Configure APIC for Device Administration with ISE and TACACS+

Contents

Introduction

This document describes the procedure to integrate APIC with ISE for administrator users authentication with TACACS+ Protocol.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Application Policy Infrastructure Controller (APIC)
- Identity Services Engine (ISE)
- TACACS protocol

Components Used

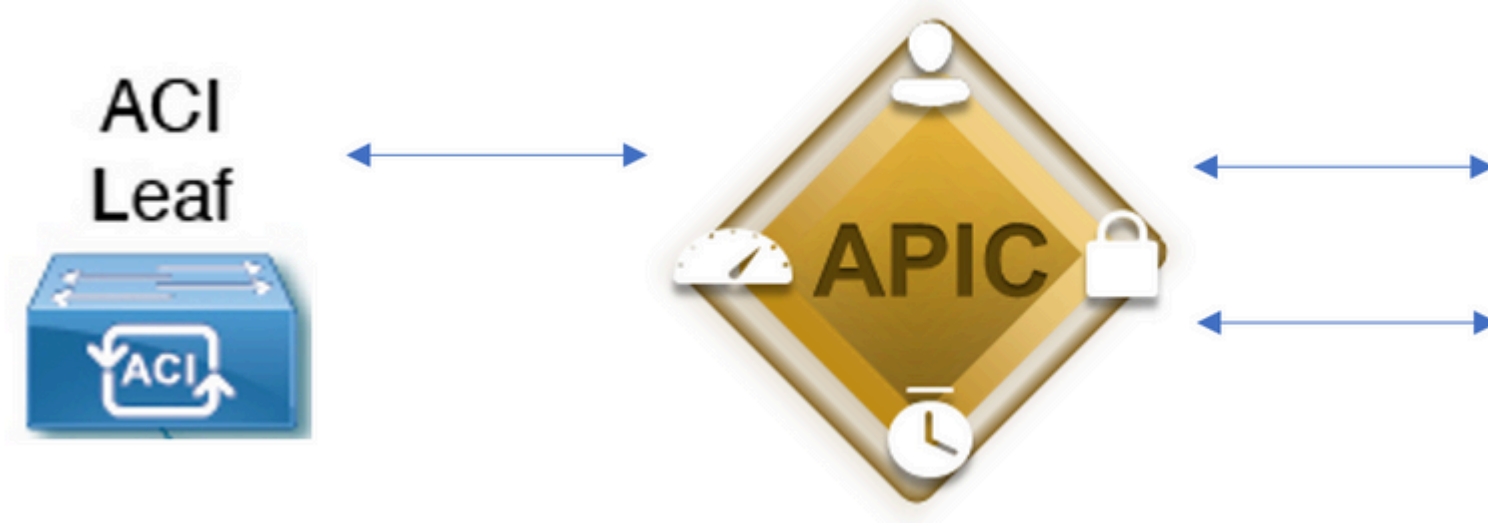
The information in this document is based on these software and hardware versions:

- APIC version 4.2(7u)
- ISE version 3.2 Patch 1

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, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Integration Diagram

Authentication Procedure

Step 1.Log into the APIC application with Admin User Credentials.

Step 2. The authentication process triggers and ISE validates the credentials locally or through Active Directory.

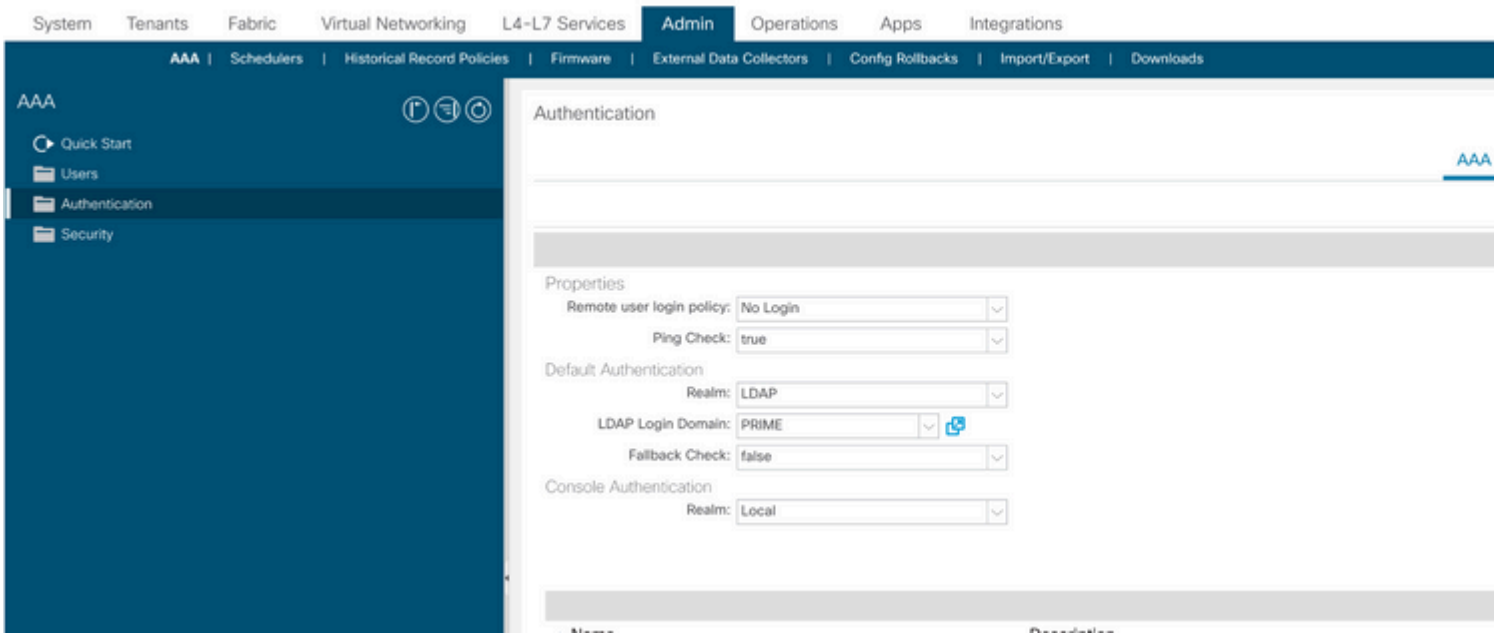
Step 3. Once authentication is successful, ISE sends a permit packet to authorize access to the APIC.

Step 4. ISE shows a successful authentication live log.

Note: APIC replicates TACACS+ configuration to leaf switches that are part of the fabric.

