Integrazione del sistema FireSIGHT con ACS 5.x per l'autenticazione utente RADIUS

Sommario

- Introduzione
- Prerequisiti
  - Requisiti
  - Componenti usati
- Configurazione
  - Configurazione ACS 5.x
    - Configurazione di dispositivi e gruppi di dispositivi di rete
    - Aggiunta di un gruppo di identità in ACS
    - Aggiunta di un utente locale ad ACS
    - Configurazione del criterio ACS
  - Configurazione di FireSight Management Center
    - Configurazione dei criteri di sistema di FireSight Manager
    - Abilita autenticazione esterna
- Verifica
- Discussioni correlate nella Cisco Support Community

Introduzione

In questo documento viene descritta la procedura di configurazione necessaria per integrare un Cisco FireSIGHT Management Center (FMC) o un dispositivo gestito Firepower con Cisco Secure Access Control System 5.x (ACS) per l'autenticazione utente RADIUS (Remote Authentication Dial In User Service).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione iniziale del sistema FireSIGHT e del dispositivo gestito tramite GUI e/o shell
- Configurazione dei criteri di autenticazione e autorizzazione in ACS 5.x
- Conoscenze base di RADIUS

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Secure Access Control System 5.7 (ACS 5.7)
- Cisco FireSight Manager Center 5.4.1

Le versioni precedenti sono le versioni più recenti attualmente disponibili. Questa funzionalità è supportata in tutte le versioni ACS 5.x e FMC 5.x.

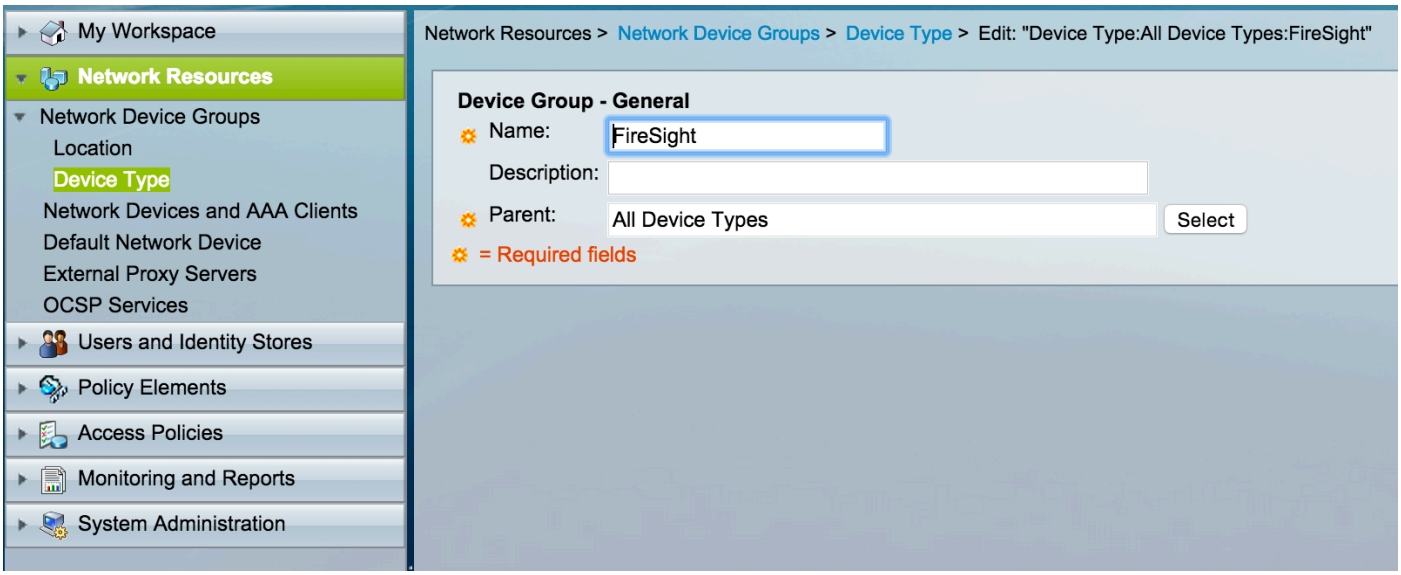
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

