

使用思科身份服务引擎(RADIUS)的AsyncOS外部身份验证

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[网络图](#)

[步骤1.创建身份验证组。](#)

[步骤2.创建本地用户进行身份验证。](#)

[步骤3.创建授权配置文件。](#)

[步骤4.创建授权策略。](#)

[验证](#)

[故障排除](#)

[相关信息](#)

简介

本文档介绍在邮件安全设备(ESA)/安全管理设备(SMA)和思科身份服务引擎(ISE)之间成功实施RADIUS外部身份验证所需的配置。

先决条件

要求

Cisco 建议您了解以下主题：

- 验证、授权和记帐 (AAA)
- RADIUS类属性。
- 思科ISE身份管理和授权策略。
- Cisco ESA/SMA用户角色。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科ISE 2.4
- 思科ESA 13.5.1、13.7.0
- 思科SMA 13.6.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

相关产品

未测试所用组件部分所列版本之外的版本。

背景信息

RADIUS类属性

对于记帐，RADIUS服务器在所有记帐数据包中包含的值是任意值。

类属性在ISE(RADIUS)中按组配置。

当用户被视为与其关联的属性为25的ISE/VPN组的一部分时，NAC根据身份服务引擎服务器(ISE)中配置的映射规则实施策略。

配置

网络图

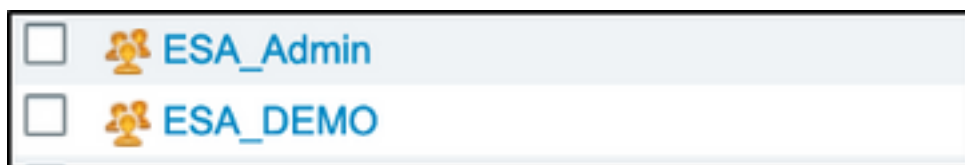


身份服务引擎接受来自ESA/SMA的身份验证请求，并将其与用户身份和组进行匹配。

步骤1.创建身份验证组。

登录ISE服务器并创建身份组：

导航至管理(Administration)->身份管理(Identity Management)->组(Groups)->用户身份组(User Identity Group)。如图所示。



注意：思科建议在ISE中为分配的每个ESA/SMA角色设置身份组。

步骤2.创建本地用户进行身份验证。

在此步骤中，创建新用户或分配已存在于我们在步骤1中创建的身份组的用户。请登录到ISE并导航至Administration -> Identity Management -> Identities，然后创建新用户或分配给您创建的组中的用户。如图所示。

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

User Groups

- ALL_ACCOUNTS (default)
- Anyconnect
- Dot1X
- Employee
- ESA_Admin
- ESA_DEMO
- ESA_Diego_Admins
- ESA_Monitor
- GROUP_ACCOUNTS (default)
- GuestType_Contractor (default)
- GuestType_Daily (default)
- GuestType_Weekly (default)

步骤3.创建授权配置文件。

RADIUS身份验证可以在没有授权配置文件的情况下成功完成，但是，不分配角色。要完成设置，请导航至策略(Policy)->策略元素(Policy Elements)->结果(Results)->授权(Authorization)->授权配置文件(Authorization profile)。

