Integration von FireSIGHT System mit ACS 5.x für RADIUS-Benutzerauthentifizierung

Inhalt

Einführung

In diesem Dokument werden die Konfigurationsschritte beschrieben, die zur Integration eines Cisco FireSIGHT Management Center (FMC) oder eines FirePOWER Managed Device in das Cisco Secure Access Control System 5.x (ACS) für die RADIUS-Benutzerauthentifizierung (Remote Authentication Dial In User Service) erforderlich sind.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Erstkonfiguration von FireSIGHT-Systemen und verwalteten Geräten über GUI und/oder Shell
- Konfigurieren von Authentifizierungs- und Autorisierungsrichtlinien auf ACS 5.x
- Grundlegendes RADIUS-Wissen

Verwendete Komponenten

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

- Cisco Secure Access Control System 5,7 (ACS 5.7)

- Cisco FireSight Manager Center 5.4.1

Die oben genannten Versionen sind die aktuellen Versionen. Diese Funktion wird von allen ACS 5.x-Versionen und FMC 5.x-Versionen unterstützt.

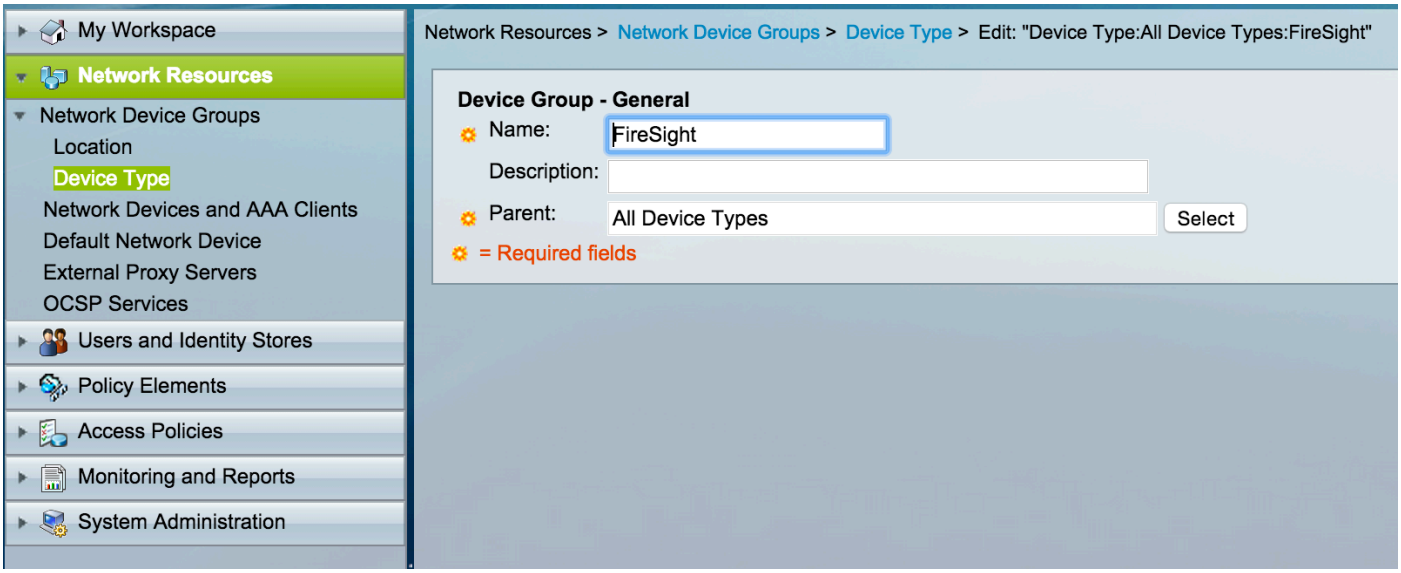
Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines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

