Intégration de système de FireSIGHT avec ACS 5.x pour l'authentification d'utilisateur RADIUS

Contenu

Introduction

Ce document décrit l'étape nécessaire de configuration pour intégrer un centre de Gestion de Cisco FireSIGHT (FMC) ou le périphérique géré de FirePOWER avec le Système de contrôle d'accès sécurisé Cisco 5.x (ACS) pour l'authentification à distance se connectent l'authentification de l'utilisateur de service d'utilisateur (RADIUS).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration initiale de système et de périphérique géré de FireSIGHT par l'intermédiaire de GUI et/ou de shell
- Configurer des stratégies d'authentification et d'autorisation sur ACS 5.x
- La connaissance de base de RADIUS

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Système de contrôle d'accès sécurisé Cisco 5.7 (ACS 5.7)
- Centre 5.4.1 de gestionnaire de Cisco FireSIGHT

Au-dessus des versions sont les dernières versions disponibles actuellement. La caractéristique est prise en charge sur toutes les versions ACS 5.x et versions FMC 5.x.

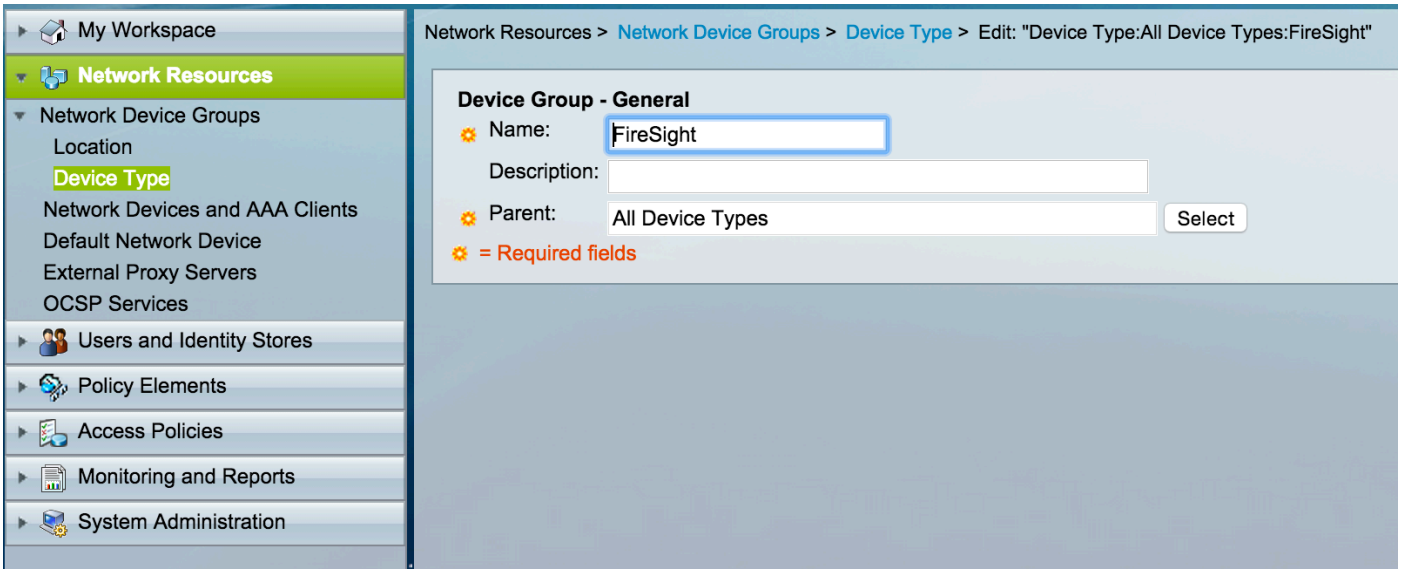
Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configuration

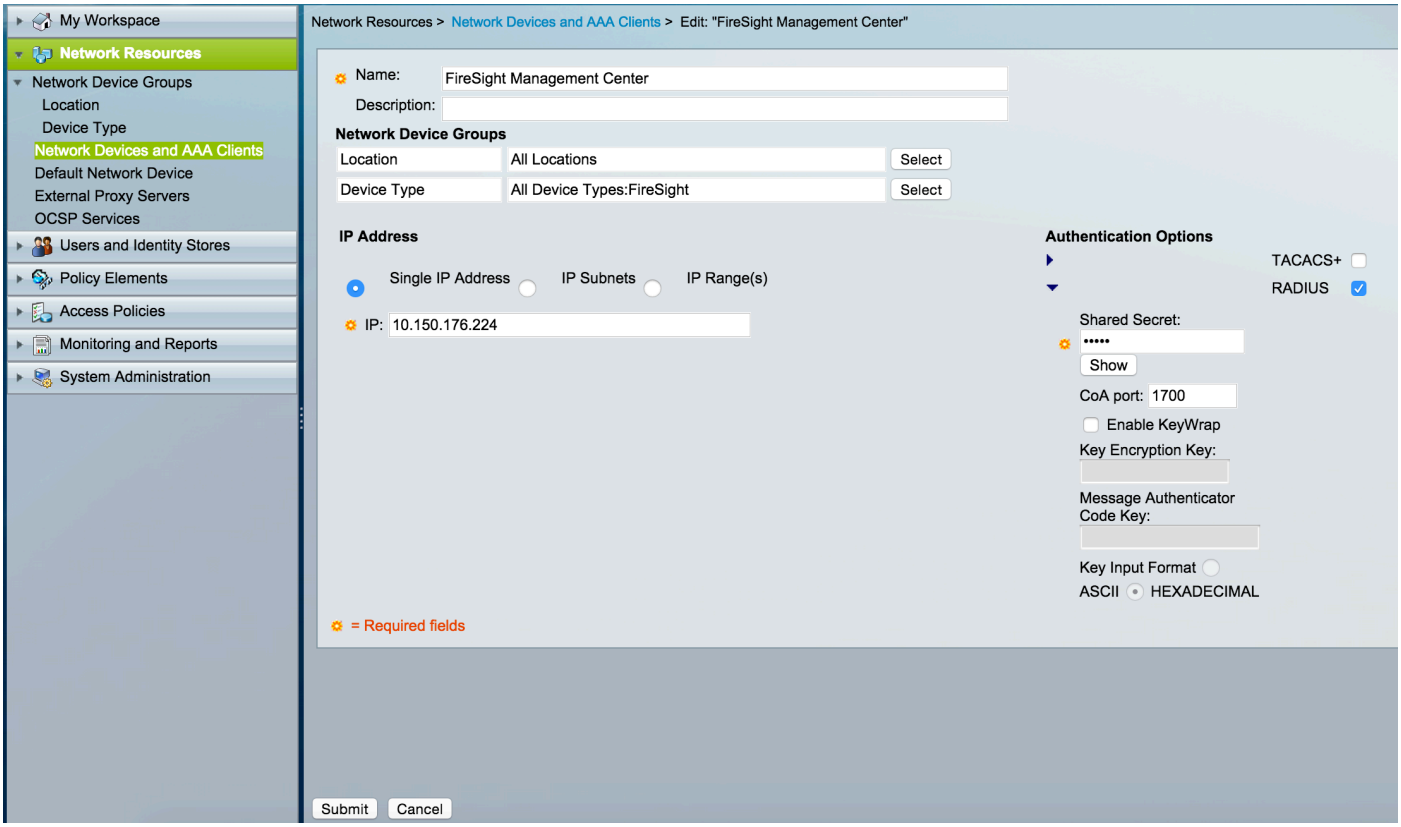
Configuration ACS 5.x

Configurer des périphériques et des groupes de périphériques réseau de réseau

- Du GUI ACS, naviguez vers le **groupe de périphériques réseau**, cliquez sur en fonction le **type de périphérique** et créez un groupe de périphériques. Dans le tir d'écran d'exemple qui suit, le type de périphérique FireSIGHT a été configuré. Ce type de périphérique sera mis en référence dans la définition de règle de stratégie d'autorisation dans une étape postérieure. Cliquez sur **Save**.



- Du GUI ACS, naviguez vers le **groupe de périphériques réseau**, cliquez sur en fonction les **clients de NetwokDevices et d'AAA** et ajoutez un périphérique. Fournissez un nom et une adresse IP descriptifs de périphérique. Le centre de Gestion de FireSIGHT est défini dans l'exemple ci-dessous.



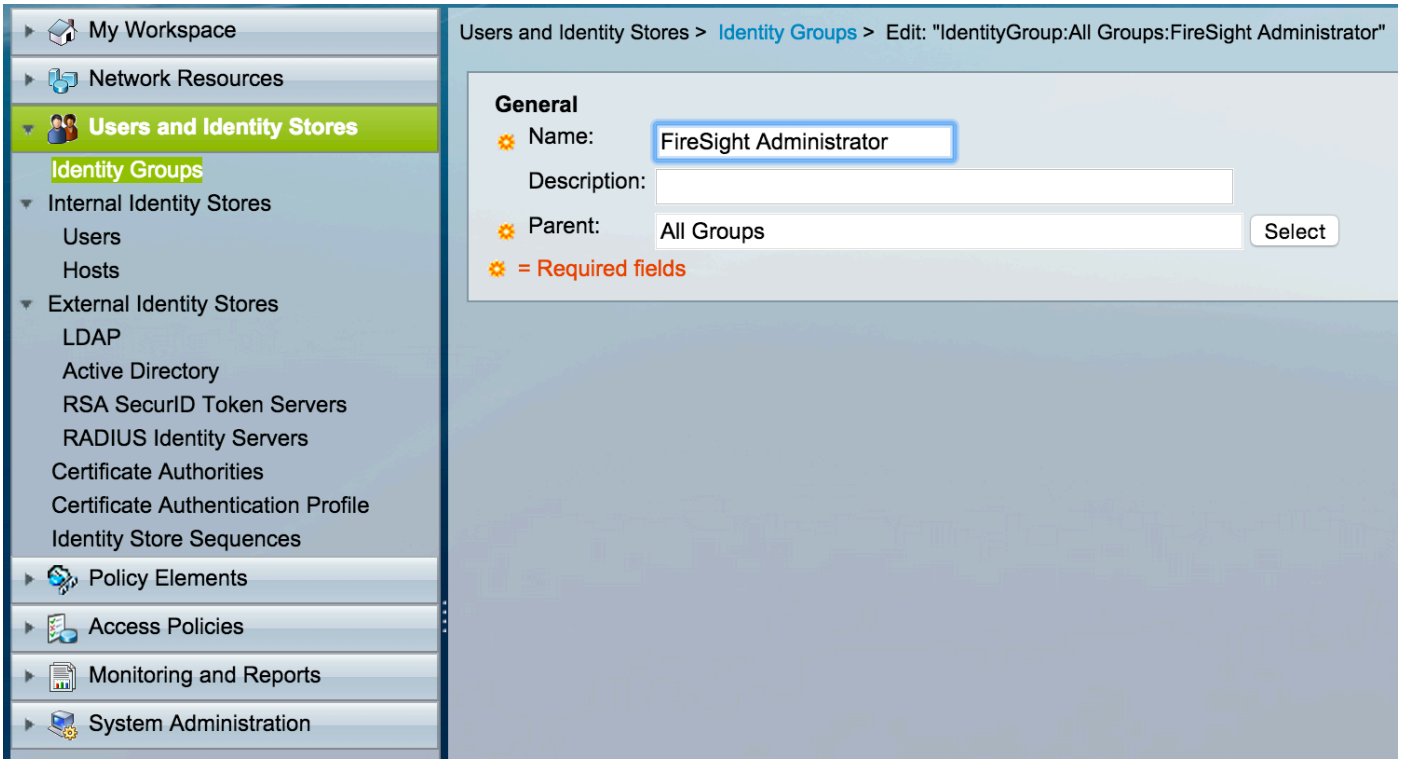
- **Aux groupes de périphériques réseau,** configurez le **type de périphérique** mêmes que le groupe de périphériques créé dans l'étape ci-dessus.

- Cochez la case à côté des **options d'authentification,** sélectionnez la case de RADIUS et introduisez la clé **secrète partagée** qui sera utilisée pour ce NAD. Notez la même chose la clé que secrète partagée sera utilisée de nouveau plus tard quand configurant le serveur de RADIUS au centre de Gestion de FireSIGHT. Pour passer en revue la valeur principale de texte brut, cliquez sur le bouton d'**exposition**. Cliquez sur **Submit**.

- Répétez les étapes ci-dessus pour tous les centres et périphériques gérés de Gestion de FireSIGHT qui exigeront l'authentification d'utilisateur RADIUS/autorisation pour l'accès GUI et/ou de shell.

