Verificar a Exclusão de Cliente 802.1X em uma WLC AireOS

Contents

Introdução

Este documento descreve a Exclusão de Cliente 802.1X em uma Controladora Wireless LAN (WLC) AireOS.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- WLC Cisco AireOS
- Protocolo 802.1X
- Serviço de Usuário de Discagem de Autenticação Remota (RADIUS)
- Identity Service Engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas no AireOS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A Exclusão de cliente 802.1X é uma opção importante para ter em um autenticador 802.1X, como uma WLC. Isso serve para evitar uma sobrecarga da infraestrutura do servidor de autenticação por clientes EAP (Extensible Authentication Protocol) que sejam hiperativos ou funcionem incorretamente.

Casos de usuário

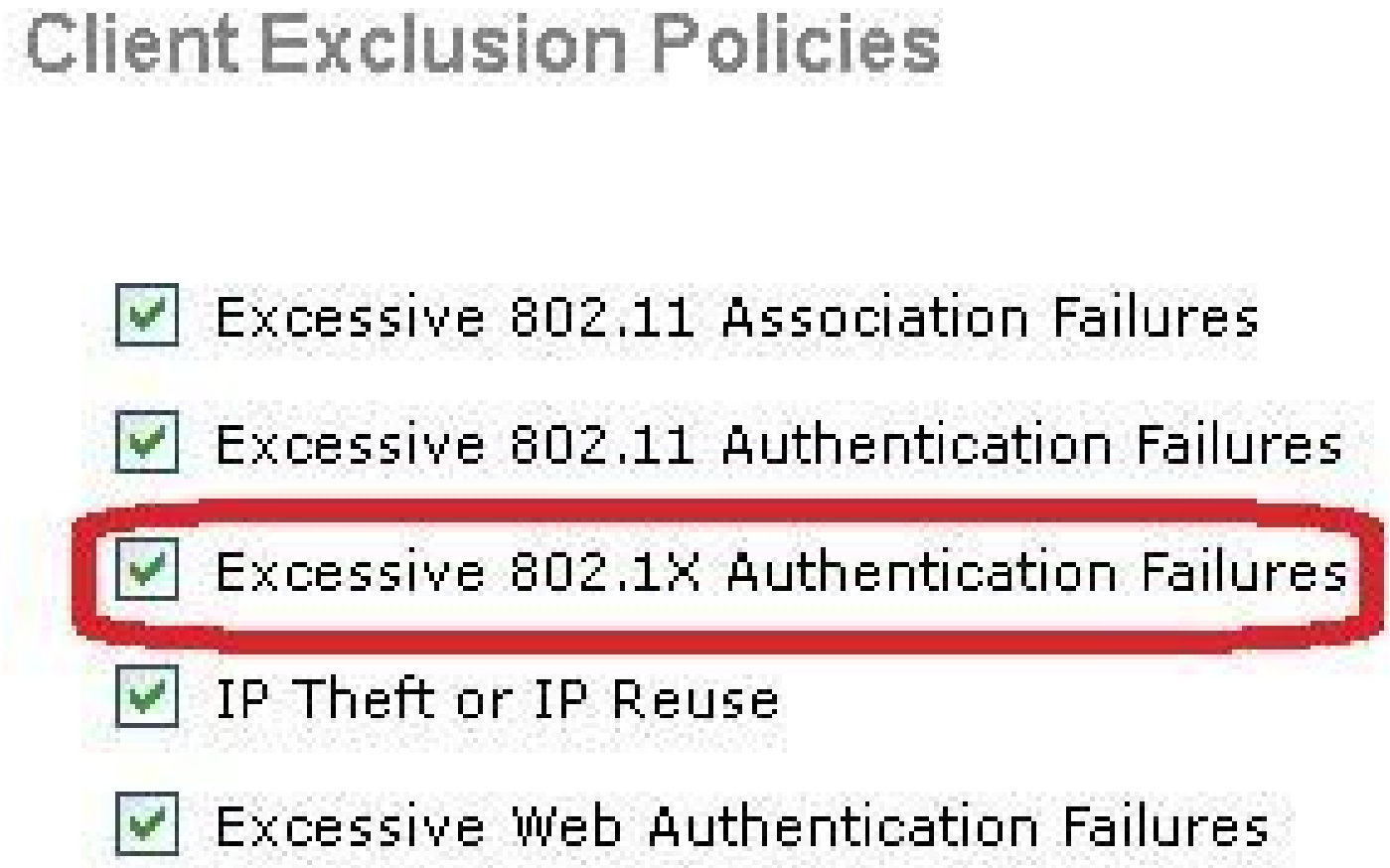
Exemplos de uso incluem:

- Um suplicante EAP configurado com credenciais incorretas. A maioria dos suplicantes, como os suplicantes EAP, cessam as tentativas de autenticação após algumas falhas sucessivas. No entanto, alguns suplicantes EAP continuam tentando reautenticar em caso de falha, possivelmente muitas vezes por segundo. Alguns clientes sobrecarregam servidores RADIUS e causam uma negação de serviço (DoS) para toda a rede.
- Após um grande failover de rede, centenas ou milhares de clientes EAP podem tentar se autenticar simultaneamente. Como resultado, os servidores de autenticação podem ser sobrecarregados e fornecer uma resposta lenta. Se os clientes ou autenticador atingirem o tempo limite antes que a resposta lenta seja processada, poderá ocorrer um ciclo vicioso em que as tentativas de autenticação continuem atingindo o tempo limite e, em seguida, tente processar a resposta novamente.

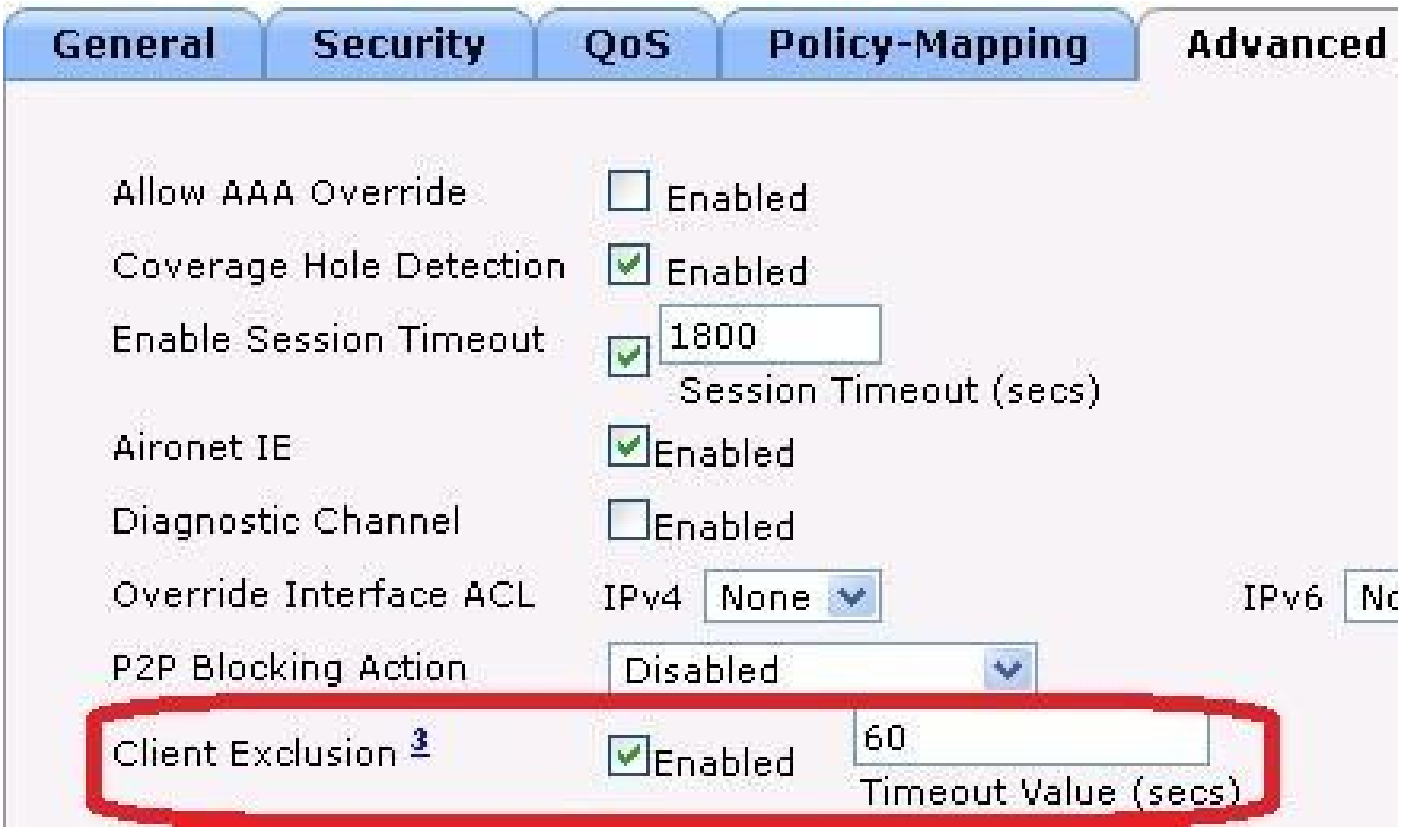
Observação: um mecanismo de controle de admissão é necessário para permitir que as tentativas de autenticação tenham êxito.

Como funciona a exclusão de cliente 802.1X?

A Exclusão de cliente 802.1X impede que os clientes enviem tentativas de autenticação por um período de tempo após falhas excessivas de autenticação 802.1X. Em uma AireOS WLC 802.1X, a exclusão de cliente é globalmente habilitada navegando para Security > Wireless Protection Policies > Client Exclusion Policies por padrão e pode ser vista nesta imagem.



A Exclusão de Cliente pode ser habilitada ou desabilitada por WLAN. Por padrão, ele é ativado com um tempo limite de 60 segundos antes do AireOS 8.5 e 180 segundos a partir do AireOS 8.5.



Configurações de exclusão para proteger servidores RADIUS contra sobrecarga

Para validar se o servidor RADIUS está protegido contra sobrecarga devido a clientes sem fio que funcionam incorretamente, verifique se estas configurações estão em vigor:

- Falhas excessivas de autenticação do 802.1X são selecionadas nas Políticas globais de exclusão de cliente do WLC.
- Client Exclusion (Exclusão de cliente) está definido como Enabled (Habilitado) nas configurações avançadas de WLAN.
- O valor de tempo limite de exclusão de cliente é definido como 60 a 300 segundos.

> Observação: valores superiores a 300 segundos oferecem melhor proteção, mas podem acionar reclamações do usuário.

- Configurar temporizadores AireOS EAP e configurações do ISE Protected Extensible Authentication Protocol (PEAP)

Problemas que impedem a exclusão do 802.1X de funcionar

Várias definições de configuração, na WLC e no servidor RADIUS, podem impedir que a Exclusão de Cliente 802.1X funcione.

