Os ajustes remotos do dial-in user service da autorização (RAIO) em séries ESW2 350G controlaram o Switches

Objetivo

O Remote Authentication Dial-In User Service (RADIUS) é um protocolo do cliente ou do server que forneça um mecanismo da autenticação para que os dispositivos conectem e usem serviços de rede. Estes serviços variam do acesso aos arquivos compartilhados à impressão compartilhada. Um servidor Radius é um mecanismo que regule o acesso de usuário a uma rede de computador através das credenciais do usuário. Por exemplo, uma rede wireless pública (de WiFi) é instalada em um campus de universidade, todo o usuário NON-autorizado não pode usar esta rede, simplesmente aquelas a quem a universidade deu a uma senha podem a alcançar. O servidor Radius verifica as senhas incorporadas pelos usuários e concede ou nega o acesso como apropriado. Esta característica é útil fixar a rede contra o acesso não autorizado.

Este artigo explica como configurar ajustes do RAIO no Switches controlado série ESW2 350G.

Dispositivos aplicáveis

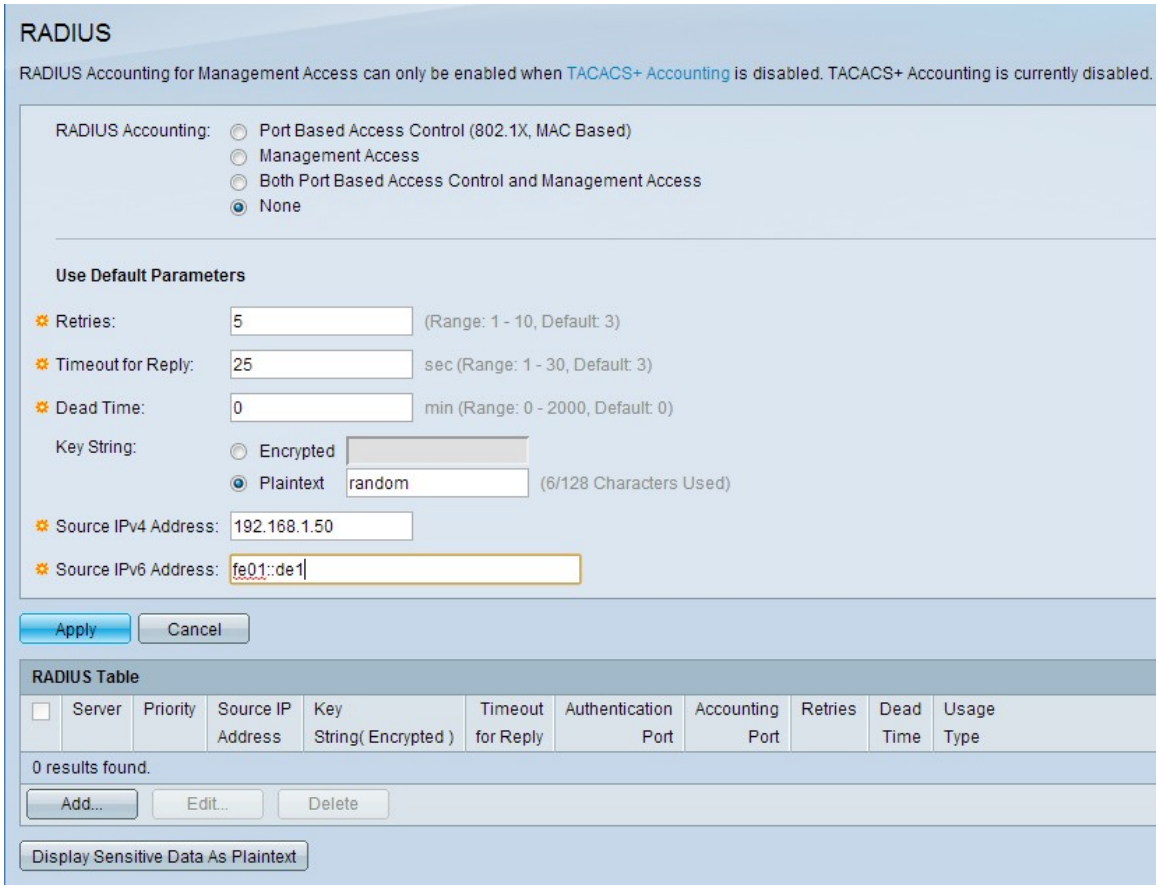
- ESW2-350G-52
- ESW2-350G-52DC

Versão de software

- 1.3.0.62

Ajustes do RAIO

Etapa 1. Entre ao utilitário de configuração da Web e escolha a **Segurança > o RAIO**. A página do *RAIO* abre:



Nota: O acesso de gerenciamento esclarecendo do RAIO pode somente ser permitido quando a contabilidade TACACS é desabilitada. Refira a *configuração do* artigo de *parâmetros TACACS+ e de server TACACS+ no Switches ESW2-350G* para obter mais informações sobre disto.

Etapa 2. Clique um botão de rádio para que o tipo da contabilidade do RAIO seja usado no campo da contabilidade do RAIO.

A contabilidade do RAIO permite que a informação seja compartilhada entre o cliente e o server. Os dados são enviados no início da sessão e no fim da sessão que indica os recursos usados durante a sessão.

- A porta baseou o controle de acesso — Esta opção especifica que o servidor Radius está usado para a porta do 802.1x que esclarece a interação do server/cliente.
