

O ISE oferece suporte ao meu dispositivo de acesso à rede?

Contents

[Introduction](#)

[O ISE suporta os protocolos RADIUS e TACACS](#)

[Guias de compatibilidade do ISE](#)

[Recursos do dispositivo de rede para ISE](#)

[Como você conhece os recursos dos seus dispositivos de rede?](#)

[Não é possível ver seu hardware ou software no Guia de compatibilidade do ISE](#)

[Perfis do dispositivo de acesso à rede \(NAD\) do ISE](#)

[Autenticação de suporte de VLAN](#)

[Problemas com o uso de VLANs de autenticação](#)

Introduction

Este documento descreve como verificar a compatibilidade do Cisco Identity Services Engine (ISE) com seu dispositivo de acesso à rede (NAD).

O ISE suporta os protocolos RADIUS e TACACS

Se seu dispositivo de rede pode emitir solicitações de controle de acesso usando os protocolos padrão RADIUS e TACACS, o ISE pode suportá-lo!

O ISE suporta RADIUS para executar o controle de acesso com quaisquer mecanismos de aplicação que o hardware e o software do dispositivo de rede suportem.

Os recursos de um determinado dispositivo de rede para fazer o controle de acesso baseado em portas com o [padrão IEEE 802.1X](#) são software - e muitas vezes dependentes de hardware! Simplesmente suportar RADIUS não significa que o dispositivo de rede suporta muitos recursos úteis de aplicação como [MAC Authentication Bypass \(MAB\)](#), [RADIUS Change of Authorization \(CoA\) \[RFC-5176\]](#), Layer-3/4 Access Control Lists (ACLs), ACLs baseadas em domínio, redirecionamento de URL ou segmentação definida por software com o [Cisco TrustSec](#). Você nem sempre pode dizer qual dispositivo de rede é capaz de fornecer e pode precisar pesquisar isso com o fornecedor ou a equipe de produtos.

Quando as pessoas perguntam; O ISE suporta meu dispositivo de rede? O que eles querem dizer é, o ISE pode me dar todos esses recursos modernos de controle de acesso mesmo com esse switch antigo e barato?

Para esses switches mais antigos e mais baratos, o ISE oferece recursos como [SNMP CoA e Authentication VLAN](#) para fornecer alguns recursos semelhantes necessários para lidar com o fluxo de convidado, BYOD e Posture.

Guias de compatibilidade do ISE

Sempre verifique os [ISE Compatibility Guides](#) para saber o que nossa equipe de garantia de qualidade (QA) validou para cada versão do ISE.

Recursos do dispositivo de rede para ISE

Essas são funções modernas de dispositivos de rede normalmente necessárias para fornecer recursos do ISE:

Capacidade do ISE	Recursos do dispositivo de rede
AAA	802.1X, MAB, Atribuição de VLAN, ACLs para download
Criação de perfis	RADIUS CoA e perfis
BYOD	CoA RADIUS, redirecionamento de URL + ID de sessão
Convidado	RADIUS CoA, redirecionamento de URL + ID de sessão, autenticação da W local
URL de origem do convidado	RADIUS CoA, redirecionamento de URL + ID de sessão, autenticação da W local
Postura	CoA RADIUS, redirecionamento de URL + ID de sessão
MDM	CoA RADIUS, redirecionamento de URL + ID de sessão
TrustSec	Classificação SGT

Então, o que você faz se o dispositivo de rede não tiver todos os recursos para o recurso ISE?

Crie um perfil de dispositivo de acesso à rede (NAD).

Como você conhece os recursos dos seus dispositivos de rede?

Os recursos para combinações validadas de hardware e software são convenientemente documentados em nossos [Guias de compatibilidade do ISE](#). Para todos os outros, você precisa pesquisar isso nos sites dos fornecedores, na documentação do produto, nos fóruns, etc. Às vezes, talvez você tenha que jogar no laboratório para descobrir o que funciona e o que não funciona e [criar um Perfil de dispositivo de rede](#) para as diferentes combinações de recursos.

Não é possível ver seu hardware ou software no Guia de compatibilidade do ISE

Só porque um modelo de hardware ou uma versão de software não está explicitamente listada, não significa que não funcionará - somente porque você não o validou com o ISE! A seção **Supported Network Access Devices** dos [ISE Compatibility Guides](#) afirma que o ISE suporta RADIUS, independentemente do fornecedor ou modelo:

O Cisco ISE oferece suporte à interoperabilidade com qualquer dispositivo de acesso à rede (NAD - Network Access Device) de cliente RADIUS da Cisco ou não Cisco que implementa comportamento RADIUS com (semelhante ao Cisco IOS 12.x) para autenticação baseada em padrões.

O ISE suporta padrões de protocolo como [RADIUS](#), seus [Padrões RFC](#) associados, e [TACACS+](#). Se seu dispositivo de rede suporta RADIUS e/ou TACACS+, o ISE pode suportá-lo!

Há muitas razões pelas quais os dispositivos da Cisco e de outros fabricantes podem não estar listados:

- Nossa equipe de controle de qualidade não pode se dar ao luxo de testar cada combinação de hardware e software com cada versão do ISE.

- **Novas plataformas de hardware** devem ser adquiridas e testadas, o que geralmente ocorre entre 6 e 9 meses após a versão do hardware.
- **Cada modelo de uma família de hardware** não é validado - um modelo é escolhido e, em seguida, é usado para representar a família de hardware.
- **Cada versão de software** não é validada - uma versão de software da plataforma lançada recomendada pela equipe da plataforma é selecionada, alguns meses antes da versão real do ISE para planejamento de validação de QA.
- Versões mais antigas do ISE não são testadas com o software de dispositivo de rede mais recente, mas ainda devem ser testadas de acordo com os padrões.

O que você pode fazer exatamente com o ISE é determinado pelos recursos de hardware e software do seu dispositivo de rede. É sempre recomendável que você experimente o hardware e o software do seu dispositivo de rede em seu laboratório com o ISE antes que ele seja implantado na produção, para que você tenha certeza de que ele se comporta conforme o esperado.

Perfis do dispositivo de acesso à rede (NAD) do ISE

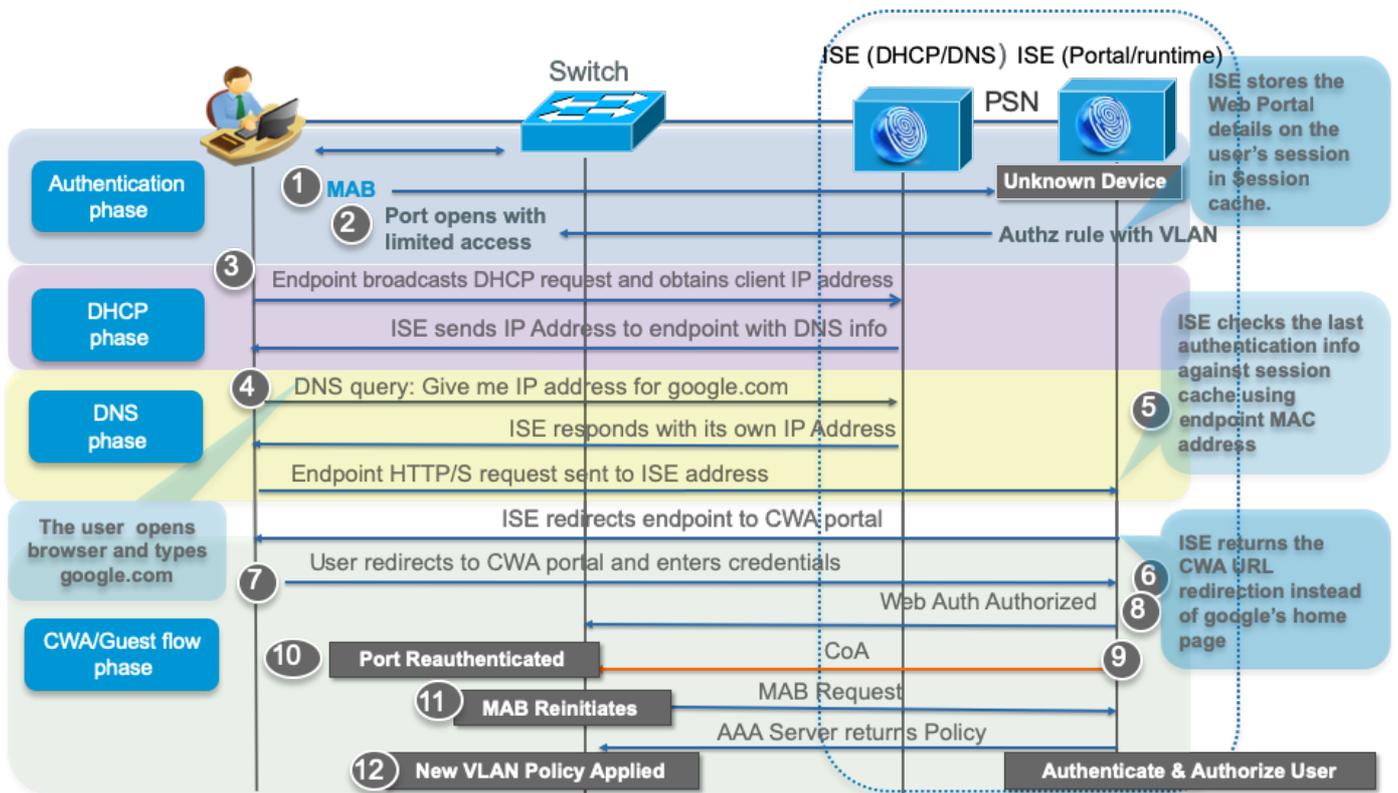
Se você tiver:

- hardware não-Cisco
- hardware de dispositivo de rede barato e de baixo custo
- hardware de dispositivo de rede mais antigo
- software de dispositivo de rede mais antigo

então você pode usar nossos [perfis e configurações de NAD de terceiros do ISE](#) ou criar seu próprio perfil NAD personalizado. Usando um perfil NAD, você pode personalizar completamente como o ISE se comunica com seu dispositivo de rede, esteja ele nas portas personalizadas para o CoA RADIUS ou se precisar usar VLANs de autenticação em vez de redirecionamento de URL.

Autenticação de suporte de VLAN

Se você tem alguns switches antigos e antigos que não podem ser 802.1X, o ISE tem a capacidade de controlar o endpoint usando VLANs de autenticação. Esse é um método de controle muito simples que usa DNS e DHCP para redirecionar o tráfego HTTP para um portal da Web no qual o usuário pode autenticar. Para obter mais informações, consulte [Suporte a dispositivos de rede de terceiros no Cisco ISE](#) nos [Guias de administradores do ISE](#).



Problemas com o uso de VLANs de autenticação

- Você não pode controlar vários dispositivos por porta.
- A filtragem de tráfego é muito grosseira com VLANs L2 - sem IP/protocolo/controle de porta L3/4 exceto com VACL ou VRF.
- Nenhuma segmentação leste/oeste em uma VLAN significa que o malware é facilmente espalhado para outros endpoints dentro das VLANs, não confiáveis ou confiáveis.