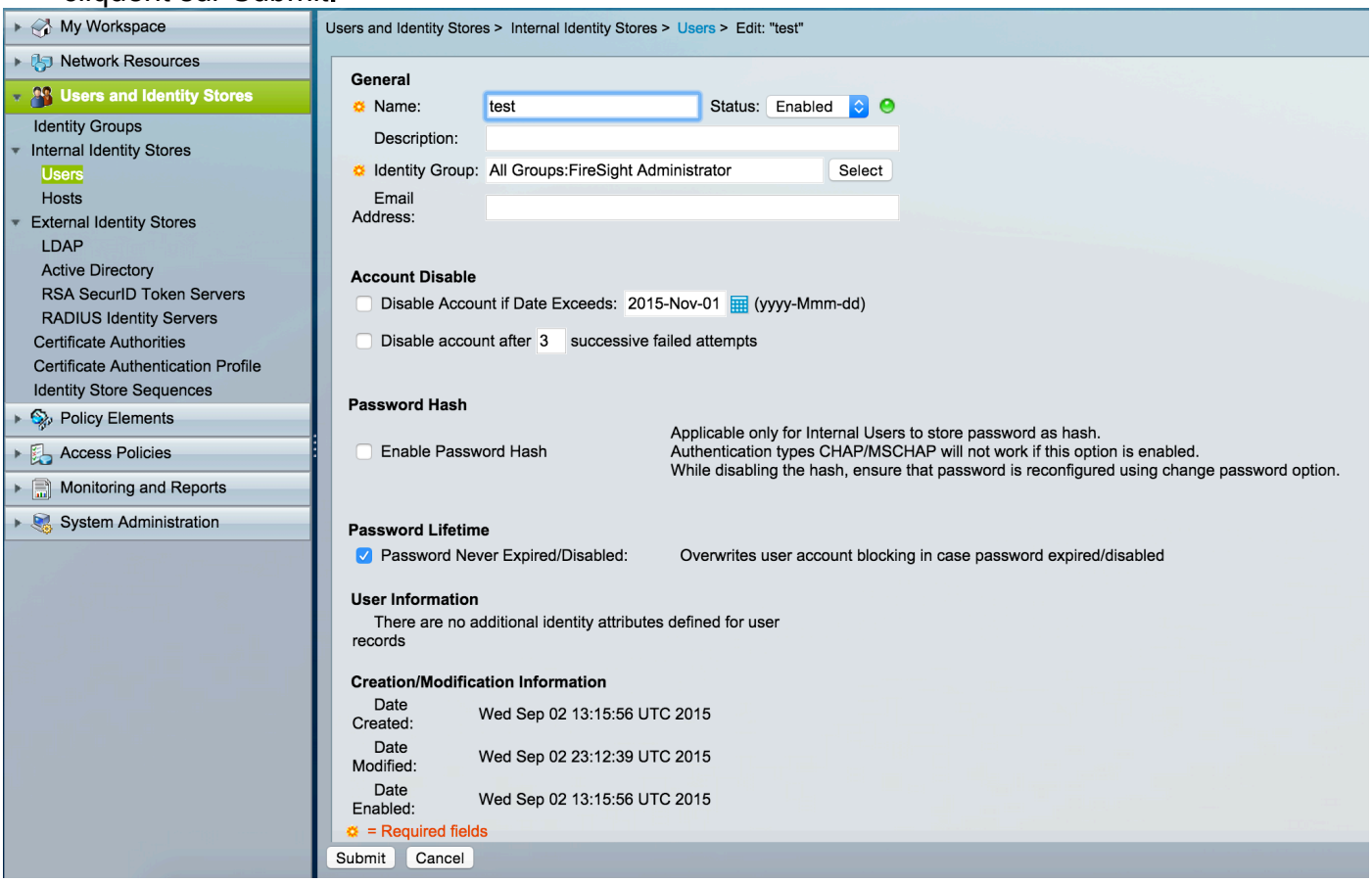
Ajouter un groupe d'Idenity dans ACS

- Naviguez vers des **utilisateurs et les mémoires d'identité,** configurent le **groupe d'identité**. Dans cet exemple, le groupe d'identité créé est « administrateur de FireSIGHT ». Ce groupe sera lié au profil d'autorisation défini dans les étapes ci-dessous.