APIC Configuration

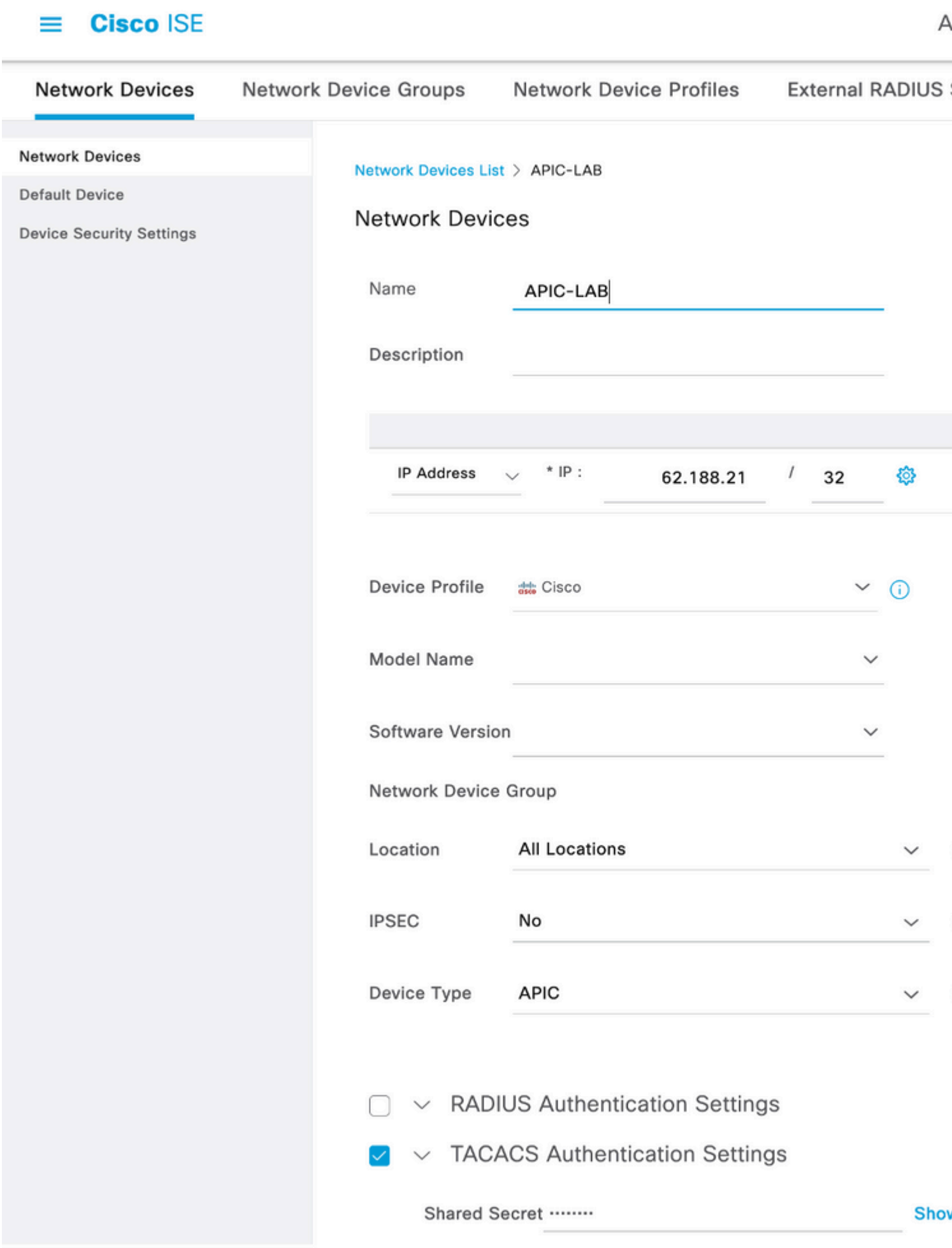
Step 1. Navigate to Admin > AAA > Authentication > AAA and choose + icon in order to create a new login domain.



APIC login admin configuration

Step 2. Define a name and realm for the new Login Domain and click + under Providers in order to create a new provider.

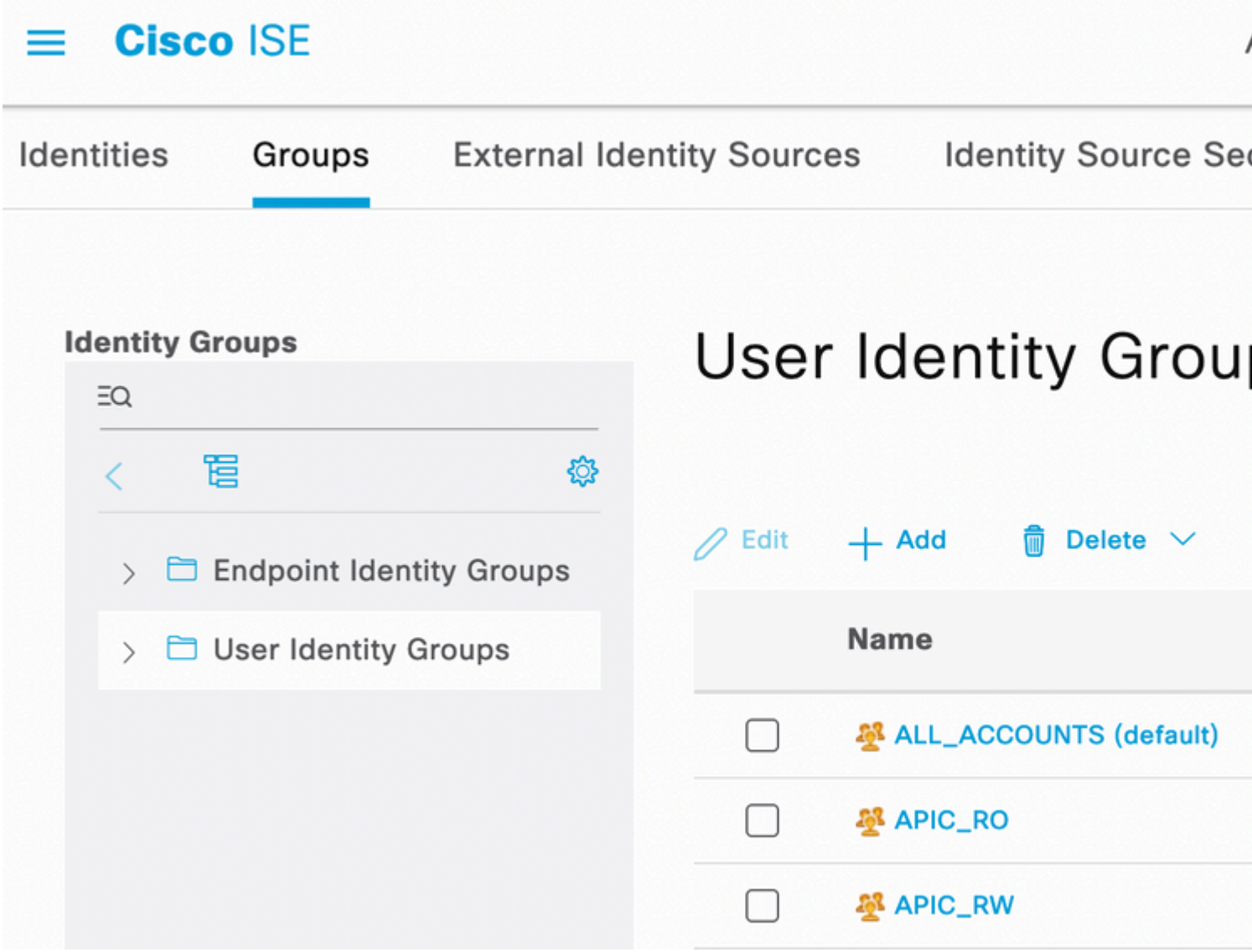
define APIC Name and IP address, choose APIC under Device Type and TACACS+ checkbox, and define the password used on APIC TACACS+ Provider configuration. Click Submit.



Repeat Step 1. and Step 2. for leaf switches.

