Intégration de système de FireSIGHT avec ISE 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 puissance de feu avec le Logiciel Cisco Identity Services Engine (ISE) pour l'authentification à distance se connectent l'authentification de l'utilisateur de service d'utilisateur (RAYON).

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 ISE
- La connaissance de base de RAYON

Composants utilisés

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

- Cisco ASA v9.2.1
- Module v5.3.1 de puissance de feu ASA
- ISE 1.2

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.

Configurez

Configuration ISE

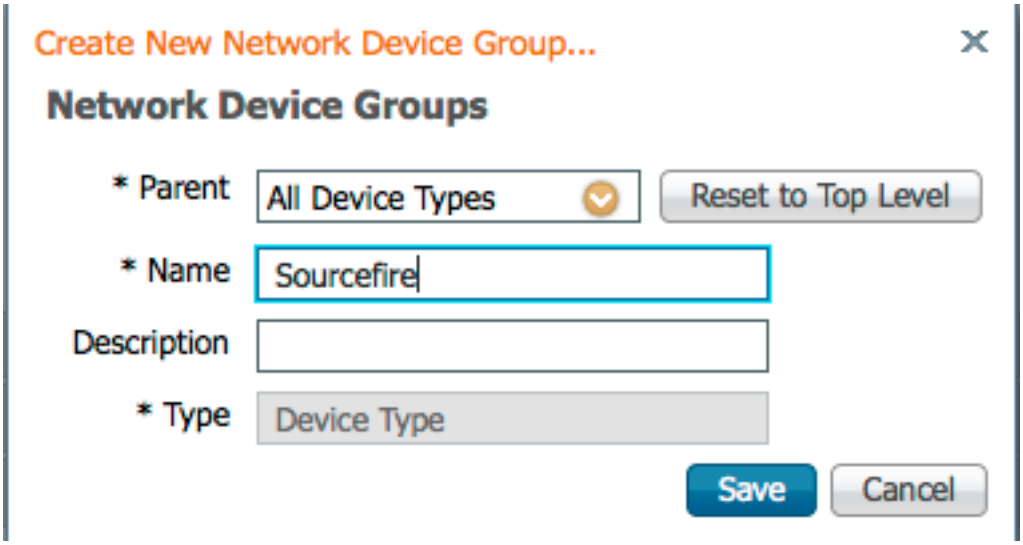
> **Conseil** : Il y a de plusieurs manières de configurer des stratégies d'authentification et d'autorisation ISE pour prendre en charge l'intégration avec les périphériques d'accès au réseau (NAD) comme Sourcefire. L'exemple ci-dessous est une manière de configurer l'intregration. La configuration d'échantillon est un point de référence et peut être adaptée pour adapter aux besoins du déploiement spécifique. Notez que la configuration d'autorisation est un processus en deux étapes. Un ou plusieurs stratégies d'autorisation seront définies sur ISE avec des paires de renvoi de valeur d'attribut RADIUS ISE (poids du commerce-paires) au FMC ou au périphérique géré. Ces poids du commerce-paires sont alors tracées à un groupe d'utilisateur local défini en configuration de politique de système FMC.

Configurer des périphériques et des groupes de périphériques réseau de réseau

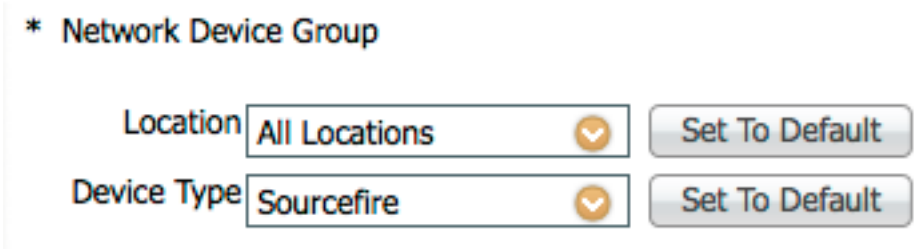
- Du GUI ISE, naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau**. Cliquez sur **+Add** pour ajouter un nouveau périphérique d'accès au réseau (NAD). Fournissez un nom et une adresse IP descriptifs de périphérique. Le FMC est défini dans l'exemple ci-dessous.

- Sous le **groupe de périphériques réseau**, cliquez sur en fonction la flèche orange à côté de **tous les types de périphérique.** Cliquez sur en fonction l'icône et choisi **créez le**

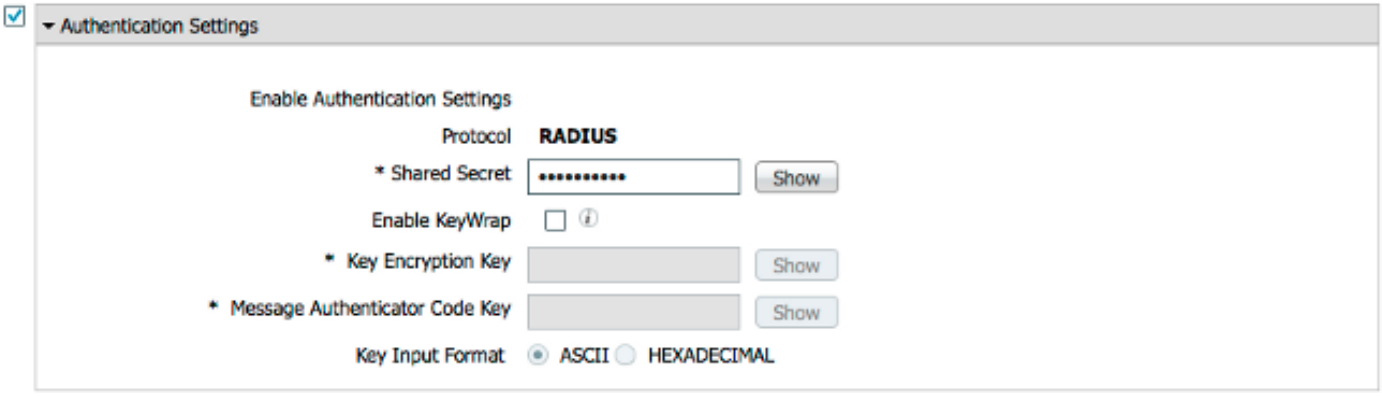
nouveau groupe de périphériques réseau. Dans le tir d'écran d'exemple qui suit, le type de périphérique Sourcefire a été configuré. Ce type de périphérique sera mis en référence dans la définition de règle de stratégie d'autorisation dans une étape postérieure. Cliquez sur **Save**.



- Cliquez sur la flèche orange de nouveau et sélectionnez le groupe de périphériques réseau configuré dans l'étape ci-dessus



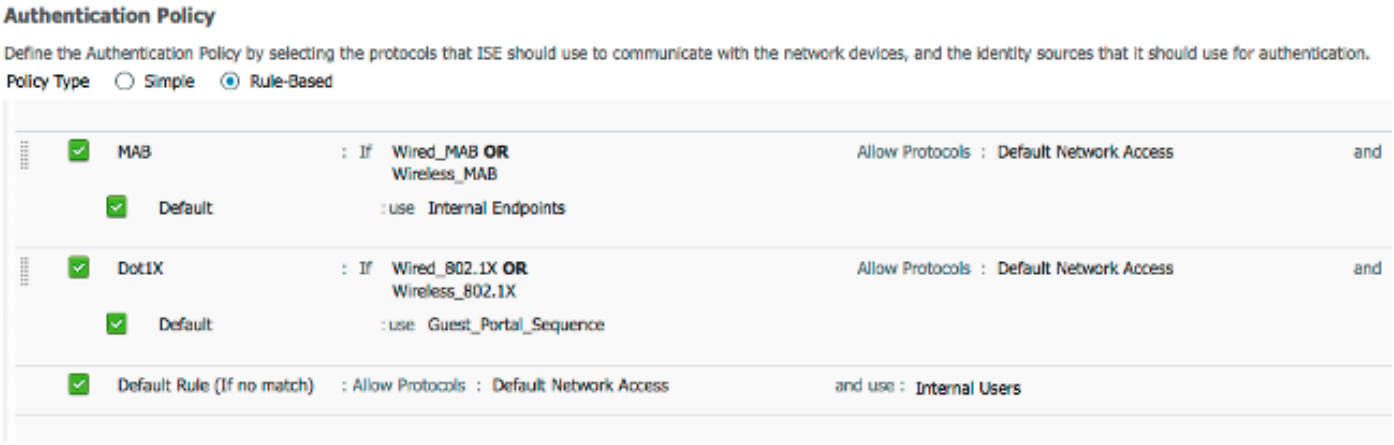
- Cochez la case à côté des **configurations d'authentification**. Introduisez la clé secrète partagée par RAYON qui sera utilisée pour ce NAD. Notez la même chose la clé que secrète partagée sera utilisée de nouveau plus tard quand configurant le serveur de RAYON sur le FireSIGHT MC. Pour passer en revue la valeur principale de texte brut, cliquez sur le bouton d'**exposition**. Cliquez sur **Save**.



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

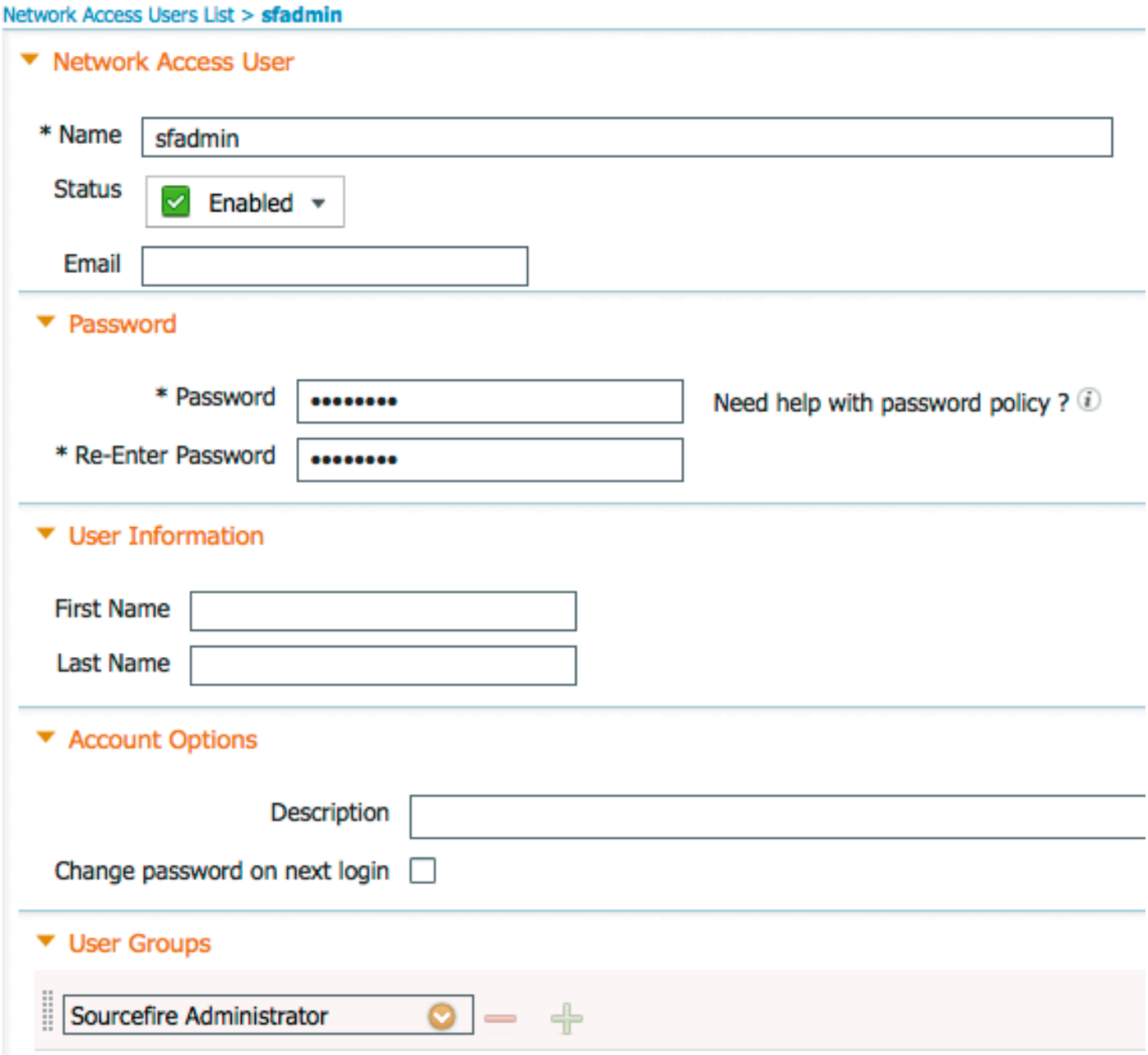
Configurer la stratégie d'authentification ISE :

- Du GUI ISE, naviguez vers la **stratégie > l'authentification**. Si utilisant des positionnements de stratégie, naviguez vers la **stratégie > les positionnements de stratégie**. L'exemple ci-dessous est pris d'un déploiement ISE qui utilise les interfaces de stratégie d'authentification par défaut et d'autorisation. La logique de règle d'authentification et d'autorisation est identique indépendamment de l'approche de configuration.
- **La règle par défaut (si aucune correspondance)** sera utilisée d'authentifier des demandes RADIUS de NADs où la méthode n'est pas en service dérivation d'authentification MAC (MAB) ou 802.1X. Comme configuré par défaut, cette règle recherchera des comptes utilisateurs dans la source locale d'identité des **utilisateurs internes d'**ISE. Cette configuration peut être modifiée pour se rapporter à une source extérieure d'identité telle que le Répertoire actif, le LDAP, etc. comme définie sous la **gestion > la Gestion de l'identité > des sources extérieures d'identité**. Dans l'intéret du simplciity, cet exemple définira des comptes utilisateurs localement sur ISE ainsi aucune modification supplémentaire à la stratégie d'authentification n'est exigée.



Ajouter un utilisateur local à ISE

- Naviguez vers la **gestion > la Gestion de l'identité > les identités > les utilisateurs**. Cliquez sur **Add**. Écrivez un nom d'utilisateur et mot de passe signicatif. Sous la sélection de **groupes d'utilisateurs**, sélectionnez un nom de groupe existant ou cliquez sur le vert + signe d'ajouter un nouveau groupe. Dans cet exemple, l'utilisateur « sfadmin » est assigné au groupe fait sur commande « administrateur de Sourcefire ». Ce groupe d'utilisateurs sera lié au profil d'autorisation défini dans l'étape **configurante de stratégie d'autorisation ISE** ci-dessous. Cliquez sur **Save**.



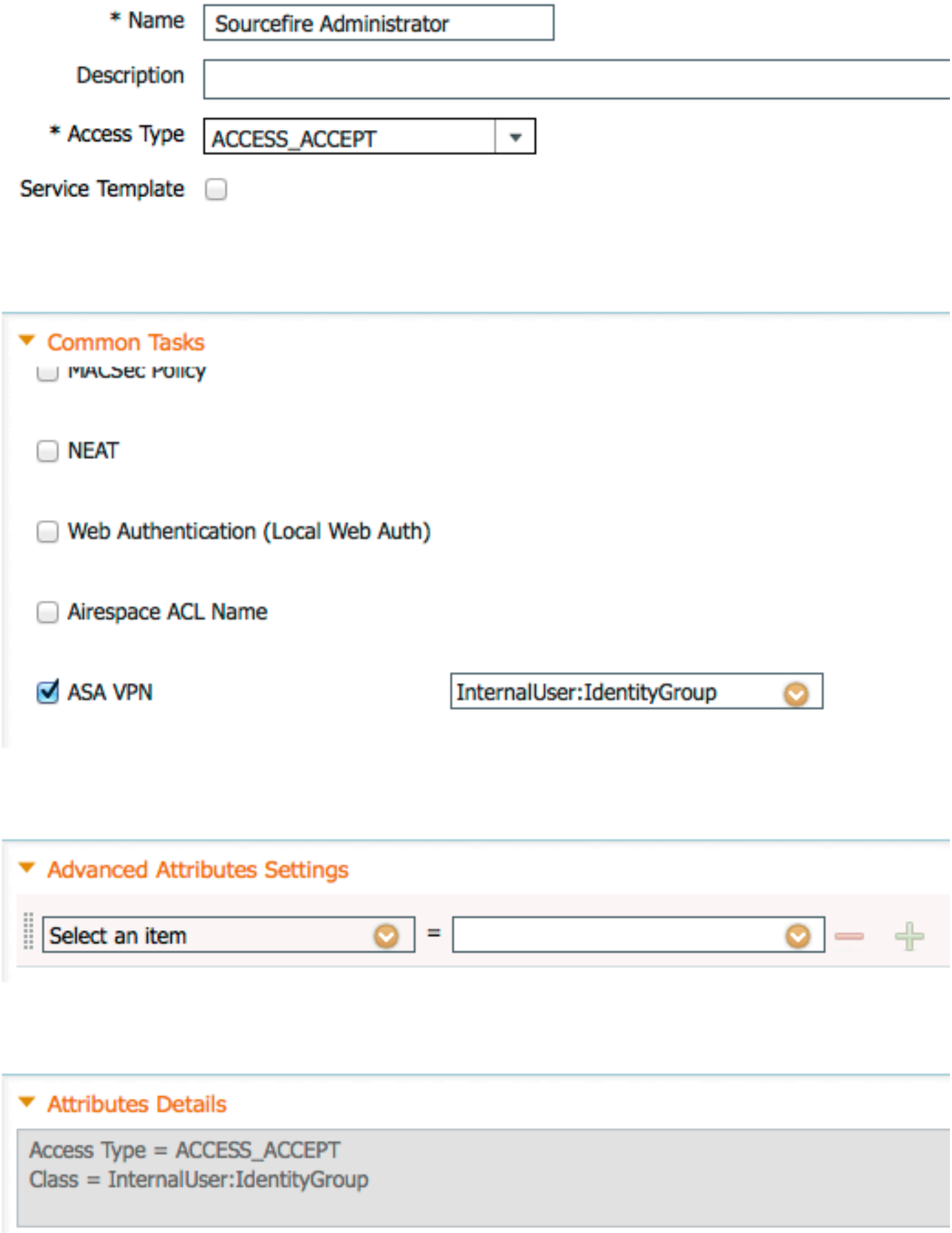
Configurer la stratégie d'autorisation ISE