Konfiguration

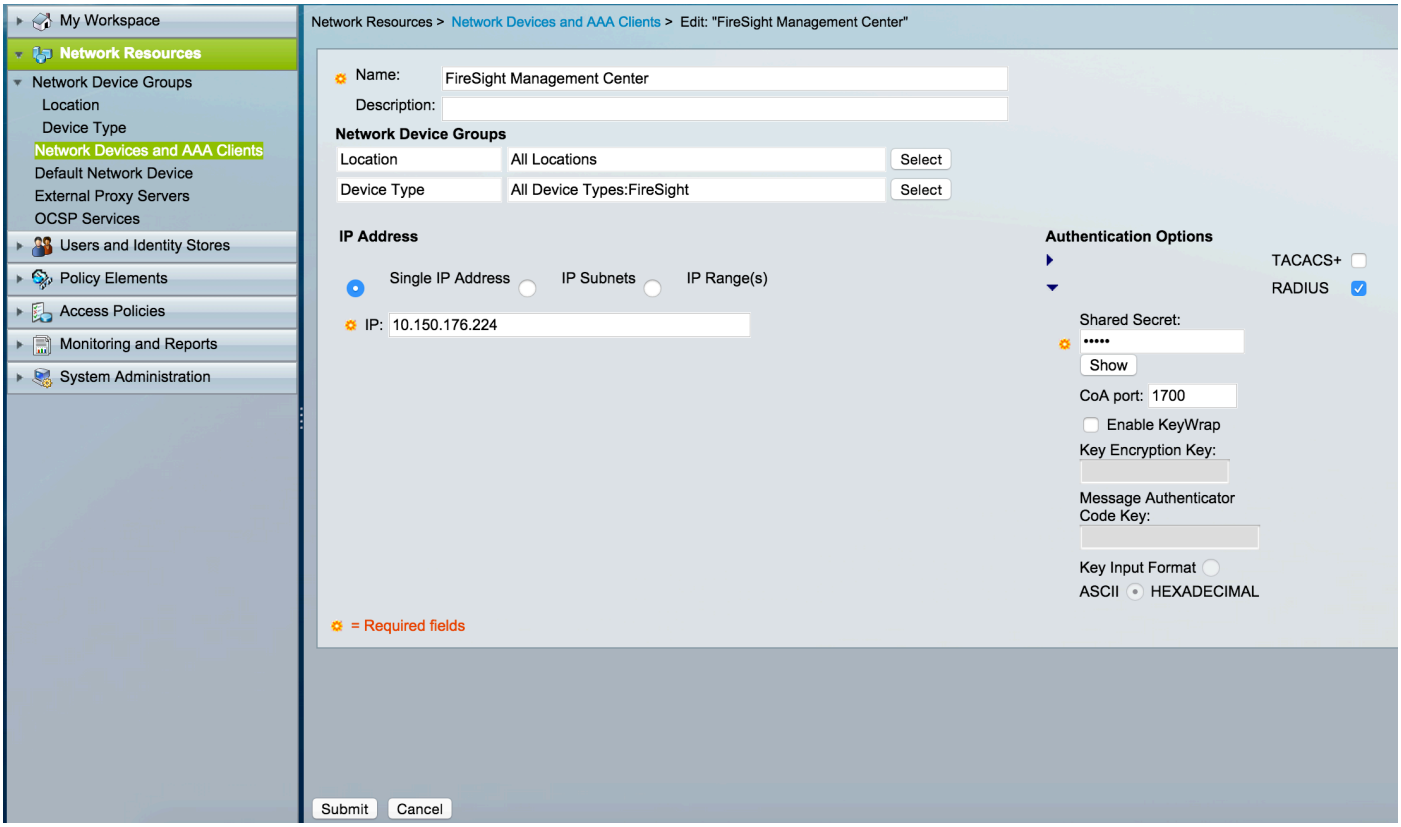
ACS 5.x-Konfiguration

Konfigurieren von Netzwerkgeräten und Netzwerkgerätegruppen

- Navigieren Sie in der ACS-GUI zur **Netzwerkgerätegruppe**, klicken Sie auf **Gerätetyp,** und erstellen Sie eine Gerätegruppe. Im folgenden Beispielbildschirm wurde der Gerätetyp FireSight konfiguriert. Auf diesen Gerätetyp wird in einem späteren Schritt in der Definition der Autorisierungsrichtlinie verwiesen. Klicken Sie auf **Speichern**.



- Navigieren Sie in der ACS-GUI zur **Netzwerkgerätegruppe**, klicken Sie auf **Netzwerkgeräte und AAA-Clients** und fügen Sie ein Gerät hinzu. Geben Sie einen beschreibenden Namen und eine Geräte-IP-Adresse an. Das FireSIGHT Management Center ist im folgenden Beispiel definiert.