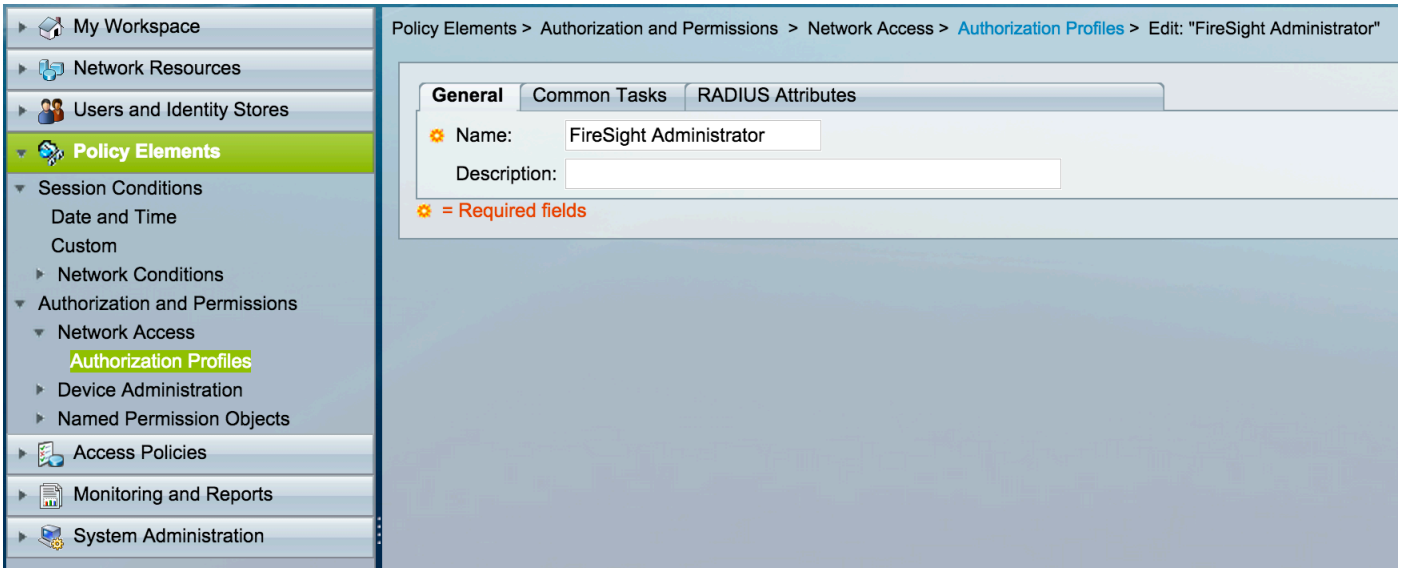
Ajouter un utilisateur local à ACS

- Naviguez vers des **utilisateurs et les mémoires d'identité,** configurent des **utilisateurs** dans la section **interne de mémoires d'identité**. Enter requried les informations pour la création d'utilisateur local, sélectionnent le **groupe d'identité** créé dedans au-dessus de l'étape et cliquent sur Submit.

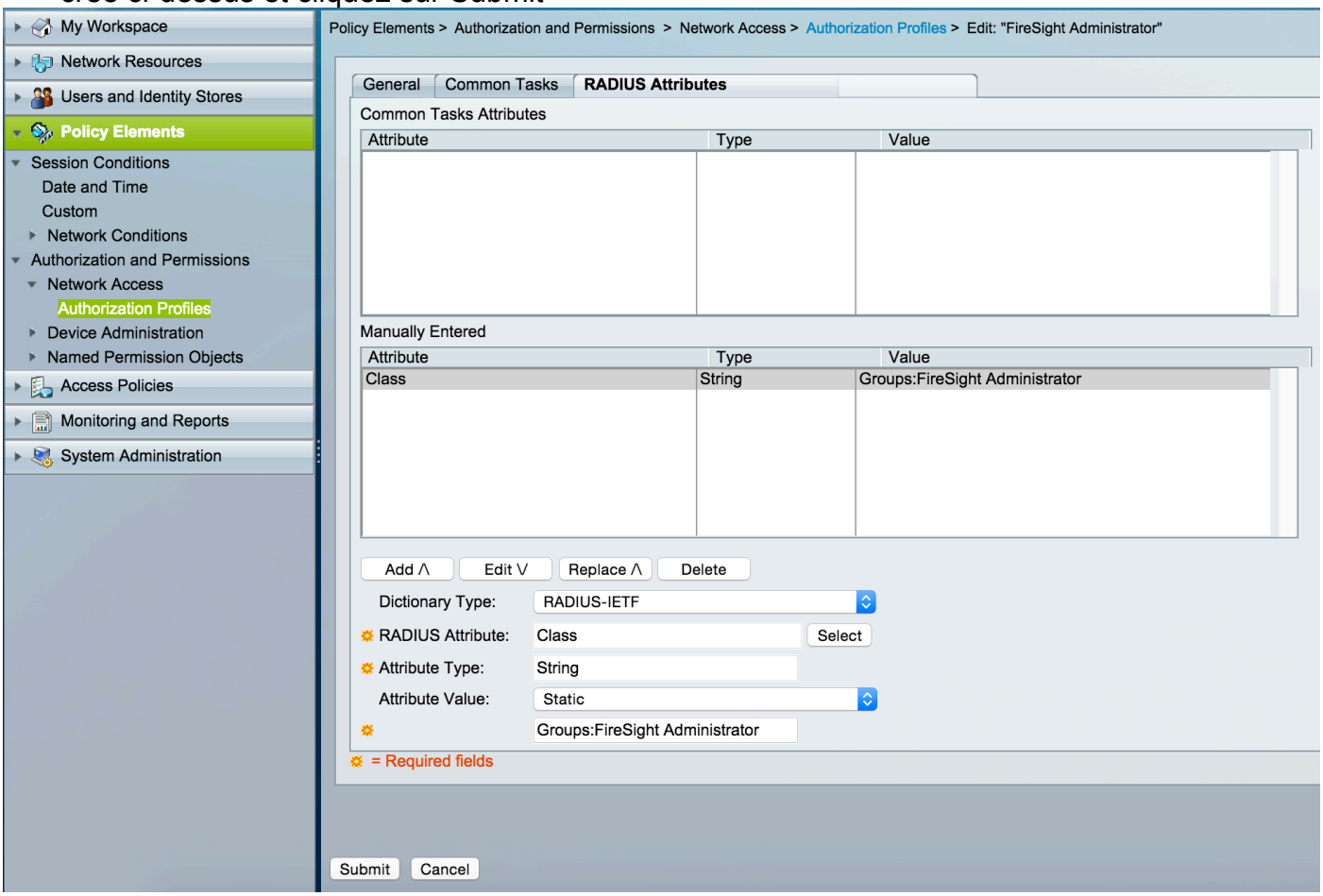


Configurer la stratégie ACS

- Dans le GUI ACS, naviguez vers des **éléments de stratégie > l'autorisation et des autorisations > des profils d'accès au réseau > d'autorisation**. Créez un nouveau profil d'autorisation avec un nom descriptif. Dans l'exemple ci-dessous, la stratégie créée est administrateur de FireSIGHT.