- Naviguez vers la **stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation**. Cliquez sur le vert + signe d'ajouter un nouveau profil d'autorisation.
- Fournissez un nom descriptif tel que l'administrateur de Sourcefire. **ACCESS_ACCEPT** choisi pour le **type d'Access**. Sous des **fonctionnalités usuelles**, le défilement au bas et cochent la case à côté d'**ASA VPN**. Cliquez sur la flèche orange et sélectionnez **InternalUser : IdentityGroup**. Cliquez sur **Save**.

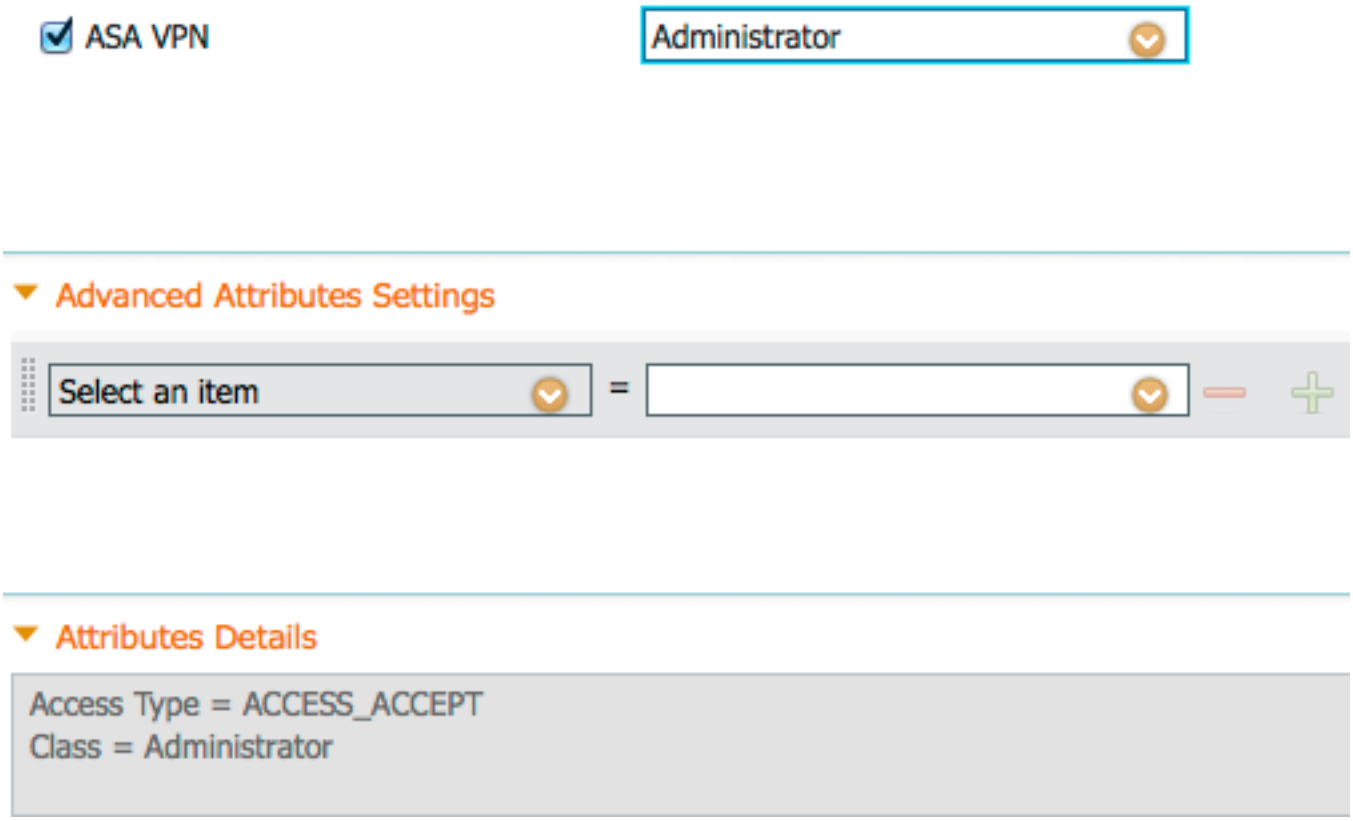
  Conseil : Puisque cet exemple utilise la mémoire d'identité d'utilisateur local ISE, l'InternalUser : L'option de groupe d'IdentityGroup est utilisée de simplifier la configuration. Si utilisant une mémoire externe d'identité, l'attribut d'autorisation ASA VPN est encore utilisé, cependant, la valeur à retourner au périphérique de Sourcefire est manuellement configurée. Par exemple, en tapant manuellement l'administrateur dans l'ASA VPN relâchez vers le bas la case aura comme conséquence une valeur des poids du commerce-paires Class-25 de la classe = de l'administrateur étant envoyés au périphérique de Sourcefire. Cette valeur peut alors être tracée à un groupe d'utilisateurs de sourcefire en tant qu'élément

de la configuration de politique de système. Pour des utilisateurs internes, l'un ou l'autre de méthode de configuration est acceptable.

Exemple d'utilisateur interne



Exemple d'utilisateur externe



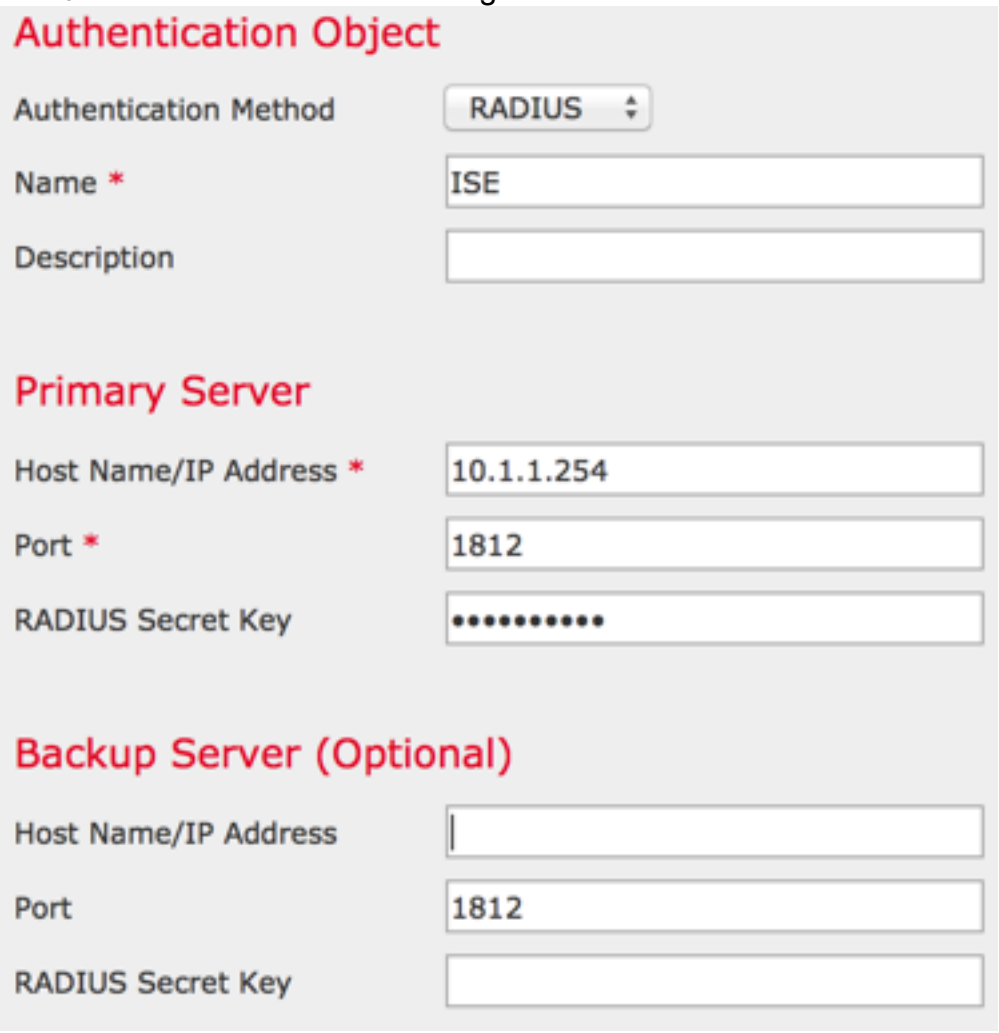
- Naviguez vers la **stratégie > l'autorisation** et configurez une nouvelle stratégie d'autorisation pour les sessions de gestion de Sourcefire. L'exemple ci-dessous utilise le **PÉRIPHÉRIQUE : État de type de périphérique** pour apparier le type de périphérique configuré dans **Configurant la** section de **périphériques et de groupes de périphériques réseau de réseau** ci-dessus. Cette stratégie est alors associée avec le profil d'autorisation d'administrateur de Sourcefire configuré ci-dessus. Cliquez sur **Save**.

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
✓	Sourcefire Administrator	if	DEVICE:Device Type EQUALS All Device Types#Sourcefire	then	Sourcefire Administrator
✓	CWA-PSN1	if	Network Access:ISE Host Name EQUALS ise12-psn1	then	CWA-PSN1
✓	CWA-PSN2	if	Network Access:ISE Host Name EQUALS ise12-psn2	then	CWA-PSN2