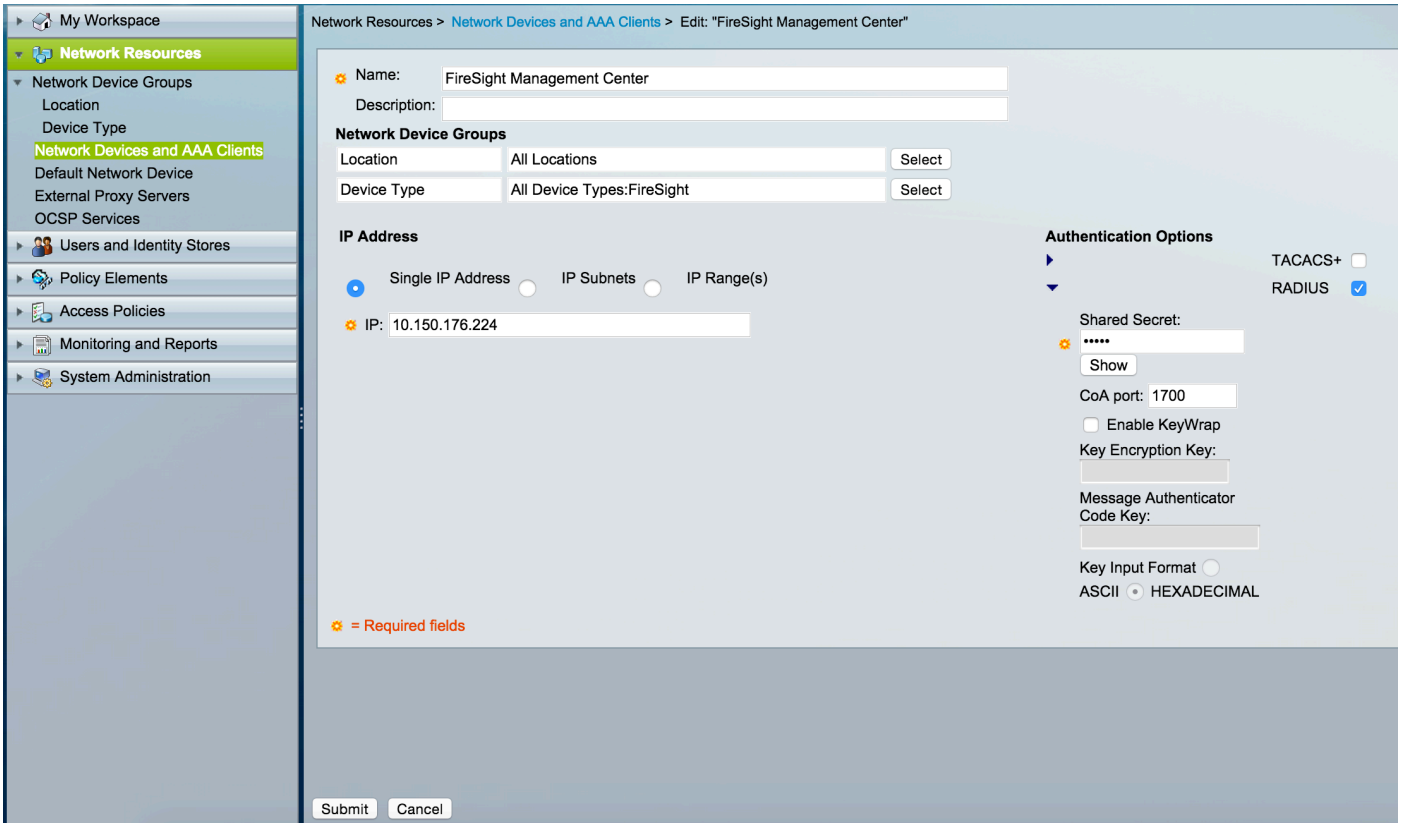
Configurazione ACS 5.x

Configurazione di dispositivi e gruppi di dispositivi di rete

- Dalla GUI di ACS, selezionare Network Device Group, fare clic su Device Type (Tipo di dispositivo), quindi creare un gruppo di dispositivi. Nello screenshot di esempio seguente è stato configurato il tipo di dispositivo FireSight. Nella definizione della regola dei criteri di autorizzazione verrà fatto riferimento a questo tipo di dispositivo in un passaggio successivo. Fare clic su Save (Salva).



- Dalla GUI di ACS, selezionare Network Device Group, fare clic su Network Devices e client AAA e aggiungere un dispositivo. Specificare un nome descrittivo e un indirizzo IP del dispositivo. Il centro di gestione FireSIGHT è definito nell'esempio riportato di seguito.



