

# Autenticação externa AsyncOS com o Cisco Identity Service Engine (Radius)

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Diagrama de Rede](#)

[Etapa 1. Crie um Grupo de Identidades para Autenticação.](#)

[Etapa 2. Criar usuários locais para autenticação.](#)

[Etapa 3. Criar perfis de autorização.](#)

[Etapa 4. Criar uma Política de Autorização.](#)

[Verificar](#)

[Troubleshoot](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve a configuração necessária entre o Email Security Appliance (ESA) / Security Management Appliance (SMA) e o Cisco Identity Services Engine (ISE) para uma implementação bem-sucedida da autenticação externa com RADIUS.

## Prerequisites

### Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Autenticação, Autorização e Auditoria (AAA)
- Atributo CLASS RADIUS.
- Políticas de gerenciamento de identidade e autorização do Cisco ISE.
- Funções de usuário do Cisco ESA/SMA.

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco ISE 2.4
- Cisco ESA 13.5.1, 13.7.0
- Cisco SMA 13.6.2

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Produtos Relacionados

A versão fora das listadas na seção de componentes usados não foi testada.

## Informações de Apoio

Atributo Radius CLASS

Usado para relatório, é um valor arbitrário que o servidor RADIUS inclui em todos os pacotes de relatório.

O atributo de classe é configurado no ISE (RADIUS) por grupo.

Quando um usuário é considerado parte do grupo ISE/VPN que tem o atributo 25 vinculado a ele, o NAC aplica a política com base nas regras de mapeamento configuradas no servidor Identity Services Engine (ISE).

## Configurar

### Diagrama de Rede

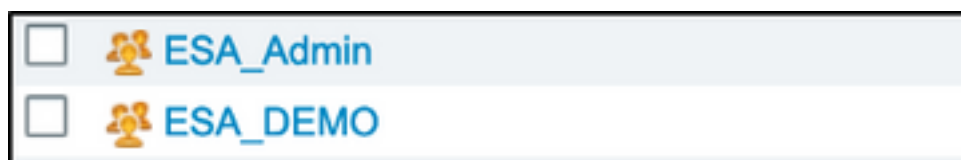


O Identity Service Engine aceita as solicitações de autenticação do ESA/SMA e as corresponde a uma identidade e grupo de usuários.

### Etapa 1. Crie um Grupo de Identidades para Autenticação.

Faça login no servidor ISE e crie um grupo de identidade:

Navegue até Administration->Identity Management->Groups->User Identity Group. Conforme mostrado na imagem.



**Note:** A Cisco recomenda um grupo de identidade no ISE para cada função ESA/SMA atribuída.

## Etapa 2. Criar usuários locais para autenticação.

Nesta etapa, crie novos usuários ou atribua usuários que já existem ao Grupo de Identidade criado na Etapa 1. Faça login no ISE e **navegue até Administration->Identity Management->Identities** e crie novos usuários ou atribua usuários no(s) grupo(s) criado(s). Conforme mostrado na imagem.

Network Access Users List > New Network Access User

**Network Access User**

\* Name

Status  Enabled

Email

**Passwords**

Password Type:

Password Re-Enter Password

\* Login Password   ⓘ

Enable Password   ⓘ

**User Information**

First Name

Last Name

**Account Options**

Description

Change password on next login

**Account Disable Policy**

Disable account if date exceeds

**User Groups**

Select an item

## Etapa 3. Criar perfis de autorização.

A autenticação RADIUS pode ser concluída com êxito sem perfis de autorização, no entanto, nenhuma função pode ser atribuída. Para concluir a configuração, **navegue para Policy->Policy->Elements->Results->Authorization->Authorization profile.**

**Note:** Crie um perfil de autorização por função a ser atribuída.

Authorization Profiles > **Aavega\_ESA\_Admin**

### Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

Service Template

Track Movement

Passive Identity Tracking

---

#### Common Tasks

Web Authentication (Local Web Auth)

Airespace ACL Name

ASA VPN

AVC Profile Name

---

#### Advanced Attributes Settings

=

**Note:** Certifique-se de usar o atributo de classe radius 25 e dê um nome. Esse nome deve corresponder à configuração em AsyncOS (ESA/SMA). Na Figura 3, Administradores é o nome do atributo CLASS.

#### Etapa 4. Criar uma Política de Autorização.

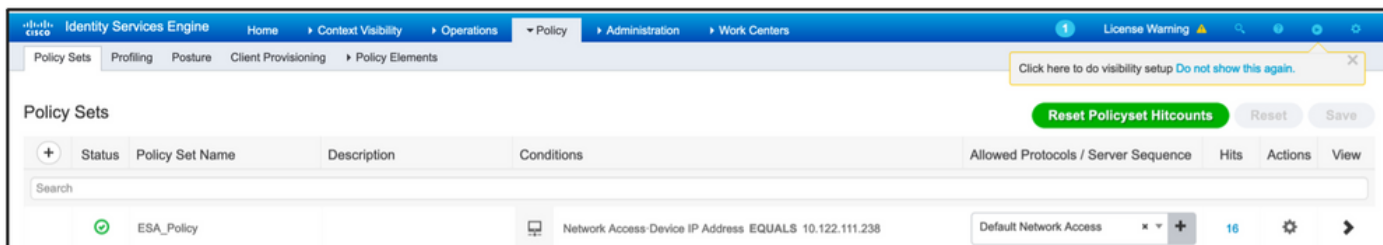
Esta última etapa permite que o servidor ISE identifique as tentativas de login do usuário e mapeie para o perfil de autorização correto.

