Manual de configuração da versão 1.01 do EAP-TLS

ID do Documento: 64064

Atualizado em: outubro 14, 2009

 Transferência PDF

 Imprimir

Feedback

Produtos Relacionados

- Access point do Cisco Aironet 1200
- Access point do Cisco Aironet 350
- Cisco Secure Access Control Server for Unix
- Cisco Secure Access Control Server for Windows

Índice

Introdução

Este documento fornece uma configuração de exemplo para a versão 1.01 da Segurança da camada do Protocolo-transporte da autenticação extensível (EAP-TLS).

Nota: Este documento supõe que você usa Microsoft Certificate Authority (CA). Quando você puder usar um certificado auto-assinado, desanima Cisco altamente esta prática, e este documento não cobre certificados auto-assinados. O período da expiração do padrão dos certificados auto-assinados é somente um ano, e você não pode mudar este ajuste. Isto é razoavelmente padrão para certificados de servidor. Contudo, o certificado auto-assinado igualmente atua como o certificado CA raiz. Consequentemente, você precisa de instalar o certificado novo em cada cliente cada ano a menos que você não verificar “validar a opção do certificado de servidor”. CA real deve estar disponível para obter de qualquer maneira os certificados de cliente, e assim, não há realmente nenhuma razão empregar certificados auto-assinados com EAP-TLS.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

- Access Point (AP) 12.02T1
- Access Control Server (ACS) 3.1, 3.2, e 3.3
- Windows 2000 e XP
- Certificate Authority (CA) da raiz da empresa

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

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Use a Command Lookup Tool (somente clientes registrados) para obter mais informações sobre os comandos usados nesta seção.

Instale o server do certificado de Microsoft (CA)

Conclua estes passos:

1. Escolha o **começo > os ajustes > o Control Panel**.
2. Clique **adicionar/removeres programar no** Control Panel.
3. Seleto **adicionar/remova componentes do Windows**.
4. Selecione serviços certificados.
5. Clique em Next.
6. Clique **sim ao** mensagem IIS.
7. Selecione uma CA raiz autônoma (ou empresa).
8. Clique em Next.
9. Nomeie CA.**Nota:** Todas as caixas restantes são opcionais.**Nota:** Não use o mesmo nome para CA que o servidor ACS, porque isto pode fazer com que os clientes PEAP falhem a autenticação. Um certificado CA raiz com o mesmo nome que o certificado de servidor confunde os clientes PEAP. Este problema não é original aos clientes Cisco. Naturalmente, se você não planeia usar o PEAP, isto não se aplica.
10. Clique em Next.O padrão do base de dados está correto.
11. Clique em Next.O IIS deve ser instalado antes que você instale CA.

Crie um certificado de servidor

Conclua estes passos:

1. Consulte a CA (**http://IP_of_CA_server/certsrv/) de** seu servidor ACS.
2. Verifique o **pedido uma** caixa do **certificado**.

3. Clique em Next.
4. Selecione o **pedido avançado**.
5. Clique em Next.
6. Seleto **submeta um pedido de certificado para este CA usando um formulário**.
7. Clique em Next.
8. Datilografe um nome na caixa do nome (CN).
9. Verifique a caixa do **certificado de autenticação de servidor** para ver se há a finalidade pretendida.**Nota:** Se você usa a empresa CA, selecione o **servidor de Web na** primeira lista.
10. Selecione estas opções sob a opção chave para criar um molde novo:**CSP — V1.0 do provedor criptográfico de base MicrosoftTamanho chave — 1024Nota:** Os Certificados criados com um tamanho chave maior de 1024 podem trabalhar para o HTTPS mas não para o PEAP.**Nota:** A empresa CA de Windows 2003 permite os tamanhos chaves maiores de 1024, mas um chave maior de 1024 não trabalham com PEAP. A autenticação pode parecer passar no ACS, mas o cliente apenas pendura na tentativa de autenticação.Verifique as **chaves de Mark como a Opção exportávelNota:** Microsoft mudou o molde do servidor de Web com a liberação da empresa CA de Windows 2003. Com esta mudança do molde, você pode já não exportar chaves, e a opção é desabilitada para fora. Não há nenhum outro molde de certificado fornecido com os serviços certificados que são para a autenticação de servidor, ou que dão a capacidade para marcar chaves como exportable. A fim criar um molde novo que faça assim, para ver a criação uma seção nova do molde de certificado.Verifique a opção da **loja de máquina local do usoNota:** Retenha as seleções do padrão para todas as outras opções.
11. Clique em Submit.Você deve receber esta mensagem: **Seu pedido do certificado foi recebido**.