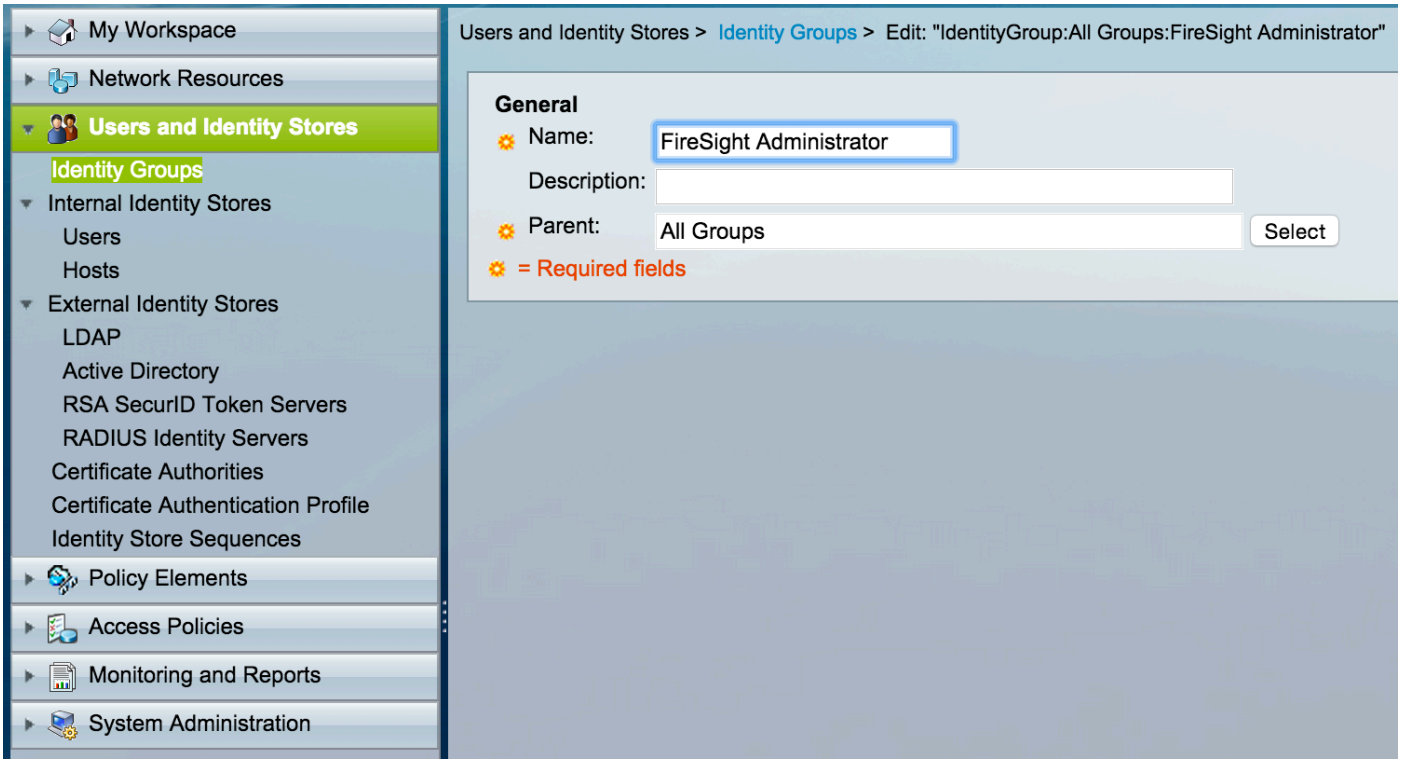
- Konfigurieren Sie in den **Netzwerkgerätegruppen den Gerätetyp** genauso wie die im oben beschriebenen Schritt erstellte Gerätegruppe.

- Aktivieren Sie das Kontrollkästchen neben **Authentifizierungsoptionen,** aktivieren Sie das Kontrollkästchen RADIUS, und geben Sie den **geheimen** Schlüssel für diese NAD ein. Beachten Sie, dass der gleiche geheime Schlüssel später erneut verwendet wird, wenn der RADIUS-Server im FireSIGHT Management Center konfiguriert wird. Um den Wert für den Nur-Text-Schlüssel zu überprüfen, klicken Sie auf die Schaltfläche **Anzeigen**. Klicken Sie auf **Senden**.

- Wiederholen Sie die oben genannten Schritte für alle FireSIGHT Management Center und Managed Devices, die eine RADIUS-Benutzerauthentifizierung bzw. -autorisierung für den Zugriff auf die Benutzeroberfläche und/oder die Shell erfordern.