注意：为每个要分配的角色创建一个授权配置文件。

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**

=

注意：确保使用radius类属性25并指定名称。此名称必须与AsyncOS(ESA/SMA)上的配置匹配。从图3中，管理员是CLASS属性名称。

步骤4.创建授权策略。

最后一步允许ISE服务器识别用户登录尝试并映射到正确的授权配置文件。

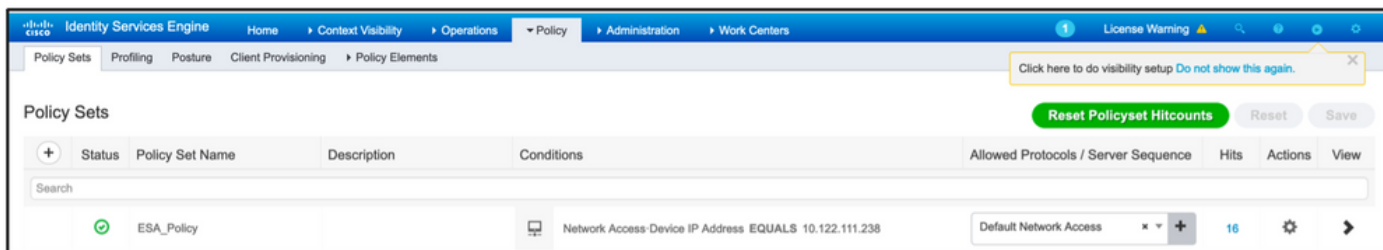
如果授权成功，ISE会返回访问接受，并将CLASS值定义到授权配置文件。

导航至策略>策略集>添加 (+符号)

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
		New Policy Set 1						

Select from list

指定名称并选择加号以添加所需条件。本实验环境使用Radius。NAS-IP-Address。保存新策略。



要正确匹配授权请求，必须添加条件。选择  图标并添加条件。

实验环境使用InternalUser-IdentityGroup并与每个授权配置文件匹配。

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

步骤5.在AsyncOS ESA/SMA中启用外部身份验证。

登录AsyncOS设备(ESA/SMA/WSA)。并导航至ESA上的系统管理>用户>外部身份验证>启用外部身份验证。

Edit External Authentication

External Authentication Settings

Enable External Authentication

Cancel Submit

提供以下值：

- RADIUS服务器主机名
- 端口
- 共享密钥
- 超时值（以秒为单位）
- 身份验证协议

选择将外部身份验证用户映射到多个本地角色（推荐）。如图所示。

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
<input type="text" value="X.X.X.X"/>	<input type="text" value="1812"/>	<input type="text" value="*****"/>	<input type="text" value="5"/>	PAP	

External Authentication Cache Timeout: seconds

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

RADIUS CLASS Attribute	Role	Add Row
<input type="text" value="Administrators"/>	Administrator	
<input type="text" value="Monitors"/>	Operator	

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

Cancel

Submit

注意：RADIUS CLASS属性必须与步骤3中定义的属性名称匹配（在映射为ASA VPN的常见任务下）。

验证

请登录到您的AsyncOS设备，确认已授予访问权限并已正确分配分配的角色。如具有访客用户角色的映像所示。

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

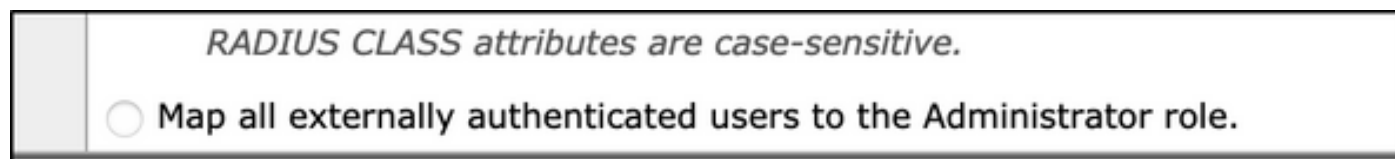
Overview > Status	Overview > Quarantines - Top 3 by Disk Usage (Policy and Virus)
System Status: Online Incoming Messages per hour: 0 Messages in Work Queue: 0	<i>No quarantines are available</i>

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

故障排除

如果登录尝试在ESA上失败，并显示消息“用户名或密码无效”。问题可能出在授权策略上。

登录ESA并从外部身份验证选择将所有外部身份验证用户映射到管理员角色。



提交并提交更改。尝试重新登录。如果登录成功，请双击ISE RADIUS授权配置文件 (CLASS属性 25) 和授权策略设置。

- [ISE 2.4](#)
- [AsyncOS](#)