Crie um molde de certificado novo

Conclua estes passos:

1. Escolha **Start > Run**.
2. Datilografe **certtmpl.msc na** caixa de diálogo da corrida, e pressione o ENTER.
3. Clicar com o botão direito o **molde do servidor de Web**, e selecione o **molde duplicado**.
4. Nomeie o molde, por exemplo, ACS.
5. Selecione a aba da **manipulação de pedido**.
6. Verifique a **chave privada reservar para ser** opção **exportada**.
7. Selecione o botão **CSP**.
8. Verifique a opção do **v1.0 do provedor criptográfico de base Microsoft**.
9. Clique em **OK**.**Nota:** Retenha as seleções do padrão para todas as outras opções.
10. Clique em Apply.
11. Clique em **OK**.
12. Abra CA MMC pressão-em.
13. Clicar com o botão direito **moldes de certificado**, e escolha **novo > molde de certificado a emitir**.
14. Escolha o molde que novo você criou.
15. Clique em **OK**.
16. Reinicie CA.O molde novo é incluído na lista do molde de certificado.

Às vezes, “`não está criado o` erro do” `objeto` ”“`CertificateAuthority.Request` ocorre quando você tenta criar um certificado novo.

Termine estas etapas a fim corrigir este erro:

1. Escolha o **Iniciar > Ferramentas Administrativas > o IIS**.
2. Expanda **sites > website padrão**.
3. Clicar com o botão direito **CertSrv**, e escolha **propriedades**.
4. Clique o botão da **configuração na** seção das configurações de aplicativo da aba do diretório virtual.
5. Selecione a aba das **opções**.
6. Verifique a opção do **estado de sessão da possibilidade**.**Nota:** Retenha as seleções do padrão para todas as outras opções.
7. Clique a **APROVAÇÃO** duas vezes.
8. Reinicie o IIS.**Nota:** 2003 CA em um domínio 2000 cujo o esquema não seja preparado para a compatibilidade 2003 com adprep/forestprep/domainprep não trabalham com EAP. Se seu navegador trava com do "uma mensagem do `controle activex fazendo download`", você precisa de executar o reparo nesta URL: http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B330389 .**Nota:** Se o campo CSP apenas indica a "`carga….`" assegure-se de que você não tenha um firewall de software na máquina que submete o pedido. ZoneAlarm de ZoneLabs causa este erro mais ou menos todas as vezes. Determinado outro software pode igualmente causar este erro.

Aprove o certificado de CA

Conclua estes passos:

1. Escolha o **iniciar > programas > ferramentas administrativas > o Certificate Authority**.
2. Expanda o certificado no painel esquerdo.
3. Selecione **durante pedidos**.
4. Clicar com o botão direito no certificado.
5. Selecione todas as tarefas.
6. Selecione a **edição**.

Instale o certificado em Windows Server

Transfira o certificado de servidor ao servidor ACS

Conclua estes passos:

1. Consulte a CA (**http://IP_of_CA_server/certsrv/) de** seu servidor ACS.
2. Selecione a **verificação em um certificado pendente**.
3. Clique em Next.
4. Selecione o certificado.
5. Clique em Next.
6. O clique **instala**.

Instale o certificado de CA no servidor ACS

Nota: Estas etapas não são necessárias se o ACS e CA são instalados no mesmo server.

