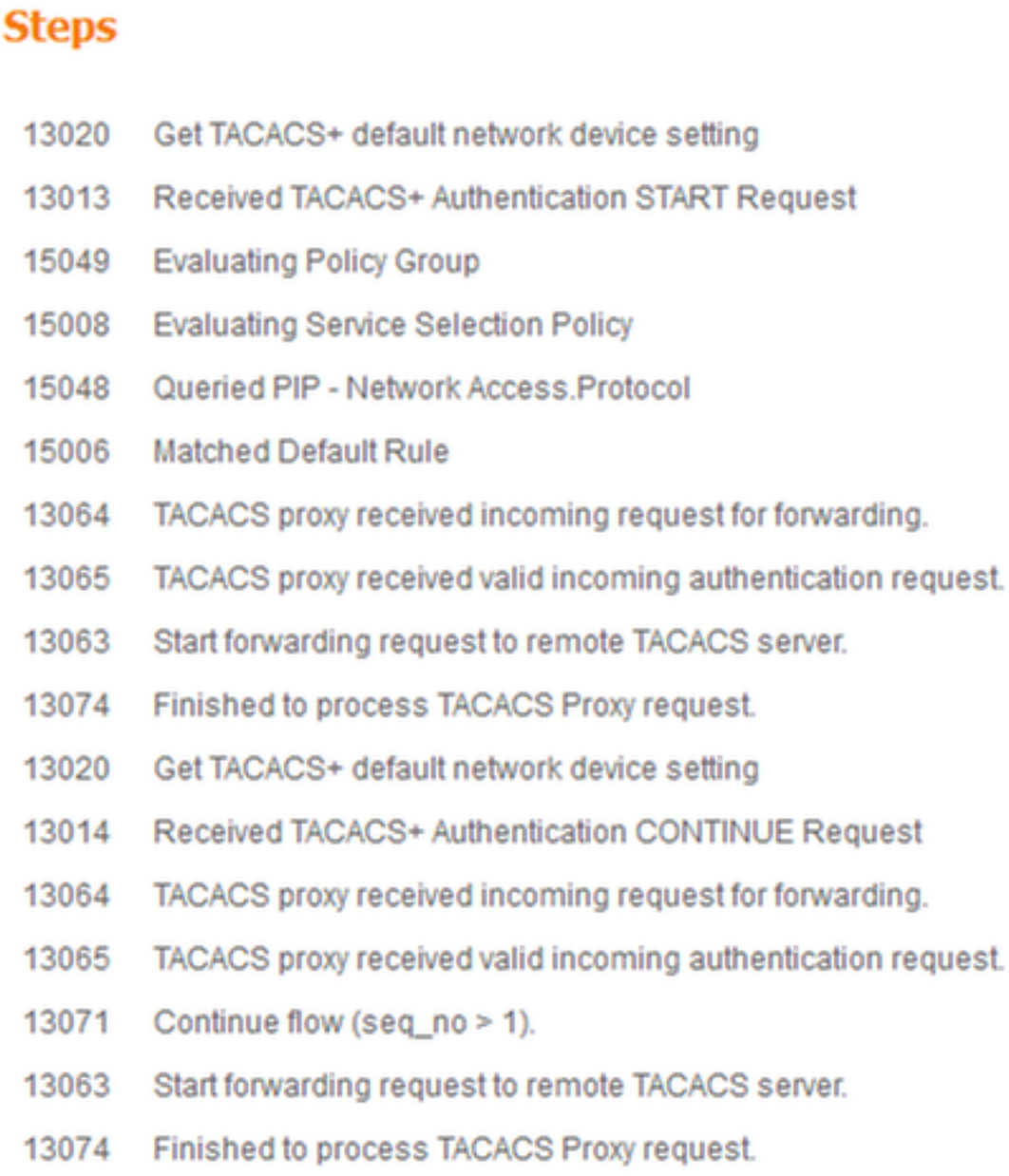
In diesem Abschnitt überprüfen Sie, ob die Konfiguration ordnungsgemäß funktioniert.

Die Überprüfung kann sowohl auf der ISE als auch auf dem ACS durchgeführt werden. Jeder Fehler in der Konfiguration der ISE oder des ACS führt zu einem Authentifizierungsfehler. ACS ist

der primäre Server, der die Authentifizierung und die Autorisierungsanfragen behandelt. Die ISE ist für den ACS-Server und von diesem aus verantwortlich und fungiert als Proxy für die Anfragen. Da das Paket beide Server durchläuft, kann die Authentifizierung oder Autorisierungsanfrage auf beiden Servern überprüft werden.

