Does ISE Support My Network Access Device?

Contents

Introduction

This document describes how to check the compatibility of the Cisco Identity Services Engine (ISE) with your Network Access Device (NAD).

ISE Supports the RADIUS and TACACS Protocols

If your network device can issue access control requests using the standard RADIUS and TACACS protocols then ISE can support it!

ISE supports RADIUS to perform access control with whatever enforcement mechanisms the network device's hardware and software supports.

The capabilities of a given network device to do port-based access control with the IEEE 802.1X standard are software - and often hardware-dependent! Simply supporting RADIUS does not mean the network device supports many useful enforcement capabilities like MAC Authentication Bypass (MAB), RADIUS Change of Authorization (CoA) [RFC-5176], Layer-3/4 Access Control Lists (ACLs), domain-based ACLs, URL-redirection or software-defined segmentation with Cisco TrustSec. You cannot always tell you what any given network device is capable of and you may need to research that with the vendor or product team.

When people ask; Does ISE support my network device? What they mean is, Can ISE give me all of these modern access control capabilities even with this old, inexpensive switch?

For these older and less expensive switches, ISE offers features like SNMP CoA and Authentication VLAN to provide some similar capabilities needed to handle Guest, BYOD, and Posture flow.

ISE Compatibility Guides

Always check the **ISE Compatibility Guides** to see what our Quality Assurance (QA) team has

Validated for each ISE release.

Network Device Capabilities for ISE

These are modern network device functions typically required to deliver ISE capabilities:

ISE Capability	Network Device Features
AAA	802.1X, MAB, VLAN Assignment, Downloadable ACLs
Profiling	RADIUS CoA and Profiling Probes
BYOD	RADIUS CoA, URL Redirection + SessionID
Guest	RADIUS CoA, URL Redirection + SessionID, Local Web Auth
Guest Originating URL	RADIUS CoA, URL Redirection + SessionID, Local Web Auth
Posture	RADIUS CoA, URL Redirection + SessionID
MDM	RADIUS CoA, URL Redirection + SessionID
TrustSec	SGT Classification

So what do you do if your network device does not have all of the features for the ISE capability?

Create a Network Access Device (NAD) Profile.

How do you Know the Capabilities of your Network Devices?

The capabilities for validated hardware and software combinations are conveniently documented in our ISE Compatibility Guides. For all others, you need to research this on the vendors' websites, product documentation, forums, etc. Sometimes you may just have to play in your lab to find out what works and what does not and create a Network Device Profile for the different combinations of capabilities.

Unable to see your Hardware or Software in the ISE Compatibility Guide

Just because a hardware model or software release is not explicitly listed, does not mean that it will not work - only that you haven't validated it with ISE! The **Supported Network Access Devices** section of the **ISE Compatibility Guides** states that ISE supports RADIUS, regardless of the vendor or model:

Cisco ISE supports interoperability with any Cisco or non-Cisco RADIUS client network access device (NA

ISE supports protocol standards like **RADIUS**, its associated **RFC Standards,** and **TACACS+** . If your network device supports RADIUS and/or TACACS+ then ISE can support it!

There are many reasons why both Cisco and non-Cisco devices may not be listed:

- Our QA team cannot afford to test every single hardware and software combination with every ISE release.
- **New hardware platforms** must be acquired and tested which usually occurs within 6-9 months after the hardware release.
- **Every model of a hardware family** is not validated - one model is picked and then it is used to represent the hardware family.
- **Every software release** is not validated - one released platform software version recommended by the platform team is picked, a few months before the actual ISE release for QA validation planning.

- Older ISE releases are not tested with newer Network Device software but still should per standards.

Exactly what you can do with ISE is then determined by your network device's hardware and software capabilities. It is always recommended that you try your network device hardware and software in your lab with ISE before it is deployed to production so you are confident that it behaves as expected.

