

Ondersteunt ISE mijn netwerktoegangsapparaat?

Inhoud

[Inleiding](#)

[ISE ondersteunt de RADIUS- en TACACS-protocollen](#)

[ISE-compatibiliteitshandleidingen](#)

[Network Device Capabilities voor ISE](#)

[Hoe weet je wat de mogelijkheden van je netwerkkaparamen zijn?](#)

[Kan uw hardware of software niet zien in de ISE-compatibiliteitsgids](#)

[Profielen van ISE Network Access Device \(NAD\)](#)

[Verificatie-VLAN-ondersteuning](#)

[Problemen met het gebruik van verificatie-VLAN's](#)

Inleiding

In dit document wordt beschreven hoe u de compatibiliteit van de Cisco Identity Services Engine (ISE) met uw Network Access Device (NAD) kunt controleren.

ISE ondersteunt de RADIUS- en TACACS-protocollen

Als uw netwerkkapparaat verzoeken voor toegangscontrole kan indienen met behulp van de standaard RADIUS- en TACACS-protocollen, kan ISE deze ondersteunen!

ISE ondersteunt RADIUS om toegangscontrole uit te voeren met alle handhavingsmechanismen die de hardware en software van het netwerkkapparaat ondersteunt.

De mogelijkheden van een bepaald netwerkkapparaat voor poortgebaseerde toegangscontrole met de [IEEE 802.1X-standaard](#) zijn software - en vaak hardwareafhankelijk! Het eenvoudigweg ondersteunen van RADIUS betekent niet dat het netwerkkapparaat veel nuttige handhavingsmogelijkheden ondersteunt, zoals [MAC Authentication Bypass \(MAB\)](#), [RADIUS Change of Authorization \(CoA\)](#) [RFC-5176], Layer-3/4 Access Control Lists (ACL's), domein-gebaseerde ACL's, URL-redirectie of software-gedefinieerde segmentatie met [Cisco TrustSec](#). U kunt u niet altijd vertellen waartoe een bepaald netwerkkapparaat in staat is en u moet dat mogelijk onderzoeken met de leverancier of het productteam.

Wanneer mensen vragen; Ondersteunt ISE mijn netwerkkapparaat? Wat ze bedoelen is: kan ISE me al deze moderne toegangscontrole mogelijkheden geven, zelfs met deze oude, goedkope switch?

Voor deze oudere en goedkopere switches biedt ISE functies zoals [SNMP CoA en Authentication VLAN](#) om een aantal vergelijkbare mogelijkheden te bieden die nodig zijn om de stroom van

gasten, BYOD en houding te verwerken.

ISE-compatibiliteitshandleidingen

Controleer altijd de [ISE Compatibility Guides](#) om te zien wat ons Quality Assurance (QA)-team heeft gevalideerd voor elke ISE-release.

Network Device Capabilities voor ISE

Dit zijn moderne netwerkkaparaatfuncties die doorgaans nodig zijn om ISE-mogelijkheden te bieden:

ISE-capaciteit	Kenmerken van netwerkkaparaaten
AAA	802.1x, MAB, VLAN-toewijzing, downloadbare ACL's
profilering	RADIUS CoA en profileringssondes
BYOD	RADIUS CoA, URL-omleiding + sessie-ID
gast	RADIUS CoA, URL-omleiding + sessie-ID, lokale webauth
URL van herkomst gast	RADIUS CoA, URL-omleiding + sessie-ID, lokale webauth
houding	RADIUS CoA, URL-omleiding + sessie-ID
MDM	RADIUS CoA, URL-omleiding + sessie-ID
TrustSec	SGT-classificatie

Dus wat doe je als je netwerkkaparaat niet alle functies voor de ISE-mogelijkheid heeft?

Maak een NAD-profiel (Network Access Device).

Hoe weet je wat de mogelijkheden van je netwerkkaparaaten zijn?