No caso de uma autorização bem-sucedida, o ISE retorna um access-accept ao longo do valor CLASS definido no Perfil de autorização.

Navegue até Política > Conjuntos de políticas > Adicionar (+ símbolo)



Atribua um nome e selecione o símbolo de adição para adicionar as condições necessárias. Este ambiente de laboratório usa um RADIUS. NAS-IP-Address (Endereço IP NAS). Salve a nova política.



Para corresponder corretamente às solicitações de autorização, as condições devem ser

adicionadas. **Selecionar** ➔ e adicionar condições.

O ambiente de laboratório usa InternalUser-IdentityGroup e corresponde a cada perfil de autorização.

Authorization Policy (5)							
+	Status	Rule Name	Conditions	Results		Hits	Actions
				Profiles	Security Groups		
+	✓	ESA Monitor	InternalUser-IdentityGroup EQUALS User Identity Groups:ESA_Monitor	ESA_Monitors	Select from list	0	⚙️
+	✓	ESA HelpDesk	InternalUser-IdentityGroup EQUALS User Identity Groups:HelpDesk	ESA_admin	Select from list	0	⚙️

**Etapa 5. Ative a autenticação externa no AsyncOS ESA/SMA.**

Faça login no AsyncOS appliance (ESA/SMA/WSA). E navegue até **System Administration > Users > External Authentication > Enable External Authentication on ESA.**

### Edit External Authentication

**External Authentication Settings**

**Enable External Authentication**

Forneça estes valores:

- Nome de host do servidor RADIUS
- Porta
- shared secret
- Valor do tempo limite (em segundos)
- Protocolo de autenticação

Selecione **Mapear usuários autenticados externamente para várias funções locais**

(recomendado). Conforme mostrado na imagem.

## Edit External Authentication

### External Authentication Settings

**Enable External Authentication**

Authentication Type: **RADIUS**

RADIUS Server Information:

RADIUS Server Hostname	Port	Shared Secret	Timeout Value (in seconds)	Authentication protocol	Add Row
X.X.X.X	1812	.....	5	PAP	

External Authentication Cache Timeout:  seconds

Group Mapping:  Map externally authenticated users to multiple local roles. (recommended)

RADIUS CLASS Attribute	Role	Add Row
Administrators	Administrator	
Monitors	Operator	

*RADIUS CLASS attributes are case-sensitive.*

Map all externally authenticated users to the Administrator role.

**Note:** O atributo CLASS de RADIUS DEVE corresponder ao nome do atributo definido na Etapa 3 (em tarefas comuns mapeadas como ASA VPN).

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Faça login no dispositivo AsyncOS e confirme se o acesso foi concedido e se a função atribuída foi atribuída corretamente. Como mostrado na imagem com a função de usuário convidado.

Cisco C000V  
Email Security Virtual Appliance

Monitor

### My Dashboard

[Printable PDF](#)

**Attention** — You can customize this "My Dashboard" page by adding report modules from different reports. Some modules are added for you by default. The Overview page can be accessed from [Monitor > Overview](#).

#### System Overview

Overview > Status	Overview > Quarantines - Top 3 by Disk Usage (Policy and Virus)
System Status: Online Incoming Messages per hour: 0 Messages in Work Queue: 0	No quarantines are available

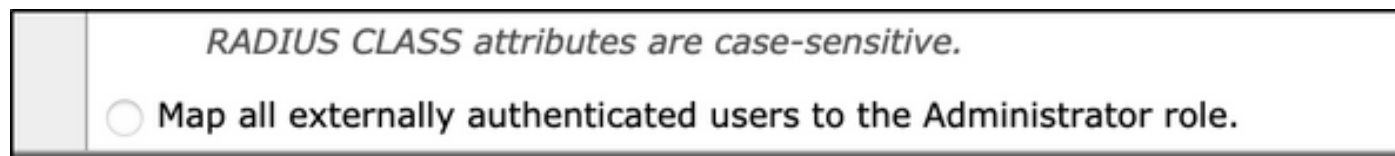
[System Status Details](#) [Local Quarantines](#)

# Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Se a tentativa de login não funcionar no ESA com a mensagem "Nome de usuário ou senha inválida". O problema pode estar na Política de autorização.

Faça login no ESA e, em Autenticação externa, selecione Mapear todos os usuários autenticados externamente para a função Administrador.



Envie e confirme as alterações. Execute uma nova tentativa de login. No caso de um login bem-sucedido, verifique duas vezes a configuração do perfil de autorização de rádio ISE (atributo CLASS 25) e da política de autorização.

## Informações Relacionadas

- [Guia do usuário do ISE 2.4](#)
- [Guia do usuário do AsyncOS](#)