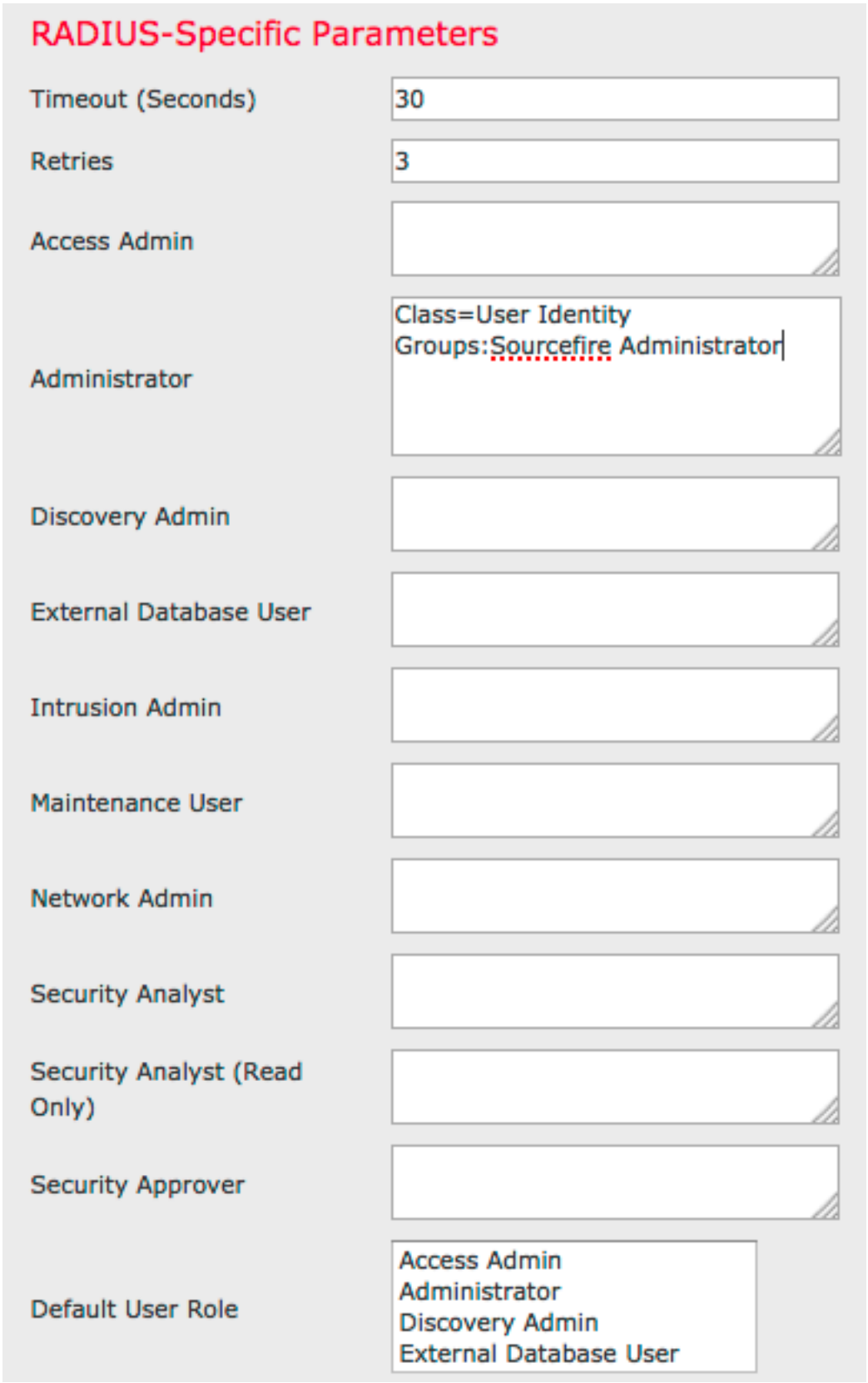
Configuration de politique de système de Sourcefire

- Ouvrez une session au 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 de connexion** + créent le bouton d'objet d'authentification pour ajouter un nouveau serveur de RAYON pour l'authentification de l'utilisateur/autorisation.
- **RAYON** choisi pour la **méthode d'authentification**. Écrivez un nom descriptif pour le serveur de RAYON. **Clé** écrivez le **nom d'hôte/adresse IP** et de **RAYON secret**. La clé secrète devrait

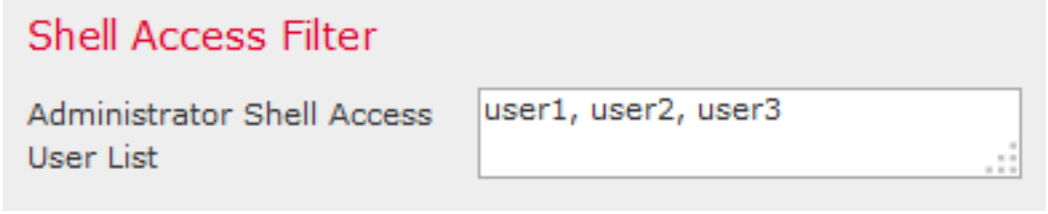
apparier la clé précédemment configurée sur ISE. Écrivez sur option un **nom/adresse IP d'**hôte de serveur de la sauvegarde ISE si on existe.



- Sous la Rayon-**particularité les paramètres** sectionnent, écrivent la chaîne des poids du commerce-paires Class-25 dans la zone de texte à côté du nom de groupe local de Sourcefire à apparier pour l'accès GUI. Dans cet exemple, l'identité de Class=User groupe : La valeur d'administrateur de Sourcefire est tracée au groupe d'administrateur de Sourcefire. C'est la valeur qu'ISE renvoie en tant qu'élément de l'ACCESS-ACCEPT. Sur option, sélectionnez un **rôle de l'utilisateur par défaut** pour les utilisateurs authentifiés qui ne font pas assigner les groupes Class-25. Cliquez sur la **sauvegarde** pour sauvegarder la configuration ou pour procéder à la section de vérifier ci-dessous au test d'authentification à ISE.



