¿ISE admite mi dispositivo de acceso a la red?

Contenido

Introducción

Este documento describe cómo comprobar la compatibilidad de Cisco Identity Services Engine (ISE) con su dispositivo de acceso a la red (NAD).

ISE admite los protocolos RADIUS y TACACS

Si su dispositivo de red puede emitir solicitudes de control de acceso mediante los protocolos estándar RADIUS y TACACS, ISE puede admitirlo.

ISE admite RADIUS para realizar el control de acceso con los mecanismos de aplicación que admitan el hardware y el software del dispositivo de red.

Las capacidades de un dispositivo de red dado para hacer el control de acceso basado en puerto con el estándar IEEE 802.1X son software, y a menudo dependen del hardware. El soporte simple de RADIUS no significa que el dispositivo de red admita muchas capacidades de aplicación útiles como MAC Authentication Bypass (MAB), RADIUS Change of Authorization (CoA) [RFC-5176], Listas de Control de Acceso de Capa 3/4 (ACL), ACL basadas en dominio, redirección de URL o segmentación definida por software con Cisco TrustSec. No siempre puede indicarle de qué es capaz un dispositivo de red determinado y es posible que deba investigarlo con el proveedor o el equipo del producto.

Cuando la gente pregunta; ¿Es ISE compatible con mi dispositivo de red? Lo que quieren decir es, ¿puede ISE darme todas estas capacidades de control de acceso modernas incluso con este switch antiguo y barato?

Para estos switches más antiguos y menos costosos, ISE ofrece funciones como SNMP CoA y Authentication VLAN para proporcionar algunas capacidades similares necesarias para gestionar el flujo de estado, BYOD y invitado.

Guías de compatibilidad de ISE

Compruebe siempre las **guías de compatibilidad de ISE** para ver qué ha validado nuestro equipo

de garantía de calidad (QA) para cada versión de ISE.

Capacidades de dispositivos de red para ISE

Estas son las funciones modernas de dispositivos de red que se suelen necesitar para ofrecer funciones de ISE:

Capacidad de ISE	Características del dispositivo de red
AAA	802.1X, MAB, asignación de VLAN, ACL descargables
Definición de perfiles	RADIUS CoA y perfiles
BYOD	RADIUS CoA, redirección URL + ID de sesión
Guest	RADIUS CoA, redirección URL + ID de sesión, autenticación web local
URL de origen de invitado	RADIUS CoA, redirección URL + ID de sesión, autenticación web local
Condición	RADIUS CoA, redirección URL + ID de sesión
MDM	RADIUS CoA, redirección URL + ID de sesión
TrustSec	Clasificación SGT

¿Qué hace si su dispositivo de red no dispone de todas las funciones para la capacidad de ISE?

Cree un perfil de dispositivo de acceso a la red (NAD).

¿Cómo conoce las capacidades de sus dispositivos de red?

Las capacidades para combinaciones de hardware y software validadas se documentan convenientemente en nuestras Guías de Compatibilidad de ISE. Para todos los demás, necesita investigar esto en los sitios web de los proveedores, la documentación de productos, los foros, etc. A veces sólo tiene que jugar en su laboratorio para averiguar qué funciona y qué no y crear un perfil de dispositivo de red para las diferentes combinaciones de capacidades.

No se puede ver el hardware o el software en la Guía de compatibilidad de ISE

Solo porque un modelo de hardware o una versión de software no se enumeran de forma explícita, no significa que no funcione, solo que no lo ha validado con ISE. La sección **Dispositivos de Acceso a la Red Soportados de las** Guías de Compatibilidad de ISE indica que ISE admite RADIUS, independientemente del proveedor o modelo:

> Cisco ISE admite la interoperabilidad con cualquier dispositivo de acceso a la red (NAD) cliente RADIUS Cisco o de terceros que implemente un comportamiento RADIUS común (similar al de Cisco IOS 12.x) pa autenticación basada en estándares.

ISE admite estándares de protocolo como RADIUS, sus Estándares RFC asociados **y TACACS+** . Si su dispositivo de red admite RADIUS o TACACS+, ISE puede admitirlo.

Hay muchas razones por las que no se pueden enumerar los dispositivos de Cisco y de otros fabricantes:

- Nuestro equipo de QA no puede permitirse probar cada combinación de hardware y software con cada versión de ISE.
- **Las nuevas plataformas de hardware** deben adquirirse y probarse, lo que suele ocurrir en los 6-9 meses posteriores a la versión del hardware.
- **Cada modelo de una familia de hardware** no se valida; se selecciona un modelo y se utiliza

para representar a la familia de hardware.
- **Cada versión de software** no se valida: se selecciona una versión de software de plataforma publicada recomendada por el equipo de la plataforma, unos meses antes de la versión de ISE real para la planificación de validación de QA.
- Las versiones anteriores de ISE no se han probado con el software de dispositivos de red más reciente, pero deben seguir los estándares.

A continuación, las capacidades de hardware y software de su dispositivo de red determinan exactamente lo que puede hacer con ISE. Siempre se recomienda probar el hardware y el software de los dispositivos de red en su laboratorio con ISE antes de que se implemente en producción, de modo que esté seguro de que se comporta como se espera.