De mogelijkheden voor gevalideerde hardware- en softwarecombinaties zijn gemakkelijk gedocumenteerd in onze [ISE Compatibility Guides](#). Voor alle anderen moet u dit onderzoeken op de websites van de leveranciers, productdocumentatie, forums, enz. Soms moet je gewoon in je lab spelen om erachter te komen wat wel en wat niet werkt en [een netwerkkaparaatprofiel maken](#) voor de verschillende combinaties van mogelijkheden.

Kan uw hardware of software niet zien in de ISE-compatibiliteitsgids

Het feit dat een hardwaremodel of softwarerelease niet expliciet wordt vermeld, betekent niet dat het niet zal werken - alleen dat u het niet hebt gevalideerd met ISE! In het gedeelte Ondersteunde netwerktoegangsapparaten van de [ISE-compatibiliteitsgidsen](#) staat dat ISE RADIUS ondersteunt, ongeacht de leverancier of het model:

Cisco ISE ondersteunt interoperabiliteit met elk Cisco- of niet-Cisco RADIUS-clientnetwerktoegangsapparaat (NAD) dat gemeenschappelijk RADIUS-gedrag (vergelijkbaar

met Cisco IOS 12.x) implementeert voor op standaarden gebaseerde verificatie.

ISE ondersteunt protocolstandaarden zoals [RADIUS](#), de bijbehorende [RFC-standaarden](#), en [TACACS+](#). Als uw netwerkapparaat RADIUS en/of TACACS+ ondersteunt, kan ISE het ondersteunen!

Er zijn veel redenen waarom zowel Cisco- als niet-Cisco-apparaten mogelijk niet worden vermeld:

- Ons QA-team kan het zich niet veroorloven om elke afzonderlijke hardware- en softwarecombinatie met elke ISE-release te testen.
- Nieuwe hardwareplatforms moeten worden aangeschaft en getest, wat meestal binnen 6-9 maanden na de hardwarerelease gebeurt.
- Elk model van een hardwarefamilie wordt niet gevalideerd - er wordt één model gekozen en vervolgens wordt het gebruikt om de hardwarefamilie weer te geven.
- Elke softwarerelease is niet gevalideerd - een vrijgegeven softwareversie die door het platformteam wordt aanbevolen, wordt gekozen, een paar maanden voor de daadwerkelijke ISE-release voor QA-validatieplanning.
- Oudere ISE-releases worden niet getest met nieuwere Network Device-software, maar moeten nog steeds voldoen aan de normen.

Wat u precies met ISE kunt doen, wordt vervolgens bepaald door de hardware- en softwaremogelijkheden van uw netwerkapparaat. Het wordt altijd aanbevolen dat u uw netwerkhardware en -software in uw lab probeert met ISE voordat deze wordt geïmplementeerd in de productie, zodat u erop kunt vertrouwen dat deze zich gedraagt zoals verwacht.

Profielen van ISE Network Access Device (NAD)

