

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configuration](#)

[ACS 5.x configuration](#)

[Configuring Network Devices and Network Device Groups](#)

[Adding an Identity Group in ACS](#)

[Adding a Local User to ACS](#)

[Configuring ACS Policy](#)

[FireSight Management Center Configuration](#)

[FireSight Manager System Policy Configuration](#)

[Enable External Authentication](#)

[Verification](#)

[Related Cisco Support Community Discussions](#)

Introduction

This document describes the configuration steps required to integrate a Cisco FireSIGHT Management Center (FMC) or Firepower Managed Device with Cisco Secure Access Control System 5.x (ACS) for Remote Authentication Dial In User Service (RADIUS) user authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- FireSIGHT System and Managed Device initial configuration via GUI and/or shell
- Configuring authentication and authorization policies on ACS 5.x
- Basic RADIUS knowledge

Components Used

The information in this document is based on these software and hardware versions:

- Cisco Secure Access Control
- Cisco FireSight Manager Center 5.4.1

Above versions are the latest versions available currently. The feature is supported on all ACS 5.x versions and FMC 5.x versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is

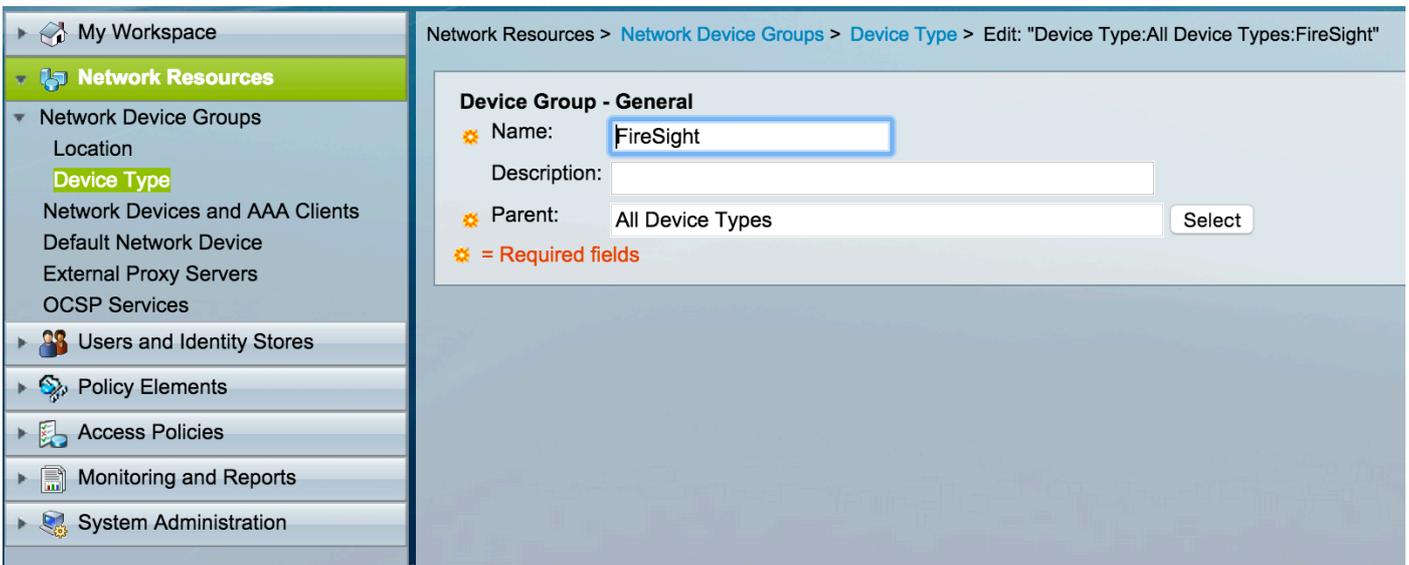
live, make sure that you understand the potential impact of any command.