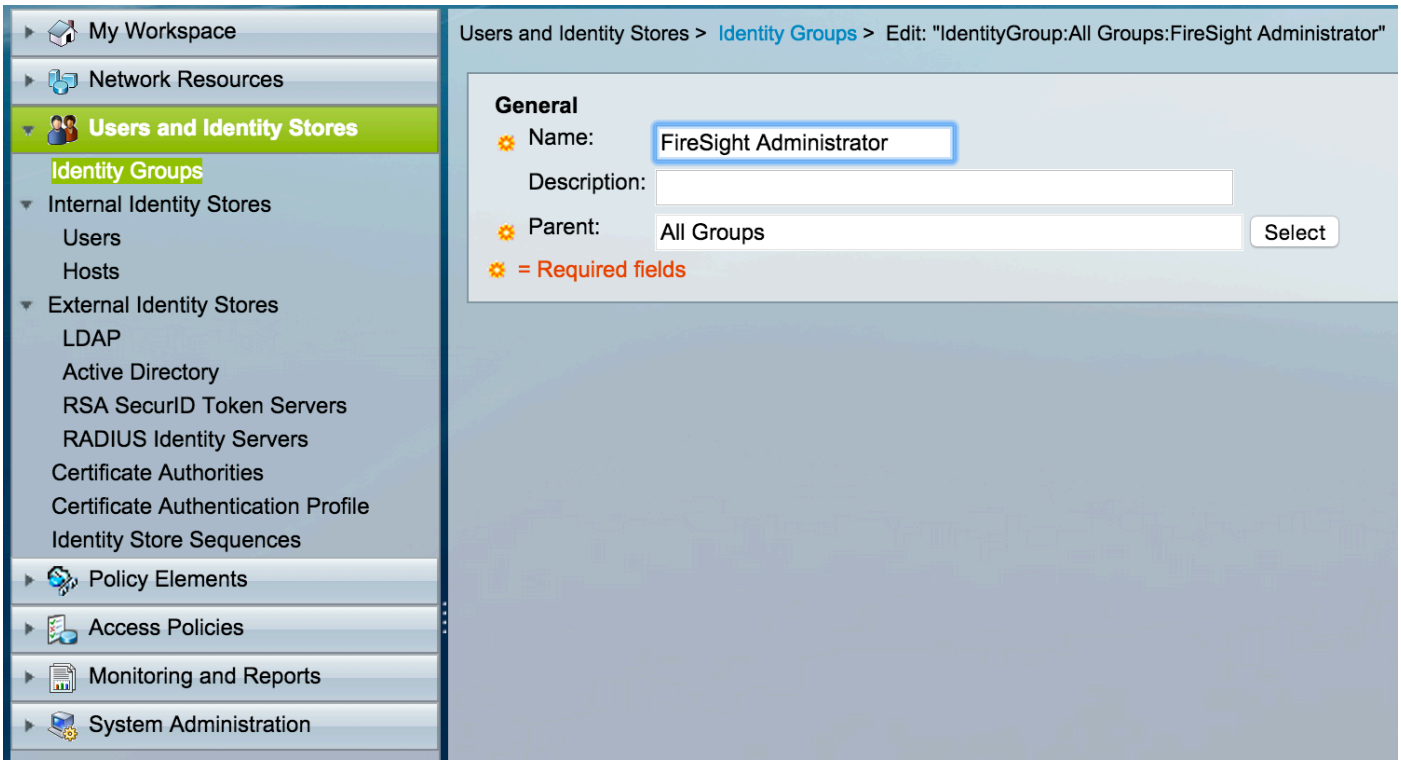
- In Gruppi di dispositivi di rete configurare Tipo di dispositivo come gruppo di dispositivi creato nel passaggio precedente.

- Selezionare la casella accanto a Opzioni di autenticazione, selezionare la casella di controllo RADIUS e immettere la chiave segreta condivisa che verrà utilizzata per questo NAD. Si noti che la stessa chiave segreta condivisa verrà utilizzata di nuovo in seguito durante la configurazione del server RADIUS nel centro di gestione FireSIGHT. Per verificare il valore della chiave in testo normale, fare clic sul pulsante Mostra. Fare clic su Invia.

- Ripetere i passaggi precedenti per tutti i centri di gestione FireSIGHT e i dispositivi gestiti che richiederanno l'autenticazione/autorizzazione utente RADIUS per l'accesso alla GUI e/o alla shell.

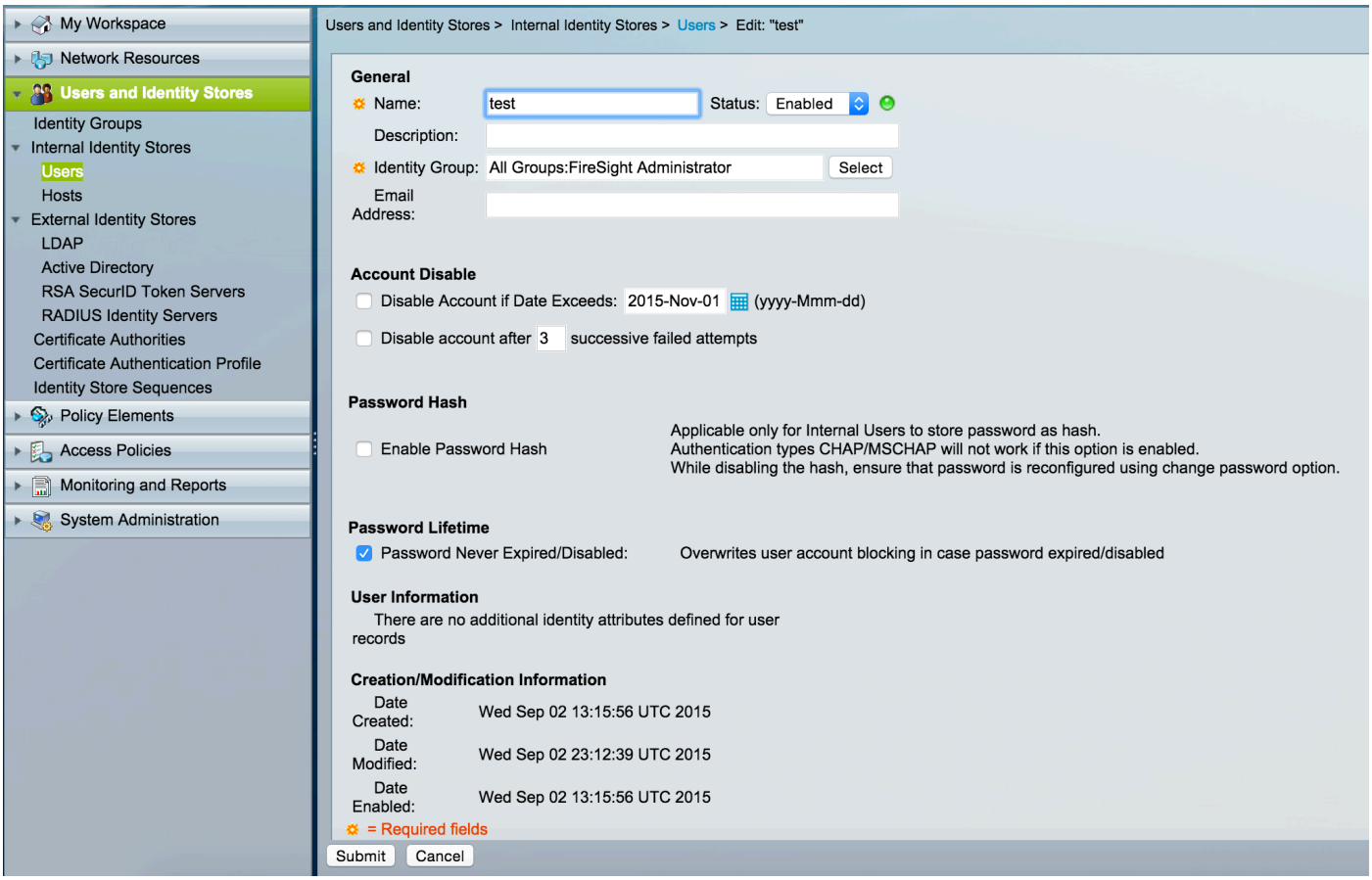
Aggiunta di un gruppo di identità in ACS