Clientes não excluídos devido às configurações do temporizador EAP da WLC

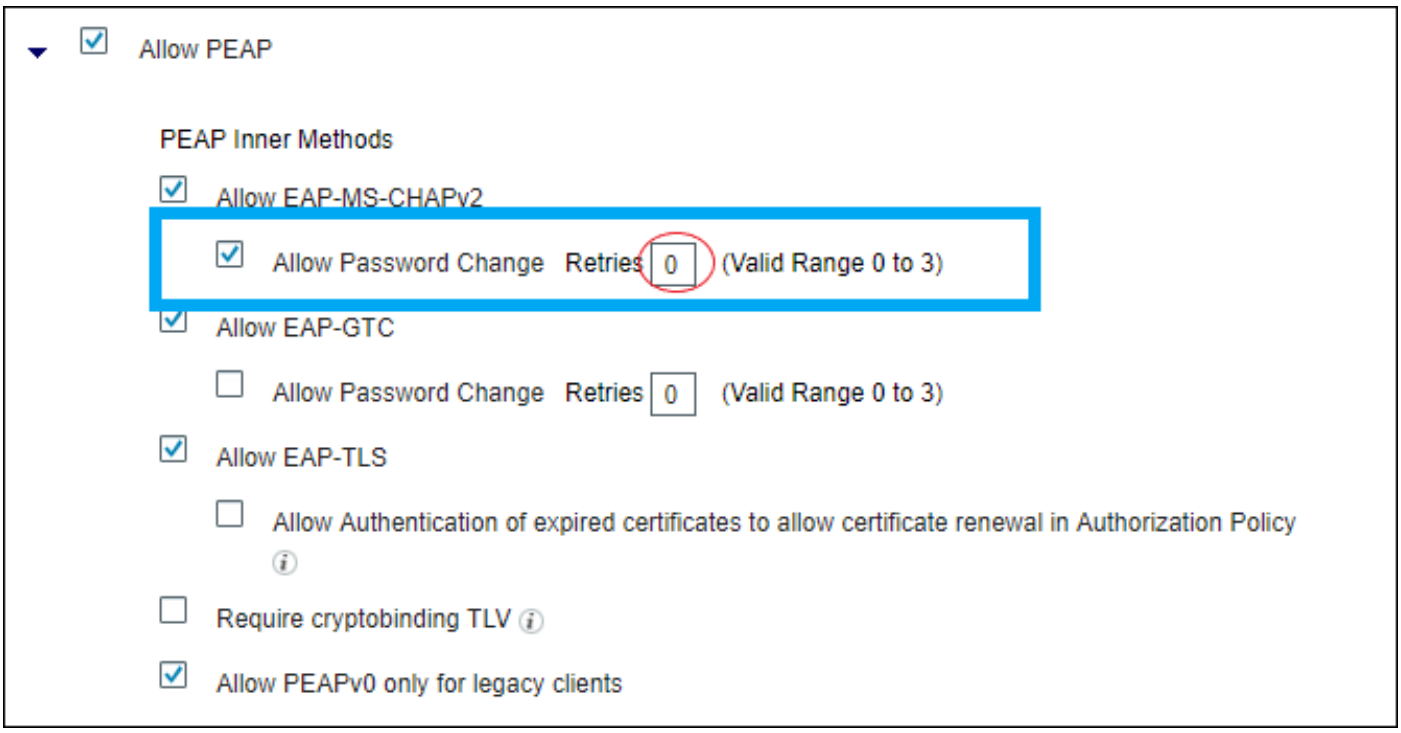
Por padrão, os clientes sem fio não são excluídos quando a Exclusão de clientes está definida como Habilitada na WLAN. Isso ocorre devido a longos intervalos de EAP padrão de 30 segundos, que fazem com que um cliente que se comporta mal nunca atinja falhas sucessivas suficientes para disparar uma exclusão. Configure tempos limite de EAP mais curtos com números maiores de retransmissões para permitir que a exclusão de cliente 802.1X entre em vigor. Consulte o exemplo de tempo limite.

```
config advanced eap identity-request-timeout 3
config advanced eap identity-request-retries 10
config advanced eap request-timeout 3
config advanced eap request-retries 10
```

Clientes não excluídos devido às configurações PEAP do ISE

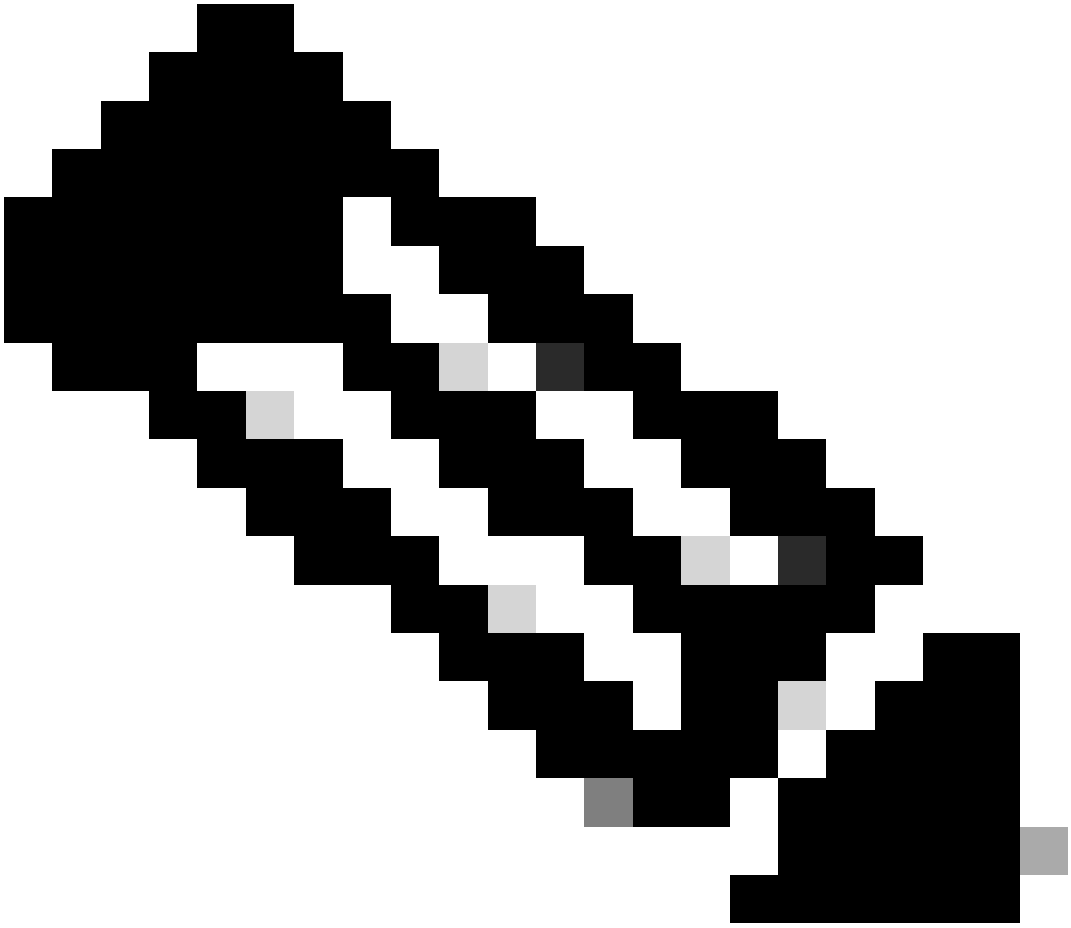
Para que a Exclusão de Cliente 802.1X funcione, o servidor RADIUS deve enviar um Access-Reject quando a autenticação falhar. Se o servidor RADIUS for ISE e se PEAP estiver em uso, a

exclusão não poderá ocorrer e isso dependerá das configurações PEAP do ISE. No ISE, navegue para Política > Resultados > Autenticação > Protocolos permitidos > Acesso padrão à rede conforme mostrado na imagem.



Se você definir Retries (circulado em vermelho à direita) como 0, o ISE deverá enviar Access-Reject imediatamente para a WLC, que deverá ativar a WLC para excluir o cliente (se tentar três vezes autenticar).

Observação: A definição de Repetições um pouco independente da caixa de seleção Permitir Alteração de Senha, ou seja, o valor de Repetições pode ser respeitado, mesmo que a opção Permitir Alteração de Senha esteja desmarcada. No entanto, se Retries for definido como 0, então Allow Password Change não funcionará.



Observação: para obter mais informações, consulte a ID de bug Cisco CSCsq16858. Somente usuários registrados da Cisco podem acessar as ferramentas e informações de bug da Cisco.

Informações Relacionadas

- Evite Derreter Redes RADIUS Sem Fio em Larga Escala
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.