

Unterstützt die ISE mein Netzwerkzugriffsgerät?

Inhalt

[Einleitung](#)

[ISE unterstützt die Protokolle RADIUS und TACACS](#)

[ISE-Kompatibilitätsrichtlinien](#)

[Netzwerkgerätefunktionen für die ISE](#)

[Woher kennen Sie die Funktionen Ihrer Netzwerkgeräte?](#)

[Ihre Hardware oder Software kann im ISE-Kompatibilitätsleitfaden nicht angezeigt werden.](#)

[ISE Network Access Device \(NAD\)-Profile](#)

[VLAN-Unterstützung für Authentifizierung](#)

[Probleme bei der Verwendung von Authentifizierungs-VLANs](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie die Kompatibilität der Cisco Identity Services Engine (ISE) mit Ihrem Netzwerkzugriffsgerät (NAD) überprüfen.

ISE unterstützt die Protokolle RADIUS und TACACS

Wenn Ihr Netzwerkgerät Zugriffskontrollanfragen mithilfe der RADIUS- und TACACS-Standardprotokolle ausgeben kann, dann kann die ISE dies unterstützen!

Die ISE unterstützt RADIUS, um die Zugriffskontrolle mit allen von der Hardware und Software des Netzwerkgeräts unterstützten Durchsetzungsmechanismen auszuführen.

Die Funktionen eines Netzwerkgeräts für eine portbasierte Zugriffskontrolle nach dem [IEEE 802.1X-Standard](#) sind softwarebasiert und häufig hardwareabhängig! Die reine Unterstützung von RADIUS bedeutet nicht, dass das Netzwerkgerät viele nützliche Durchsetzungsfunktionen wie [MAC Authentication Bypass \(MAB\)](#), [RADIUS Change of Authorization \(CoA\) \[RFC-5176\]](#), Layer-3/4-Zugriffskontrolllisten (ACLs), domänenbasierte ACLs, URL-Umleitung oder softwaredefinierte Segmentierung mit [Cisco TrustSec](#), Sie können nicht immer sagen, was ein bestimmtes Netzwerkgerät kann, und Sie müssen dies möglicherweise mit dem Anbieter oder Produktteam recherchieren.

Wenn Leute fragen: Unterstützt die ISE mein Netzwerkgerät? Sie fragen sich, ob mir die ISE all diese modernen Zugriffskontrollfunktionen bieten kann, selbst mit diesem alten, günstigen Switch.

Für diese älteren und kostengünstigeren Switches bietet die ISE Funktionen wie [SNMP-CoA und Authentifizierungs-VLAN](#), um ähnliche Funktionen bereitzustellen, die für die Abwicklung von Gast-, BYOD- und Statusdatenströmen erforderlich sind.

ISE-Kompatibilitätsrichtlinien

Informieren Sie sich in den [ISE-Kompatibilitätsleitfäden](#) über die Validierung durch unser Qualitätssicherungs-Team für die einzelnen ISE-Versionen.

Netzwerkgerätefunktionen für die ISE

Dies sind moderne Netzwerkgerätefunktionen, die in der Regel zur Bereitstellung von ISE-Funktionen erforderlich sind:

ISE-Funktionen	Netzwerkgerätefunktionen
AAA	802.1X, MAB, VLAN-Zuweisung, herunterladbare ACLs
Profilierung	RADIUS-CoA- und Profilerstellungssonden
BYOD	RADIUS-CoA, URL-Umleitung + Sitzungs-ID
Gast	RADIUS-CoA, URL-Umleitung + Sitzungs-ID, lokale Webauthentifizierung
Ursprungs-URL des Gasts	RADIUS-CoA, URL-Umleitung + Sitzungs-ID, lokale Webauthentifizierung
Status	RADIUS-CoA, URL-Umleitung + Sitzungs-ID
MDM	RADIUS-CoA, URL-Umleitung + Sitzungs-ID
TrustSec	SGT-Klassifizierung

Wie gehen Sie also vor, wenn Ihr Netzwerkgerät nicht über alle Funktionen für die ISE-Funktion verfügt?

Erstellen Sie ein Netzwerkzugriffsgerät (NAD)-Profil.

Woher kennen Sie die Funktionen Ihrer Netzwerkgeräte?