1. Conclua estes passos:

2. De seu servidor ACS, consulte a CA (**http://IP_of_CA_server/certsrv/**).
3. Seleto **recupere o certificado de CA ou a lista de revogação de certificado**.
4. Clique em Next.
5. Selecione **Base64 codificou**.
6. Clique o **certificado de CA da transferência**.
7. Clique **aberto**.
8. O clique **instala o certificado**.
9. Clique em Next.
10. **Lugar** seleto **todos os Certificados na seguinte loja**.
11. O clique **consulta**.
12. Verifique a caixa das **lojas do show physical**.
13. Expanda a lista de **Autoridades de certificação de raiz confiável**.
14. Selecione o computador local.
15. Clique em **OK**.
16. Clique em Next.
17. Clique em Finish.Uma caixa de mensagem aparece.
18. Clique em **OK**.**Nota:** Se seus certificados de cliente foram criados com CA diferente de seu certificado de servidor, você deve repetir estas etapas para a CA raiz e todos os CA intermediários envolvidos na criação do certificado de cliente.

ACS estabelecido para usar o certificado de servidor

Conclua estes passos:

1. Clique a **configuração de sistema no** servidor ACS.
2. Selecione o **certificado ACS para setup**.
3. Seleto **instale o certificado ACS**.
4. Selecione Use certificate from storage.
5. Datilografe dentro o nome do CN (o mesmo nome que você datilografou dentro etapa 8 da criação a uma seção do certificado de servidor).
6. Clique em Submit.
7. **Configuração de sistema do** clique no servidor ACS.
8. Selecione o **certificado ACS para setup**.
9. Seleto **edite o certificate trust list**.
10. Verifique a caixa de **CA**.
11. Clique em Submit.

Crie uma solicitação de assinatura de certificado

Conclua estes passos:

1. Vá à **configuração de sistema > ao certificado ACS Setup > gerenciem a solicitação de assinatura de certificado**.
2. Datilografe um nome no campo de assunto do certificado no formato do `cn=name`.
3. Datilografe um nome para o arquivo-chave privado.**Nota:** Este campo põe em esconderijo o trajeto à chave privada. Consequentemente, se você clique **submete uma** segunda vez

depois que o CSR está criado, a chave privada overwritten, e não combinará o CSR original. Isto pode conduzir à "`chave privada não combina`" o erro quando você tenta instalar o certificado de servidor.
4. Datilografe a senha da chave privada.
5. Confirme a senha.
6. Escolha um comprimento chave de 1024.**Nota:** O ACS pode gerar os tamanhos chaves maiores de 1024. Contudo, um chave maior de 1024 não trabalha com EAP. A autenticação pode parecer passar no ACS, mas o cliente apenas pendura na tentativa de autenticação.
7. Clique em Submit.
8. Copie a saída CSR no lado direito para submeter-se a CA.

Use seu CSR para criar um certificado de servidor

Conclua estes passos:

1. Consulte a CA (**http://IP_of_CA_server/certsrv/) de** seu servidor FTP.
2. Selecione o **pedido uma** opção do **certificado**.
3. Clique em Next.
4. Selecione o **pedido avançado**.
5. Clique em Next.
6. Seleto **submeta um pedido do certificado usando base64 um arquivo do PKCS codificado #10 ou uma requisição de renovação usando base64 um arquivo do PKCS codificado #7**.
7. Cole a saída de etapa 8 da criação uma seção da solicitação de assinatura de certificado no campo codificado Base64 do pedido do certificado.
8. Clique em Submit.
9. **Certificado de CA da transferência do** clique.
10. Clique a **salvaguarda**, datilografe um nome para o certificado, e salvar o a seu diretório de FTP.

Instale o certificado em uma ferramenta de windows

Transfira o certificado de CA a seu servidor FTP

Conclua estes passos:

1. Consulte a CA (**http://IP_of_CA_server/certsrv/) de** seu servidor FTP.
2. Seleto **recupere o certificado de CA ou a lista de revogação de certificado**.
3. Clique em Next.
4. Selecione **Base64 codificou**.
5. Clique o **certificado de CA da transferência**.
6. Clique a **salvaguarda**, datilografe um nome para o certificado, e salvar o a seu diretório de FTP.

Instale o certificado de CA em seu dispositivo

Termine estas etapas.