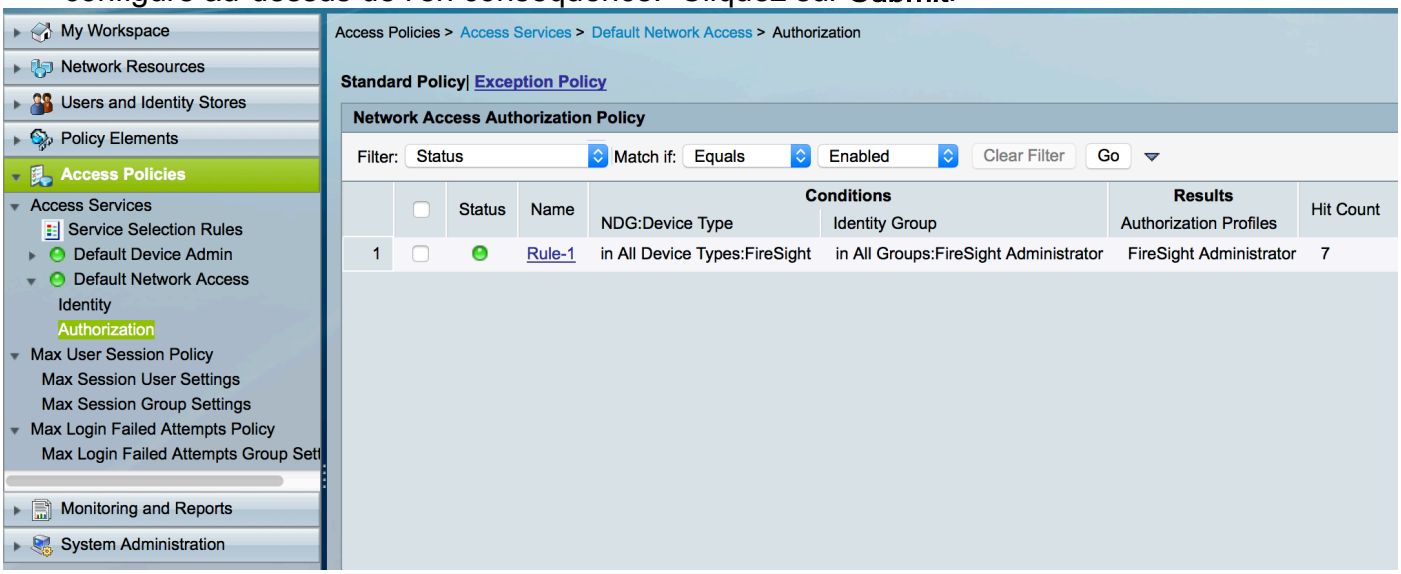


- Dans les **attributs RADIUS** tabulez, ajoutez l'attribut manuel pour autoriser le groupe d'identité créé ci-dessus et cliquez sur Submit



- Naviguez **pour accéder à des stratégies > des services d'accès > l'accès au réseau > l'autorisation de par défaut** et pour configurer une nouvelle stratégie d'autorisation pour les sessions de gestion de centre de Gestion de FireSIGHT. L'exemple ci-dessous utilise le **NDG : État de groupe de type de périphérique** et d'**identité** pour apparier le groupe configuré de type de périphérique et d'identité dans les étapes ci-dessus.