- Acesso de gerenciamento — Esta opção especifica que o servidor Radius está usado para o login de usuário que esclarece a interação do server/cliente.
- A porta baseou o controle de acesso e o acesso de gerenciamento — Esta opção especifica que o servidor Radius está usado para a contabilidade e o login de usuário da porta do 802.1X que esclarecem a interação do server/cliente.
- Nenhum — Esta opção não permite explicar no servidor Radius.

Etapa 3. No campo do Retries, incorpore o número de novas tentativas que um pedido pode ser enviado antes que uma observação da falha esteja dada.

Etapa 4. No intervalo para o campo da resposta, incorpore o tempo (nos segundos) antes que um pedido não respondido esteja enviado novamente.

Etapa 5. No campo do período inoperante, incorpore o tempo (nos minutos) antes de um

servidor Radius sem resposta é contorneado e move-se para o server disponível seguinte para tentar a conexão. Um valor de 0 significa que o servidor Radius não está contorneado.

Etapa 6. No campo chave da corda, clique o botão de rádio desejado para escolher o tipo da corda chave usar-se então entram em uma corda chave que as ajudas cifrem mensagens entre o server e o cliente. A corda chave deve combinar a corda chave do servidor Radius. Você pode entrar na corda chave das seguintes maneiras:

- Cifrado — Você pode inscrever a corda chave no formulário criptografado.
- Texto simples — Se você não cifrou a corda chave de um outro dispositivo, a seguir entre como o texto simples.

Etapa 6 (opcional). No campo de endereço do IPv4 da fonte, incorpore o endereço do IPv4 da fonte a ser usado.

Etapa 7 (opcional). No campo de endereço do IPv6 da fonte, incorpore o endereço do IPv6 da fonte a ser usado.

Nota: O IPv4 da fonte e os campos do IPv6 da fonte estão somente disponíveis se o interruptor reage do modo da camada 3. Para comutar para mergulhar o modo 3, refira o artigo *configuram configurações de sistema no Switches ESW2-350G.*

Etapa 7. O clique **aplica-se**. Uma alerta é indicada na parte superior da página para indicar se a configuração é bem sucedida ou não. Há igualmente copiar da alerta/salvaguarda a configuração no arquivo.