Configuration

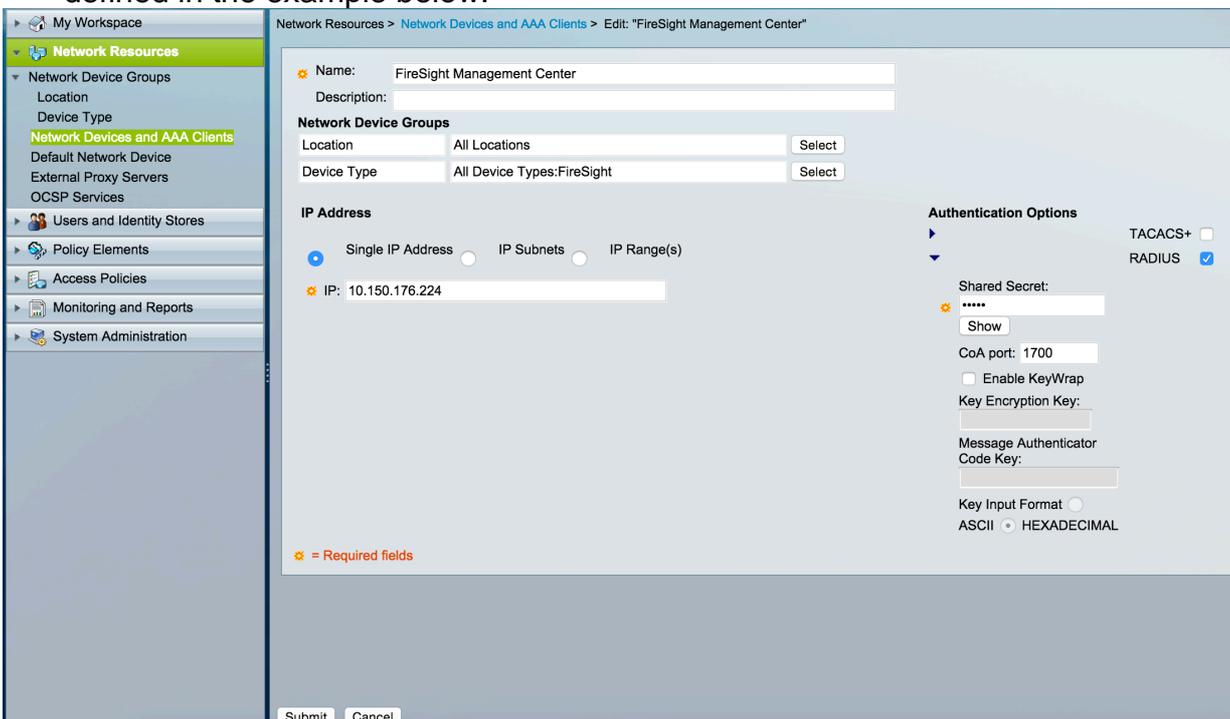
ACS 5.x configuration

Configuring Network Devices and Network Device Groups

- From the ACS GUI, navigate to **Network Device Group**, click on **Device Type** and create a Device Group. In the example screenshot that follows, the Device Type FireSight has been configured. This Device Type will be referenced in the authorization policy rule definition in a later step. Click **Save**.



- From the ACS GUI, navigate to **Network Device Group**, click on **Network Devices and AAA Clients** and add a device. Provide a descriptive name and device IP address. The FireSIGHT Management Center is defined in the example below.



- In the **Network Device Groups**, configure **Device Type** same as device group created in the step above.
- Check the box next to **Authentication Options**, select RADIUS check box and enter the **Shared secret** key that will be used for this NAD. Note the same shared secret key will be used again later when configuring the RADIUS server on the FireSIGHT Management Center. To review the plain text key value, click the **Show** button. Click **Submit**.
- Repeat the above steps for all FireSIGHT Management Centers and Managed Devices that will require RADIUS user authentication/authorization for GUI and/or shell access.

Adding an Identity Group in ACS

- Navigate to **Users and Identity Stores**, configure **Identity Group**. In this example, the identity group created is "FireSight Administrator". This group will be linked to the authorization profile defined in the steps below.

The screenshot displays the 'Users and Identity Stores' configuration page in the FireSIGHT Management Center. The left-hand navigation pane shows the hierarchy: My Workspace > Network Resources > Users and Identity Stores > Identity Groups. The main content area is titled 'Users and Identity Stores > Identity Groups > Edit: "IdentityGroup:All Groups:FireSight Administrator"'. Under the 'General' section, the 'Name' field is set to 'FireSight Administrator', the 'Description' field is empty, and the 'Parent' dropdown is set to 'All Groups'. A legend indicates that fields with a gear icon are required.

Adding a Local User to ACS

- Navigate to **Users and Identity Stores**, configure **Users** in **Internal** section. Enter required information for Local User creation, select the **Identity Group** created in above step and click **Submit**.

The screenshot shows the 'Users and Identity Stores' configuration page for a local user. The left-hand navigation pane shows the hierarchy: My Workspace > Network Resources > Users and Identity Stores > Internal Identity Stores > Users. The main content area is titled 'Users and Identity Stores > Internal Identity Stores > Users > Edit: "test"'. Under the 'General' section, the 'Name' field is set to 'test', the 'Status' is 'Enabled', and the 'Identity Group' dropdown is set to 'All Groups:FireSight Administrator'. The 'Account Disable' section has 'Disable account if Date Exceeds: 2015-Nov-01' and 'Disable account after: 3 successive failed attempts'. The 'Password Hash' section has 'Enable Password Hash' checked. The 'Password Lifetime' section has 'Password never Expires/Disabled' checked. The 'User Information' section shows 'There are no additional identity attributes defined for user records'. The 'Creation/Modification Information' section shows the user was created on Wed Sep 02 13:15:56 UTC 2015 and modified on Wed Sep 02 23:12:39 UTC 2015. A legend indicates that fields with a gear icon are required.