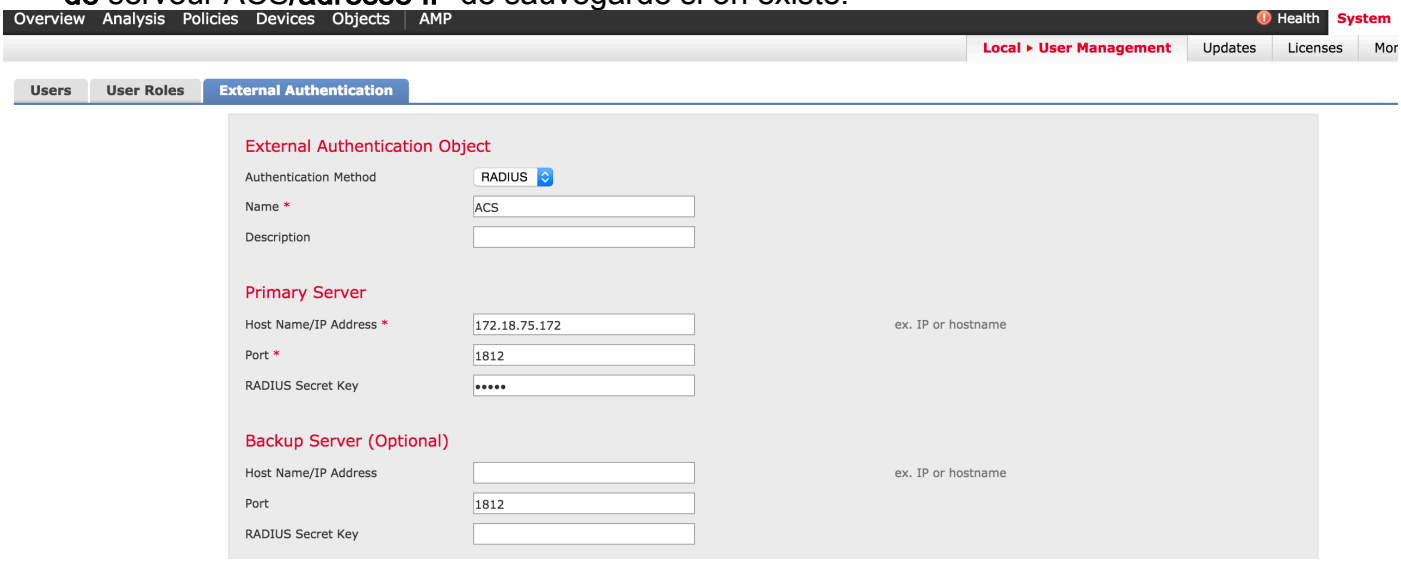
- Cette stratégie est alors associée avec le profil d'autorisation d'administrateur de FireSIGHT configuré au-dessus de l'en conséquence. Cliquez sur **Submit**.



Configuration de centre de Gestion de FireSIGHT

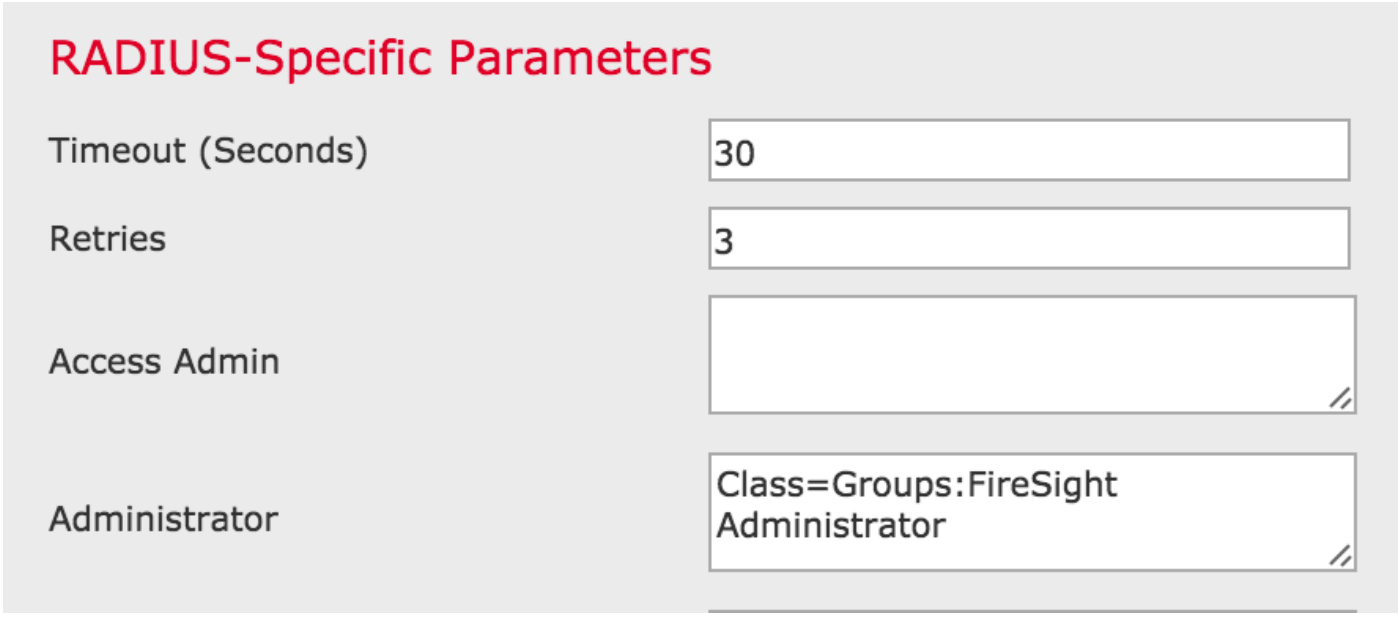
Configuration de politique de système de gestionnaire de FireSIGHT