- Passare a Utenti e archivi identità e configurare il gruppo di identità. In questo esempio, il gruppo di identità creato è "FireSight Administrator". Questo gruppo verrà collegato al profilo di autorizzazione definito nei passaggi seguenti.



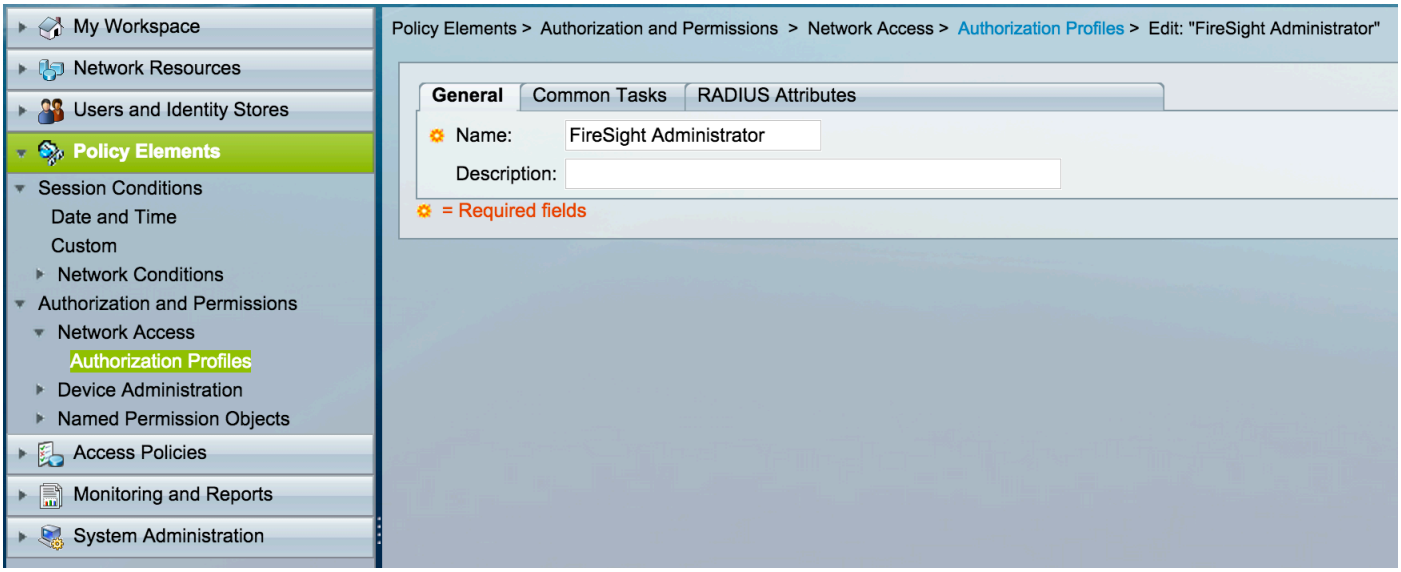
Aggiunta di un utente locale ad ACS

- Passare alla sezione Utenti e archivi identità, configurare gli utenti nella sezione Archivi identità interni. Immettere le informazioni necessarie per la creazione dell'utente locale, selezionare il gruppo di identità creato nel passaggio precedente e fare clic su Invia.

