

AsyncOS-Externe Authentifizierung mit Cisco Identity Service Engine (Radius)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfiguration](#)

[Netzwerkdiagramm](#)

[Schritt 1: Erstellen Sie eine Identitätsgruppe für die Authentifizierung.](#)

[Schritt 2: Erstellen Sie lokale Benutzer für die Authentifizierung.](#)

[Schritt 3: Erstellen von Autorisierungsprofilen.](#)

[Schritt 4: Erstellen einer Autorisierungsrichtlinie.](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einführung

Dieses Dokument beschreibt die Konfiguration, die zwischen der E-Mail Security Appliance (ESA)/Security Management Appliance (SMA) und der Cisco Identity Services Engine (ISE) für die erfolgreiche Implementierung einer externen Authentifizierung mit RADIUS erforderlich ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Authentifizierung, Autorisierung und Abrechnung (AAA)
- RADIUS CLASS-Attribut.
- Cisco ISE-Identitätsmanagement- und Autorisierungsrichtlinien.
- Cisco ESA/SMA-Benutzerrollen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco ISE 2.4
- Cisco ESA 13.5.1, 13.7.0

- Cisco SMA 13.6.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Verwandte Produkte

Die Version außerhalb der im Abschnitt "verwendete Komponenten" aufgelisteten wurde nicht getestet.

Hintergrundinformationen

Radius-CLASS-Attribut

Wird für Accounting verwendet, ist dies ein willkürlicher Wert, den der RADIUS-Server in allen Accounting-Paketen enthält.

Das Klassenattribut wird in ISE (RADIUS) auf Gruppenbasis konfiguriert.

Wenn ein Benutzer als Teil der ISE/VPN-Gruppe gilt, an die das Attribut 25 gebunden ist, setzt der NAC die Richtlinie auf der Grundlage der konfigurierten Zuordnungsregeln im Identity Services Engine-Server (ISE) durch.

Konfiguration

Netzwerkdiagramm





Identity Service Engine akzeptiert die Authentifizierungsanforderungen von ESA/SMA und vergleicht sie mit einer Benutzeridentität und -gruppe.

Schritt 1: Erstellen Sie eine Identitätsgruppe für die Authentifizierung.

Melden Sie sich beim ISE-Server an, und erstellen Sie eine Identitätsgruppe:

Navigieren Sie zu **Administration > Identity Management > Groups > User Identity Group**. Wie im Bild gezeigt.

<input type="checkbox"/>	 ESA_Admin
<input type="checkbox"/>	 ESA_DEMO

Hinweis: Cisco empfiehlt für jede zugewiesene ESA/SMA-Rolle eine Identitätsgruppe in der ISE.

Schritt 2: Erstellen Sie lokale Benutzer für die Authentifizierung.

In diesem Schritt erstellen Sie neue Benutzer oder weisen Sie Benutzer zu, die bereits der in Schritt 1 erstellten Identitätsgruppe vorhanden sind. Melden Sie sich bei der ISE an, **navigieren Sie zu Administration->Identity Management->Identities** und erstellen Sie entweder neue Benutzer oder weisen Sie Benutzer in der/den von Ihnen erstellten Gruppe(n) zu. Wie im Bild gezeigt.

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

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)

Schritt 3: Erstellen von Autorisierungsprofilen.

Die RADIUS-Authentifizierung kann ohne Autorisierungsprofile erfolgreich abgeschlossen werden, es können jedoch keine Rollen zugewiesen werden. Die vollständige Einrichtung finden Sie unter **Richtlinien->Richtlinienelemente->Ergebnisse->Autorisierungs->Autorisierungsprofil**.

Hinweis: Erstellen Sie pro zuzuweisender Rolle ein Autorisierungsprofil.

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

=

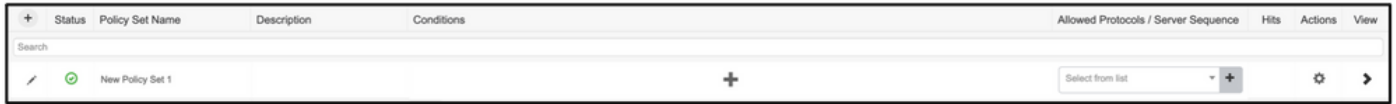
Hinweis: Stellen Sie sicher, dass Sie das radius class-Attribut 25 verwenden und einen Namen angeben. Dieser Name muss mit der Konfiguration auf AsyncOS (ESA/SMA) übereinstimmen. In Abbildung 3 ist "Administratoren" der CLASS-Attributname.

Schritt 4: Erstellen einer Autorisierungsrichtlinie.

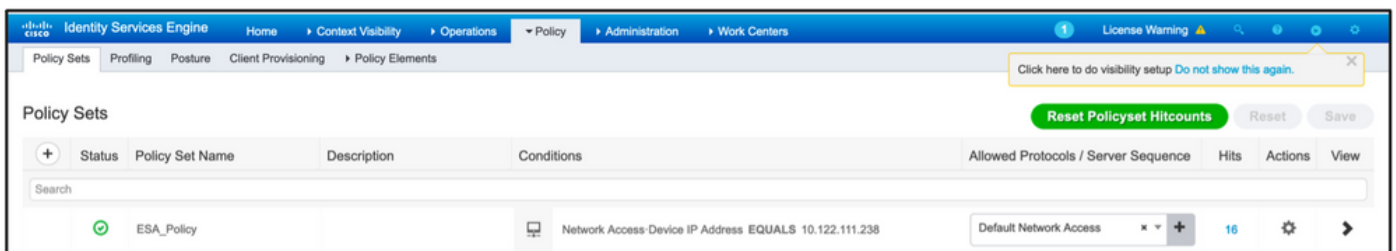
Im letzten Schritt kann der ISE-Server Anmeldeversuche von Benutzern identifizieren und dem richtigen Autorisierungsprofil zuordnen.

Im Falle einer erfolgreichen Autorisierung gibt die ISE einen access-accept-Wert zurück, der dem im Autorisierungsprofil definierten CLASS-Wert entspricht.

Navigieren Sie zu Richtlinien > Richtlinienansätze > Hinzufügen (+-Symbol).



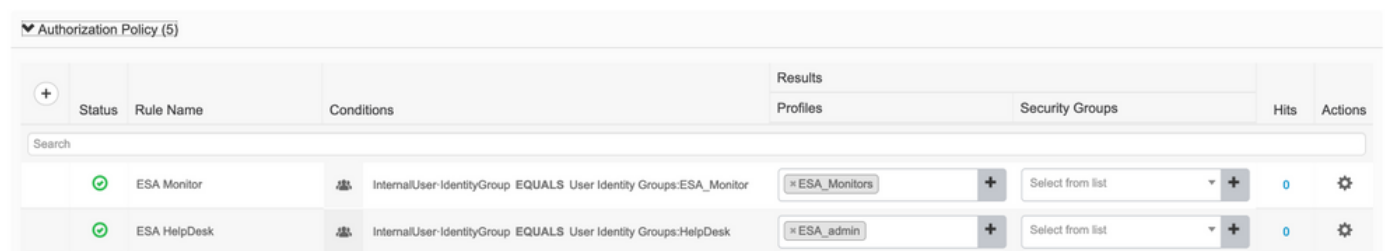
Weisen Sie einen Namen zu, und wählen Sie das Pluszeichen aus, um die erforderlichen Bedingungen hinzuzufügen. Diese Laborumgebung verwendet einen Radius. NAS-IP-Adresse Speichern Sie die neue Richtlinie.



Damit die Autorisierungsanfragen ordnungsgemäß abgeglichen werden, müssen die Bedingungen

hinzugefügt werden. **Auswählen**  und fügen Sie Bedingungen hinzu.

Die Laborumgebung verwendet InternalUser-IdentityGroup und stimmt mit den einzelnen Autorisierungsprofilen überein.



Schritt 5: Aktivieren Sie die externe Authentifizierung in AsyncOS ESA/SMA.

Melden Sie sich bei der AsyncOS-Appliance (ESA/SMA/WSA) an. Navigieren Sie zu **Systemverwaltung > Benutzer > Externe Authentifizierung > Externe Authentifizierung aktivieren** auf der ESA.

Edit External Authentication



Geben Sie folgende Werte an:

- Hostname des RADIUS-Servers
- Anschluss
- Gemeinsamer geheimer Schlüssel
- Timeoutwert (in Sekunden)
- Authentifizierungsprotokoll

Wählen Sie **Extern authentifizierte Benutzer mehreren lokalen Rollen zuordnen (empfohlen)**. Wie im Bild gezeigt.

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	
	<input type="text" value="X.X.X.X"/>	<input type="text" value="1812"/>	<input type="text" value="....."/>	<input type="text" value="5"/>	PAP	Add Row 🗑️

External Authentication Cache Timeout: seconds

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

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

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

Cancel
Submit

Hinweis: RADIUS CLASS-Attribut MUSS mit dem in Schritt 3 definierten Attributnamen übereinstimmen (unter häufigen Aufgaben, die ASA VPN zugeordnet sind).

Überprüfung

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Melden Sie sich bei Ihrer AsyncOS-Appliance an, und bestätigen Sie, dass der Zugriff gewährt und die zugewiesene Rolle ordnungsgemäß zugewiesen wurde. Wie im Bild mit der Rolle des Gastbenutzers dargestellt.

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

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

Wenn der Anmeldeversuch bei der ESA nicht funktioniert, erhalten Sie die Meldung "Ungültiger Benutzername oder Kennwort". Das Problem kann in der Autorisierungsrichtlinie vorliegen.

Melden Sie sich bei der ESA an, und wählen Sie bei der externen Authentifizierung die Option Alle extern authentifizierten Benutzer der Administratorrolle zuordnen aus.

RADIUS CLASS attributes are case-sensitive.

Map all externally authenticated users to the Administrator role.

Senden und bestätigen Sie die Änderungen. Führen Sie einen neuen Anmeldeversuch durch. Bei erfolgreicher Anmeldung überprüfen Sie das ISE Radius Authorization Profile (CLASS-Attribut 25) und die Einrichtung der Autorisierungsrichtlinie.

Zugehörige Informationen

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