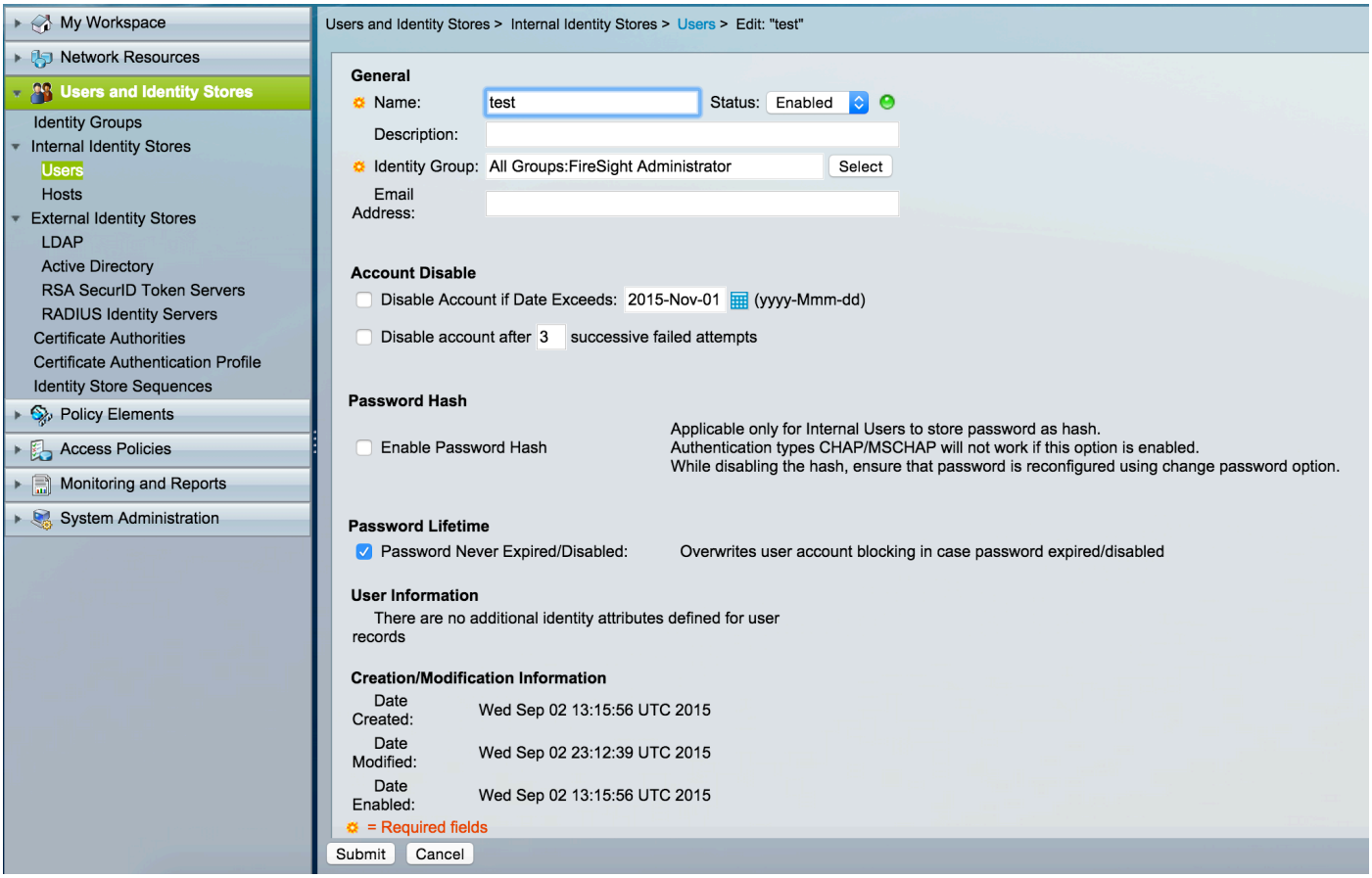
Hinzufügen einer Identitätsgruppe in ACS

- Navigieren Sie zu **Benutzer und Identitätsdaten, und** konfigurieren Sie **Identitätsgruppe**. In diesem Beispiel wird die Identitätsgruppe "FireSight Administrator" erstellt. Diese Gruppe wird mit dem in den folgenden Schritten definierten Autorisierungsprofil verknüpft.



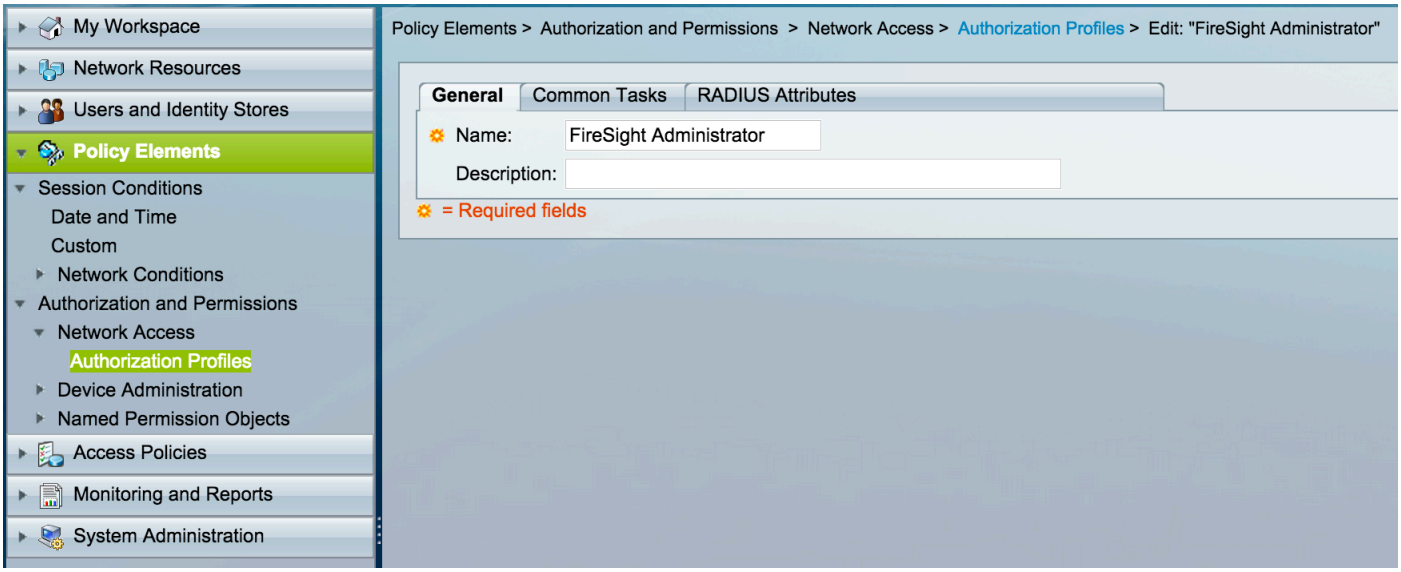
Hinzufügen eines lokalen Benutzers zum ACS