Netzwerkgeräte werden mit der ISE als TACACS-Server und nicht mit dem ACS konfiguriert. Daher erreicht die Anfrage zunächst die ISE, und basierend auf den konfigurierten Regeln entscheidet die ISE, ob die Anfrage an einen externen Server weitergeleitet werden muss. Dies kann in den TACACS Live-Protokollen auf der ISE überprüft werden.

Um die Live-Protokolle auf der ISE anzuzeigen, navigieren Sie zu **Operations > TACACS > Live Logs (Vorgänge > TACACS > Live-Protokolle).** Live-Berichte können auf dieser Seite eingesehen werden. Sie können die Details einer bestimmten Anfrage überprüfen, indem Sie auf das Lupensymbol für die spezielle Anfrage klicken, die von Interesse ist.



Um die Authentifizierungsberichte auf dem ACS anzuzeigen, gehen Sie zu **Monitoring and**

Reports > Launch Monitoring and Report Viewer > Monitoring and Reports > Reports > AAA Protocol > TACACS Authentication. Wie die ISE können die Details einer bestimmten Anfrage überprüft werden, indem Sie auf das Lupensymbol für die jeweilige Anfrage klicken, die von Interesse ist.

Fehlerbehebung

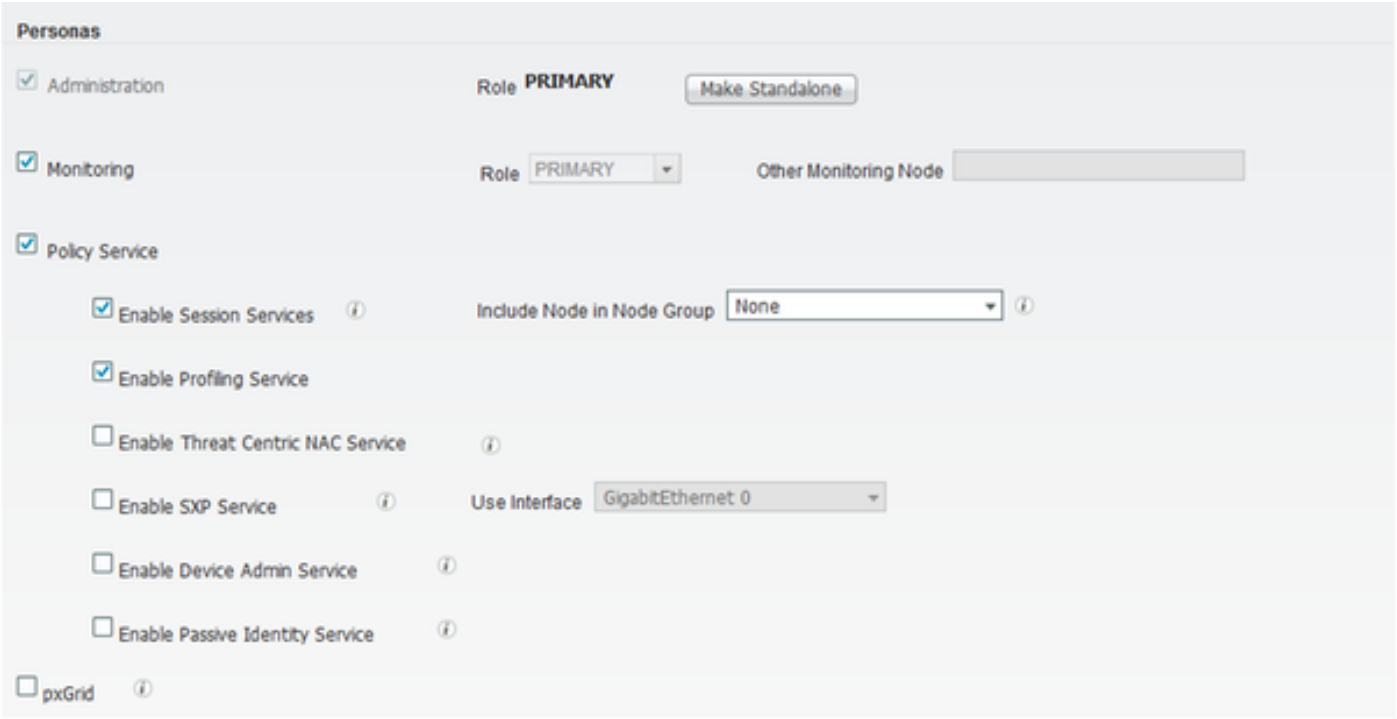
Dieser Abschnitt enthält Informationen zur Fehlerbehebung bei Ihrer Konfiguration.

1. Wenn die Details des Berichts zur ISE die in der Abbildung dargestellte Fehlermeldung anzeigen, weist dieser auf einen ungültigen, auf der ISE oder auf dem Netzwerkgerät (NAD) konfigurierten gemeinsamen geheimen Schlüssel hin.

