

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 Sistema 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.

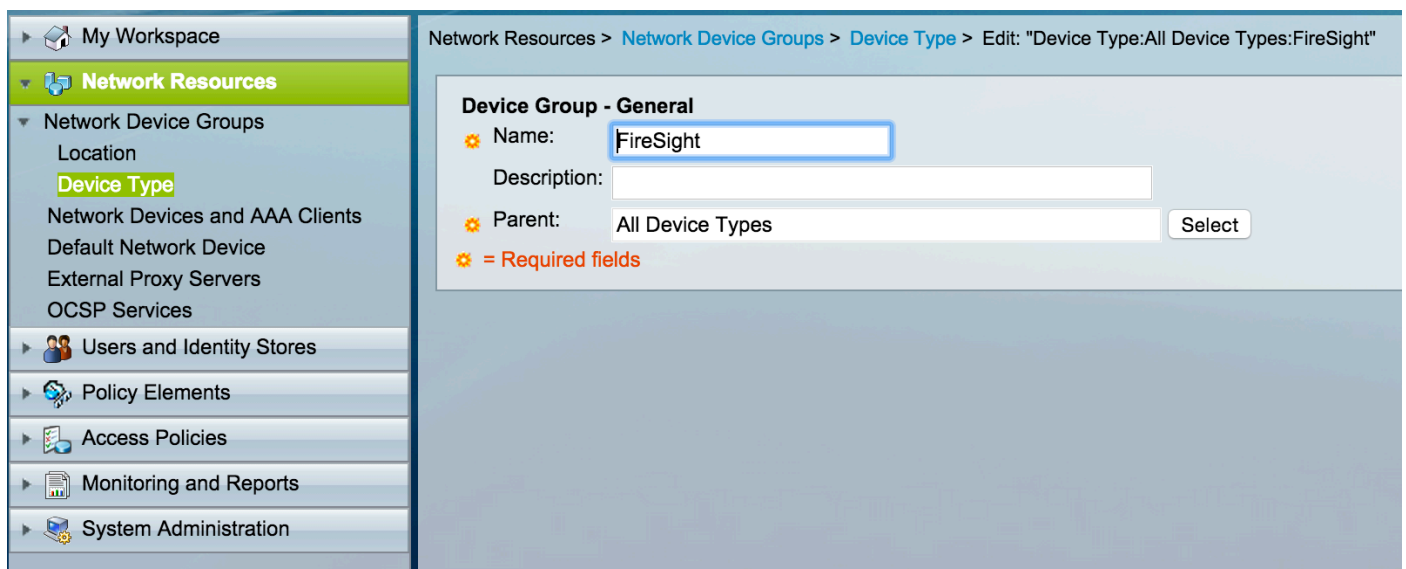
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Network Resources > Network Devices and AAA Clients > Edit: "FireSight Management Center"

Name: FireSight Management Center
Description:

Network Device Groups
Location: All Locations [Select]
Device Type: All Device Types:FireSight [Select]

IP Address
 Single IP Address IP Subnets IP Range(s)
 IP: 10.150.176.224

Authentication Options
 TACACS+ RADIUS
 Shared Secret: ***** [Show]
 CoA port: 1700
 Enable KeyWrap
 Key Encryption Key:
 Message Authenticator Code Key:
 Key Input Format: ASCII HEXADECIMAL

* = Required fields

Submit Cancel

- 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. Nota La stessa chiave segreta condivisa verrà utilizzata 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 richiedono 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**, 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.

My Workspace

Network Resources

Users and Identity Stores

Identity Groups

Internal Identity Stores

Users

Hosts

External Identity Stores

LDAP

Active Directory

RSA SecurID Token Servers

RADIUS Identity Servers

Certificate Authorities

Certificate Authentication Profile

Identity Store Sequences

Policy Elements

Access Policies

Monitoring and Reports

System Administration

Users and Identity Stores > Identity Groups > Edit: "IdentityGroup:All Groups:FireSight Administrator"

General

Name: FireSight Administrator

Description:

Parent: All Groups Select

= Required fields

Aggiunta di un utente locale ad ACS

- Passare alla sezione **Utenti e archivi identità**, configurare **gli utenti in 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**.

My Workspace

Network Resources

Users and Identity Stores

Identity Groups

Internal Identity Stores

Users

Hosts

External Identity Stores

LDAP

Active Directory

RSA SecurID Token Servers

RADIUS Identity Servers

Certificate Authorities

Certificate Authentication Profile

Identity Store Sequences

Policy Elements

Access Policies

Monitoring and Reports

System Administration

Users and Identity Stores > Internal Identity Stores > Users > Edit: "test"

General

Name: test Status: Enabled ⬇ ⬆

Description:

Identity Group: All Groups:FireSight Administrator Select

Email Address:

Account Disable

Disable Account if Date Exceeds: 2015-Nov-01 📅 (yyyy-Mmm-dd)

Disable account after 3 successive failed attempts

Password Hash

Enable Password Hash

Applicable only for Internal Users to store password as hash. Authentication types CHAP/MSCHAP will not work if this option is enabled. While disabling the hash, ensure that password is reconfigured using change password option.