ISE Network Access Device (NAD) Profiles

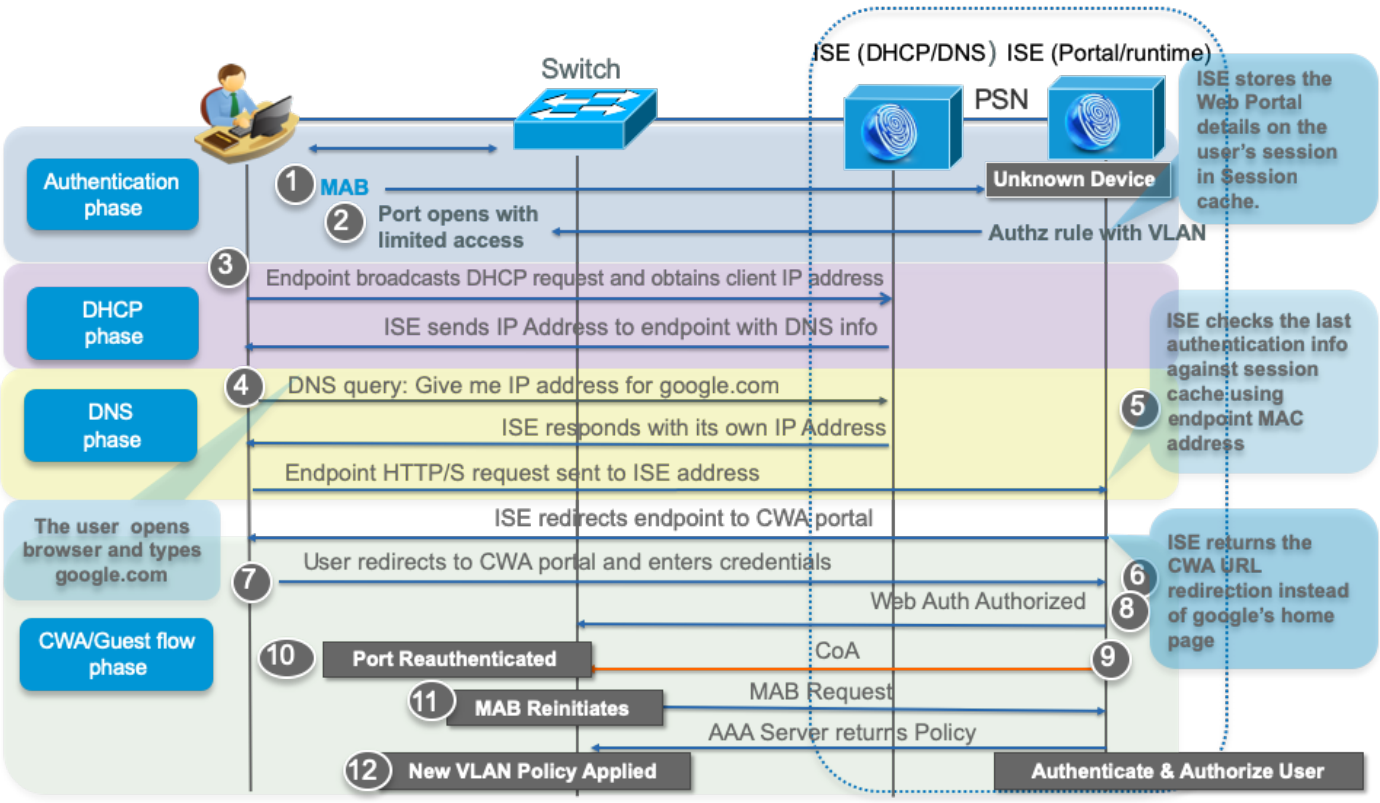
If you have :

- non-Cisco hardware
- inexpensive, low-end network device hardware
- older network device hardware
- older network device software

then you can use our ISE Third-Party NAD Profiles and Configs or create your own custom NAD profile. Using a NAD profile, you can completely customize how ISE communicates with your network device whether it is on custom ports for RADIUS CoA or if you need to use Authentication VLANs instead of URL Redirection.

Authentication VLAN Support

If you have some old, legacy switches that are incapable of 802.1X, ISE does have the ability to control endpoint using Authentication VLANs. This is a very crude method of control that uses DNS and DHCP to redirect HTTP traffic to a web portal where the user may authenticate. For more information, see Third-Party Network Device Support in Cisco ISE in the ISE Administrators Guides.



Problems with using Authentication VLANs

- You cannot control multiple devices per port.
- Traffic filtering is very crude with L2 VLANs - no L3/4 IP/protocol/port control except with a VACL or VRF.
- No East/West segmentation within a VLAN means malware is easily spread to other endpoints within VLANs, whether untrusted or trusted.