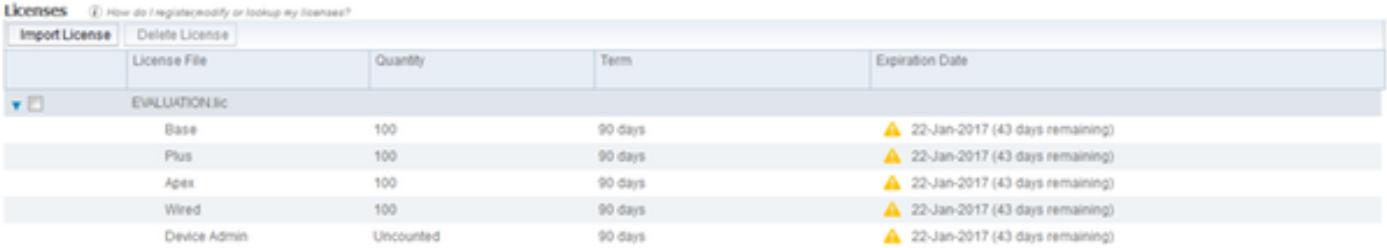
Message Text	TACACS: Invalid TACACS+ request packet - possibly mismatched Shared Secrets

2. Wenn für eine Anfrage auf der ISE kein Authentifizierungsbericht vorliegt, der Endbenutzer jedoch den Zugriff auf ein Netzwerkgerät verweigert, weist dies in der Regel auf mehrere Dinge hin.

- Die Anfrage selbst erreichte den ISE-Server nicht.
- Wenn die Geräteadministrationspersönlichkeit auf der ISE deaktiviert ist, wird jede TACACS+-Anforderung an die ISE unbemerkt verworfen. In den Berichten und Live Logs werden keine Protokolle angezeigt, die auf dasselbe hinweisen. Navigieren Sie dazu zu **Administration > System > Deployment > [Knoten auswählen].** Klicken Sie auf **Bearbeiten** und beachten Sie das Kontrollkästchen **Enable Device Admin Service** (Geräteadministratordienst aktivieren) unter der Registerkarte **General Settings (Allgemeine Einstellungen**), wie in der Abbildung gezeigt. Dieses Kontrollkästchen muss aktiviert werden, damit die Geräteverwaltung mit der ISE arbeiten kann.



- Wenn keine Device Administration-Lizenz vorhanden ist, die abgelaufen ist, werden alle TACACS+-Anfragen unbemerkt verworfen. In der GUI werden keine Protokolle für dasselbe angezeigt. Navigieren Sie zu **Administration > System > Licensing (Administration > System > Licensing),** um die Gerätemanagerlizenz zu überprüfen.