1. Vai à **configuração de sistema > ao certificado ACS Setup > a instalação da autoridade de certificação ACS**.
2. **Arquivo de certificado de CA da transferência do** clique.
3. Datilografe o endereço IP ou nome do host do servidor FTP no campo do servidor FTP.
4. Datilografe um nome de usuário válido que o Cisco Secure ACS possa usar para alcançar o servidor FTP no campo do início de uma sessão.
5. Datilografe a senha correta para o username no campo de senha.
6. Datilografe o caminho relativo do diretório raiz do servidor FTP ao diretório que contém o arquivo de certificado de CA no campo remoto do diretório de FTP.
7. Datilografe o nome do arquivo de certificado de CA no campo de nome de arquivo remoto FTP.
8. Clique em Submit.
9. Verifique o nome de arquivo no campo.
10. Clique em Submit.
11. Reinicie os serviços ACS na **configuração de sistema > no controle de serviço**.**Nota:** Se você salta as etapas no certificado de CA da transferência a seu servidor FTP e as instala o certificado de CA em suas seções uma do dispositivo destas duas situações pode elevarar:Você não pode permitir o EAP-TLS, e um Mensagem de Erro parece indicar que o certificado de servidor não está instalado mesmo que o certificado seja instalado.Alternativamente, o `tipo` falha `não configurada EAP` ocorre nas falhas de tentativa mesmo que o tipo EAP seja configurado.**Nota:** Igualmente note que, se você usou um intermediário CA para criar seu certificado de servidor, você precisa de repetir estas etapas para cada CA na corrente entre a CA raiz e o certificado de servidor (que incluem o certificado CA raiz). Adicionalmente, se você criou seus certificados de cliente com CA diferente de seu certificado de servidor, você deve repetir estas etapas para a CA raiz e todos os CA intermediários envolvidos na criação do certificado de cliente.

Instale o certificado de servidor em seu dispositivo

Conclua estes passos:

1. Vá à **instalação da configuração de sistema > do certificado ACS**.
2. Clique em Install ACS Certificate (Instalar certificado ACS).
3. Selecione o certificado lido da opção de arquivo.
4. Clique o link de **arquivo certificado da transferência**.
5. Datilografe o endereço IP ou nome do host do servidor FTP no campo do servidor FTP.
6. Datilografe um nome de usuário válido que o Cisco Secure ACS possa usar para alcançar o servidor FTP no campo do início de uma sessão.
7. Datilografe a senha correta no campo de senha.
8. Datilografe o caminho relativo do diretório raiz do servidor FTP ao diretório que contém o arquivo de certificado de servidor no campo remoto do diretório de FTP.
9. Datilografe o nome do arquivo de certificado de servidor no campo de nome de arquivo remoto FTP.
10. Clique em Submit.
11. Datilografe o trajeto e a senha para a chave privada. Refira etapas 3 e 4 da criação uma seção da solicitação de assinatura de certificado.
12. Clique em Submit.

Outras tarefas

Configurar ajustes da autenticação global

Conclua estes passos:

1. Clique a **configuração de sistema no** servidor ACS.
2. Clique a **instalação da autenticação global**.
3. A verificação **permite o EAP-TLS**.
4. Selecione umas ou várias opções da verificação de certificado. Se você seleciona todos os métodos, o ACS tenta cada método em ordem até que uma verificação bem-sucedida ocorra ou até o último método falhar.
5. Clique em Submit.
6. Reinicie o PC.

Estabelecer o AP no ACS

Termine estas etapas para estabelecer o AP no ACS:

1. Clique a **configuração de rede no** servidor ACS.
2. O clique **adiciona a entrada** a fim adicionar um cliente de AAA.
3. Especifique estes valores nas caixas:Endereço IP de Um ou Mais Servidores Cisco ICM NT do cliente de AAA — IP_of_your_APChave — Compõe um chave (se certifique que a chave combina a chave secreta compartilhada AP)Autentique usando-se — RAIO (Cisco Aironet)
4. Clique em Submit.
5. Reinicie o PC.**Nota:** Não mude alguns dos padrões na instalação do cliente de AAA.

Configurar o AP

Nota: O rede-EAP é necessário se você quer instalar o ACU.