- Navigieren Sie zu **Benutzern und Identitätsdaten,** konfigurieren Sie **Benutzer** im Abschnitt **Interne Identitätsdatenbanken**. Geben Sie die erforderlichen Informationen für die lokale Benutzererstellung ein, wählen Sie die oben erstellte **Identitätsgruppe** aus, und klicken Sie auf **Senden.**

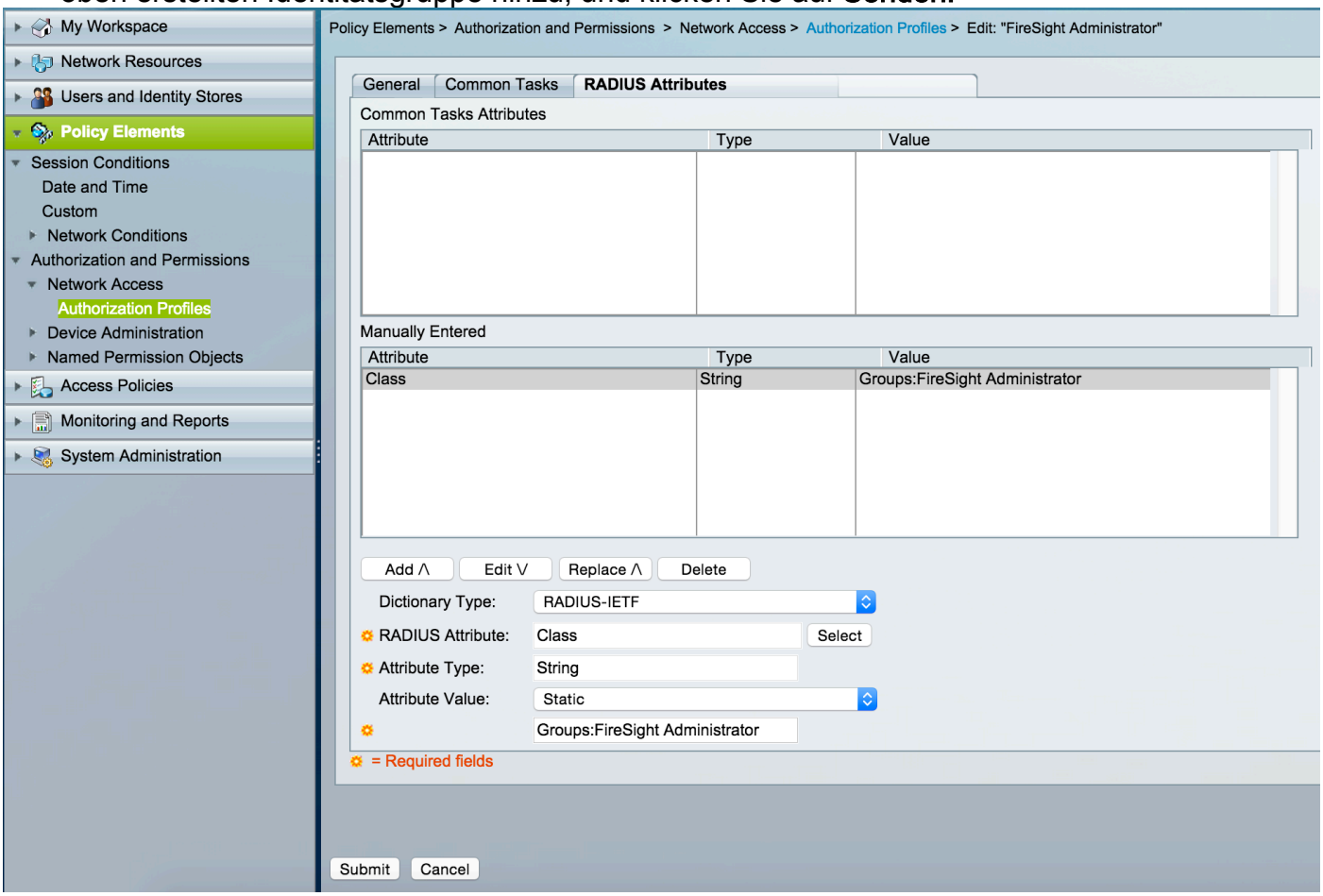


Konfigurieren der ACS-Richtlinie

- Navigieren Sie in der ACS-GUI zu **Richtlinienelementen > Autorisierung und Berechtigungen > Netzwerkzugriff > Autorisierungsprofile**. Erstellen Sie ein neues Autorisierungsprofil mit einem beschreibenden Namen. Im folgenden Beispiel ist die erstellte Richtlinie FireSight Administrator.

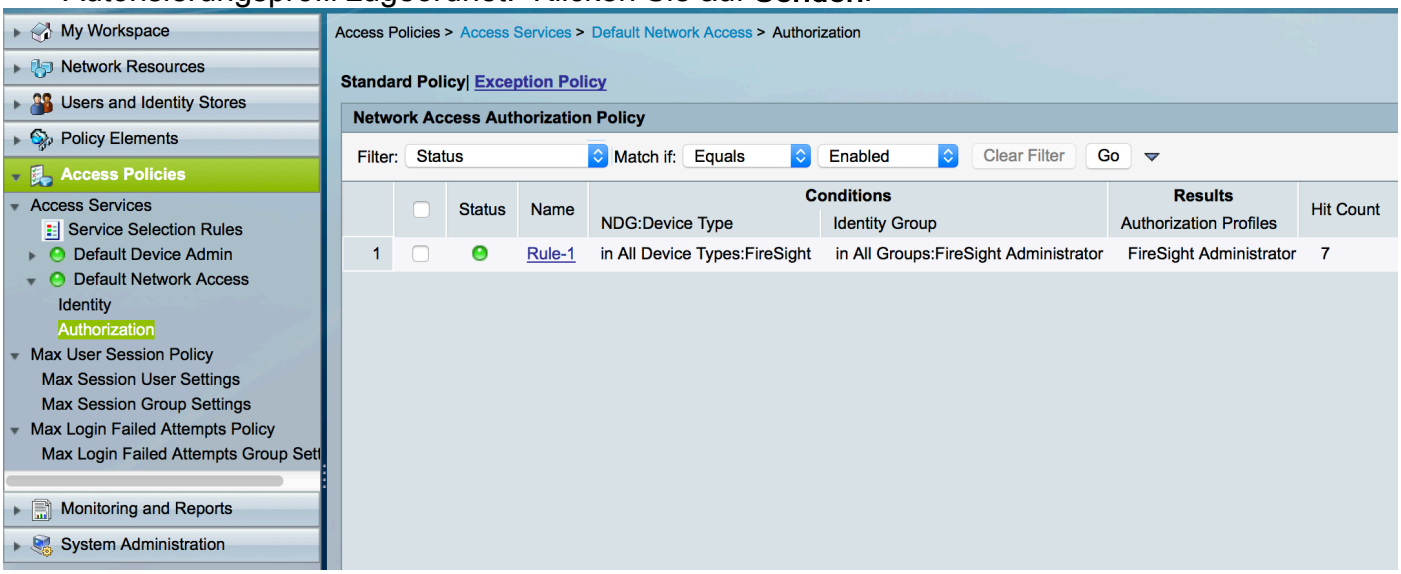


- Fügen Sie auf der Registerkarte **RADIUS-Attribute** das manuelle Attribut zur Autorisierung der oben erstellten Identitätsgruppe hinzu, und klicken Sie auf **Senden.**



- Zum **Zugriff** navigieren **Richtlinien > Zugriffsdienste > Standard-Netzwerkzugriff > Autorisierung** und konfigurieren Sie eine neue Autorisierungsrichtlinie für die FireSight Management Center-Verwaltungssitzungen. Im folgenden Beispiel wird das **NDG** verwendet.**:Gerätetyp** & **Identity Group** Bedingung, um mit dem in den oben beschriebenen Schritten konfigurierten Gerätetyp und der Identitätsgruppe übereinstimmen zu können.

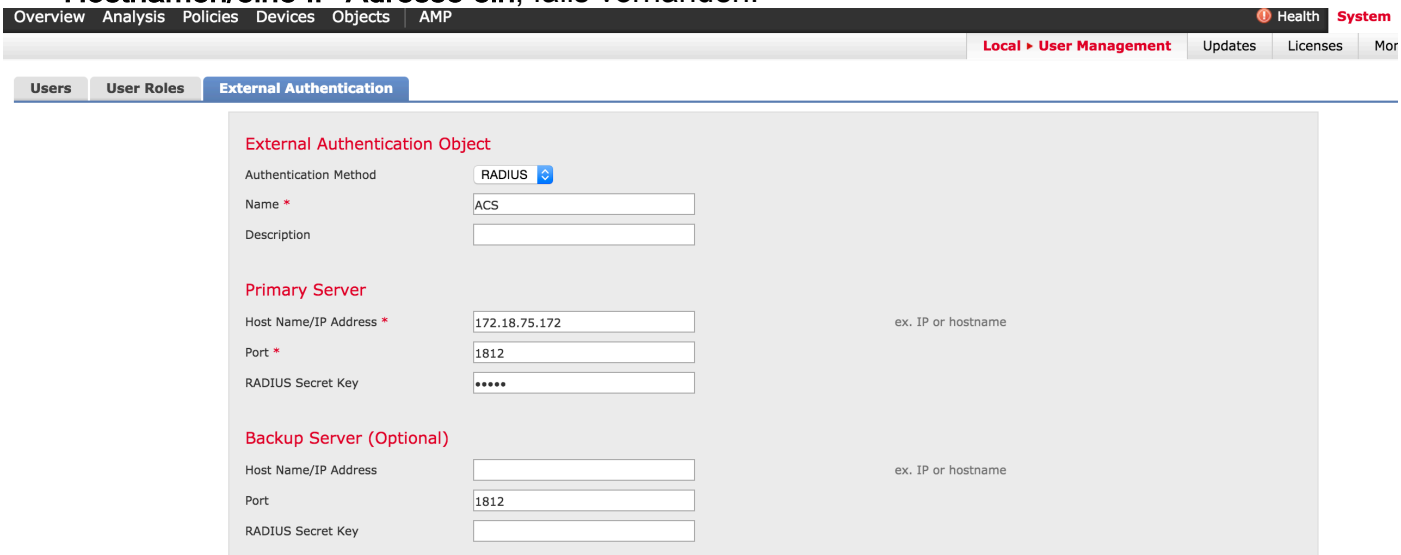
- Diese Richtlinie wird dann dem oben als **Ergebnis** konfigurierten FireSight Administrator-Autorisierungsprofil zugeordnet. Klicken Sie auf **Senden**.



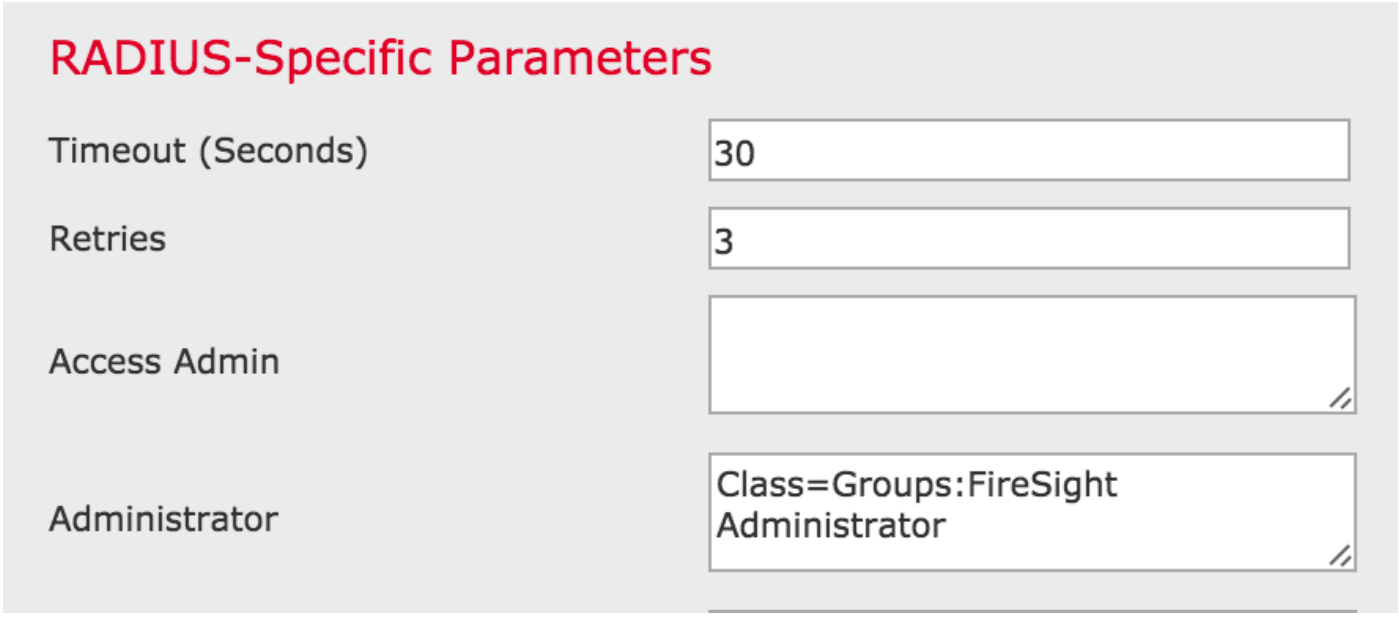
Konfiguration des FireSight Management Center