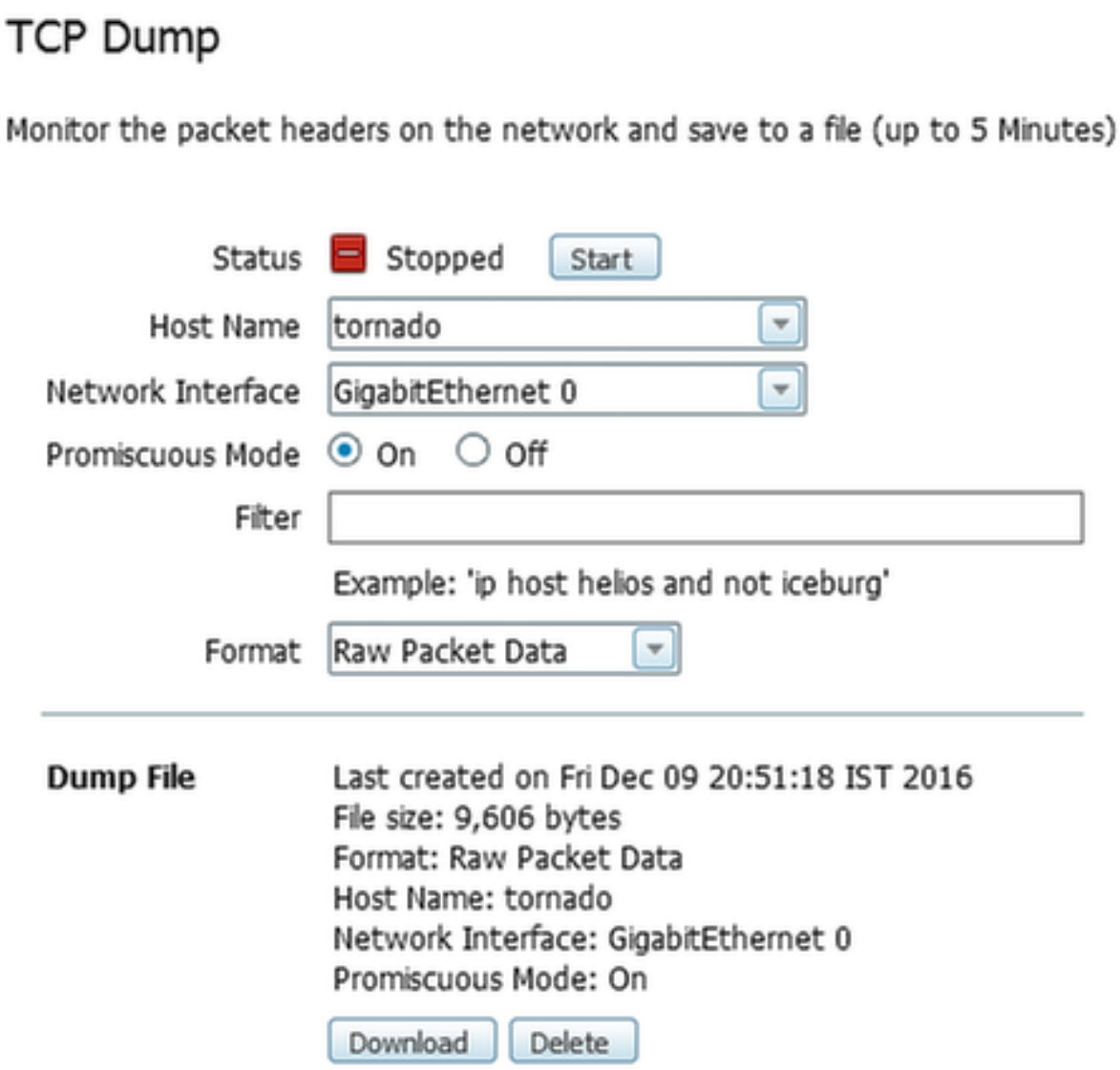


- Wenn das Netzwerkgerät nicht konfiguriert ist oder auf der ISE eine falsche IP-Adresse für das Netzwerkgerät konfiguriert wurde, wird das Paket von der ISE automatisch verworfen. Es wird keine Antwort an den Client zurückgesendet, und in der GUI werden keine Protokolle angezeigt. Dies ist eine Änderung des Verhaltens in ISE für TACACS+ im Vergleich zu ACS, der mitteilt, dass die Anfrage von einem unbekannten Netzwerkgerät oder AAA-Client einging.

- Die Anfrage wurde an das ACS gesendet, aber die Antwort wurde nicht an die ISE zurückgesendet. Dieses Szenario kann anhand der Berichte auf dem ACS überprüft werden, wie in der Abbildung dargestellt. In der Regel ist dies auf einen ungültigen geheimen Schlüssel zurückzuführen, entweder auf dem für die ISE konfigurierten ACS oder auf der für den ACS konfigurierten ISE.

- Die Antwort wird nicht gesendet, selbst wenn die ISE nicht konfiguriert ist oder die IP-Adresse der Management-Schnittstelle der ISE nicht in der Konfiguration der Netzwerkgeräte auf dem ACS konfiguriert ist. In einem solchen Szenario kann die Meldung in der Abbildung auf dem ACS beobachtet werden.

- Wenn ein erfolgreicher Authentifizierungsbericht auf dem ACS angezeigt wird, aber keine Berichte auf der ISE angezeigt werden und der Benutzer abgelehnt wird, könnte dies ein Problem im Netzwerk sein. Dies kann durch eine Paketerfassung auf der ISE mit den erforderlichen Filtern überprüft werden. Um eine Paketerfassung für die ISE zu erfassen, navigieren Sie zu **Operations > Troubleshoot > Diagnostic Tools > General tools > TCP Dump.**



3. Wenn die Berichte auf der ISE, aber nicht auf dem ACS angezeigt werden können, kann dies entweder bedeuten, dass die Anfrage aufgrund einer falschen Konfiguration der Richtliniensätze auf der ISE, die anhand des detaillierten Berichts über die ISE behoben werden kann, nicht an das ACS gesendet wurde, oder aufgrund eines Netzwerkproblems, das durch eine Paketerfassung auf dem ACS identifiziert werden kann.

4. Wenn die Berichte sowohl auf der ISE als auch auf dem ACS angezeigt werden, dem Benutzer jedoch weiterhin der Zugriff verweigert wird, handelt es sich in der Konfiguration der Zugriffsrichtlinien auf dem ACS häufiger um ein Problem, das anhand des detaillierten Berichts über das ACS behoben werden kann. Außerdem muss der Rückverkehr von der ISE zum

Netzwerkgerät zugelassen werden.