Configuring ACS Policy

- In the ACS GUI, navigate to **Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles**. Create a new authorization profile with a descriptive name. In the example below, policy created is FireSight Administrator.

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"

General Common Tasks RADIUS Attributes

Name: FireSight Administrator
Description:

= Required fields

- In the **RADIUS attributes** tab, add manual attribute for authorizing the Identity Group created above and Click **Submit**

Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit: "FireSight Administrator"

General Common Tasks **RADIUS Attributes**

Common Tasks Attributes

Attribute	Type	Value

Manually Entered

Attribute	Type	Value
Class	String	Groups:FireSight Administrator

Add ^ Edit v Replace ^ Delete

Dictionary Type: RADIUS-IETF

RADIUS Attribute: Class Select

Attribute Type: String

Attribute Value: Static

Groups:FireSight Administrator

= Required fields

Submit Cancel

- Navigate to **Access Policies > Access Services > Default Network Access > Authorization** and configure a new authorization policy for the FireSight Management Center administration sessions. The example below uses the **NDG:Device Type & Identity Group** condition to match the device type and identity group configured in the above steps.

- This policy is then associated with the FireSight Administrator authorization profile configured above as a **Result**. Click **Submit**.

The screenshot shows the configuration page for a Network Access Authorization Policy. The breadcrumb trail is: Access Policies > Access Services > Default Network Access > Authorization. The page title is "Standard Policy | Exception Policy". The policy name is "Network Access Authorization Policy". The filter is set to "Status" with a dropdown arrow, "Match if" is set to "Equals", and "Enabled" is selected. A "Clear Filter" button and a "Go" button with a dropdown arrow are also present. Below the filter is a table with the following data:

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

FireSight Management Center Configuration

FireSight Manager System Policy Configuration

- Login to the FireSIGHT MC and navigate to **System > Local > User Management**. Click on the **External Authentication** tab. Click the **+ Create Authentication Object** button to add a new RADIUS server for user authentication/authorization.
- Select **RADIUS** for the **Authentication Method**. Enter a descriptive name for the RADIUS server. Enter the **Host Name/IP Address** and **RADIUS Secret Key**. The secret key should match the key previously configured on ACS. Optionally enter a backup ACS server **Host Name/IP address** if one exists.

The screenshot shows the configuration page for an External Authentication Object. The breadcrumb trail is: Overview > Analysis > Policies > Devices > Objects > AMP > Local > User Management. The page title is "External Authentication Object". The authentication method is set to "RADIUS". The name is "ACS". The description is empty. The primary server configuration is as follows:

Field	Value	Notes
Host Name/IP Address *	172.18.75.172	ex. IP or hostname
Port *	1812	
RADIUS Secret Key	*****	

The backup server configuration is optional and currently empty:

Field	Value	Notes
Host Name/IP Address		ex. IP or hostname
Port	1812	
RADIUS Secret Key		

- Under the **RADIUS-Specific Parameters** section, in this example, the **Class=Groups:FireSight Administrator** value is mapped to the FireSight Administrator group. This is the value that ACS returns as part of the ACCESS-ACCEPT. Click **Save** to save the configuration or proceed to the Verify section below to test authentication with ACS.

The screenshot shows the RADIUS-Specific Parameters section. The parameters are as follows:

Parameter	Value
Timeout (Seconds)	30
Retries	3
Access Admin	
Administrator	Class=Groups:FireSight Administrator

- Under **Shell Access Filter**, enter a comma separated list of users to restrict shell/SSH sessions.

Enable External Authentication

Finally, complete these steps in order to enable external authentication on the FMC:

1. Navigate to **System > Local > System Policy**.
2. Select **External Authentication** on the left panel.
3. Change the *Status* to **Enabled** (disabled by default).
4. Enable the added ACS RADIUS server.
5. Save the policy and reapply the policy on the appliance.

Verification

- To test user authentication against ACS, scroll down to the **Additional Test Parameters** section and enter a username and password for the ACS user. Click **Test**. A successful test will result in a **green** Success: Test Complete message at the top of the browser window.



- To view the results of the test authentication, go to the **Test Output** section and click the **black** arrow next to **Show Details**. In the example screenshot below, note the "radiusauth - response: |Class=Groups:FireSight Administrator|" value received from ACS. This should match the Class value associated with the local FireSight group configured on the FireSIGHT MC above. Click **Save**.