Nota: Para copiar/configuração da salvaguarda no arquivo, consulta *para copiar ou salvar a configuração no interruptor ESW2-350G.*

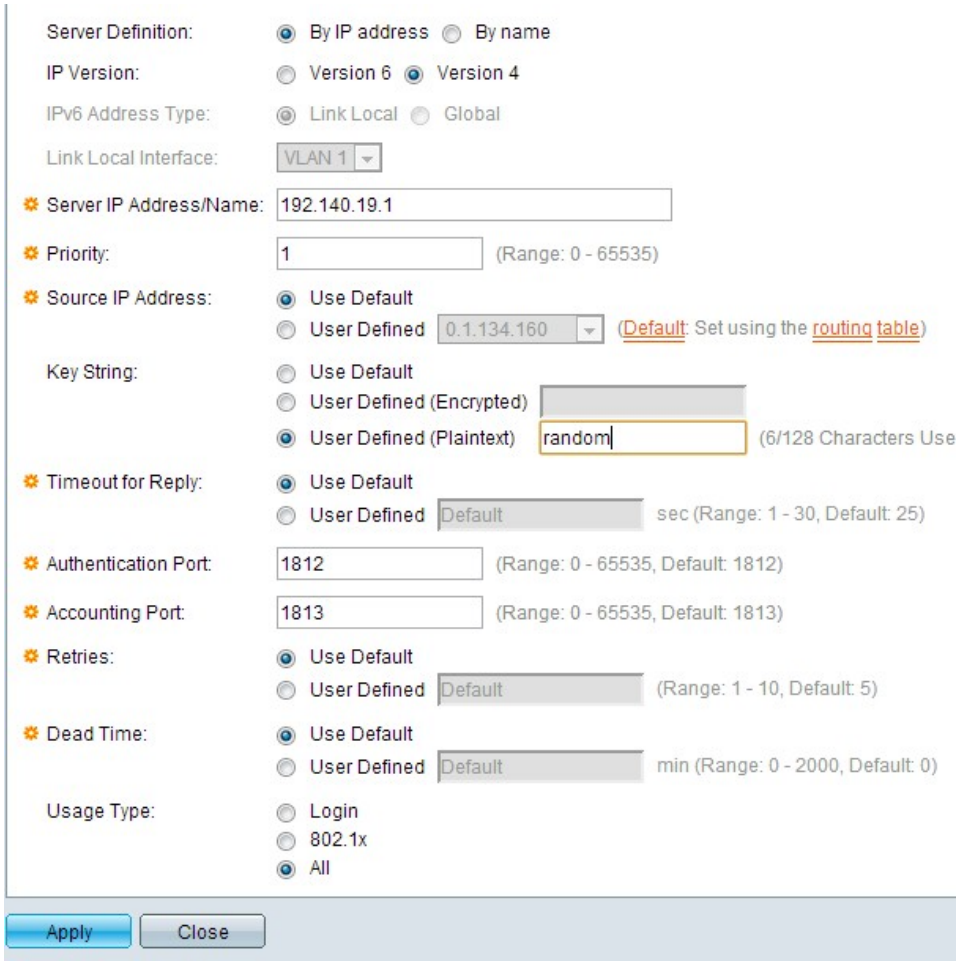
Etapa 8. Clique **dados sensíveis do indicador como o texto simples** para indicar dados sensíveis no texto simples.

Controle servidores Radius

A tabela do RAIO permite que um usuário adicione ou edite um servidor radius configurado.

Este procedimento mostra como adicionar um servidor Radius.

Etapa1. Na tabela do RAIO, o clique **adiciona** para adicionar um servidor Radius. O indicador do servidor Radius adicionar aparece.



Nota: Para editar um servidor Radius atual, o clique **edita** e edita as propriedades do servidor Radius.

Etapa 2. No campo de definição do server, clique o botão de rádio desejado para escolher se o servidor Radius é especificado pelo endereço IP de Um ou Mais Servidores Cisco ICM NT ou pelo nome.