Password Lifetime

Password Never Expired/Disabled: Overwrites user account blocking in case password expired/disabled

User Information

There are no additional identity attributes defined for user records

Creation/Modification Information

Date Created: Wed Sep 02 13:15:56 UTC 2015

Date Modified: Wed Sep 02 23:12:39 UTC 2015

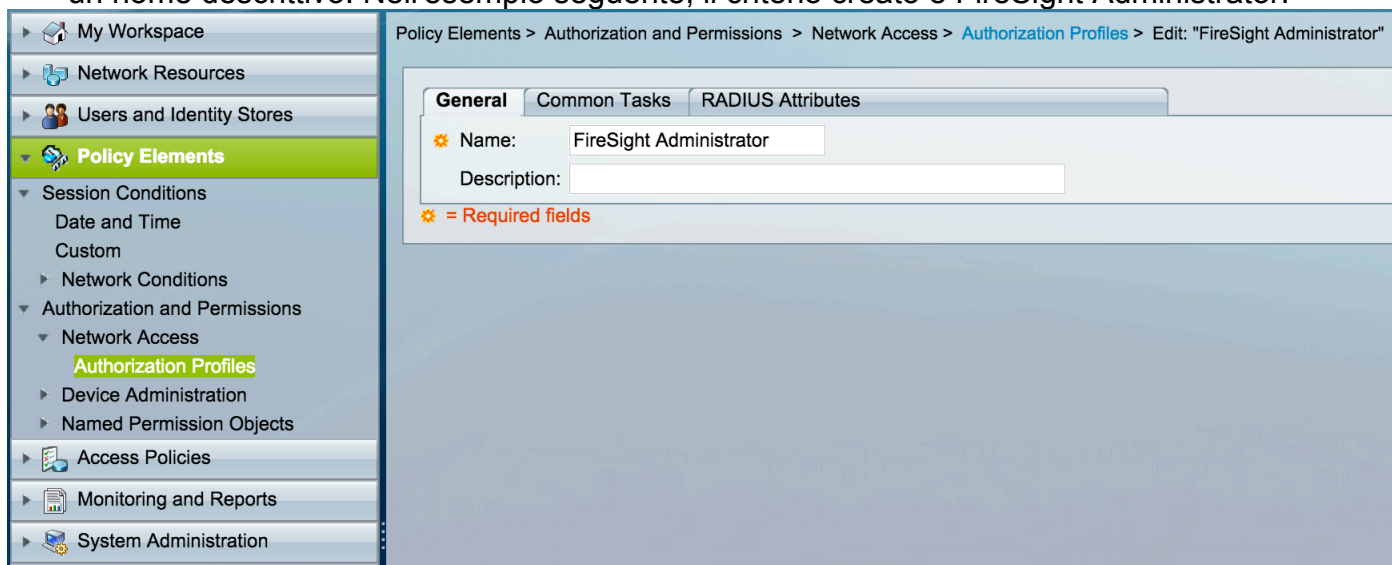
Date Enabled: Wed Sep 02 13:15:56 UTC 2015