Perfiles de dispositivos de acceso a la red (NAD) ISE

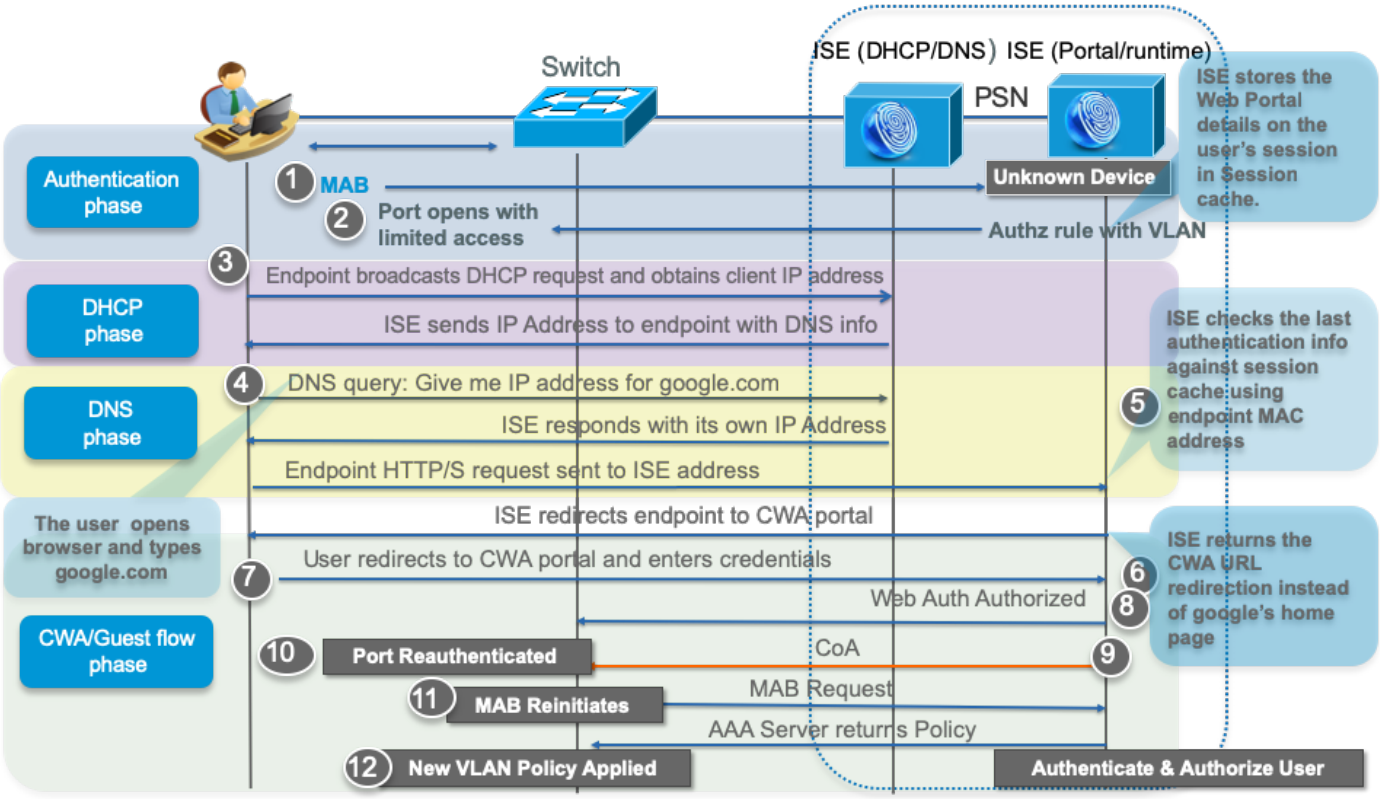
Si tiene:

- hardware que no es de Cisco
- hardware de dispositivo de red barato y de gama baja
- hardware de dispositivo de red más antiguo
- software de dispositivo de red más antiguo

a continuación, puede utilizar nuestros perfiles y configuraciones de terceros de ISE y crear su propio perfil NAD personalizado. Con un perfil NAD, puede personalizar completamente cómo ISE se comunica con su dispositivo de red, tanto si se encuentra en puertos personalizados para RADIUS CoA como si necesita utilizar VLAN de autenticación en lugar de URL Redirection.

Soporte de VLAN de Autenticación

Si tiene algunos switches antiguos que no son capaces de 802.1X, ISE tiene la capacidad de controlar el terminal mediante VLAN de autenticación. Este es un método de control muy crudo que utiliza DNS y DHCP para redirigir el tráfico HTTP a un portal web donde el usuario puede autenticarse. Para obtener más información, vea Soporte de dispositivos de red de terceros en Cisco ISE en las Guías de administradores de ISE.



Problemas con el Uso de VLAN de Autenticación

- No puede controlar varios dispositivos por puerto.
- El filtrado de tráfico es muy crudo con VLAN L2 - no hay control de puerto/protocolo/IP L3/4 excepto con una VACL o VRF.
- Ninguna segmentación horizontal dentro de una VLAN significa que el malware se propaga fácilmente a otros terminales dentro de las VLAN, ya sean no fiables o confiables.