- Pelo endereço IP de Um ou Mais Servidores Cisco ICM NT — Esta opção define o servidor Radius pelo endereço IP de Um ou Mais Servidores Cisco ICM NT.
- Por nome — Esta opção define o servidor Radius pelo nome.

Etapa 3. No campo da versão IP, clique o botão de rádio desejado para escolher se o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius é versão 6 ou versão 4.

- Versão 6 — Esta opção ajusta o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius ao endereço conhecido do IPv6.
- Versão 4 — Esta opção ajusta o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius ao endereço conhecido do IPv4.

Nota: Se o IPv4 é escolhido, o campo do tipo de endereço do IPv6 e o campo da interface local do link estão escurecidos.

Etapa 4. Se você clicou o botão de rádio da versão 6 em etapa 3, a seguir escolha o tipo de endereço do IPv6. As opções são:

- Local do link — Os anfitriões em uma rede única são identificados excepcionalmente no

endereço do IPv6. FE80 é o prefixo de um endereço local de link. Este endereço não é roteável fora da rede. Somente um endereço local de link é apoiado.

• Global — O endereço global do IPv6 é um endereço do unicast global que seja roteável fora da rede local.

Etapa 5. Da lista de drop-down da interface local do link escolha a interface local desejada do link das relações disponíveis do IPv6 criadas no interruptor.

Etapa 6. No endereço IP do servidor/campo de nome, incorpore o nome ou o endereço IP de Um ou Mais Servidores Cisco ICM NT para o servidor Radius baseado em sua escolha a etapa 2.

Passo 7. No campo de prioridade, incorpore um nível da prioridade para o servidor Radius. A fim autenticar um usuário, a prioridade determina a ordem que o interruptor tenta conectar com os servidores Radius. O valor 0 é a prioridade máxima.

Nota: Se o interruptor é incapaz de conectar ao servidor Radius com a prioridade mais alta então o interruptor tenta conectar com o server o mais prioritário seguinte.

Etapa 8. No campo chave da corda, entre em uma corda chave que as ajudas cifrem mensagens entre o server e o cliente. A corda chave deve combinar a corda chave do servidor Radius. Você pode inscrever a corda chave em maneiras diferentes como segue:

• Padrão do uso — Ajusta a corda chave do servidor Radius à corda do padrão.

• Definido pelo utilizador — Permite que um usuário inscreva a corda chave no campo adjacente. Você pode incorporar valores definidos por usuário a um as duas maneiras como segue:

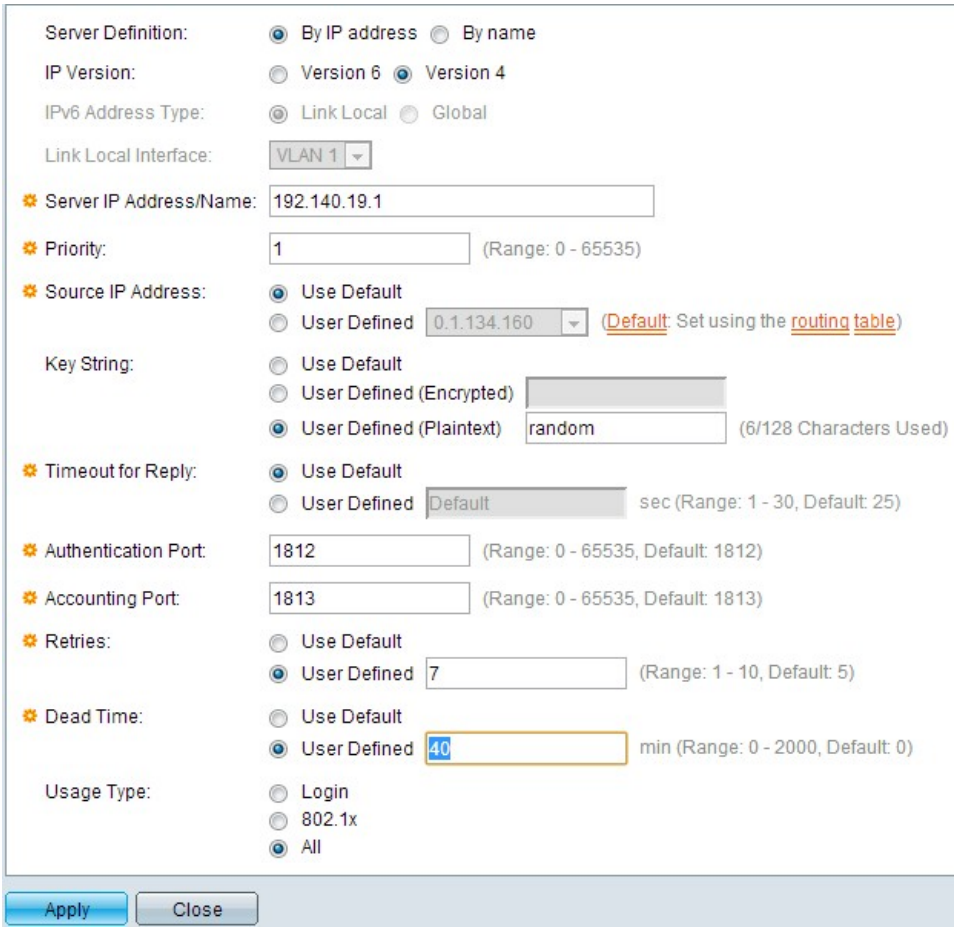
– Cifrado — Você pode inscrever a corda chave no formulário criptografado.