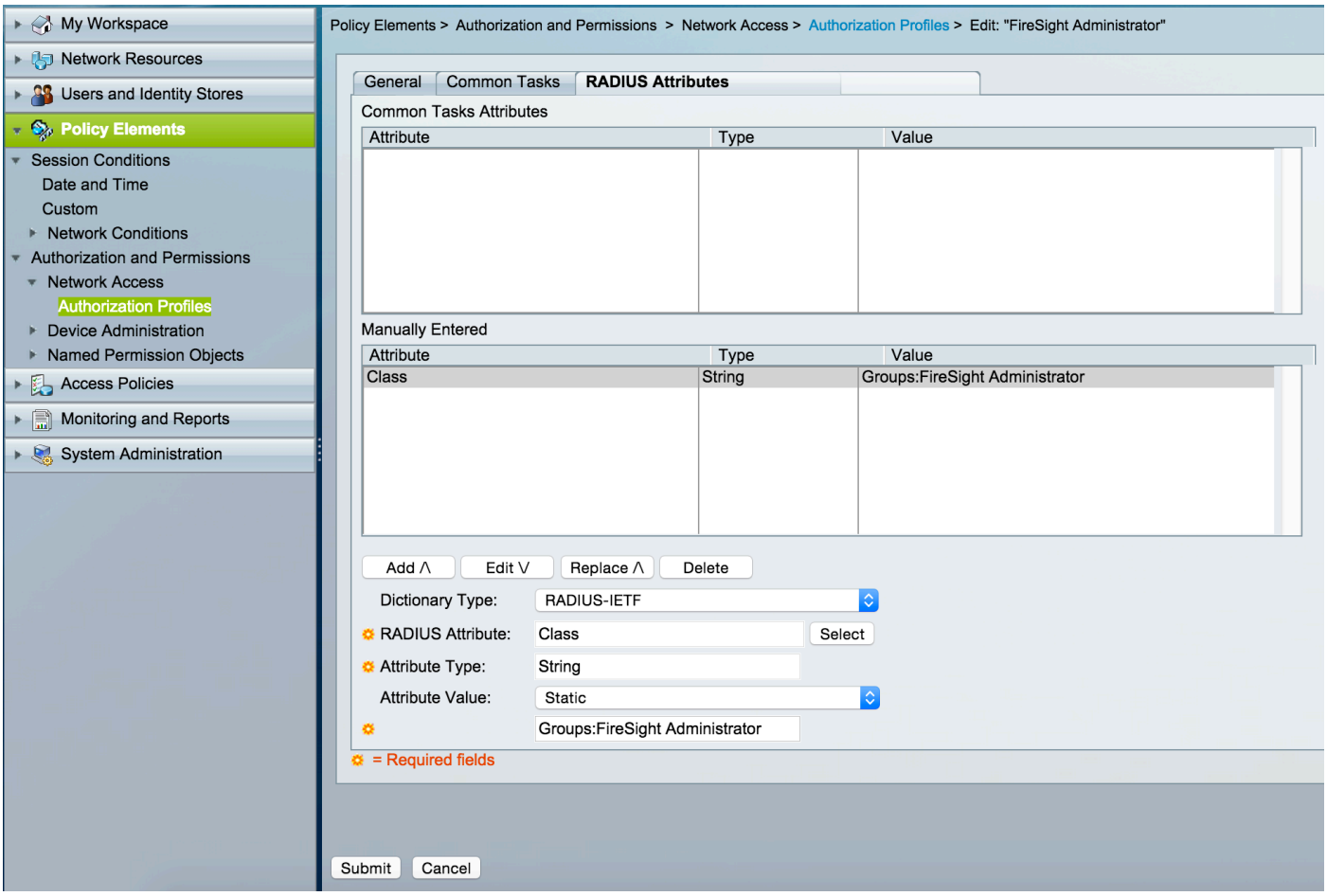


Configurazione del criterio ACS

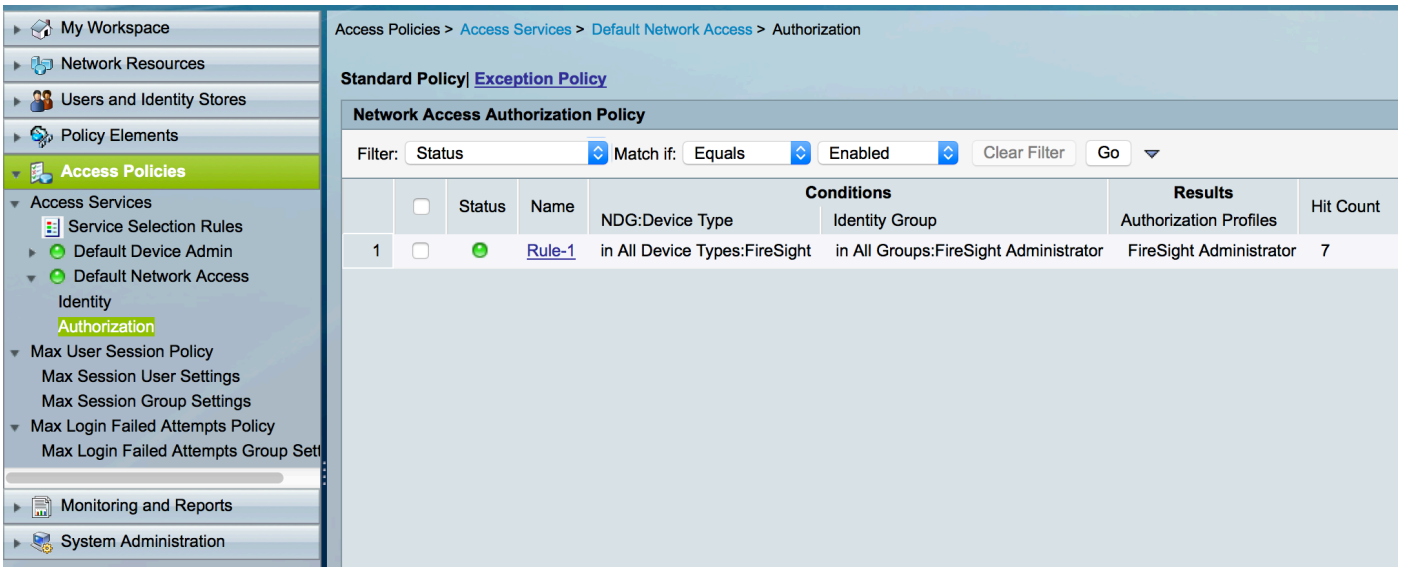
- Nell'interfaccia utente di ACS, selezionare Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles (Elementi criteri > Autorizzazioni e autorizzazioni > Accesso alla rete > Profili di autorizzazione). Creare un nuovo profilo di autorizzazione con un nome descrittivo. Nell'esempio riportato di seguito, il criterio creato è FireSight Administrator.