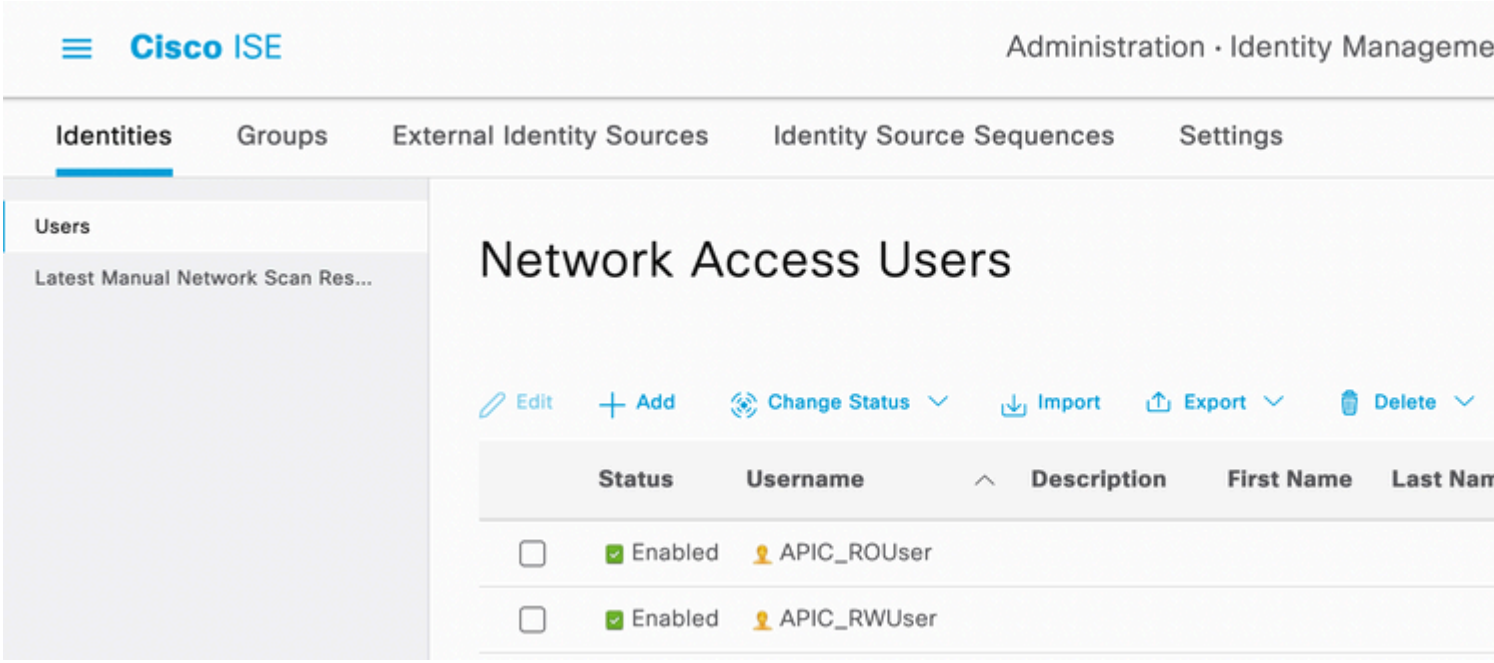
: This document includes both Internal users and AD Administrator groups as identity sources, however, the test is performed with the Identity Source of the internal users. The result is the same for AD groups.

Step 4. (Optional) Navigate to **â˜°** > Administration > Identity Management > Groups. Choose User Identity Groups and click Add. Create one group for **read only Admin** users and **Admin** users.



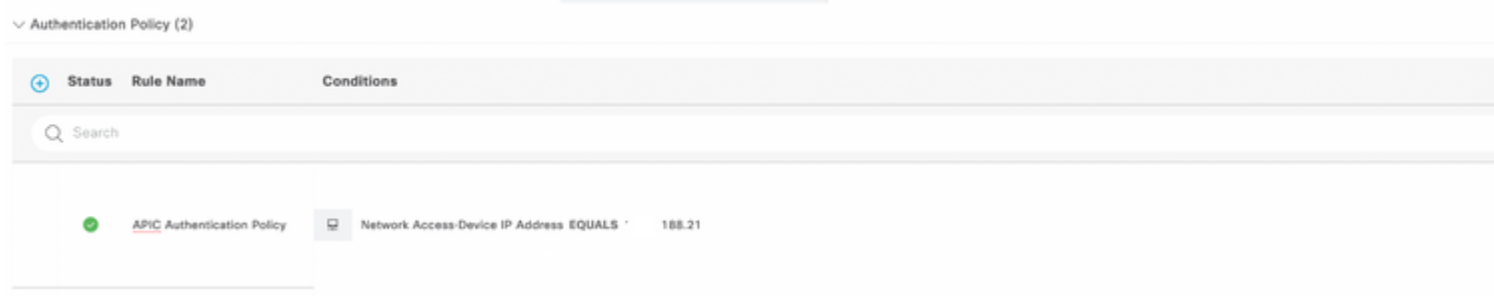
Identity Group

Step 5. (Optional) Navigate to **â˜°** > Administration > Identity Management > Identity. Click Add and create one Read Only Admin user and Admin user. Assign each user to each group created in Step 4.



Step 6. Navigate to **â˜°** > Administration > Identity Management > Identity Source Sequence. Choose Add, define a name, and choose AD Join Points and Internal Users Identity Source from the list.

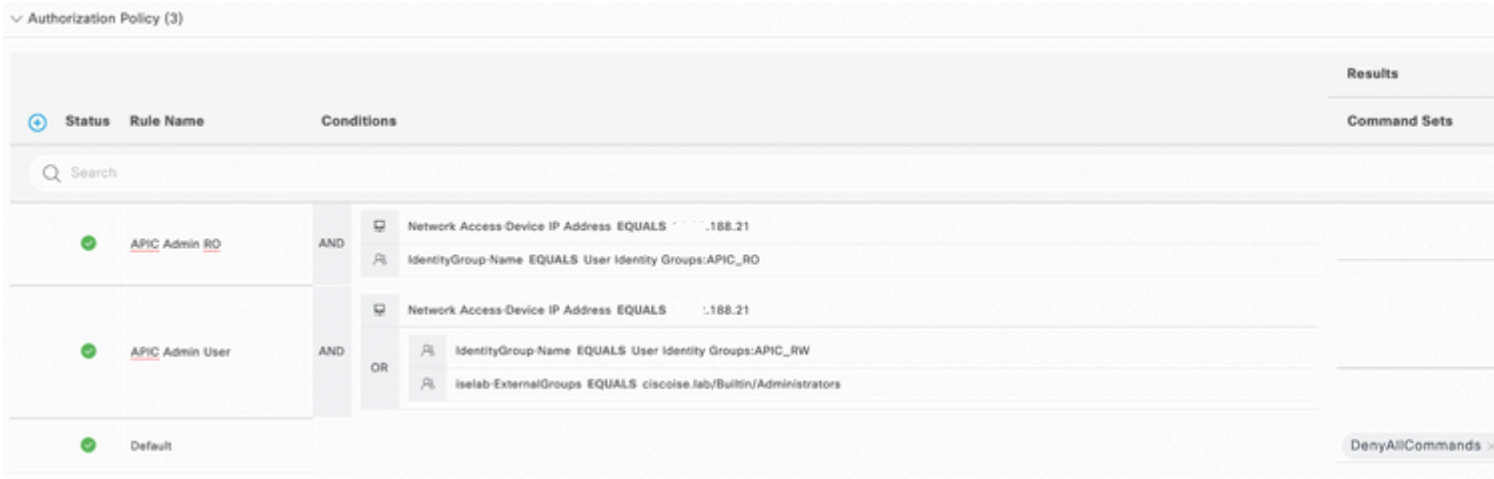
and create an authentication policy. Define a name and choose the device IP address as the condition. Then choose the Identity Source Sequence created in Step 6.



Authentication Policy

Note: Location or other attributes can be used as an Authentication condition.

Step 11. Create an Authorization profile for each Admin User type, define a name, and choose an internal user and/or AD user group as the condition. Additional conditions such as APIC can be used. Choose the proper shell profile on each authorization policy and click Save.



TACACS Authorization profile

Verify

Step 1. Log in on APIC UI with User Admin credentials. Choose the TACACS option from the list.