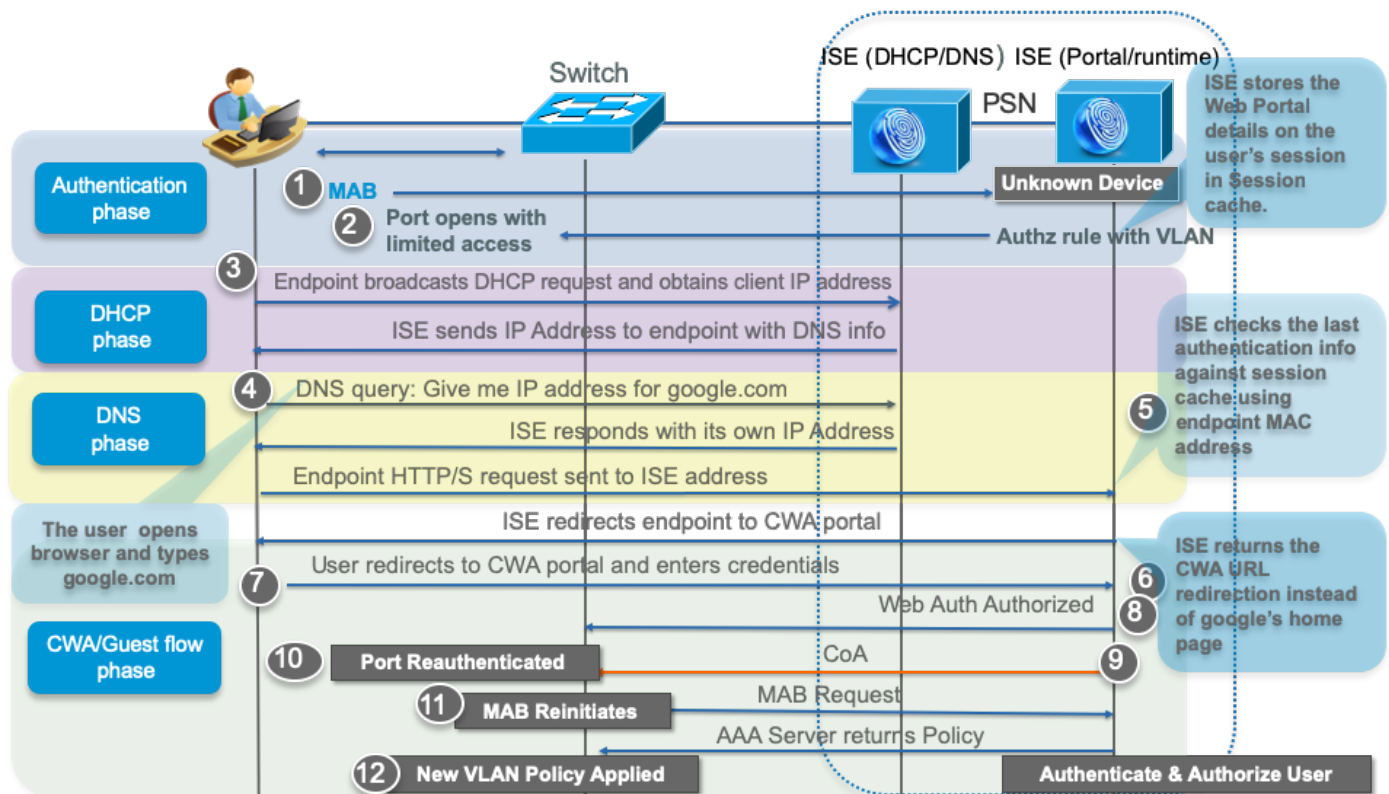
Als je hebt:

- niet-Cisco-hardware
- Goedkope, low-end hardware voor netwerkapparaten
- Oudere netwerkapparaathardware
- Oudere netwerkapparaatsoftware

dan kunt u onze [ISE NAD-profielen en -configuraties van derden](#) gebruiken of uw eigen aangepaste NAD-profiel maken. Met behulp van een NAD-profiel kunt u volledig aanpassen hoe ISE communiceert met uw netwerkapparaat, of het nu op aangepaste poorten voor RADIUS CoA is of dat u verificatie-VLAN's moet gebruiken in plaats van URL-omleiding.

Verificatie-VLAN-ondersteuning

Als u een aantal oude, oudere switches hebt die niet in staat zijn 802.1X te gebruiken, heeft ISE de mogelijkheid om endpoint te besturen met behulp van verificatie-VLAN's. Dit is een zeer ruwe methode van controle die DNS en DHCP gebruikt om HTTP-verkeer om te leiden naar een webportaal waar de gebruiker kan verifiëren. Zie [Ondersteuning netwerkapparaten van derden in Cisco ISE](#) in de [ISE-beheerdershandleidingen voor](#) meer informatie.



Problemen met het gebruik van verificatie-VLAN's

- U kunt niet meerdere apparaten per poort besturen.
- Verkeersfiltering is zeer ruw met L2 VLAN's - geen L3/4 IP/protocol/poortcontrole behalve met een VACL of VRF.
- Geen Oost/West-segmentatie binnen een VLAN betekent dat malware gemakkelijk kan worden verspreid naar andere eindpunten binnen VLAN's, ongeacht of deze niet vertrouwd of vertrouwd zijn.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.