Cisco Secure Services Client com exemplo de configuração PEAP/GTC WPA

Índice

Introdução

Este documento descreve como configurar o Wi-Fi Protected Access (WPA) protegido da placa de token do protocolo extensible authentication (PEAP) /Generic (GTC) no Cisco Secure Services Client.

Pré-requisitos

Componentes Utilizados

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

- Versão 4.0 do Cisco Secure Services ClientO Cisco Secure Services Client está disponível para a transferência do centro de software de Cisco.com (clientes registrados somente).
- Windows XP SP2 ou 2000 mínimos SP4

Convenções

Para obter mais informações sobre das convenções de documento, refira as convenções dos dicas técnicas da Cisco.

Configurar o Cisco Secure Services Client com PEAP/GTC WPA

Para configurar o Cisco Secure Services Client com PEAP/GTC WPA, termine estas etapas:

1. Clicar com o botão direito o ícone de bandeja de sistema do Cisco Secure Services Client, e escolha **aberto**.**Nota:** Se você não é conectado a uma rede, seu ícone de bandeja de sistema é não ofuscante.A caixa de diálogo da empresa da conexão aparece.

2. Clique a aba das **redes da criação**.A área das redes da criação indica as redes que transmitem seu Service Set Identifier (SSID).
3. Clique o botão da **rede da criação**.A caixa de diálogo do perfil da rede aparece.
4. Na área de rede, configurar estas opções:No campo de nome, dê entrada com um nome para sua rede.Este nome aparece como o SSID para esta rede. Para este exemplo, o nome é *demo_network*.Verifique o **disponível a toda a** caixa de verificação dos **usuários (perfil público)**.Verifique **automaticamente a** caixa de verificação da **conexão do usuário do estabelecimento**, e verifique-a que a caixa de verificação de conexão da máquina do estabelecimento não está verificada automaticamente.Verifique **antes da** caixa de verificação da **conta de usuário (carta inteligente/senha dos apoios somente)**.**Nota:** Quando **antes que a** caixa de verificação da **conta de usuário (carta inteligente/senha dos apoios somente)** esteja verificada, a autenticação continua imediatamente depois que as credenciais estão incorporadas, mas antes que o logon de domínio ocorra. Se você usa certificados de usuário, não verifique **antes da** caixa de verificação da **conta de usuário (carta inteligente/senha dos apoios somente)**. Porque não estão disponíveis antes do fazer logon de Windows, você não pode usar certificados de usuário com logons de domínio.
5. Na área sumária da configuração de rede, clique o **botão Modify Button**.A caixa de diálogo da autenticação de rede aparece.
6. Na caixa de diálogo da autenticação de rede, configurar estas opções:Na área das credenciais, clique o **único sinal do uso no** botão de rádio das **credenciais**.Na área dos métodos de autenticação, clique a **volta no** botão de rádio, e clique então o **uso “anônimo” como a identidade**.A volta no botão de rádio povoa a lista do protocolo indicada na área dos métodos de autenticação. O uso “anônimo” como o botão de rádio da identidade limita a lista somente aos Protocolos de autenticação em túnel.Verifique a caixa de verificação **PEAP**, e clique-a então **configuram**.A caixa de diálogo do método de EAP configurar aparece.Desmarcar a caixa de verificação do **certificado de cliente do uso**.Verifique o **certificado de servidor da validação** e **permita** caixas de seleção **rápidas da ressunção da sessão**.Do menu suspenso em túnel do método, escolha o **GTC**.Clique a **APROVAÇÃO** para retornar à caixa de diálogo da autenticação de rede, e clique então a **APROVAÇÃO** para retornar à caixa de diálogo do perfil da rede.
7. Na área dos dispositivos de acesso da caixa de diálogo do perfil da rede, o clique **adiciona**.A caixa de diálogo do dispositivo de acesso adicionar aparece.
8. Na caixa de diálogo dos dispositivos de acesso adicionar, escolha o dispositivo que você quer configurar, e clique-o então **adicionam o acesso**.**Nota:** Se o dispositivo que você quer configurar estiver dentro da escala, o SSID para esse dispositivo aparece na lista de dispositivos de acesso disponível. Se o dispositivo não aparece, incorpore o SSID para o dispositivo ao campo do acesso (SSID), incorpore as configurações de porta à área das configurações de porta do Cisco 1100, e clique-as então **adicionam o acesso**.
9. Na caixa de diálogo do perfil da rede, **APROVAÇÃO do** clique a retornar à caixa de diálogo da empresa da conexão.
10. Na caixa de diálogo da empresa da conexão, escolha **confiado que os server > controlam máquina/todos os server confiados usuários do** menu do cliente.Máquina do controlo/todos os usuários confiou que caixa de diálogo dos server aparecem.
11. O clique **adiciona a regra do server**.A caixa de diálogo confiada do server aparece.
12. Na caixa de diálogo confiada do server, configurar estas opções:No campo de nome da regra, dê entrada com um nome para a regra.Do menu suspenso do método da validação, escolha o **certificado**.No fósforo ALGUMA área da regra da validação certificada, configura opções para a regra.Para construir uma regra, você deve saber que o índice do certificado

de servidor e para incorporar aqueles valores ao fósforo TODA A validação certificada ordena a área. Por exemplo, se o nome alternativo sujeito contém o Domain Name de um server, *mtgcorpserver.mtgcorp.com*, escolhe **extremidades com do** menu suspenso alternativo sujeito do nome, e inscreve então **mtgcorp.com no** campo de texto.Clique a **APROVAÇÃO** para retornar a máquina do controlo/toda a caixa de diálogo confiada usuários dos server.

13. Em máquina do controlo/todos os usuários confiou a caixa de diálogo dos server, clique **perto do** retorno à caixa de diálogo da empresa da conexão.

A configuração está completa, e você pode conectar à rede.

Conecte à rede

Para conectar a sua rede nova, termine estas etapas:

1. Na caixa de diálogo da empresa da conexão, clique a aba das **redes do controlo**.
2. Desligue de toda a rede que for conectada ao adaptador usado por sua rede nova.
3. Do liste de redes, selecione o perfil novo da rede, e o clique **conecta**.

Em cima da configuração bem-sucedida e da conexão, os indicadores do ícone de bandeja de sistema do Cisco Secure Services Client esverdeiam.

Nota: Se o software antivírus está instalado em seu computador e está configurado para analisar gramaticalmente o diretório do log do Cisco Secure Services Client, você pode experimentar ciclos da alta utilização da CPU com autenticação de Cisco Secure Services Client. Para melhorar o desempenho, configurar seu software antivírus para excluir o diretório do log do Cisco Secure Services Client.

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems