Konfigurieren von SNMP CoA in Identity Services Engine 2.1 und höher

Inhalt

[Einführung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Hintergrundinformationen](#)
[ISE konfigurieren](#)
[Konfigurieren der SNMP-Einstellungen von NAD](#)
[Konfigurieren der SNMP CoA-Einstellungen des Netzwerkgeräteprofils](#)
[Von ISE unterstützte OIDs](#)
[Erneute Authentifizierung](#)
[Port-Bounce](#)
[Port-Herunterfahren](#)
[Überprüfen](#)
[Fehlerbehebung](#)

Einführung

Dieses Dokument beschreibt die CoA-Funktion (Change of Authorization) unter Verwendung von Simple Network Management Protocol (SNMP).

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse des SNMP-Protokolls
- Frühere Kenntnis von regulären Ausdrücken
- Frühere Kenntnisse der Cisco Identity Service Engine (ISE)
- Identity Service Engine 2.1.
- Von SNMP unterstützte Switches

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf ISE Version 2.1.

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 eines Befehls verstehen.

Hintergrundinformationen

Diese neue Funktion wurde in ISE 2.1 eingeführt. Diese Funktion ergänzt eine weitere neue Funktion in ISE-VIZ., Weiterleitung durch ISE selbst und ist nicht von Netzwerkgeräten abhängig. Selbst wenn die ISE eine Weiterleitungs-URL direkt an den Endclient sendet, sollte der Endpunkt nach der Authentifizierung im Portal mit anderen Richtlinien für den entsprechenden Netzwerkzugriff verwendet werden. Dazu hat die ISE in früheren Versionen ein RADIUS-CoA gesendet. Einige Netzwerkgeräte verstehen kein RADIUS-CoA, das von der ISE gesendet wird. Da SNMP von fast allen Network Access Devices (NADs) unterstützt wird, wurde CoA, das SNMP verwendet, in einem solchen Szenario zu einer gangbaren Option. Ein SNMP-CoA wird von einer von der ISE an eine NAD gesendeten SNMP-SetRequest durchgeführt, um bestimmte Objekt-Identifikatoren (OIDs) festzulegen, die den Betriebsstatus eines Ports verwalten.

ISE konfigurieren

Auf der ISE müssen zwei Einstellungen konfiguriert werden, damit die SNMP-CoA funktioniert.

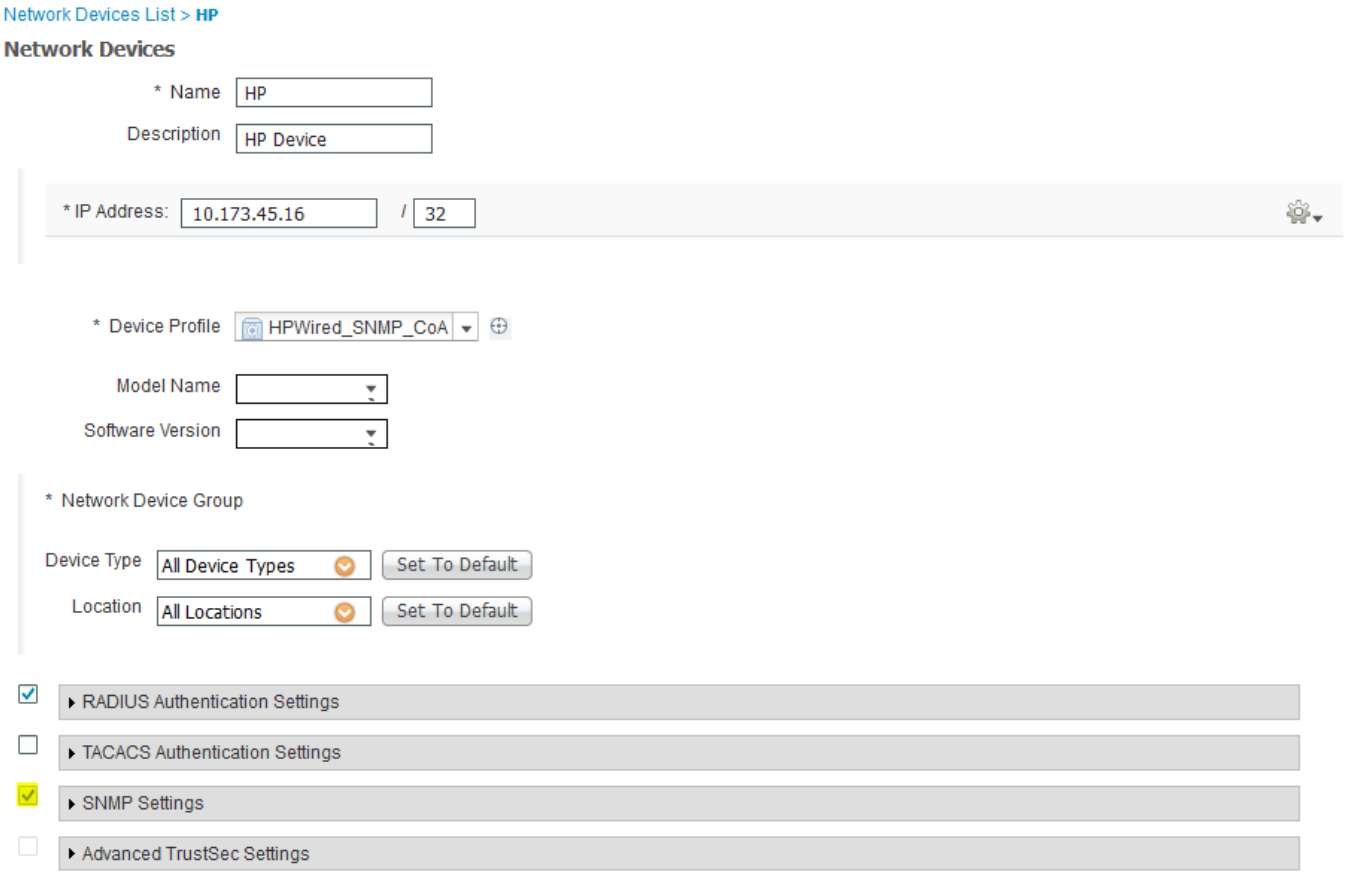
1. SNMP-Servereinstellungen einer NAD.

2. SNMP-CoA-Einstellungen eines NAD-Profils.

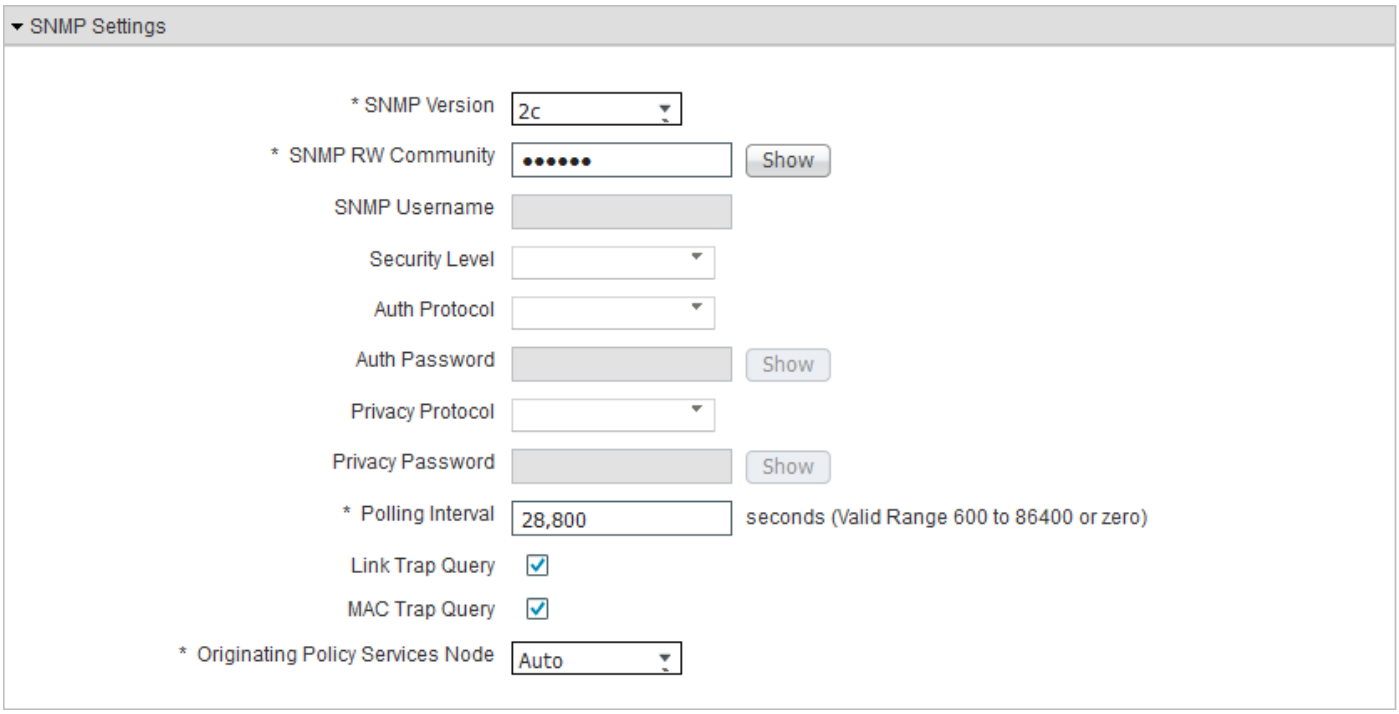
Um die SNMP-Servereinstellungen auf der ISE für eine NAD zu konfigurieren, navigieren Sie zu **Administration > Network Resources > Network Devices.**

Konfigurieren der SNMP-Einstellungen von NAD

Wählen Sie eine NAD aus. Unter den TACACS-Authentifizierungseinstellungen ist ein Kontrollkästchen verfügbar, um die SNMP-Einstellungen wie im Bild gezeigt zu bearbeiten.



Füllen Sie die Einstellungen entsprechend den Anforderungen aus. Im Bild wird ein Beispiel angezeigt.

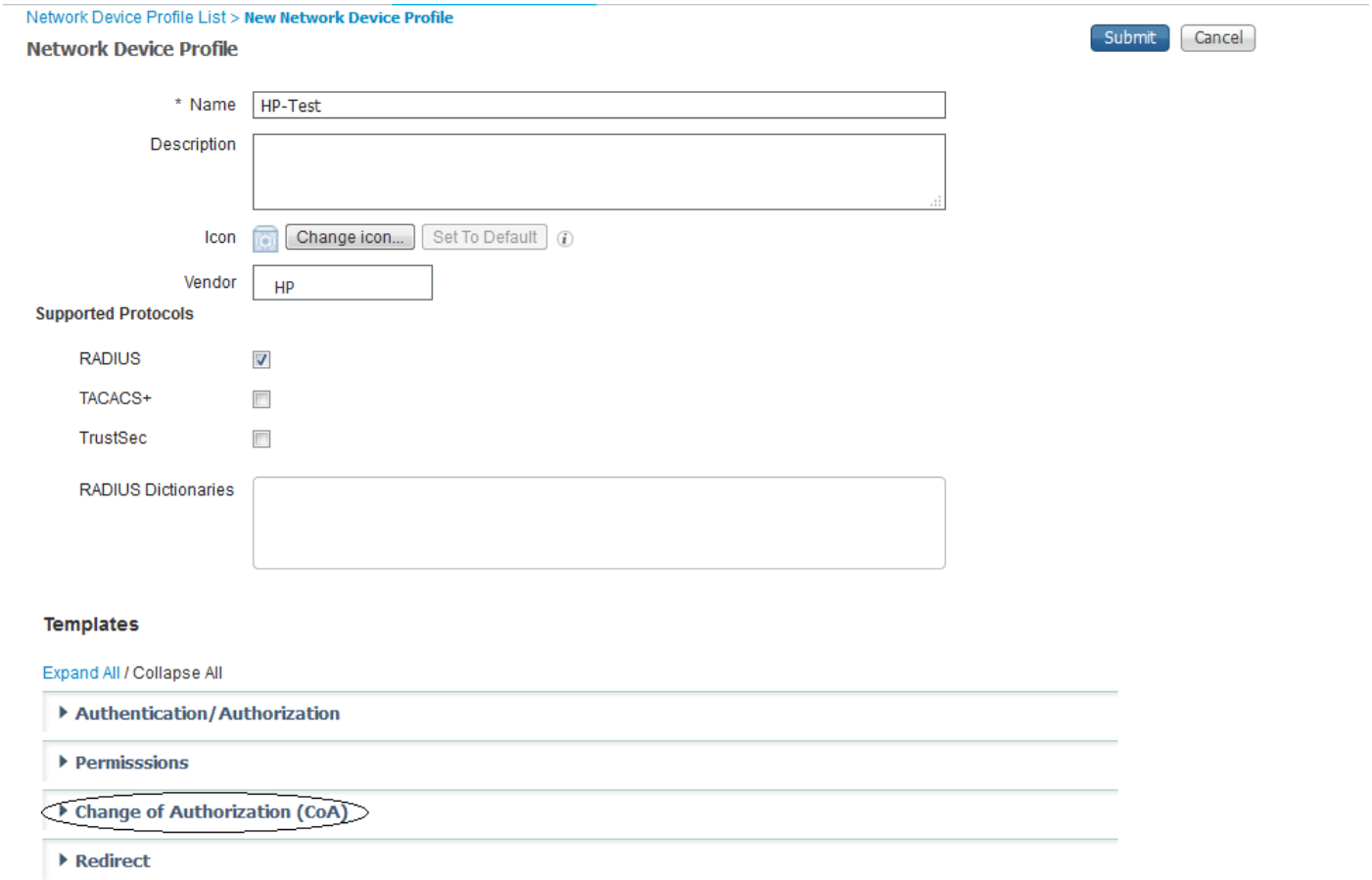


Konfigurieren der SNMP CoA-Einstellungen des Netzwerkgeräteprofils

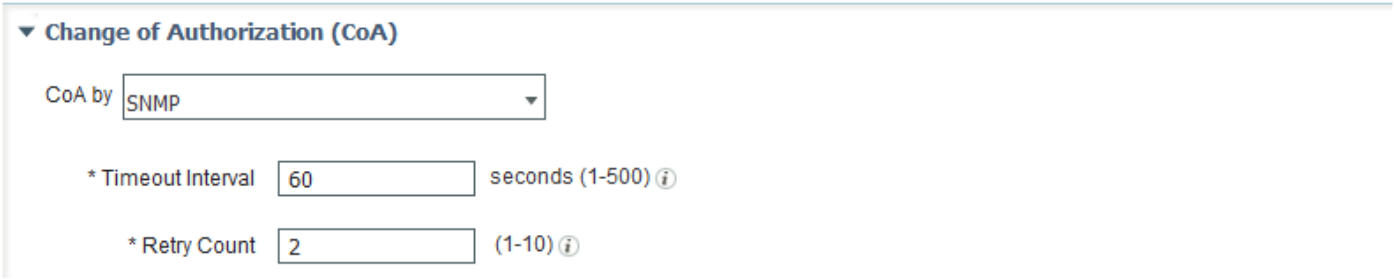
Um die SNMP-CoA-Einstellungen für ein Netzwerkgeräteprofil zu konfigurieren, navigieren Sie zu **Administration > Network Resources> Network Device Profiles (Verwaltung > Netzwerkressourcen > Netzwerkgeräteprofile).**

Wählen Sie das Netzwerkgeräteprofil aus, für das SNMP CoA konfiguriert werden soll, und erweitern Sie die Registerkarte **Autorisierungsänderung**, wie im Bild gezeigt.

> **Hinweis**: Die SNMP-Einstellungen der Standard-Netzwerkgeräteprofile können nicht bearbeitet werden.



Wählen Sie den CoA-Typ als **SNMP aus**, und bearbeiten Sie die Einstellungen für SNMP-Zeitüberschreitung und erneutes Wiederholen. Diese Einstellungen können je nach Anforderung festgelegt werden. In diesem Bild wird ein Beispiel angezeigt.



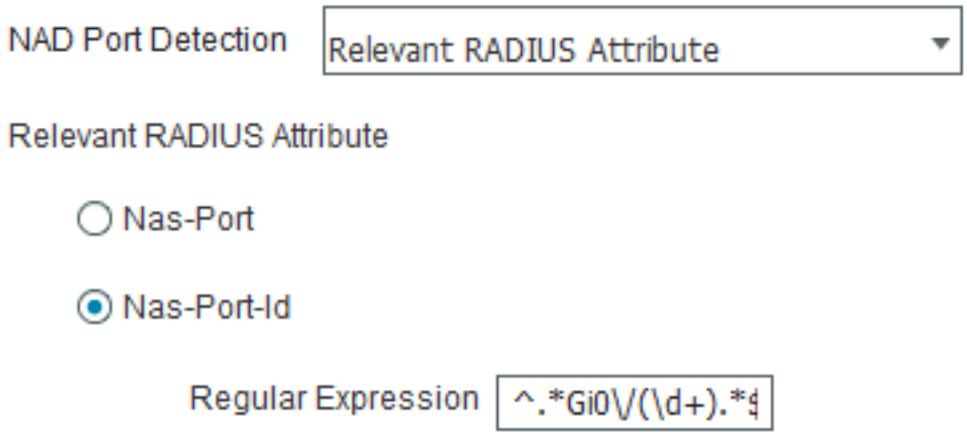
Konfigurieren Sie jetzt die NAD-Port-Erkennungsmethode, mit der die ISE den Port kennt, für den die OIDs festgelegt werden sollen. Die einzige verfügbare Methode besteht derzeit darin, diese Informationen aus dem entsprechenden RADIUS-Attribut aus den Accounting-Informationen abzurufen.

Die aktuell verfügbaren RADIUS-Attribute, die diese Informationen liefern, sind NAS-Port und NAS-Port-ID. Jedes dieser Attribute kann anhand des vom NAD unterstützten Attributs ausgewählt werden. Die meisten NADs unterstützen NAS-Port-IDs. Unterschiedliche Anbieter haben verschiedene Möglichkeiten, die auf dem NAD verfügbaren Schnittstellen darzustellen.

Eine Standardmethode zum Extrahieren der Informationen ist möglicherweise nicht möglich. Daher werden in der ISE reguläre Ausdrücke verwendet, um die Zeichenfolgen anzupassen, die dem NAS-Port-Id-Attributwert zugeordnet werden sollen. Hier wird ein Beispiel gezeigt, um die Ports in Form von Gi0/x zu entsprechen.

^.*Gi0\/(\d+).*$

Dieser Ausdruck bedeutet im Wesentlichen (^)startmuster (.*)Übereinstimmung mit einer beliebigen Anzahl von Instanzen eines beliebigen Checks (Gi0)match 'Gi0' (\/)match '/' (\d+)match einer oder mehreren Instanzen einer beliebigen Ziffer (.)match any charecter (*) (.*) match any number of instance of any charecter ($)end pattern. Dieses Beispiel kann wie in diesem Bild gezeigt konfiguriert werden.



Von ISE unterstützte OIDs

Standardmäßig stellt die ISE Optionen bereit, um drei Arten von OIDs zu konfigurieren, um einen Vorgang für die Ports auszuführen, die durch den NAS-Port-ID-Attributwert identifiziert werden.

1. Erneute Authentifizierung

2. Port-Bounce

3. Port-Herunterfahren

Erneute Authentifizierung

Die Reauthentifizierung der OID wird von den meisten Anbietern in Standard-MIBs möglicherweise nicht unterstützt. Die Informationen dieser OID können von Anbieter zu Anbieter variieren.

> **Hinweis**: Diese Option ist für eine mögliche zukünftige Erweiterung vorgesehen, wenn ein Gerät eine OID zur Verwaltung von Benutzersitzungen basierend auf der MAC-Adresse unterstützt.

Port-Bounce

Port-Bounce verwendet eine OID für den Port, die zwei Werte hat: einen für das Herunterfahren

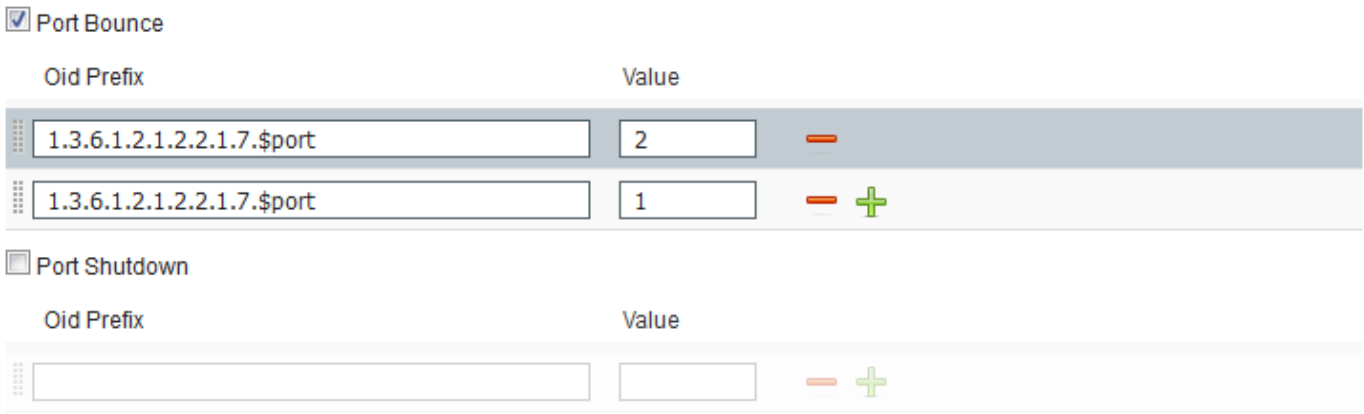
des Ports und den anderen für das Ausschalten des Ports. Hierbei handelt es sich um standardmäßige OIDs, die von den meisten Anbietern verwendet werden.

1.3.6.1.2.1.2.2.1.7.$port ist die OID

Wenn der Wert auf 2 festgelegt ist, wird der Port heruntergefahren, und wenn der Wert auf 1 festgelegt ist, wird der Port deaktiviert.

Port-Herunterfahren

Wählen Sie die gewünschte Operation aus, die an diesem bestimmten Port durchgeführt werden soll, wie im Bild gezeigt.

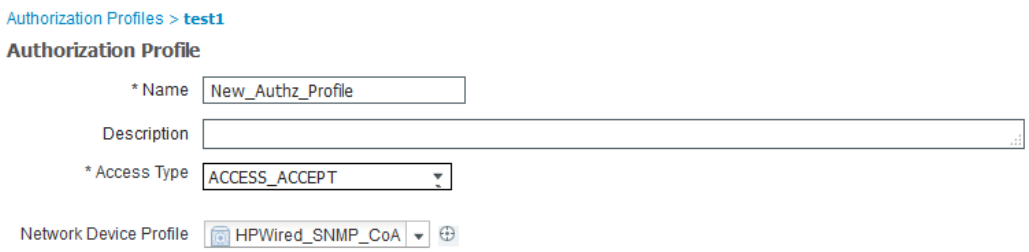


> **Vorsicht**: Die Reihenfolge, in der die OID-Werte gesendet werden, ist sehr wichtig. Denn die Reihenfolge, in der die OID-Werte festgelegt werden, ist die Reihenfolge, in der die Vorgänge auf dem Port ausgeführt werden. Wenn sie in umgekehrter Reihenfolge wie 1 und 2 eingestellt werden, wird ein Port zuerst deaktiviert und dann heruntergefahren, wodurch der Port im Prinzip ausgeschaltet wird.

Senden Sie die Änderungen an das Geräteprofil.

Dieses Geräteprofil kann in jedem Autorisierungsprofil verwendet werden, das berücksichtigt werden muss. Jeder CoA-Vorgang, der für einen Endpunkt ausgeführt werden muss, wird als SNMP SetRequest an den Switch gesendet, dessen konfigurierte OIDs auf dem Port festgelegt werden, an dem der Endpunkt angeschlossen ist. Im folgenden Beispiel können Sie das NAD-Profil im Autorisierungsprofil konfigurieren.

Um eine neue Autorisierungsrichtlinie zu erstellen oder die bereits vorhandene zu bearbeiten, navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile,** wie im Bild gezeigt.



Hinweis: Der Switch muss mit der ISE als SNMP-Server konfiguriert werden und sollte den gleichen Community-String verwenden, der auf der ISE konfiguriert wurde. Die Konfiguration von Switch wird in diesem Dokument nicht behandelt.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.