Se você usa a rotação chave da transmissão, você não precisa de ajustar uma chave enquanto a chave deve já ser ajustada. Se a chave não é ajustada, vá **Setup o avanço do > Rádio** e ajustar um valor para a rotação da chave da transmissão. Você provavelmente não precisa de ajustar este nenhuns mais baixos então minutos 5 (300 segundos). Depois que você ajusta o valor, clique a **APROVAÇÃO**, e retorne à página do Radio Data Encryption.

VxWorks

Conclua estes passos:

1. Abra o AP.
2. Escolha o **Authentication Server do Instalação > Segurança >**.
3. Incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT ACS.
4. Incorpore o segredo compartilhado. Este valor deve combinar a chave ACS.
5. Verifique a caixa da **autenticação de EAP**.
6. Clique em **OK**.
7. Escolha o **Radio Data Encryption do Instalação > Segurança >**.

8. Verifique a caixa **aberta**.
9. Se você não usa a rotação chave da transmissão, selecione a **chave de WEP 1** e **128**.
10. Mude Use of Data Encryption por estações à **criptografia total** (se você não pode mudar este, o clique **se aplica** primeiramente).
11. Clique em **OK**.

Interface da WEB IO AP

Conclua estes passos:

1. Escolha a **Segurança > o gerenciador do servidor**.
2. Escolha o RAIO da lista do servidor atual.
3. Datilografe o endereço IP de Um ou Mais Servidores Cisco ICM NT ACS.
4. Datilografe o segredo compartilhado. Este valor deve combinar a chave no ACS.
5. Verifique a caixa da **autenticação de EAP**.
6. Da lista da autenticação de EAP, escolha o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius.
7. Clique a **APROVAÇÃO na** caixa de diálogo de advertência.
8. Clique em Apply.

Gerenciador de SSID (criptografia de WEP somente)

Termine estas etapas para a criptografia de WEP somente:

1. Escolha o SSID da lista atual SSID, ou especifique um SSID novo no campo SSID.
2. Verifique a caixa da **autenticação aberta**.
3. Escolha **com o EAP da** lista.
4. Verifique a caixa da **rede EAP**.
5. Clique em Apply.

Gerenciador de criptografia (criptografia de WEP somente)

Termine estas etapas para a criptografia de WEP somente:

1. Escolha a **Segurança > o gerenciador de criptografia**.
2. Clique o botão de rádio da **criptografia de WEP**.
3. Escolha imperativo da lista.
4. Clique o botão de rádio da **chave de criptografia 1**.
5. Especifique a chave.
6. Escolha o **128 da** lista do tamanho chave.
7. Clique em Apply.**Nota:** A configuração difere se você usa o WPA. Veja o suplemento ao gerenciamento chave WPA na extremidade deste documento para detalhes.

Transfira e instale o certificado CA raiz para o cliente

Esta etapa *é exigida* para *cada* cliente para que o EAP-TLS trabalhe nesse cliente. Conclua estes passos:

1. Consulte a CA (**http://IP_of_CA_server/certsrv/) do** PC cliente.
2. Seleto **recupere um certificado de CA**.
3. Clique em Next.
4. Selecione **Base64 codificou**.
5. Clique o **certificado de CA da transferência**.
6. Clique **aberto**.
7. O clique **instala o certificado**.
8. Clique em Next.
9. **Lugar** seleto **todos os Certificados na seguinte loja**.
10. O clique **consulta**.
11. Verifique a caixa das **lojas do show physical**.
12. Expanda **Autoridades de certificação de raiz confiável**, e selecione o **computador local**.
13. Clique em **OK**.
14. Clique em Next.
15. Clique em Finish.
16. **A APROVAÇÃO do** clique na caixa de mensagem com a `importação era` mensagem `bem sucedida`.

Crie o certificado de cliente

Empresa CA

Conclua estes passos:

1. Consulte a CA (**http://IP_of_CA_server/certsrv/) da** conta de usuário do cliente.
2. Selecione o **pedido uma** opção do **certificado**.
3. Clique em Next.
4. Selecione o **pedido avançado**.
5. Clique em Next.
6. Seleto **submeta um pedido de certificado para este CA usando um formulário**.
7. Clique em Next.
8. Escolha o **usuário na** lista do molde de certificado.
9. Ajuste estes valores sob as opções chaves:CSP — V1.0 do provedor criptográfico de base MicrosoftTamanho chave — 1024Todas as outras opções — Retenha os valores padrão
10. Clique em Submit.Uma caixa de mensagem aparece com `seu pedido do certificado foi…` mensagem `recebida`.

