

Autenticação de admin HTTP na versão 1.01 AP

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Informações de Apoio](#)

[Configuração ACS](#)

[Configuração da interface](#)

[Configuração do usuário](#)

[Configuração de grupo](#)

[Configuração de rede](#)

[Configuração AP para VxWorks](#)

[Configuração do usuário](#)

[Configuração do servidor](#)

[Configuração AP para IO](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este original fornece uma configuração de exemplo para a autenticação de admin HTTP na versão 1.01 do Access Point (AP).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 2.6.4 e mais recente do Access Control Server (ACS)

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 sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Convenções

Para obter mais informações sobre as convenções de documento, refira [convenções dos dicas técnicas da Cisco](#).

Informações de Apoio

Não há nenhuma opção para configurar o TACACS+ ou a contabilidade ou o comando `authorization` do RAIO para sessões de `exec` no GUI. Estas opções podem ser configuradas no CLI, mas não são recomendadas. Se você configura estas opções, podem severamente atolar o AP e o ACS com contabilidade ou pedidos de autorização (cada elemento de cada página deve ser explicado ou autorizado para).

Configuração ACS

Configuração da interface

Termine estas etapas para configurar a relação:

1. Em TACACS+ (Cisco IOS), selecione a caixa de grupo para o primeiro campo novo `undefined` do serviço.
2. No campo do serviço, entre em **Aironet**.
3. No campo do protocolo, incorpore o **shell**.
4. Nas opções de configuração avançadas, escolha **características > indicador que do TACACS+ avançado um indicador para cada serviço selecionou**.
5. Clique em Submit.

Configuração do usuário

Termine estas etapas para configurar o usuário:

1. Nas configurações avançadas de TACAS+, selecione o **shell (exec)**.
2. Selecione o nível de privilégio.
3. No campo, incorpore **15**.
4. Clique em Submit.

Configuração de grupo

Termine estas etapas para configurar o grupo:

1. Escolha o **TACACS+**.
2. Escolha o **shell > os atributos feitos sob encomenda de Aironet**.
3. Nos atributos feitos sob encomenda coloque, incorpore o **aironet: admin-capability=write+ident+firmware+admin+snmp**.
4. Clique em Submit.

5. Reinício.

Configuração de rede

Termine estas etapas para configurar a rede:

1. Crie o NAS para o AP usando o TACACS+ como o protocolo.
2. A chave é o segredo compartilhado do AP.
3. Clique em Submit.
4. Reinício.

Nota: Se você está usando um servidor de tokens com uma senha de uma vez, você precisa de configurar o token que põe em esconderijo a fim evitar continuamente ser alertado para senhas do nível 1 e do nível 15. Termine estas etapas para configurar pôr em esconderijo do token:

1. Incorpore a configuração de grupo para o grupo a que seus usuários admin pertencem.
2. Escolha **ajustes da placa de token**.
3. Selecione a **duração**.
4. Escolha uma duração que equilibre suas necessidades para a Segurança e a conveniência.

Se sua sessão típica admin dura cinco minutos ou menos, a seguir um valor da duração de cinco minutos é o melhor. Se sua sessão executa mais por muito tempo de cinco minutos, você está alertado outra vez para a sua senha em cinco intervalos minutos. Note que a opção de sessão não trabalha sem explicar permitido. Também, note que pôr em esconderijo do token é de fato para *todos* os usuários no grupo, e para as sessões de *todo* o grupo com todos os dispositivos (não apenas sessões de exec ao AP).

Configuração AP para VxWorks

Configuração do usuário

Conclua estes passos:

1. Escolha o > **segurança da instalação** > o novo usuário do > **Add da informação de usuário**.
2. Adicionar um novo usuário com potencialidades administrativas completas (todos os ajustes da capacidade verificados).
3. Clique **para trás**. Você é retornado à página da instalação de segurança.
4. **Gerenciador de usuário** do clique. A página de instalação do gerenciador de usuário publica-se.
5. Permita o **gerenciador de usuário**.
6. Clique em **OK**.

Configuração do servidor

Conclua estes passos:

1. Escolha o > **segurança** > o **Authentication Server** da instalação.
2. Incorpore o endereço IP do servidor TACACS+.
3. Selecione o tipo de servidor de TACACS.
4. No campo, entre na **porta 49**.

5. No campo, incorpore o **segredo compartilhado**.
6. Escolha a caixa da **autenticação de usuário**.

Configuração AP para IO

Termine estas etapas para configurar o AP para IO:

1. Escolha a **Segurança > o gerenciador do servidor**.
2. Escolha um server configurado TACACS+, ou configurar um novo.
3. Clique em Apply.
4. Escolha o IP do server TACACS+ na gota-para baixo da Autenticação de admin (TACACS+).
5. Clique em Apply.
6. Escolha a **Segurança > o acesso Admin**.
7. Crie um usuário local com o acesso de leitura/gravação (se você não tem feito tão já).
8. Clique em Apply.
9. Escolha o Authentication Server somente ou o Authentication Server (se não encontrado na lista local).
10. Clique em Apply.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- [Apoio de produtos Aironet 1200 Series](#)
- [Suporte por tecnologia do Terminal Access Controller Access Control System \(TACACS+\)](#)
- [Sustentação do produto do Cisco Secure Access Control Server para Windows](#)
- [Sustentação do produto do Cisco Secure Access Control Server para Unix](#)
- [Suporte Técnico - Cisco Systems](#)