= Required fields

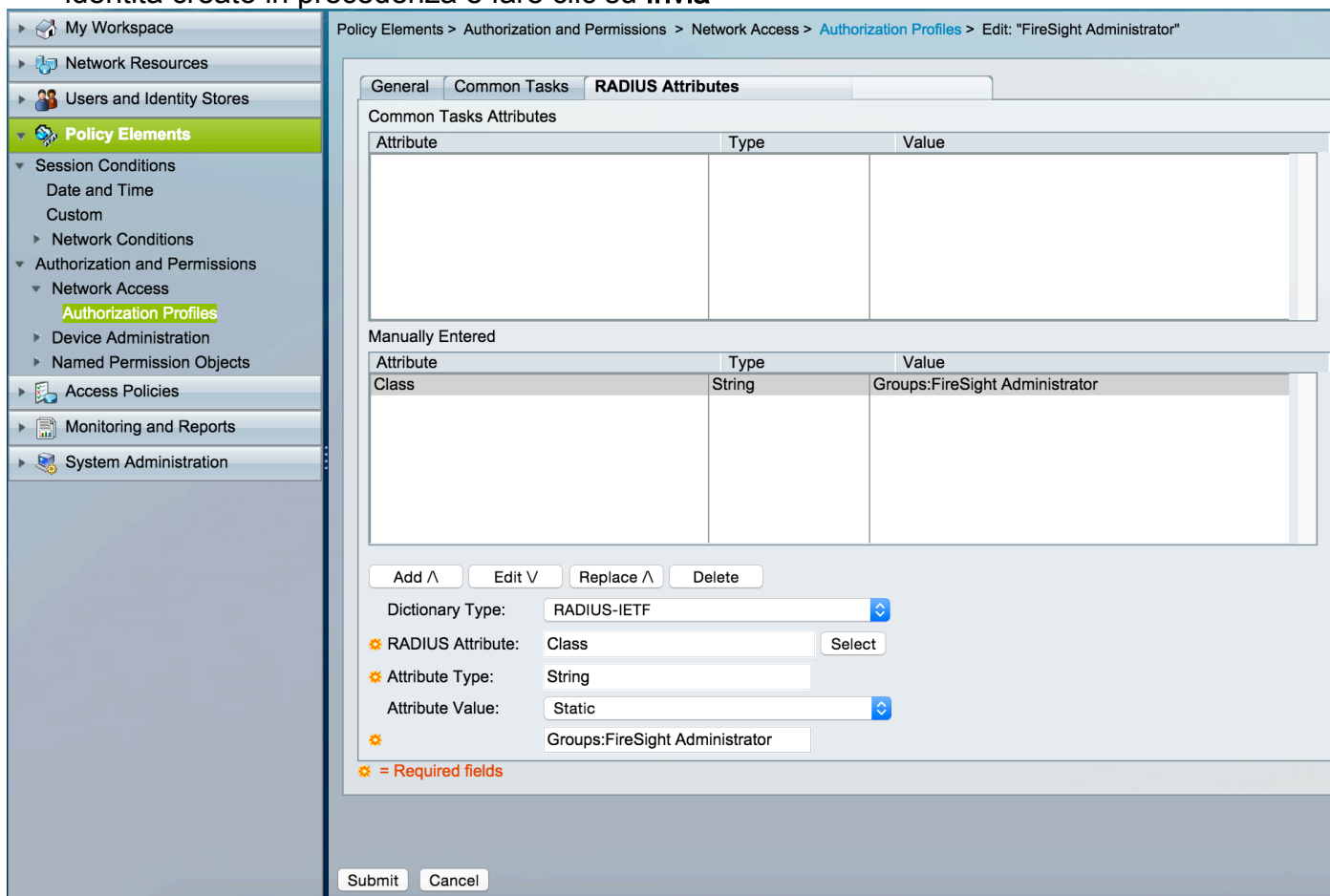
Submit Cancel

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 seguente, 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**



- Passa ad **Access Criteri > Servizi di accesso > Accesso alla rete predefinito > Autorizzazione** e configurare un nuovo criterio di autorizzazione per le sessioni di amministrazione di FireSight Management Center. Nell'esempio seguente viene utilizzato il **NDG:Tipo di dispositivo & Condizione del gruppo di identità** corrispondente al tipo di dispositivo e al 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**.

Access Policies > Access Services > Default Network Access > Authorization

Standard Policy | [Exception Policy](#)

Network Access Authorization Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	<input type="checkbox"/>	Status	Name	Conditions	Results	Hit Count	
				NDG:Device Type	Identity Group	Authorization Profiles	
1	<input type="checkbox"/>	Enabled	Rule-1	in All Device Types:FireSight	in All Groups:FireSight Administrator	FireSight Administrator	7

Configurazione di FireSight Management Center

Configurazione dei criteri di sistema di FireSight Manager

- Accedere a FireSIGHT MC e selezionare **Sistema > Locale > Gestione utente**. 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 configurata in precedenza in ACS. Facoltativamente, immettere un **nome host/indirizzo IP del server ACS di backup**, se esistente.

Overview Analysis Policies Devices Objects AMP Health System

Local > User Management Updates Licenses Mor

Users User Roles **External Authentication**

External Authentication Object

Authentication Method: RADIUS

Name *: ACS

Description:

Primary Server

Host Name/IP Address *: 172.18.75.172 ex. IP or hostname

Port *: 1812

RADIUS Secret Key: *****

Backup Server (Optional)

Host Name/IP Address: ex. IP or hostname

Port: 1812

RADIUS Secret Key:

- Sotto la **Parametri specifici di 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. Clic **Salva** per salvare la configurazione o passare alla sezione Verifica seguente per verificare l'autenticazione con ACS.

RADIUS-Specific Parameters

Timeout (Seconds)

Retries

Access Admin

Administrator

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

Shell Access Filter

Administrator Shell Access
User List

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 ha esito positivo, il risultato sarà un successo **verde**:
Messaggio Test Complete nella parte superiore della finestra del browser.

Additional Test Parameters

User Name

Password



Success



Test Complete.

- 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 la risposta "radiusauth: |Class=Groups:FireSight Administrator|" ricevuto da ACS. Questo valore deve corrispondere al valore Class associato al gruppo FireSight locale configurato nel MC FireSIGHT sopra riportato. Fare clic su **Salva**.

Test Output

Show Details



```
check_auth_radius: szUser: test
RADIUS config file: /var/tmp/_bcEn4h_wF/radiusclient_0.conf
radiusauth - response: |User-Name=test|
radiusauth - response: |Class=Groups:FireSight Administrator|
radiusauth - response: |Class=CACS:██████████-acs/229310634/47|
"test" RADIUS Authentication OK
check_is_radius_member attrib match found: |Class=Groups:FireSight Administrator| - |Class=Groups:FireSight Administrator| *****
role_bee2eb18-e129-11df-a04a-42c66f0a3b36:
```

*Required Field

Save

Test

Cancel