CA autônomo

Conclua estes passos:

1. Consulte a CA (**http://IP_of_CA_server/certsrv/) da** conta de usuário do cliente.
2. Selecione o **pedido uma** opção do **certificado**.
3. Clique em Next.
4. Selecione o **pedido avançado**.
5. Clique em Next.
6. Seleto **submeta um pedido de certificado para este CA usando um formulário**.

7. Clique em Next.
8. Datilografe o username no campo do CN. Este valor deve combinar o username na base de dados de autenticação.
9. Selecione o certificado de autenticação de cliente para a finalidade pretendida.
10. Ajuste estes valores sob as opções chaves:CSP — V1.0 do provedor criptográfico de base MicrosoftTamanho chave — 1024Todas as outras opções — Retenha os valores padrão
11. Clique em Submit.Uma caixa de mensagem aparece com `seu pedido do certificado foi…` mensagem `recebida`.

Aprove o certificado de cliente de CA

Conclua estes passos:

1. Escolha o **iniciar > programas > ferramentas administrativas > o Certificate Authority** para abrir CA.
2. Expanda o certificado à esquerda.
3. Clique **durante pedidos**.
4. Clicar com o botão direito no certificado e selecione todas as tarefas.
5. Selecione a **edição**.

Instale o certificado de cliente no PC cliente

Conclua estes passos:

1. Consulte a CA (**http://IP_of_CA_server/certsrv/) da** conta de usuário do cliente.
2. Selecione a **verificação em um certificado pendente**.
3. Clique em Next.
4. Selecione o certificado.
5. Clique em Next.
6. O clique **instala.Nota:** A fim verificar a instalação certificada, vá ao Microsoft Internet explorer, e selecione **ferramentas > opções de internet > índice > Certificados**. Um certificado com o nome do usuário entrado - a identificação ou a obrigação username estam presente.

Confie o certificado de cliente no ACS

Você precisa de executar estas etapas somente se os certificados de cliente e o certificado de servidor foram criados com os CA diferentes.

1. Assegure-se de que os certificados de CA do certificado CA raiz e do intermediário estejam instalados conforme as etapas na instalação o certificado de CA no servidor ACS e instale-se o certificado de CA em suas seções do dispositivo.
2. Vá à **configuração de sistema > ao certificado ACS Setup no** ACS.
3. Clique em Edit Certificate Trust List.
4. Verifique a caixa ao lado da CA raiz que criou o certificado de cliente.
5. Clique em Submit.

Setup o cliente para o EAP-TLS

Conclua estes passos:

1. Escolha o **Iniciar > Painel de Controle > Conexões de Rede**.
2. Clicar com o botão direito a rede Wireless, e selecione **propriedades**.
3. Clique a aba da **rede Wireless**.
4. Assegure-se de que os **indicadores do uso a configurar…** estejam verificados.
5. O clique **configura** se você vê o SSID na lista. Se não, o clique **adiciona**.
6. Põe no SSID.
7. Verifique o **WEP** e a **chave é fornecido para mim automaticamente** caixas de seleção.
8. Selecione a aba da **autenticação**.**Nota:** Se você não vê a aba da autenticação, o serviço do 802.1X está instalado em um estado desabilitado. A fim resolver esta edição, você deve permitir o serviço de configuração sem fio na lista de serviços. Conclua estes passos:Clicar com o botão direito o **meu computador**, e seleto **controle**.Clique **serviços e aplicativos**.Clique em **Services**.Ajuste o valor Startup para o serviço a **automático**.Comece o serviço.**Nota:** Se a aba da autenticação esta presente mas é não disponível, esta indica que o direcionador do adaptador de rede não apoia o 802.1x corretamente. Refira a utilização da autenticação do 802.1x nos computadores de cliente que estão executando o Windows 2000 .
9. Assegure-se de que que **permite o controle de acesso de rede que usa-se…** é verificado.
10. Selecione a **placa inteligente ou o outro certificado** para o tipo EAP, e clique **propriedades**.
11. Selecione o **certificado do uso nesta opção de computador**.
12. Verifique a caixa de verificação da **seleção de certificado simples do uso**.
13. Verifique a caixa para ver se há CA sob o certificado do root confiável.
14. Clique a **APROVAÇÃO** extremamente.