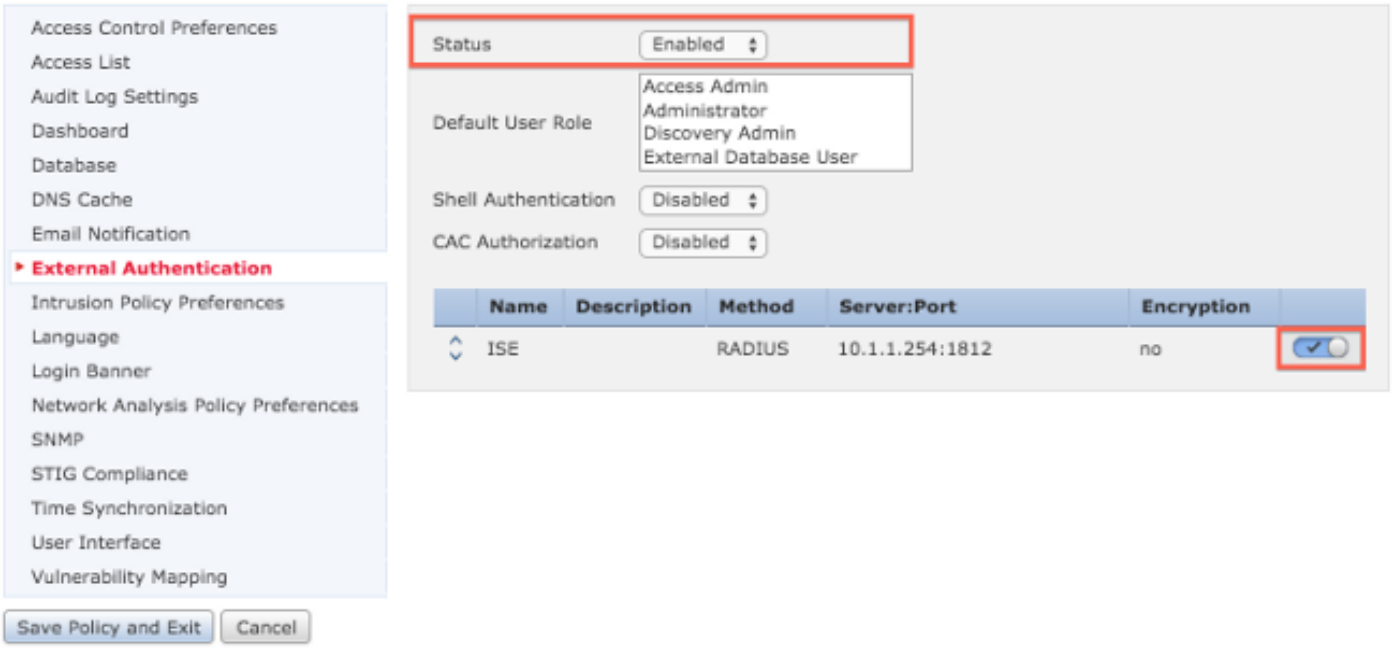
- Sous le **filtre d'Access de shell**, écrivez une virgule liste séparée d'utilisateurs pour limiter des sessions shell/SSH.



Authentification externe d'enable

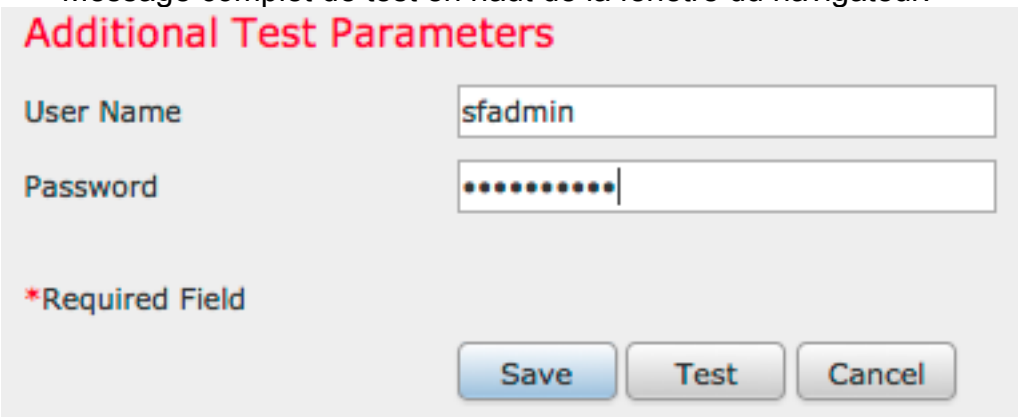
En conclusion, terminez-vous ces étapes afin d'activer l'authentification externe sur le FMC :

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 de RAYON ISE.
5. Sauvegardez la stratégie et réappliquez la stratégie sur l'appliance.



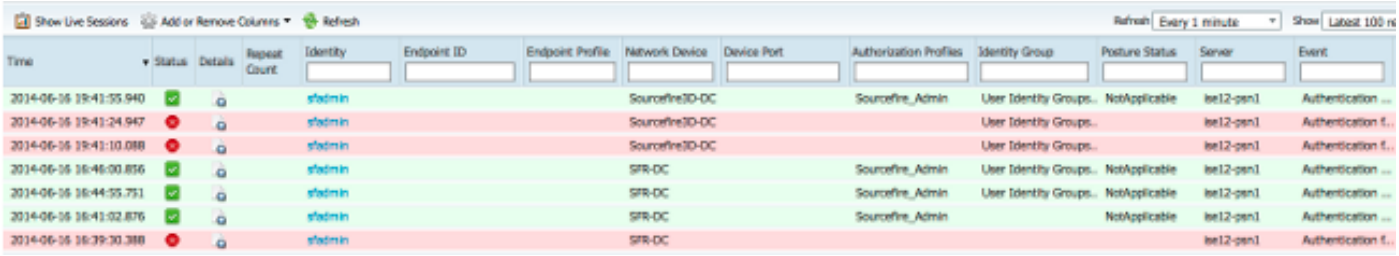
Vérifiez

- Pour tester l'authentification de l'utilisateur contre ISE, 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 ISE. **Test de** clic. Un essai réussi aura comme conséquence un succès vert : Message complet de test en haut de la fenêtre du navigateur.