– Texto simples — Se você não tem a corda chave cifrada de um outro dispositivo, a seguir você pode entrar como o texto simples.

Etapa 9. No intervalo para o campo da resposta, clique o botão de rádio para ajustar a hora (nos segundos) para que o interruptor espera o o servidor Radius para responder.

• Padrão do uso — Ajusta o tempo ao valor padrão.

• Definido pelo utilizador — Permite que um usuário incorpore o tempo ao campo adjacente.



Etapa 10. No campo de porta de autenticação, entre no número de porta usado pelo servidor Radius para pedidos de autenticação.

Etapa 11. No campo de porta de relatório, entre no número de porta usado pelo servidor Radius para pedidos explicando.

Etapa 12. No campo do Retries, clique o botão de rádio para o número de pedidos que estão enviados ao servidor Radius antes que uma observação da falha ocorra.

- Padrão do uso — Usa o número padrão de novas tentativas.
- Definido pelo utilizador — Permite que um usuário incorpore o número de novas tentativas ao campo adjacente.

Etapa 13. No campo do período inoperante, clique o botão de rádio pelo tempo nos minutos antes que um servidor Radius esteja contorneado sendo sem resposta.

- Padrão do uso — Usa o tempo padrão.
- Definido pelo utilizador — Permite que um usuário incorpore o tempo ao campo adjacente.

Nota: Se você seleciona a opção padrão do uso em etapa 8, na etapa 9, na etapa 12 e na etapa 13, a configuração do raio padrão está usada. Veja a *configuração do* artigo de *ajustes do raio padrão.*

Etapa 14. No uso datilografe o campo, escolhem uma opção para o tipo do autenticação de servidor Radius.

- Início de uma sessão — Autentica o usuário para o servidor Radius.

- 802.1X — Usa a autenticação do 802.1X.
- Todos — Executa ambas as autenticações.

Etapa 15. Clique **dados sensíveis do indicador como o texto simples** para indicar dados sensíveis no texto simples.

Etapa 16. Clique em Apply. Uma alerta é indicada na parte superior da página para indicar se a configuração é bem sucedida ou não. Há igualmente copiar da alerta/salvaguarda a configuração no arquivo. O indicador fecha-se e a tabela do RAIO é atualizada.

Nota: Para copiar/configuração da salvaguarda no arquivo, consulta *para copiar ou salvar a configuração no interruptor ESW2-350G.*