Faça à máquina o suplemento à autenticação

A autenticação da máquina do EAP-TLS *exige* o diretório ativo e uma raiz CA da empresa a fim adquirir um certificado para a autenticação da máquina do EAP-TLS, o computador deve ter a Conectividade à empresa CA através de uma conexão ligada com fio ou através da conexão Wireless com Segurança do 802.1x desabilitada. Esta é a *única* maneira de obter um certificado da máquina válido (com “máquina” no campo do “molde de certificado”). Quando terminado, o certificado da máquina é instalado nos **Certificados (computador local) > pessoal >** dobrador dos **Certificados** quando visto nos Certificados (computador local) MMC pressão-em. O certificado contém o nome de máquina totalmente qualificado AD no assunto e em campos SAN. Um certificado que carregasse o nome do computador mas não foi criado como descrito nesta seção não é um certificado da máquina verdadeiro (com a “máquina” no campo do molde de certificado). Tal certificado não é usado para a autenticação da máquina mas um pouco o OS vê um certificado como um certificado de usuário normal.

Instalação ACS para permitir a autenticação da máquina

Conclua estes passos:

1. Vá às **bases de dados de usuário externo > à configuração do base de dados**.
2. Clique em Windows Database.
3. Clique em Configurar.
4. Verifique a caixa de verificação da **autenticação da máquina do EAP-TLS da possibilidade**.
5. Clique em Submit.

Configurar o domínio para a inscrição automática do certificado

Conclua estes passos:

1. Abra os usuários e os computadores MMC pressão-sobre em um controlador de domínio.
2. Clicar com o botão direito a entrada de domínio e selecione **propriedades**.
3. Vá à aba da **política do grupo**.
4. selecione a **política do domínio padrão**.
5. O clique **edita**.
6. Vá ao **Configuração de Computador > Configurações do Windows > Configurações de Segurança > às políticas da chave pública**.
7. Clicar com o botão direito **ajustes automáticos do pedido do certificado**.
8. Escolha o **pedido do certificado novo > automático**.
9. Clique em Next.
10. Destaque o **computador**.
11. Clique em Next.
12. Verifique a empresa CA.
13. Clique em Next.
14. Clique em Finish.

Setup o cliente de autenticação da máquina

Unir ao domínio

Se o cliente se juntou ao domínio antes que você configurou a inscrição automática, o certificado deveu ser emitido à máquina a próxima vez que você recarrega o computador depois que a inscrição automática está configurada sem a necessidade re-de se juntar ao computador ao domínio.

Termine estas etapas para juntar-se ao domínio:

1. Log em Windows com uma conta que tenha privilégios do administrado.
2. Clicar com o botão direito no **meu computador** e escolha **propriedades**.
3. Selecione a aba do **nome de computador**.
4. Clique a **mudança**.
5. Datilografe o hostname no campo de nome de computador.
6. Selecione o **domínio**.
7. Datilografe o nome do domínio.
8. Clique em **OK**.Uma caixa de diálogo do início de uma sessão aparece.
9. Entre com credenciais de uma conta que tenha a permissão se juntar ao domínio.O computador junta-se ao domínio.
10. Reinicie o computador.O computador é agora um membro do domínio, e tem um certificado para CA e um certificado da máquina instalados.

Suplicante do EAP-TLS da instalação para a autenticação da máquina

Conclua estes passos:

1. Escolha o **Iniciar > Painel de Controle > Conexões de Rede**.
2. Clicar com o botão direito a conexão de rede e selecione **propriedades**.
3. Selecione a aba da **autenticação**.
4. A verificação **autentica como o computador**.

Suplemento ao gerenciamento chave WPA

Esta seção é aplicável ao Cisco IOS AP 12.02(13)JA1, ACS 3.2, e XP SP1 com correção dinâmica de WPA. De acordo com a documentação nesta seção, os clientes do Windows 2000 não apoiam nativamente o gerenciamento chave WPA e você deve usar o software do cliente do vendedor a fim obter este apoio. Refira a vista geral da atualização da segurança Wireless WPA em Windows XP .