Die Funktionen für validierte Hardware- und Softwarekombinationen sind in unseren [ISE-Kompatibilitätsleitfäden](#) dokumentiert. Für alle anderen müssen Sie dies auf den Websites der Anbieter, in der Produktdokumentation, in Foren usw. recherchieren. Manchmal müssen Sie einfach in Ihrer Übung spielen, um herauszufinden, was funktioniert und was nicht, und [ein Netzwerkgeräteprofil](#) für die verschiedenen Kombinationen von Funktionen [erstellen](#).

Ihre Hardware oder Software kann im ISE-Kompatibilitätsleitfaden nicht angezeigt werden.

Nur weil ein Hardwaremodell oder eine Softwareversion nicht explizit aufgeführt ist, heißt das nicht, dass es nicht funktioniert - nur dass Sie es nicht mit der ISE validiert haben! Im Abschnitt Unterstützte Netzwerkzugriffsgeräte der [ISE-Kompatibilitätsleitfäden](#) wird angegeben, dass die ISE RADIUS unterstützt, unabhängig vom Anbieter oder Modell:

Die Cisco ISE unterstützt die Interoperabilität mit allen RADIUS-Netzwerkzugriffsgeräten (Network Access Devices, NAD) von Cisco oder anderen Anbietern, die gebräuchliches

RADIUS-Verhalten (ähnlich wie Cisco IOS 12.x) für eine standardbasierte Authentifizierung implementieren.

Die ISE unterstützt Protokollstandards wie [RADIUS](#), die zugehörigen [RFC-Standards](#) und [TACACS+](#). Wenn Ihr Netzwerkgerät RADIUS und/oder TACACS+ unterstützt, dann kann es von der ISE unterstützt werden!

Es gibt viele Gründe, warum Geräte von Cisco und von Drittanbietern möglicherweise nicht aufgeführt werden:

- Unser QA-Team kann es sich nicht leisten, jede einzelne Hardware- und Softwarekombination mit jeder ISE-Version zu testen.
- Neue Hardwareplattformen müssen angeschafft und getestet werden, was in der Regel innerhalb von 6-9 Monaten nach der Hardware-Veröffentlichung geschieht.
- Jedes Modell einer Hardwarefamilie wird nicht validiert - ein Modell wird ausgewählt und dann zur Darstellung der Hardwarefamilie verwendet.
- Jede Softwareversion wird nicht validiert - eine vom Plattform-Team empfohlene Version der Plattform wird ausgewählt, einige Monate vor der eigentlichen ISE-Version für die QA-Validierungsplanung.
- Ältere ISE-Versionen werden nicht mit neuerer Software für Netzwerkgeräte getestet, sollten jedoch Standards entsprechen.

Was genau Sie mit der ISE tun können, hängt dann von den Hardware- und Softwarefunktionen Ihres Netzwerkgeräts ab. Es wird immer empfohlen, die Hardware und Software Ihres Netzwerkgeräts vor der Bereitstellung in der Produktionsumgebung in Ihrem Labor mit der ISE auszuprobieren, um sicherzustellen, dass sich diese wie erwartet verhält.

ISE Network Access Device (NAD)-Profile

Wenn Folgendes zutrifft:

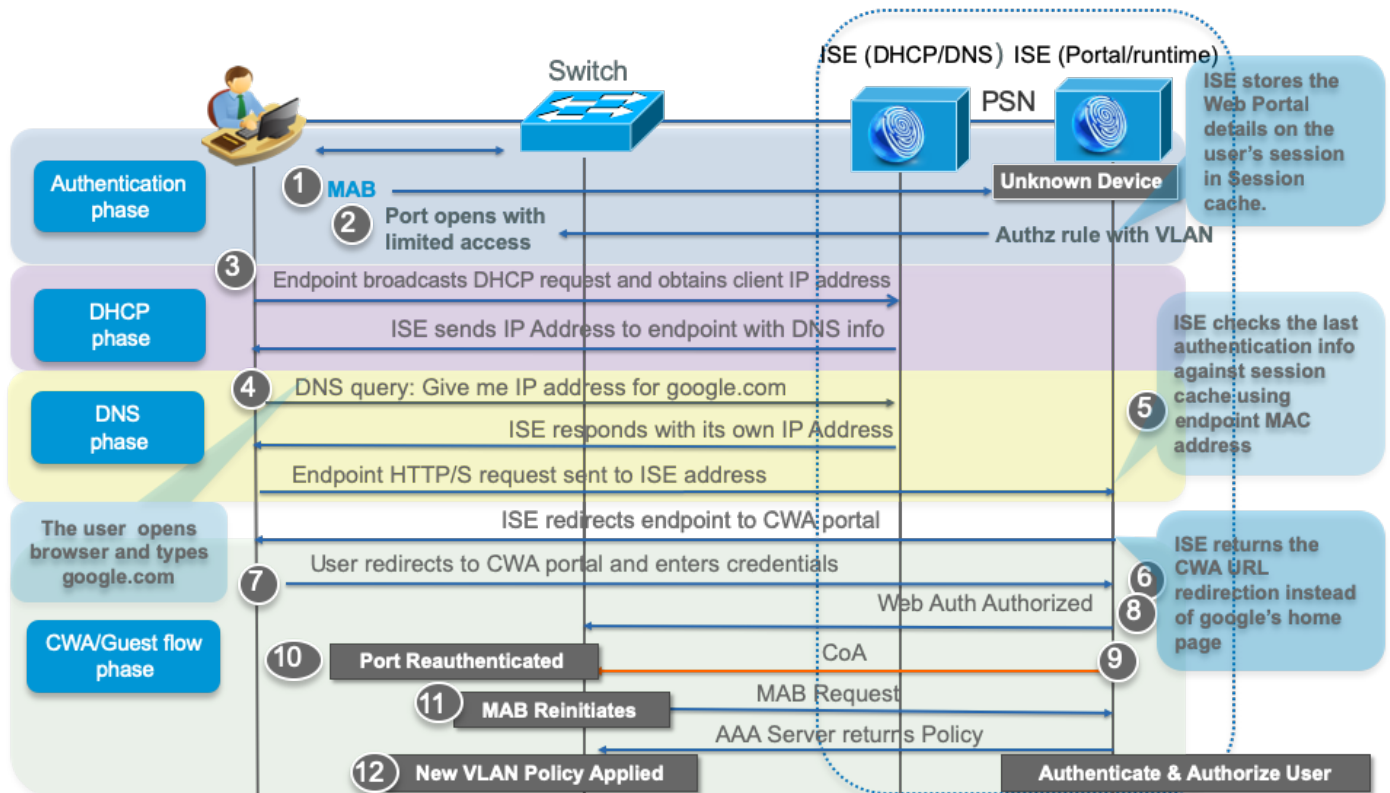
- Nicht von Cisco stammende Hardware
- kostengünstige Hardware für einfache Netzwerkgeräte
- ältere Netzwerkgerätehardware
- ältere Netzwerkgerätesoftware

können Sie unsere [ISE-NAD-Profile und -Konfigurationen von Drittanbietern](#) verwenden oder ein eigenes benutzerdefiniertes NAD-Profil erstellen. Mithilfe eines NAD-Profils können Sie die Kommunikationsweise der ISE mit Ihrem Netzwerkgerät vollständig anpassen, unabhängig davon, ob es sich um benutzerdefinierte Ports für RADIUS-CoA handelt oder ob Sie Authentifizierungs-VLANs anstelle der URL-Umleitung verwenden müssen.

VLAN-Unterstützung für Authentifizierung

Wenn Sie einige alte Legacy-Switches haben, die 802.1X nicht unterstützen, kann die ISE die Endpunkte mithilfe von Authentifizierungs-VLANs steuern. Dies ist eine sehr einfache

Kontrollmethode, die DNS und DHCP verwendet, um HTTP-Datenverkehr an ein Webportal umzuleiten, in dem sich der Benutzer authentifizieren kann. Weitere Informationen finden Sie unter [Third-Party Network Device Support in Cisco ISE](#) in den [ISE Administrators Guides](#).



Probleme bei der Verwendung von Authentifizierungs-VLANs

- Sie können nicht mehrere Geräte pro Port steuern.
- Die Datenverkehrsfilerung ist bei L2-VLANs sehr grob: Es gibt keine L3/4-IP/Protokoll/Port-Steuerung außer bei einer VACL oder VRF.
- Keine Ost/West-Segmentierung innerhalb eines VLAN bedeutet, dass Malware leicht auf andere Endpunkte innerhalb von VLANs verbreitet werden kann, unabhängig davon, ob diese vertrauenswürdig oder nicht vertrauenswürdig sind.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.