Konfiguration der FireSight Manager-Systemrichtlinien

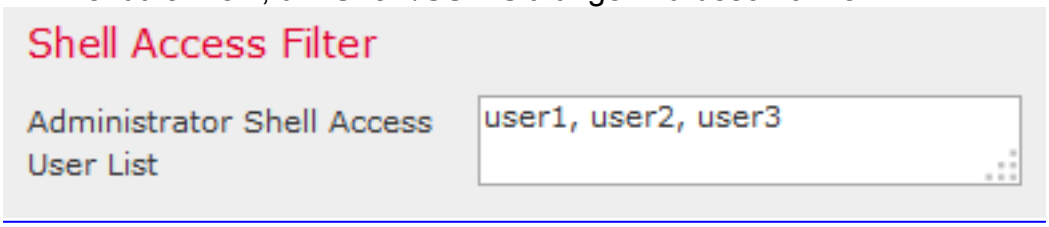
- Melden Sie sich beim FireSIGHT MC an, und navigieren Sie zu **System > Local > User Management**. Klicken Sie auf die Registerkarte **Externe Authentifizierung**. Klicken Sie auf die Schaltfläche **+ Create Authentication Object (Authentifizierungsobjekt erstellen)**, um einen neuen RADIUS-Server für die Benutzerauthentifizierung/-autorisierung hinzuzufügen.
- Wählen Sie **RADIUS** als **Authentifizierungsmethode aus**. Geben Sie einen beschreibenden Namen für den RADIUS-Server ein. Geben Sie den **Hostnamen/die IP-Adresse** und den **geheimen RADIUS-Schlüssel ein**. Der geheime Schlüssel muss mit dem zuvor auf ACS konfigurierten Schlüssel übereinstimmen. Geben Sie optional einen Backup-ACS-Server-**Hostnamen/eine IP-Adresse ein**, falls vorhanden.



- Im **RADIUS-spezifische Parameter** in diesem Beispiel wird der Wert Class=Groups:FireSight Administrator der FireSight-Administratorgruppe zugeordnet. Dies ist der Wert, den ACS im Rahmen der ACCESS-ACCEPT zurückgibt. Klicken **Speichern** um die Konfiguration zu speichern, oder fahren Sie mit dem Abschnitt Überprüfen unten fort, um die Authentifizierung mit ACS zu testen.



- Geben Sie unter **Shell Access Filter (Shell-Zugriffsfilter)** eine kommagetrennte Liste von Benutzern ein, um Shell-/SSH-Sitzungen zu beschränken.



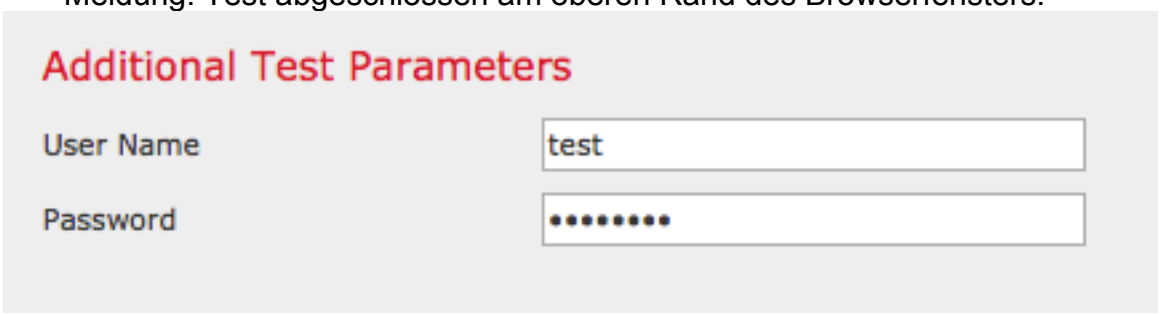
Externe Authentifizierung aktivieren

Führen Sie abschließend die folgenden Schritte aus, um die externe Authentifizierung auf dem FMC zu aktivieren:

1. Navigieren Sie zu **System** > **Lokal** > **Systemrichtlinie**.
2. Wählen Sie **Externe Authentifizierung** im linken Bereich aus.
3. Ändern Sie den *Status* in **Aktiviert** (standardmäßig deaktiviert).
4. Aktivieren Sie den hinzugefügten ACS RADIUS-Server.
5. Speichern Sie die Richtlinie, und wenden Sie die Richtlinie erneut auf die Appliance an.

Überprüfung

- Um die Benutzerauthentifizierung mit ACS zu testen, scrollen Sie nach unten zum Abschnitt **Zusätzliche Testparameter** und geben Sie einen Benutzernamen und ein Kennwort für den ACS-Benutzer ein. Klicken Sie auf **Test.** Ein erfolgreicher Test führt zu einer grünen Meldung: Test abgeschlossen am oberen Rand des Browserfensters.



- Um die Ergebnisse der Testauthentifizierung anzuzeigen, gehen Sie zum Abschnitt **Testausgabe**, und klicken Sie auf den **schwarzen** Pfeil neben **Details anzeigen**. Beachten Sie im folgenden Beispielbildschirm den Abschnitt "radiusauth - response: |Class=Groups:FireSight Administrator|"-Wert erhalten von ACS. Dieser Wert muss mit dem Class-Wert übereinstimmen, der der lokalen FireSight-Gruppe zugeordnet ist, die oben im FireSIGHT MC konfiguriert wurde. Klicken Sie auf **Speichern**.