

# AsyncOS externe verificatie met Cisco Identity Services Engine (RADIUS)

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Netwerkdigram](#)

[Stap 1. Maak een identiteitsgroep voor verificatie.](#)

[Stap 2. Maak lokale gebruikers voor verificatie.](#)

[Stap 3. Maak vergunningsprofielen.](#)

[Stap 4. Maak een vergunningenbeleid.](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

## Inleiding

Dit document beschrijft de configuratie die vereist is tussen de E-mail security applicatie (ESA)/security applicatie (SMA) en Cisco Identity Services Engine (ISE) voor een succesvolle implementatie van externe verificatie met RADIUS.

## Voorwaarden

### Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Verificatie, autorisatie en accounting (AAA)
- RADIUS-CLASS kenmerk.
- Cisco ISE-beleid voor identiteitsbeheer en autorisatie.
- Cisco ESA/SMA-gebruikersrollen.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

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

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Verwante producten

Versie buiten de genoemde onderdelen in het gebruikte deel werd niet getest.

## Achtergrondinformatie

RADIUS-CLASS kenmerken

Gebruikt voor accounting, is het een willekeurige waarde die de RADIUS server in alle accounting pakketten bevat.

De klasseneigenschap wordt in ISE (RADIUS) ingesteld per groep.

Wanneer een gebruiker geacht wordt deel uit te maken van de ISE/VPN-groep die 25 aan de groep heeft gekoppeld, dwingt NAC het beleid af op basis van de geconfigureerde mapping-regels in de server van Identity Services Engine (ISE).

## Configureren

### Netwerkdigram

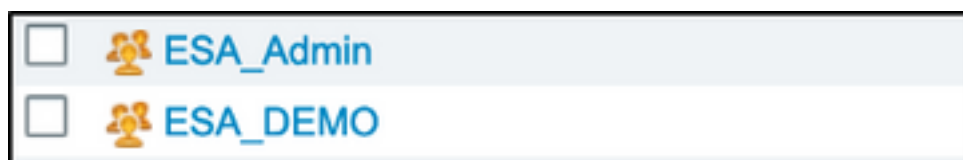


Identity Services Engine accepteert de verificatieverzoeken van ESA/SMA en past ze aan met een gebruikersidentiteit en -groep.

### Stap 1. Maak een identiteitsgroep voor verificatie.

Inloggen op de ISE-server en een identiteitsgroep maken:

Navigeren in naar **Administratie->identiteitsbeheer->Groepen->Gebruikersgroep**. Zoals in de afbeelding wordt weergegeven.



**Opmerking:** Cisco raadt een identiteitsgroep in ISE aan voor elke ESA/SMA toegewezen rol.

## Stap 2. Maak lokale gebruikers voor verificatie.

In deze stap kunt u nieuwe gebruikers maken of gebruikers toewijzen die al bestaan aan de Identity Group die we in Stap 1 hebben gemaakt. Meld u aan bij ISE en **navigeer naar Administration->Identity Management->Identificaties** en maakt u nieuwe gebruikers of toewijzen aan gebruikers in de groep(en) die u hebt gemaakt. Zoals in de afbeelding wordt weergegeven.

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)

## Stap 3. Maak vergunningsprofielen.

RADIUS-verificatie kan met succes worden voltooid zonder autorisatie profielen, maar er worden geen rollen toegewezen. Voor een volledige installatie kunt u navigeren naar **Policy->Policy-Elementen->Resultaten->autorisatie-profiel**.

**Opmerking:** Eén autorisatieprofiel per te toewijzen rol maken.

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

=

**Opmerking:** Zorg ervoor dat u de eigenschap Straalklasse 25 gebruikt en geef een naam. Deze naam moet overeenkomen met de configuratie op AsyncOS (ESA/SMA). Afbeelding 3 Administrateurs is de CLASS-attributen naam.

## Stap 4. Maak een vergunningenbeleid.

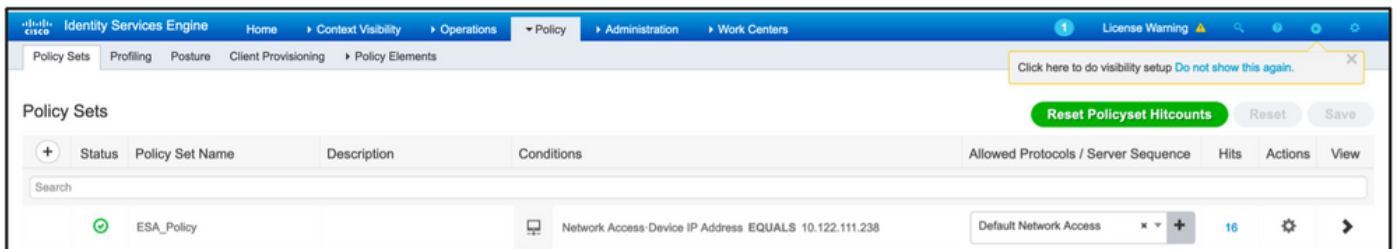
In deze laatste stap kan ISE-server het gebruikerslogbestand in pogingen identificeren en in kaart brengen naar het juiste machtigingsprofiel.

