

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**.

Network Resources > Network Device Groups > Device Type > Edit: "Device Type:All Device Types:FireSight"

Device Group - General

Name:

Description:

Parent:

= Required fields

- 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.

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

Name:

Description:

Network Device Groups

Location:

Device Type:

IP Address

☒ Single IP Address ☐ IP Subnets ☐ IP Range(s)

IP:

Authentication Options

TACACS+ ☐

RADIUS ☒

Shared Secret:

CoA port:

☐ Enable KeyWrap

Key Encryption Key:

Message Authenticator Code Key:

Key Input Format: ☐ ASCII ☐ HEXADECIMAL

= Required fields

- 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.

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

General

Name:

Description:

Parent:

= Required fields

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**.

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

General

Name: Status: Enabled

Description:

Identity Group:

Email:

Address:

Account Disable

☐ Disable Account if Date Exceeds: 2015-Nov-01 (yyyy-MM-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 enabling the hash, ensure that password is reconfigured using change password option.

Password Lifetime

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

User Information

There are no additional identity attributes defined for user records

Creation/Modification Information

Date: Wed Sep 02 13:15:58 UTC 2015

Created: Wed Sep 02 13:15:58 UTC 2015

Modified: Wed Sep 02 13:15:58 UTC 2015

Date: Wed Sep 02 13:15:58 UTC 2015

Enabled: ☐

= Required fields

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.

The screenshot shows the ACS GUI with the left sidebar expanded to 'Policy Elements' > 'Authorization and Permissions' > 'Network Access' > 'Authorization Profiles'. The main panel displays the configuration for the 'FireSight Administrator' profile. The 'General' tab is active, showing the 'Name' field set to 'FireSight Administrator' and an empty 'Description' field. A legend indicates that orange asterisks denote required fields.

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**

The screenshot shows the same ACS GUI with the 'RADIUS Attributes' tab selected. It displays two tables: 'Common Tasks Attributes' (empty) and 'Manually Entered' (containing one entry). Below the tables are controls for adding, editing, replacing, or deleting attributes, along with dropdowns for Dictionary Type, Attribute Type, and Attribute Value. The 'Manually Entered' table shows an attribute named 'Class' of type 'String' with the value 'Groups:FireSight Administrator'.

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 FireSight Management Center interface. On the left is a navigation pane with categories like My Workspace, Network Resources, Users and Identity Stores, Policy Elements, Access Policies, Monitoring and Reports, and System Administration. The 'Access Policies' section is expanded, showing 'Service Selection Rules', 'Default Device Admin', 'Default Network Access', 'Identity', 'Authorization' (highlighted), 'Max User Session Policy', 'Max Session User Settings', 'Max Session Group Settings', 'Max Login Failed Attempts Policy', and 'Max Login Failed Attempts Group Settings'. The main content area shows the 'Network Access Authorization Policy' configuration. It includes a breadcrumb trail: 'Access Policies > Access Services > Default Network Access > Authorization'. Below this, there are tabs for 'Standard Policy' and 'Exception Policy'. The 'Exception Policy' tab is active, showing a table of policies. The table has columns for 'Filter', 'Status', 'Name', 'Conditions', 'Results', and 'Hit Count'. A single policy is listed with the name 'Rule-1' and a hit count of 7. The 'Conditions' column shows 'NDG:Device Type' and 'Identity Group'. The 'Results' column shows 'Authorization Profiles' and 'FireSight Administrator'.

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 'External Authentication Object' configuration page in the FireSight Management Center. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'AMP'. The 'Objects' tab is active, and the 'Local > User Management' section is selected. The 'External Authentication' tab is also active. The main content area is titled 'External Authentication Object' and contains the following fields:

- Authentication Method:** A dropdown menu set to 'RADIUS'.
- Name *:** A text field containing 'ACS'.
- Description:** An empty text field.
- Primary Server:**
 - Host Name/IP Address *:** A text field containing '172.18.75.172'.
 - Port *:** A text field containing '1812'.
 - RADIUS Secret Key:** A text field containing '*****'.
- Backup Server (Optional):**
 - Host Name/IP Address:** An empty text field.
 - Port:** A text field containing '1812'.
 - RADIUS Secret Key:** An empty text field.

- 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 of the configuration page. It contains the following fields:

- Timeout (Seconds):** A text field containing '30'.
- Retries:** A text field containing '3'.
- Access Admin:** A text field containing 'Groups:FireSight Administrator'.
- Administrator:** A text field containing 'Groups:FireSight Administrator'.

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



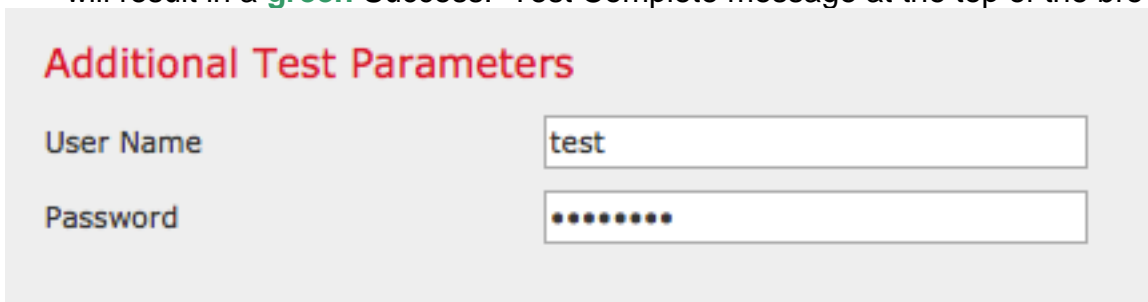
Enable External Authentication

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**.