- Nella scheda Attributi RADIUS, aggiungere un attributo manuale per autorizzare il gruppo di identità creato in precedenza e fare clic su Invia



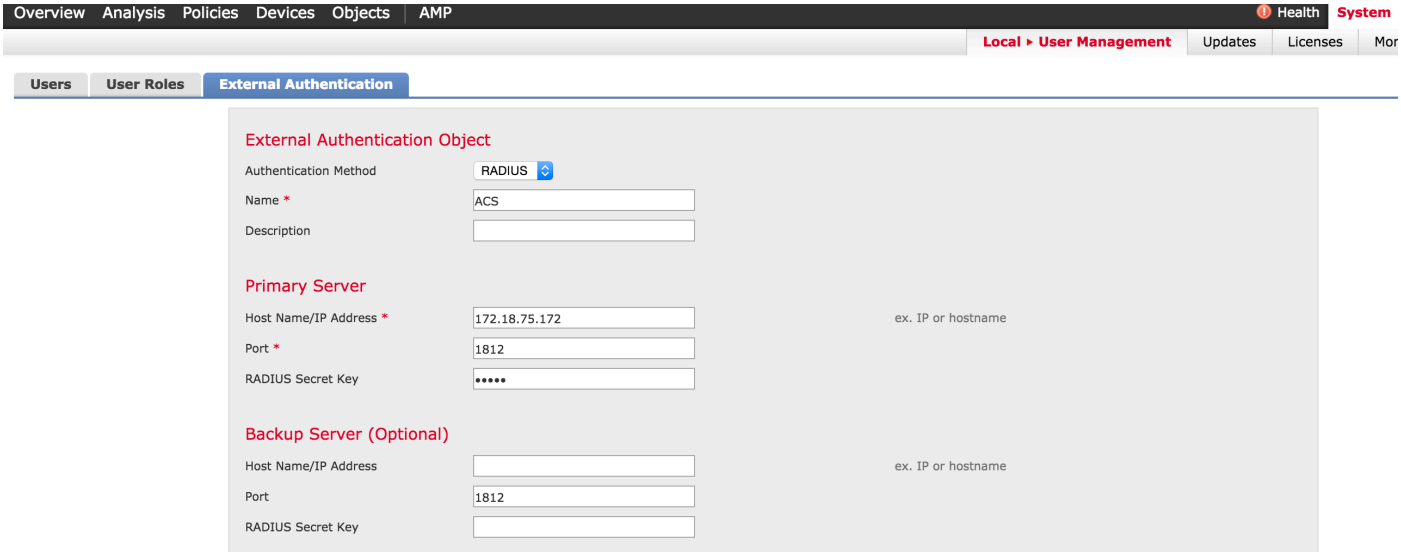
- Passare a Criteri di accesso > Servizi di accesso > Accesso di rete predefinito > Autorizzazione e configurare un nuovo criterio di autorizzazione per le sessioni di amministrazione di FireSight Management Center. Nell'esempio seguente viene utilizzata la condizione NDG:Device Type & Identity Group per stabilire una corrispondenza tra il tipo di dispositivo e il gruppo di identità configurati nei passaggi precedenti.
- Questo criterio viene quindi associato al profilo di autorizzazione dell'amministratore FireSight configurato in precedenza come Risultato. Fare clic su Invia.