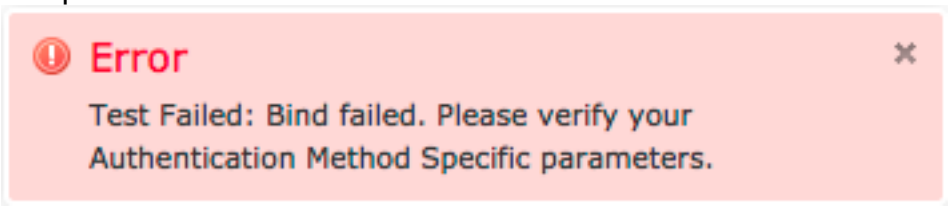
- Pour visualiser les résultats du test d'authentification, aller à la **section de sortie de test** et cliquer sur la flèche **noire** à côté des **détails d'exposition**. Dans le tir d'écran d'exemple ci-dessous, notez le « radiusauth - réponse : |Groupes d'identité de Class=User : Administrateur de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

- Du GUI d'admin ISE, naviguez vers des **exécutions > des authentifications** pour vérifier le succès ou échec du test d'authentification de l'utilisateur.

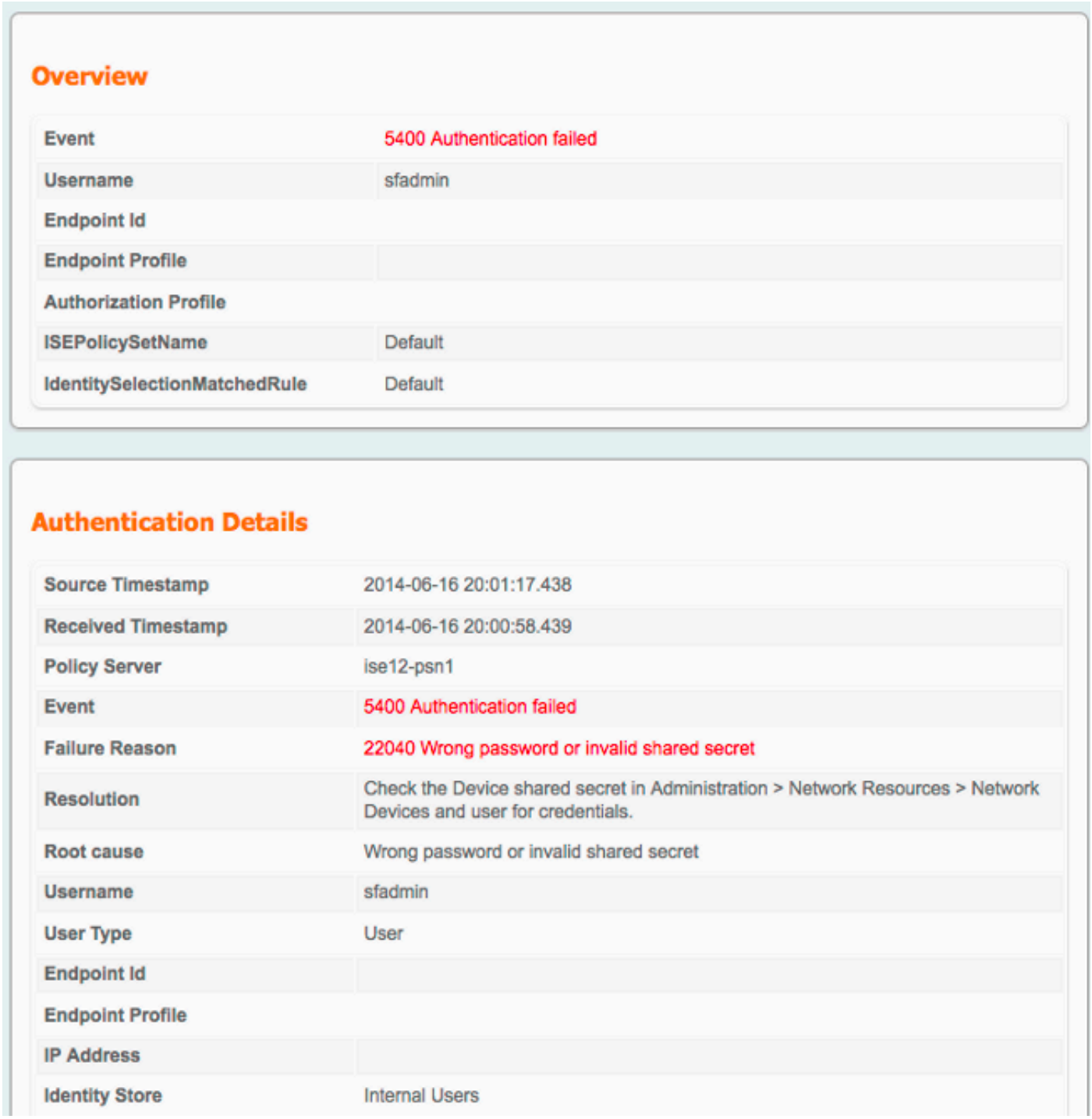


Dépannez

- En testant l'authentification de l'utilisateur contre ISE, l'erreur suivante est indicative d'une non-concordance principale secrète de RAYON ou d'un nom d'utilisateur incorrect/de mot de passe.



- Du GUI d'admin ISE, naviguez vers des **exécutions > des authentifications**. Un événement rouge est indicatif d'une panne tandis qu'un événement vert est indicatif d'une authentification/d'autorisation/de modification réussies de l'autorisation. Cliquez sur en fonction  l'icône pour passer en revue les détails de l'événement d'authentification.



Overview

Event	5400 Authentication failed
Username	sfadmin
Endpoint Id	
Endpoint Profile	
Authorization Profile	
ISEPolicySetName	Default
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-06-16 20:01:17.438
Received Timestamp	2014-06-16 20:00:58.439
Policy Server	ise12-psn1
Event	5400 Authentication failed
Failure Reason	22040 Wrong password or invalid shared secret
Resolution	Check the Device shared secret in Administration > Network Resources > Network Devices and user for credentials.
Root cause	Wrong password or invalid shared secret
Username	sfadmin
User Type	User
Endpoint Id	
Endpoint Profile	
IP Address	
Identity Store	Internal Users

Informations connexes

Support et documentation techniques - Cisco Systems