In het geval van een geslaagde vergunning, geeft ISE een toegangsaanvaarding terug volgens de CLASS-waarde die in het machtigingsprofiel is gedefinieerd.

## Navigeren in naar beleid > Beleidssets > Toevoegen (+ symbool)



Pas een naam aan en selecteer het plus-symbool om de gewenste voorwaarden toe te voegen. Deze labomgeving gebruikt een Straal. NAS-IP-Address. Bewaar het nieuwe beleid.



Om aan de vergunningsaanvragen te voldoen, moeten de voorwaarden worden toegevoegd.



**Selecteren** pictogram en voeg voorwaarden toe.

Lab-omgeving gebruikt interne gebruiker-IdentityGroup en overeenkomsten voor elk autorisatieprofiel.

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	⚙️		

## Stap 5. Schakel externe verificatie in AsyncOS ESA/SMA.

Log in op AsyncOS-apparaat (ESA/SMA/WSA). En **navigeer naar** **Systeembeheer > Gebruikers > Externe verificatie > Externe verificatie inschakelen voor verificatie op ESA.**

### Edit External Authentication

**External Authentication Settings**

**Enable External Authentication**

Cancel Submit

Geef deze waarden op:

- Hostnaam voor RADIUS-servers
- Port
- Gedeeld geheim
- Time-outwaarde (in seconden)
- Verificatieprotocol

Selecteer **Map extern geauthentiseerde gebruikers op meerdere lokale rollen (aanbevolen)**. Zoals in de afbeelding wordt weergegeven.

## 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	
	<span style="border: 1px solid #ccc; padding: 2px;">X.X.X.X</span>	1812	••••••••	5	PAP	
<a href="#" style="font-size: small;">Add Row</a>						

External Authentication Cache Timeout: 0 seconds

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

RADIUS CLASS Attribute	Role <span style="font-size: small;">?</span>	
Administrators	Administrator	
Monitors	Operator	
<a href="#" style="font-size: small;">Add Row</a>		

*RADIUS CLASS attributes are case-sensitive.*

Map all externally authenticated users to the Administrator role.

Cancel
Submit

**Opmerking:** RADIUS-CLASS kenmerk MOET overeenkomen met de eigenschap naam die in stap 3 is gedefinieerd (onder gemeenschappelijke taken die als ASA VPN zijn ingedeeld).

## Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Log in op uw AsyncOS-apparaat en controleer of er toegang is verleend en de toegewezen rol is correct toegewezen. Zoals in de afbeelding wordt weergegeven met de rol van de gastgebruiker.

Cisco C000V Email Security Virtual Appliance
Email Security Appliance is getting...

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](#).

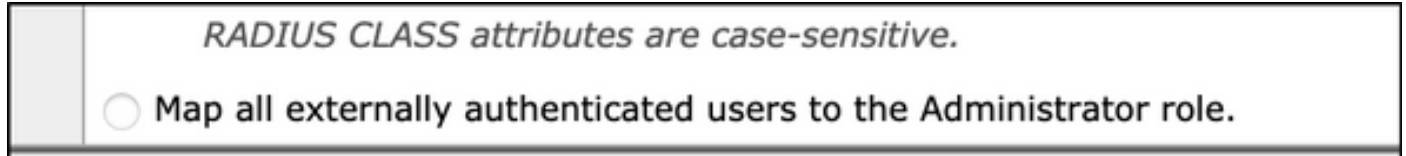
System Overview	
Overview > Status	Overview > Quarantines - Top 3 by Disk Usage (Policy and Virus)
<div style="display: flex; justify-content: space-between;"> <div> <p style="font-size: x-small;">System Status: Online</p> <p style="font-size: x-small;">Incoming Messages per hour: 0</p> <p style="font-size: x-small;">Messages in Work Queue: 0</p> </div> <div style="font-size: x-small;">No quarantines are available</div> </div>	
<a href="#">System Status Details</a>	<a href="#">Local Quarantines</a>

## Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Indien loggen in poging niet werkt aan ESA met het bericht "Ongeldige gebruikersnaam of wachtwoord". De kwestie zou op het vergunningenbeleid kunnen liggen.

Meld u aan bij ESA en selecteer vanuit Externe Verificatie Alle extern geauthentiseerde gebruikers naar de Administrator-rol in kaart.



Breng de wijzigingen aan en bevestig ze. Doe een nieuwe inlogpoging. In het geval van een succesvol inlogbestand, dubbelcontrole ISE Radius Authorization Profile (CLASS attribuut 25) en Authorization Policy Setup.

Gerelateerde informatie

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