- Ouvrez une session à FireSIGHT MC et naviguez vers le **système > les gens du pays > la gestion des utilisateurs**. Cliquez sur en fonction le clic de tableau d'**authentification externe** + créent le bouton d'objet d'authentification pour ajouter un nouveau serveur de RADIUS pour l'authentification de l'utilisateur/autorisation.
- **RADIUS** choisi pour la **méthode d'authentification**. Écrivez un nom descriptif pour le serveur de RADIUS. **Clé** écrivez le **nom d'hôte/adresse IP** et de **RADIUS secret**. La clé secrète devrait apparier la clé précédemment configurée sur ACS. Écrivez sur option un **nom d'hôte de** serveur ACS**/adresse IP** de sauvegarde si on existe.

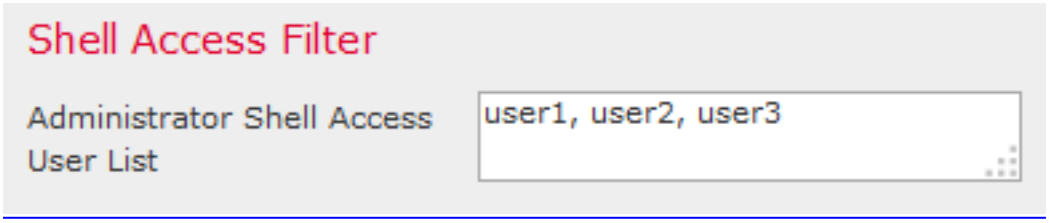


- Sous la section de **paramètres de RADIUS-particularité**, dans cet exemple, le Class=Groups : La valeur d'administrateur de FireSIGHT est tracée au groupe d'administrateur de FireSIGHT. C'est la valeur qu'ACS renvoie en tant qu'élément de l'ACCESS-ACCEPT.

  Cliquez sur la **sauvegarde** pour sauvegarder la configuration ou pour procéder à la section de vérifier ci-dessous au test d'authentification à ACS.



- Sous le **filtre d'Access de shell**, écrivez une virgule liste séparée d'utilisateurs pour limiter des sessions shell/SSH.



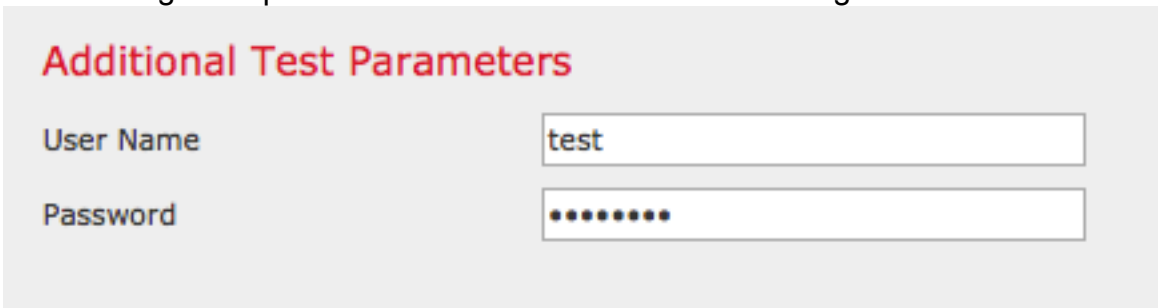
Authentification externe d'enable

En conclusion, terminez-vous ces étapes afin d'activer l'authentification externe sur le FMC :

1. Naviguez vers le **système** > la **stratégie de gens du pays** > de **système**.
2. **Authentification externe** choisie sur le panneau gauche.
3. Changez l'*état à* **activer** (désactivé par défaut).
4. Activez le serveur ajouté ACS RADIUS.
5. Sauvegardez la stratégie et réappliquez la stratégie sur l'appliance.

Vérification

- Pour tester l'authentification de l'utilisateur contre ACS, faites descendre l'écran à la section **supplémentaire de paramètres de test** et écrivez un nom d'utilisateur et mot de passe pour l'utilisateur ACS. **Test de** clic. Un essai réussi aura comme conséquence un succès vert : Message complet de test en haut de la fenêtre du navigateur.



- Pour visualiser les résultats du test d'authentification, aller à la **section de sortie de test** et cliquer sur la flèche **noire** à côté des **détails d'exposition**. Dans le tir d'écran d'exemple ci-dessous, notez le « radiusauth - réponse : |Class=Groups : Administrateur de FireSIGHT| » valeur reçue d'ACS. Ceci devrait apparier la valeur de classe associée avec le groupe configuré local de FireSIGHT sur FireSIGHT MC ci-dessus. Cliquez sur **Save**.