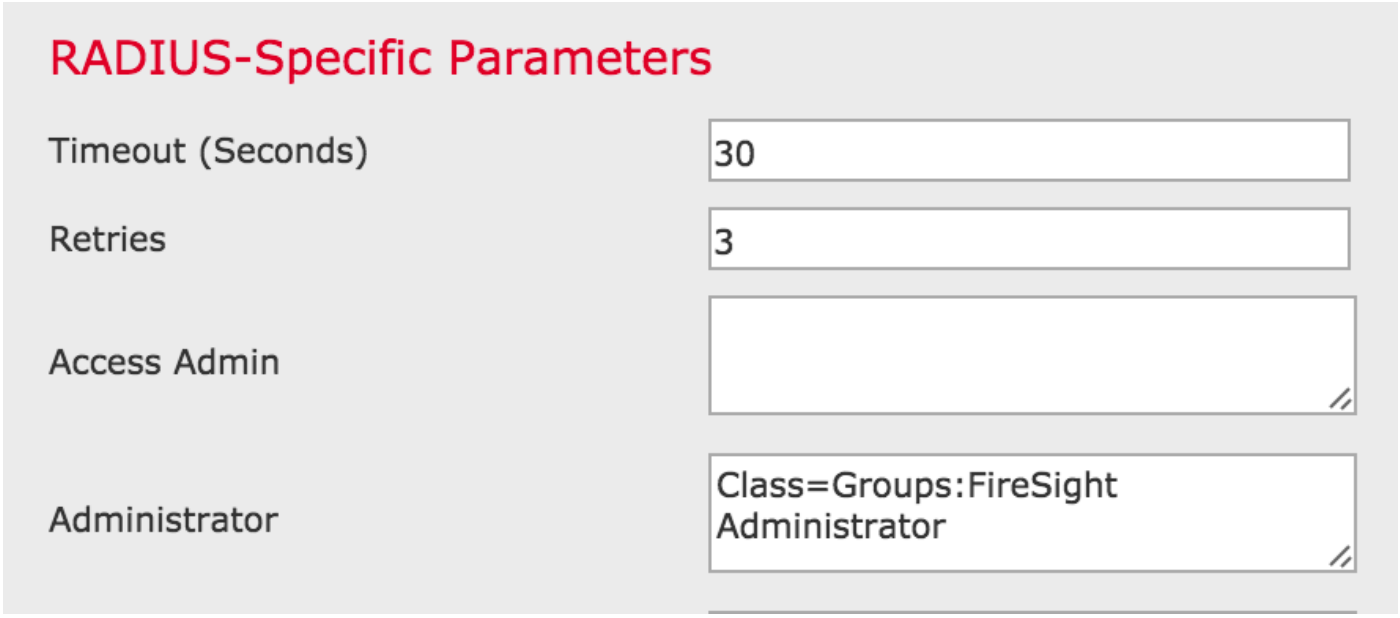
Configurazione di FireSight Management Center

Configurazione dei criteri di sistema di FireSight Manager

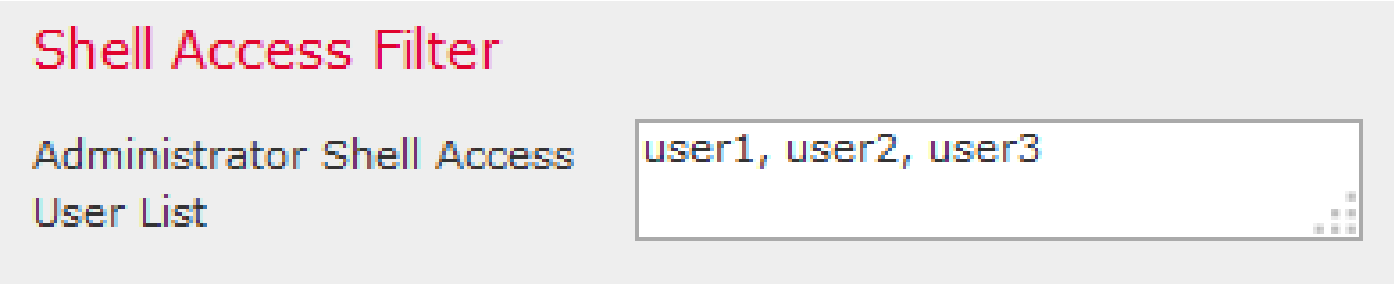
- Accedere a FireSIGHT MC e selezionare System > Local > User Management (Sistema > Locale > Gestione utenti). Fare clic sulla scheda Autenticazione esterna. Fare clic sul pulsante + Crea oggetto di autenticazione per aggiungere un nuovo server RADIUS per l'autenticazione/autorizzazione utente.
- Selezionare RADIUS per il metodo di autenticazione. Immettere un nome descrittivo per il server RADIUS. Immettere il nome host/indirizzo IP e la chiave privata RADIUS. La chiave segreta deve corrispondere alla chiave precedentemente configurata su ACS. Facoltativamente, immettere un nome host o un indirizzo IP del server ACS di backup, se esistente.



- Nella sezione Parametri specifici RADIUS, in questo esempio, il valore Class=Groups:FireSight Administrator viene mappato al gruppo FireSight Administrator. Questo è il valore restituito da ACS come parte di ACCESS-ACCEPT. Fare clic su Save (Salva) per salvare la configurazione o passare alla sezione Verify (Verifica) per verificare l'autenticazione con ACS.



- In Shell Access Filter, immettere un elenco di utenti separati da virgole per limitare le sessioni shell/SSH.



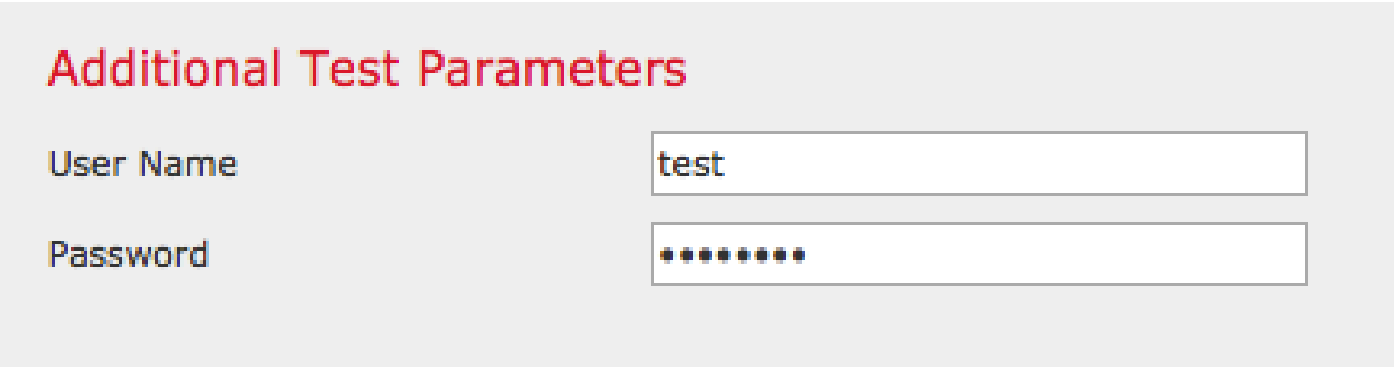
Abilita autenticazione esterna

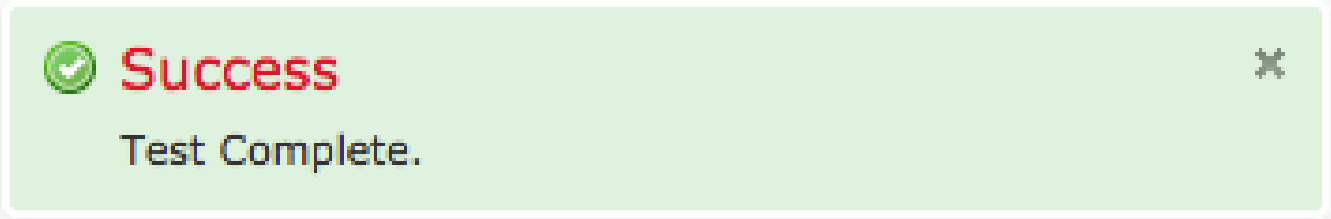
Infine, completare i passaggi seguenti per abilitare l'autenticazione esterna nel CCP:

1. Passare a Sistema > Locale > Criterio di sistema.
2. Selezionare External Authentication (Autenticazione esterna) nel pannello sinistro.
3. Modificare lo stato in Abilitato (disattivato per impostazione predefinita).
4. Abilitare il server RADIUS ACS aggiunto.
5. Salvare il criterio e applicarlo nuovamente all'accessorio.

Verifica

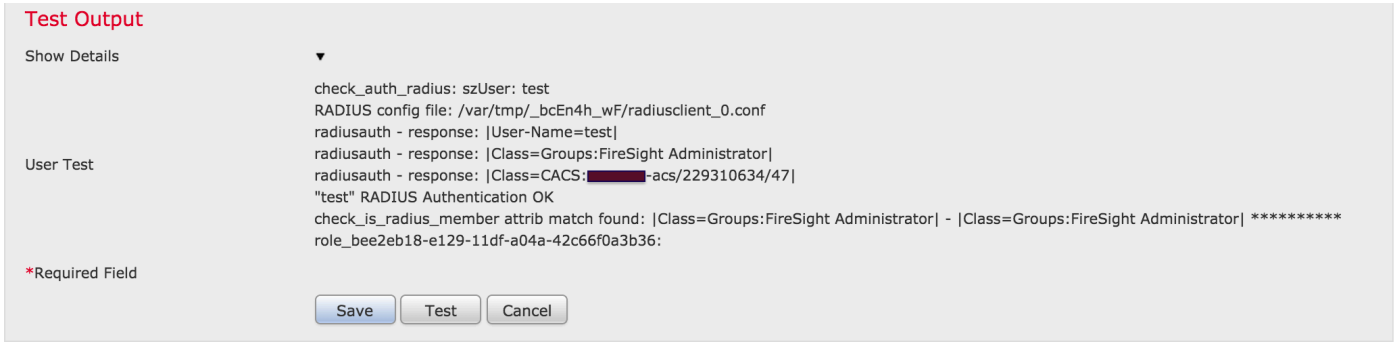
- Per verificare l'autenticazione dell'utente in base ad ACS, scorrere verso il basso fino alla sezione Parametri di test aggiuntivi e immettere un nome utente e una password per l'utente ACS. Fare clic su Test. Se il test viene superato, nella parte superiore della finestra del browser verrà visualizzato il messaggio verde Operazione riuscita: Test completato.





- Per visualizzare i risultati dell'autenticazione di test, andare alla sezione Output test e fare clic sulla freccia nera accanto a Mostra dettagli. Nello screenshot di esempio riportato di seguito, notare il messaggio "radiusauth - risposta: Valore |Class=Groups:FireSight

Administrator|" ricevuto da ACS. Deve corrispondere al valore Class associato al gruppo FireSight locale configurato nell'MC FireSIGHT precedente. Fare clic su Save (Salva).



Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).