O ACU Cisco não apoia o gerenciamento chave WPA para o EAP host-baseado (EAP-TLS e PEAP) atualmente. Você deve instalar um cliente da terceira, por exemplo, o cliente Odyssey do funk ou os aegis cliente de Meetinghouse. Refira documentos do adaptador de Wireless LAN para Windows para mais informações sobre do apoio WPA para o Produtos da Cisco. Esta informação é aplicável ao Windows mobile 2003 clientes (do Pocket PC) igualmente.

O gerenciamento chave WPA é basicamente o mesmo, mas difere nestes dois procedimentos:

1. Configurar o AP.
2. Estabelecer o cliente XP para o EAP-TLS e o WPA.

Configurar o AP

Conclua estes passos:

1. Vá à **Segurança > ao gerenciador de criptografia**.
2. Clique a **opção de cifra WEP**.
3. Escolha o **TKIP**.
4. Clique em Apply.
5. Vá à **Segurança > ao gerenciador de SSID**.
6. Escolha o SSID da lista atual SSID. Alternativamente, você pode especificar um SSID novo no campo SSID.
7. Verifique a **autenticação aberta**.
8. Escolha **com o EAP da** lista.
9. Verifique a **rede EAP**.
10. Selecione **imperativo da** lista sob o gerenciamento chave autenticado.
11. Clique o **WPA**.
12. Clique em Apply.

Estabelecer o cliente XP para o EAP-TLS e o WPA

Conclua estes passos:

1. Escolha o **Iniciar > Painel de Controle > Conexões de Rede**.
2. Clicar com o botão direito a rede Wireless, e selecione **propriedades**.

3. Selecione a aba da **rede Wireless**.
4. Assegure-se de que os **indicadores do uso para configurar a** opção estejam verificados.
5. O clique **configura** se você vê o SSID na lista. Se não, o clique **adiciona**.
6. Põe no SSID.
7. Escolha o **WPA** para a autenticação de rede.
8. Escolha o **TKIP** para a criptografia de dados.
9. Selecione a aba da **autenticação**.
10. Assegure-se de que que **permite a utilização do controle de acesso de rede** é verificada.
11. Selecione a **placa inteligente ou o outro certificado** para o tipo EAP.
12. Clique em Propriedades.
13. Selecione o **certificado do uso nesta opção de computador**.
14. Verifique a caixa de verificação da **seleção de certificado simples do uso**.
15. Verifique a caixa para ver se há CA sob o certificado do root confiável.
16. Clique a **APROVAÇÃO** extremamente.

Verificar

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

Troubleshooting

Erro: Problema com o certificado ao conectar ao WLAN

Este erro aparece no cliente Wireless.

```
O server do “server> <Authentication” apresentou um certificado válido emitido “pelo name> <CA”,
mas “o name> <CA” não é configurado como uma âncora válida da confiança para este perfil.
```

Solução

A fim resolver esta edição, você pode exportar o certificado de raiz de CA que emitiu o certificado ao Authentication Server a um arquivo. Copie o arquivo ao cliente Wireless e execute então este comando de um comando prompt elevado.

```
certutil - empresa - addstore NTAuth CA_CertFilename.cer
```

Refira a alerta de segurança de Windows aparece ao conectar a uma rede Wireless em uma máquina do grupo de trabalho para mais informação.

Informações Relacionadas

- Cisco Secure ACS para página de suporte do Windows
- Cisco Secure ACS para página de suporte do UNIX
- Suporte Técnico e Documentação - Cisco Systems

Obrigado para seu feedback.

Abra um caso de suporte (exige um contrato de serviço Cisco.)

Cisco relacionado apoia discussões da comunidade

Cisco apoia a comunidade é um fórum para que você faça e responda a perguntas, sugestões da parte, e colabora com seus pares.

Refira convenções dos dicas técnicas da Cisco para obter informações sobre das convenções usadas neste documento.

Atualizado em: outubro 14, 2009
ID do Documento: 64064