

PEAP sob redes Wireless unificadas com ACS 5.1 e server de Windows 2003

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Configurar](#)

[Diagrama de Rede](#)

[Empresa 2003 de Windows Setup com IIS, Certificate Authority, DNS, DHCP \(CA\)](#)

[CA \(democa\)](#)

[Secure ACS 5.1 de Cisco 1121](#)

[A instalação usando o dispositivo da série CSACS-1121](#)

[Instale o servidor ACS](#)

[Configuração de controle de Cisco WLC5508](#)

[Crie a configuração necessária para WPAv2/WPA](#)

[Autenticação de PEAP](#)

[Instale os moldes de certificado Pressão-em](#)

[Crie o molde de certificado para o servidor de Web ACS](#)

[Permita o molde de certificado novo do servidor de Web ACS](#)

[Instalação do certificado ACS 5.1](#)

[Configurar o certificado Exportable para o ACS](#)

[Instale o certificado no software ACS 5.1](#)

[Configurar a loja da identidade ACS para o diretório ativo](#)

[Adicionar um controlador ao ACS como um cliente de AAA](#)

[Configurar políticas de acesso ACS para o Sem fio](#)

[Crie a política de acesso ACS e a regra do serviço](#)

[Configuração de cliente para o PEAP usando Windows zero toques](#)

[Execute uma instalação básica e uma configuração](#)

[Instale o adaptador de rede Wireless](#)

[Configurar a conexão de rede Wireless](#)

[Pesquise defeitos a autenticação wireless com ACS](#)

[A autenticação de PEAP falha com servidor ACS](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento descreve como configurar o acesso wireless seguro usando controladores de

LAN Wireless, o software Microsoft Windows 2003 e o Cisco Secure Access Control Server (ACS) 5.1 via Protected Extensible Authentication Protocol (PEAP) com a versão 2 do Microsoft Challenge Handshake Authentication Protocol (MS-CHAP).

Nota: Para obter informações sobre do desenvolvimento de fixe o Sem fio, refira o [modelo do Web site do Wi-fi](#) de Microsoft e do [Sem fio da segurança do Cisco](#).

Pré-requisitos

Requisitos

Há uma suposição que o instalador tem a instalação de Windows 2003 do conhecimento do gerenciamento de recursos básicos e a instalação do controlador de LAN do Cisco Wireless enquanto este documento cobre somente as configurações específicas para facilitar os testes.

Para a instalação inicial e a informação de configuração para os controladores do Cisco 5508 Series, refira o [guia de instalação do controlador wireless do Cisco 5500 Series](#). Para a instalação inicial e a informação de configuração para os controladores do Cisco 2100 Series, refira o [guia de início rápido: Controlador do Wireless LAN do Cisco 2100 Series](#).

Microsoft Windows 2003 Guias de Instalação e Configuração pode ser encontrado em [instalar Windows Server 2003 R2](#).

Antes que você comece, instale o Microsoft Windows server 2003 com sistema operacional SP1 em cada um dos server no laboratório de teste e atualize todos os pacotes de serviços. Instale os controladores e o Lightweight Access Points (regações) e assegure-se de que as atualizações de software mais recente estejam configuradas.

Windows Server 2003 com SP1, edição de empreendimento, é usado de modo que a inscrição automática de Certificados do usuário e da estação de trabalho para a autenticação de PEAP possa ser configurada. A inscrição automática do certificado e autorenewal facilitam distribuir Certificados e melhorar a Segurança automaticamente expirando e renovando Certificados.

Componentes Utilizados

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

- Controlador do Cisco ou Series que corridas 7.0.98.0
- Protocolo do Access point do peso leve de Cisco 1142 (LWAPP) AP
- Empresa de Windows 2003 com Internet Information Server (IIS), Certificate Authority (CA), DHCP, e Domain Name System (DNS) instalado
- Dispositivo do sistema de controle de acesso seguro de Cisco 1121 (ACS) 5.1
- Profissional de Windows XP com SP (e pacotes de serviços actualizados) e placa de interface da rede Wireless (NIC) (com apoio CCX v3) ou suplicante da terceira parte.
- Cisco 3750 Switch

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.

[Diagrama de Rede](#)

Este documento utiliza a seguinte configuração de rede:

Cisco fixa a topologia de lab wireless

O propósito principal deste documento é fornecer-lhe o procedimento passo a passo para executar o PEAP sob redes Wireless unificadas com ACS 5.1 e o servidor de empreendimento de Windows 2003. A ênfase principal está na inscrição automática do cliente de modo que o cliente auto-registre e tome o certificado do server.

Nota: A fim adicionar o acesso protegido por wi-fi (WPA)/WPA2 com o padrão de codificação do Temporal Key Integrity Protocol (TKIP) /Advanced (AES) ao profissional de Windows XP com SP, referem a [atualização do elemento de informação dos serviços do abastecimento WPA2/Wireless \(WPS IE\) para Windows XP com pacote de serviços 2](#).

[Empresa 2003 de Windows Setup com IIS, Certificate Authority, DNS, DHCP \(CA\)](#)

[CA \(democa\)](#)

CA é um computador que execute Windows Server 2003 com SP2, edição de empreendimento, e execute estes papéis:

- Um controlador de domínio para o **domínio demo.local** que executa o IIS
- Um servidor DNS para o **domínio de DNS demo.local**
- Um servidor DHCP
- CA raiz da empresa para o **domínio demo.local**

Execute estas etapas a fim configurar CA para estes serviços:

1. [Execute uma instalação básica e uma configuração.](#)
2. [Configurar o computador como um controlador de domínio.](#)
3. [Levante o nível funcional do domínio.](#)
4. [Instale e configure o DHCP.](#)
5. [Instale serviços certificados.](#)
6. [Verifique permissões de administrador para Certificados.](#)

7. [Adicionar computadores ao domínio.](#)
8. [Permita o acesso Wireless aos computadores.](#)
9. [Adicionar usuários ao domínio.](#)
10. [Permita o acesso Wireless aos usuários.](#)
11. [Adicionar grupos ao domínio.](#)
12. [Adicionar usuários ao grupo dos wirelessusers.](#)
13. [Adicionar computadores de cliente ao grupo dos wirelessusers.](#)

Execute a instalação básica e a configuração

Execute estas etapas:

1. Instale Windows Server 2003 com SP2, edição de empreendimento, como um server autônomo.
2. Configurar o protocolo TCP/IP com o endereço IP de Um ou Mais Servidores Cisco ICM NT de *10.0.10.10* e a máscara de sub-rede de *255.255.255.0*.

Configurar o computador como um controlador de domínio

Execute estas etapas:

1. A fim começar o assistente de instalação de diretório ativo, escolha o **Iniciar > Executar**, **datilografe dcpromo.exe**, e clique a **APROVAÇÃO**.
2. Na boa vinda à página do assistente de instalação de diretório ativo, clique **em seguida**.
3. Na página da compatibilidade do sistema operacional, clique **em seguida**.
4. No tipo página, **controlador de domínio** seletor para **um domínio novo** e clique do controlador de domínio **em seguida**.
5. Na página nova do domínio da criação, no **domínio** seletor em uma **floresta nova** e no clique **em seguida**.
6. Na instalação ou configurar a página DNS, selecione o **nenhum, apenas instale e configurar o DNS neste computador** e clique-o **em seguida**.
7. Na página do Domain Name, no tipo **demo.local** e no clique novos em seguida.
8. Na página do Domain Name de NetBIOS, dê entrada com o nome de netbios do domínio como o **programa demonstrativo** e clique-o **em seguida**.
9. Nos dobradores que do base de dados e do log os lugar paginam, aceitam o base de dados do padrão e registram diretórios dos dobradores e clicam-nos **em seguida**.
10. Na página compartilhada do volume de sistema, verifique que o local da pasta do padrão está correto e clique-o **em seguida**.
11. Nas permissões pagine, verifique que as **permissões compatíveis somente com Windows 2000 ou Windows Server 2003 sistemas operacionais** estão selecionadas e clique **em seguida**.
12. Nos serviços de diretório restaure a página da senha de administração do modo, deixe a placa de caixas de senha e clique-a **em seguida**.
13. Reveja a informação na página de sumário e clique-a **em seguida**.
14. Quando você é feito com a instalação de diretório ativo, clique o **revestimento**.
15. Quando alertado para reiniciar o computador, clique o **reinício agora**.

Levante o nível funcional do domínio

Execute estas etapas:

1. Abra os **domínios e as confianças do diretório ativo** pressão-do dobrador das **ferramentas administrativas** (**iniciar > programas > ferramentas administrativas > domínios e confianças do diretório ativo**), e clicar com o botão direito então o computador de domínio **CA.demo.local**.
2. Clique o **nível funcional do domínio do aumento**, e selecione então **Windows Server 2003** na página do nível funcional do domínio do aumento.
3. Clique o **aumento**, clique a **APROVAÇÃO**, e clique então a **APROVAÇÃO** outra vez.

[Instale e configurar o DHCP](#)

Execute estas etapas:

1. Instale o **protocolo de configuração dinâmica host (DHCP)** como um componente de **serviço de rede** usando **adiciona ou remove programas** no Control Panel.
2. Abra o **DHCP** pressão-do dobrador das **ferramentas administrativas** (**iniciar > programas > ferramentas administrativas > DHCP**), e destaque então o servidor DHCP, **CA.demo.local**.
3. Clique a **ação**, e clique-a então **autorizam** a fim autorizar o serviço DHCP.
4. Na árvore de console, clicar com o botão direito **CA.demo.local**, e clique então o espaço novo.
5. Na página de boas-vindas do wizard de escopo novo, clique **em seguida**.
6. No espaço nomeie a página, tipo **CorpNet** no campo de nome.
7. Clique **em seguida** e preencha estes parâmetros: Comece o endereço IP **10.0.20.1** Termine o endereço IP **10.0.20.200** Comprimento - **24** Máscara de sub-rede - **255.255.255.0**
8. Clique **em seguida** e entre em **10.0.20.1** para o endereço IP de Um ou Mais Servidores Cisco ICM NT do começo e em **10.0.20.100** para que o endereço IP de Um ou Mais Servidores Cisco ICM NT da extremidade seja excluído. Em seguida, clique em **Avançar**. Isto reserva os endereços IP de Um ou Mais Servidores Cisco ICM NT na escala de **10.0.20.1** a **10.0.20.100**. Estes endereços IP de Um ou Mais Servidores Cisco ICM NT da reserva não são distribuídos pelo servidor DHCP.
9. Na página da duração de aluguel, clique **em seguida**.
10. Configurar as opções de DHCP paginam, escolhem **sim, eu quero configurar agora estas opções** e clicá-las **em seguida**.
11. Na página do roteador (gateway padrão) adicionar o endereço de roteador padrão de **10.0.20.1** e clique-o **em seguida**.
12. Na página do Domain Name e dos servidores DNS, datilografe **demo.local** no campo do domínio do pai, datilografe **10.0.10.10** no campo do endereço IP de Um ou Mais Servidores Cisco ICM NT, e clique então o clique de **Addand** em seguida.
13. Nas **VITÓRIAS** que os server paginam, clicam **em seguida**.
14. Na página do espaço da ativação, escolha **sim, eu quero ativar agora este espaço** e clicá-lo **em seguida**.
15. Quando você termina com a página nova do wizard de escopo, clique o **revestimento**.

[Instale serviços certificados](#)

Execute estas etapas:

Nota: O IIS deve ser instalado antes que você instale serviços certificados e o usuário deve ser parte da empresa Admin OU.

1. No Control Panel, aberto **adicionar ou remova programas**, e clique-os então **adicionam/removem componentes do Windows**.
2. Na página do Wizard de Componentes de Windows, escolha serviços certificados, e clique-os então em seguida.
3. No tipo página de CA, escolha a CA raiz da empresa e clique-a em seguida.
4. Em CA que identifica a página de informação, datilografe o *democa* no Common Name para esta caixa de CA. Você pode igualmente incorporar os outros detalhes opcionais. Clique então **em seguida** e aceite os padrões na página das configurações de base de dados do certificado.
5. Clique em Next. Após a conclusão da instalação, clique o **revestimento**.
6. Clique a **APROVAÇÃO** depois que você lê o mensagem de advertência sobre a instalação do IIS.

[Verifique permissões de administrador para Certificados](#)

Execute estas etapas:

1. Escolha o **Iniciar > Ferramentas Administrativas > a autoridade de certificação**.
2. Clicar com o botão direito o **democa CA** e clique então **propriedades**.
3. Na ABA de segurança, clique **administradores** na lista do grupo ou de nomes de usuário.
4. Nas permissões de administradores aliste, verifique que estas opções estão ajustadas **para reservar**: Emita e controle Certificados Controle CA Peça Certificados Se qualquer um são ajustados para negar ou não selecionados, ajuste as permissões **reservar**.
5. Clique a **APROVAÇÃO** para fechar a caixa de diálogo das propriedades de CA do democa, e feche então a autoridade de certificação.

[Adicionar computadores ao domínio](#)

Execute estas etapas:

Nota: Se o computador é adicionado já ao domínio, continue [adicionar usuários ao domínio](#).

1. Abra os **usuários e os computadores de diretório ativo** pressão-em.
2. Na árvore de console, expanda **demo.local**.
3. Clicar com o botão direito **computadores**, clique **novo**, e clique então o **computador**.
4. No objeto novo – A caixa de diálogo do computador, datilografa o nome do computador no campo de nome de computador e clica-o **em seguida**. Este exemplo usa o *cliente* do nome de computador.
5. Na caixa de diálogo controlada, clique **em seguida**.
6. No objeto novo – Caixa de diálogo do computador, **revestimento** do clique.
7. Repita etapas 3 com 6 a fim criar contas do computador adicional.

[Permita o acesso Wireless aos computadores](#)

Execute estas etapas:

1. Na árvore de console dos usuários e dos computadores de diretório ativo, clique o dobrador dos **computadores** e clicar com o botão direito no computador para que você quer atribuir o acesso Wireless. Este exemplo mostra o procedimento com computador cliente qual você adicionou em **propriedades do** clique de etapa 7., e vai então ao **guia de discagem de entrada**.
2. Na permissão de acesso remoto, escolha **permitem o acesso** e clicam a **APROVAÇÃO**.

[Adicionar usuários ao domínio](#)

Execute estas etapas:

1. Na árvore de console dos usuários e dos computadores de diretório ativo, clicar com o botão direito **usuários**, clique **novo**, e clique então o **usuário**.
2. No objeto novo – A caixa de diálogo do usuário, datilografa o nome do usuário Wireless. Este exemplo usa o *wirelessuser* do nome no campo de nome, e o *wirelessuser* no campo de nome de logon do usuário. Clique em Next.
3. No objeto novo – A caixa de diálogo do usuário, datilografa uma senha de sua escolha na senha e confirma campos de senha. Cancele o **usuário deve mudar a senha na** caixa de verificação **seguinte do fazer logon**, e clicam **em seguida**.
4. No objeto novo – Caixa de diálogo do usuário, **revestimento do** clique.
5. Repita etapas 2 a 4 a fim criar contas de usuário adicionais.

[Permita o acesso Wireless aos usuários](#)

Execute estas etapas:

1. Na árvore de console dos usuários e dos computadores de diretório ativo, clique a **pasta de usuários**, clicar com o botão direito o **wirelessuser**, clique **propriedades**, e vá então ao **guia de discagem de entrada**.
2. Na permissão de acesso remoto, escolha **permitem o acesso** e clicam a **APROVAÇÃO**.

[Adicionar grupos ao domínio](#)

Execute estas etapas:

1. Na árvore de console dos usuários e dos computadores de diretório ativo, clicar com o botão direito **usuários**, clique **novo**, e clique então o **grupo**.
2. No objeto novo – Agrupe a caixa de diálogo, datilografe o nome do grupo no campo de nome do grupo e clique a **APROVAÇÃO**. Este documento usa os *wirelessusers* do nome do grupo.

[Adicionar usuários ao grupo dos wirelessusers](#)

Execute estas etapas:

1. Na placa dos detalhes de usuários e de computadores de diretório ativo, fazer duplo clique no grupo *WirelessUsers*.
2. Vá à aba dos membros e o clique **adiciona**.
3. Nos usuários seletos, os contatos, caixa de diálogo dos computadores, ou dos grupos,

datilografam o nome dos usuários que você quer adicionar ao grupo. Este exemplo mostra como adicionar o *wirelessuser* do usuário ao grupo. Clique em **OK**.

4. No múltiplo os nomes encontraram a caixa de diálogo, **APROVAÇÃO** do clique. A conta de usuário do wirelessuser é adicionada ao grupo dos wirelessusers.
5. **APROVAÇÃO** do clique a fim salvar mudanças ao grupo dos wirelessusers.
6. Repita este procedimento para adicionar mais usuários ao grupo.

[Adicionar computadores de cliente ao grupo dos wirelessusers](#)

Execute estas etapas:

1. Repita etapas 1 e 2 nos [usuários adicionar à seção de grupo dos wirelessusers](#) deste documento.
2. Nos usuários seletos, a caixa de diálogo dos contatos, ou dos computadores, datilografa o nome do computador que você quer adicionar ao grupo. Este exemplo mostra como adicionar o computador nomeado *cliente* ao grupo.
3. Clique **tipos de objeto**, cancele a caixa de verificação dos **usuários**, e verifique então **computadores**.
4. Clique a **APROVAÇÃO** duas vezes. A conta do computador de cliente é adicionada ao grupo dos wirelessusers.
5. Repita o procedimento para adicionar mais computadores ao grupo.

[Secure ACS 5.1 de Cisco 1121](#)

[A instalação usando o dispositivo da série CSACS-1121](#)

O dispositivo CSACS-1121 é instalado com o software ACS 5.1. Esta seção dá-lhe uma vista geral do processo de instalação e das tarefas que você deve executar antes de instalar o ACS.

1. Conecte o CSACS-1121 ao console da rede e do dispositivo. Veja o [capítulo 4, “cabos de conexão.”](#)
2. Põe acima o dispositivo CSACS-1121. Veja o [capítulo 4, “pondo acima o dispositivo da série CSACS-1121.”](#)
3. Execute o **comando setup** na alerta CLI configurar as configurações inicial para o servidor ACS. Veja executar o programa de instalação.

[Instale o servidor ACS](#)

Esta seção descreve o processo de instalação para o servidor ACS no dispositivo da série CSACS-1121.

- [Execute o programa de instalação](#)
- [Verifique o processo de instalação](#)
- [Tarefas da Cargo-instalação](#)

Para informações detalhadas sobre da instalação do server do Cisco Secure ACS refira a [instalação e promova o guia para o Cisco Secure Access Control System 5.1.](#)

Configuração de controle de Cisco WLC5508

Crie a configuração necessária para WPAv2/WPA

Execute estas etapas:

Nota: A suposição é que o controlador tem a conectividade básica à rede e o IP reachability à interface de gerenciamento é bem sucedido.

1. Consulte a <https://10.0.1.10> a fim entrar ao controlador.
2. Clique em login.
3. Entre com o usuário padrão *admin* e senha padrão *admin*.
4. Crie uma relação nova para o mapeamento VLAN sob o menu do **controlador**.
5. Clique **relações**.
6. Clique em **New**.
7. No campo de nome da relação, inscreva o *empregado*. (Este campo pode ser todo o valor que você gostar.)
8. No campo do ID de VLAN, incorpore *20*. (Este campo pode ser todo o VLAN que for levado dentro a rede.)
9. Clique em Apply.
10. Configurar a informação como isto conecta > edita mostras do indicador: Conecte o endereço IP 10.0.20.2 Máscara de rede - 255.255.255.0 Gateway - 10.0.10.1 DHCP preliminar - 10.0.10.10
11. Clique em Apply.
12. Clique a aba **WLAN**.
13. Escolha **criam novo**, e o clique **vai**.
14. Dê entrada com um nome de perfil, e, no campo WLAN SSID, inscreva o *empregado*.
15. Escolha um ID para o WLAN, e o clique **aplica-se**.
16. Configurar a informação para este WLAN quando os WLAN > editam o indicador aparecem. **Nota:** WPAv2 é o método de criptografia escolhido da camada 2 para este laboratório. A fim permitir que o WPA com clientes TKIP-MIC associe a este SSID, você pode igualmente verificar o **modo de compatibilidade WPA** e **permitir aos clientes WPA2 TKIP** caixas ou aos aqueles clientes que não apoiam o método de criptografia de AES 802.11i.
17. No os WLAN > editam a tela, clicam o **tab geral**.
18. Certifique-se de que a caixa do estado está verificada para ver se há **permitido** e a **relação** apropriada (empregado) é escolhido. Também, certifique-se verificar a caixa de verificação **permitida** para ver se há a transmissão SSID.
19. Clique na guia Security.
20. Sob o secundário-menu da camada 2, verifique **WPA + WPA2** para ver se há a Segurança de camada 2. Para a criptografia WPA2, verifique **AES + TKIP** a fim permitir clientes TKIP.
21. Escolha o **802.1x** como o método de autenticação.
22. Salte o secundário-menu da camada 3 porque não se exige. Uma vez que o servidor Radius é configurado, o server apropriado pode ser escolhido do menu da autenticação.
23. **O QoS** e os **guias avançada** podem ser deixados no padrão a menos que todas as configurações especiais forem exigidas.
24. Clique o **menu Segurança** para adicionar o servidor Radius.

25. Sob o secundário-menu do RAIIO, clique a **autenticação**. Então, clique **novo**.
26. Adicionar o endereço IP de Um ou Mais Servidores Cisco ICM NT do servidor Radius (10.0.10.20) que é o servidor ACS configurado mais cedo.
27. Certifique-se de que a chave compartilhada combina o cliente de AAA configurado no servidor ACS. Certifique-se de que a caixa do **usuário de rede** está verificada e clique **aplicam-se**.
28. A configuração básica está agora completa e você pode começar a testar o PEAP.

Autenticação de PEAP

O PEAP com versão MS-CHAP 2 exige Certificados nos servidores ACS mas não nos clientes Wireless. O auto registro de Certificados do computador para os servidores ACS pode ser usado para simplificar um desenvolvimento.

A fim configurar o server de CA para fornecer a inscrição automática para o computador e os certificados de usuário, termine os procedimentos nesta seção.

Nota: Microsoft mudou o molde do servidor de Web com a liberação da empresa CA de Windows 2003 de modo que as chaves fossem já não exportable e a opção fosse esmaecida para fora. Não há nenhum outro molde de certificado fornecido com os serviços certificados que são para a autenticação de servidor e dão a capacidade para marcar as chaves porque exportable que estão disponíveis na gota-para baixo assim que você tem que criar um molde novo que faça assim.

Nota: O Windows 2000 permite chaves exportable e estes procedimentos não precisam de ser seguidos se você usa o Windows 2000.

Instale os moldes de certificado Pressão-em

Execute estas etapas:

1. Escolha o **Iniciar > Executar**, incorpore o *mmc*, e clique a **APROVAÇÃO**.
2. No menu de arquivo, o clique **adiciona/remove Pressão-em**, e clica então **adiciona**.
3. Sob Pressão-em, os **moldes de certificado do** clique duas vezes, **fim do** clique, e clicam então a **APROVAÇÃO**.
4. Na árvore de console, **moldes de certificado do** clique. Todos os moldes de certificado aparecem na placa dos detalhes.
5. A fim contornear etapas 2 a 4, incorpore *certtmpl.msc em que* abre os moldes de certificado pressão-.

Crie o molde de certificado para o servidor de Web ACS

Execute estas etapas:

1. Na placa dos detalhes dos moldes de certificado pressão-em, clique o molde do **servidor de Web**.
2. No menu de ação, clique o **molde duplicado**.
3. No campo de nome do indicador do molde, incorpore o *ACS*.
4. Vá à aba da **manipulação de pedido** e a verificação **permite que a chave privada seja exportada**. Igualmente assegure-se de que a **assinatura e a criptografia** estejam

selecionadas do menu suspenso da finalidade.

5. Escolha **pedidos deve usar um dos seguintes CSP** e verificar o **v1.0 do provedor criptográfico de base Microsoft**. Desmarcar todos os outros CSP que forem verificados, e clique a **APROVAÇÃO**.
6. Vá à aba do **nome do sujeito**, escolha a **fonte** no pedido, e clique a **APROVAÇÃO**.
7. Vá à **ABA de segurança**, destaque o **grupo de Admins do domínio**, e certifique-se de que a opção **se registrar** está verificada sob reservado. **Nota:** Se você escolhe construir desta verificação da informação do diretório ativo somente o **nome principal de usuário (UPN)** e para desmarcar o **nome do email incluir** no nome do sujeito e no email nomeie porque um nome do email não foi dado entrada com para a conta de usuário Wireless nos usuários e nos computadores de diretório ativo pressão-em. Se você não desabilita estas duas opções, a inscrição automática tenta usar o email, que conduz a um erro Auto-inscrição.
8. Há umas medidas de segurança adicional se necessário impedir que os Certificados estejam eliminados automaticamente. Estes podem ser encontrados sob a aba das exigências da emissão. Isto não é discutido mais neste documento.
9. Clique a **APROVAÇÃO** a fim salvar o molde e mover-se em emitir este molde do Certificate Authority pressão-em.

[Permita o molde de certificado novo do servidor de Web ACS](#)

Execute estas etapas:

1. Abra a autoridade de certificação pressão-em. Execute etapas 1 a 3 na [criação o molde de certificado para a](#) seção do [servidor de Web ACS](#), escolha a opção do **Certificate Authority**, escolha o **computador local**, e clique o **revestimento**.
2. Na árvore de console do Certificate Authority, expanda **ca.demo.local**, e clicar com o botão **direito então** moldes de certificado.
3. Vai a **novo >** o **molde de certificado a emitir**.
4. Clique o **molde de certificado ACS**.
5. Clique a **APROVAÇÃO** e abra os **usuários e os computadores de diretório ativo pressão-em**.
6. Na árvore de console, fazer duplo clique **usuários e computadores de diretório ativo**, clicar com o botão direito **demo.local**, e clique então **propriedades**.
7. Na aba da política do grupo, a **política do domínio padrão** do clique, e clica então **edita**. Isto abre o editor do objeto da política do grupo pressão-em.
8. Na árvore de console, expanda o **Configuração de Computador > Configurações do Windows > Configurações de Segurança >** as **políticas da chave pública**, e escolha então **ajustes automáticos do pedido do certificado**.
9. Clicar com o botão direito **ajustes automáticos do pedido do certificado**, e escolha o **pedido do certificado novo > automático**.
10. Na boa vinda à página automática do assistente de configuração do pedido do certificado, clique **em seguida**.
11. Na página do molde de certificado, clique o **computador**, e clique-o então **em seguida**.
12. Quando você termina a página automática do assistente de configuração do pedido do certificado, clique o **revestimento**. O tipo do certificado do computador aparece agora na placa dos detalhes do editor do objeto da política do grupo pressão-em.
13. Na árvore de console, expanda a **configuração do usuário >** os **ajustes do >** **segurança dos ajustes de Windows >** as **políticas da chave pública**.
14. Na placa dos detalhes, fazer duplo clique **ajustes Auto-inscrição**.

15. Escolha **registram Certificados automaticamente** e a verificação **renova certificados expirados, atualiza-os durante Certificados e remove-os os Certificados revogados e os Certificados da atualização que usam moldes de certificado.**
16. Clique em OK.

[Instalação do certificado ACS 5.1](#)

[Configurar o certificado Exportable para o ACS](#)

Nota: O servidor ACS deve obter um certificado de servidor do server da CA raiz da empresa a fim autenticar um cliente PEAP WLAN.

Nota: Certifique-se de que o gerenciador de IIS não está aberto durante o processo de instalação do certificado como problemas das causas com informação posta em esconderijo.

1. Entre ao servidor ACS com direitos de uma administração de conta.
2. Vá à **administração do sistema > à configuração > aos Certificados de servidor local**. Clique em Add.
3. Quando você escolhe um método da criação do certificado de servidor, escolha **gerenciem a solicitação de assinatura de certificado**. Clique em Next.
4. Incorpore um assunto e um comprimento chave do certificado como o exemplo, a seguir clique o **revestimento**: Assunto do certificado - **CN=acs.demo.local** Comprimento chave - **1024**
5. O ACS alertará que uma solicitação de assinatura de certificado esteve gerada. Clique em **OK**.
6. Sob a administração do sistema, vão à **configuração > aos Certificados de servidor local > as requisições de assinatura proeminentes**. **Nota:** A razão para esta etapa é que Windows 2003 não permite chaves exportable e você precisa de gerar um pedido do certificado baseado no certificado ACS que você criou mais cedo aquele faz.
7. Escolha a entrada da **solicitação de assinatura de certificado**, e clique a **exportação**.
8. Salvar o arquivo do **.pem** do certificado ACS ao desktop.

[Instale o certificado no software ACS 5.1](#)

Execute estas etapas:

1. Abra um navegador e conecte a CA o server URL **http://10.0.10.10/certsrv**.
2. O indicador dos serviços certificados de Microsoft aparece. Escolha o **pedido um certificado**.
3. Clique para submeter um **pedido do certificado avançado**.
4. No pedido avançado, o clique **submete um pedido do certificado usando um base-64-encoded...**
5. No campo da solicitação salva, se as licenças da Segurança do navegador, consultam ao arquivo e à inserção precedentes do pedido do certificado ACS.
6. As configurações de segurança do navegador não podem reservar alcançar o arquivo em um disco. Em caso afirmativo, **APROVAÇÃO** do clique para executar uma pasta manual.
7. Encontre o arquivo ACS *.pem da exportação precedente ACS. Abra o arquivo usando um editor de texto (por exemplo, bloco de notas).
8. Destaque o índice inteiro do arquivo, e clique a **cópia**.
9. Retorne ao indicador do pedido do certificado de Microsoft. **Cole** o índice copiado no campo

da solicitação salva.

10. Escolha o **ACS** como o molde de certificado, e o clique **submete-se**.
11. Uma vez que o certificado é emitido, escolha **Base64 codificado**, e clique o **certificado da transferência**.
12. Clique a **salv guarda** a fim salvar o certificado ao desktop.
13. Vão ao **ACS > a administração do sistema > a configuração > os Certificados de servidor local**. Escolha o **certificado assinado de CA do ligamento**, e clique-o **em seguida**.
14. O clique **consulta**, e encontra o certificado salvar.
15. Escolha o certificado ACS que foi emitido pelo server de CA, e clique **aberto**.
16. Também, verifique a caixa do protocolo para ver se há o **EAP**, e clique o **revestimento**.
17. O certificado CA-emitido ACS aparecerá no certificado do local ACS.

[Configurar a loja da identidade ACS para o diretório ativo](#)

Execute estas etapas:

1. Conecte ao ACS e ao início de uma sessão com a conta admin.
2. Vá aos **usuários e a identidade armazena > identidade externo armazena > diretório ativo**.
3. Incorpore o domínio *demo.local* do diretório ativo, *incorpore a senha* do server, e clique TestConnection. **Clique a ordem OKIN** para continuar.
4. Clique **mudanças da salvaguarda**. **Nota:** Para obter mais informações sobre do procedimento da integração ACS 5.x refira [ACS 5.x e mais tarde: Integração com exemplo de configuração do microsoft ative directory](#).

Adicionar um controlador ao ACS como um cliente de AAA

Execute estas etapas:

1. Conecte ao ACS, e vá aos **recursos de rede > aos dispositivos de rede e aos clientes de AAA**. O clique **cria**.
2. Participe nestes campos: Nome - **wlcIP - 10.0.1.10** Caixa de seleção do RAIO - **Verificado** Segredo compartilhado - **Cisco**
3. O clique **submete-se** quando terminado. O controlador aparecerá porque uma entrada na lista de dispositivos de rede ACS.

[Configurar políticas de acesso ACS para o Sem fio](#)

Execute estas etapas:

1. No ACS, vá às **políticas de acesso > aos serviços do acesso**.
2. No indicador dos serviços do acesso, o clique **cria**.
3. Crie um serviço do acesso, e dê entrada com um nome (por exemplo WirelessAD). Escolha **baseado no molde do serviço**, e clique **seleto**.
4. No diálogo do Web page, escolha o **acesso de rede – simples**. Clique em **OK**.
5. No diálogo do Web page, escolha o **acesso de rede – simples**. Clique em **OK**. Uma vez que o molde é selecionado, clique **em seguida**.
6. Sob protocolos permitidos, verifique as caixas para ver se há **Allow MS-CHAPv2** e **permita o PEAP**. Clique em **Finish**.

7. Quando o ACS o alerta ativar o serviço novo, clique **sim**.
8. No acesso novo preste serviços de manutenção que apenas foi criado/ativado, expanda e escolha à **identidade**. Para a fonte da identidade, clique **seleto**.
9. Escolha **AD1** para o diretório ativo que foi configurado no ACS, **APROVAÇÃO** do clique.
10. Confirme a fonte da identidade é AD1, e a **salv guarda** do clique **muda**.

Crie a política de acesso ACS e a regra do serviço

Execute estas etapas:

1. Vá às **políticas de acesso** > às **regras de seleção do serviço**.
2. O clique **cria na** janela de política da seleção do serviço. Dê à regra nova um nome (por exemplo, *WirelessRule*). Verifique a caixa para ver se há o **protocolo** para combinar o **raio**.
3. Escolha o **raio**, e clique a **APROVAÇÃO**.
4. Sob resultados, escolha **WirelessAD** para o serviço (criado na etapa precedente).
5. Uma vez que a regra wireless nova é criada, escolha e **mova** esta regra para a parte superior, que será a primeira regra para identificar a autenticação RADIUS wireless usando o diretório ativo.

Configuração de cliente para o PEAP usando Windows zero toques

Em nosso exemplo, o CLIENTE é um computador que execute o profissional de Windows XP com SP que atua como um cliente Wireless e obtém o acesso aos recursos do intranet através do Sem fio AP. Termine os procedimentos nesta seção a fim configurar o CLIENTE como um cliente Wireless.

Execute uma instalação básica e uma configuração

Execute estas etapas:

1. Conecte o CLIENTE ao segmento de rede do intranet usando um cabo do Ethernet conectado ao hub.
2. No CLIENTE, instale o profissional de Windows XP com SP2 como um computador do membro nomeado CLIENTE do domínio demo.local.
3. Instale o profissional de Windows XP com SP2. Isto deve ser instalado a fim ter o apoio PEAP. **Nota:** O Windows Firewall é girado automaticamente sobre no profissional de Windows XP com o SP2. Não desligue o Firewall.

Instale o adaptador de rede Wireless

Execute estas etapas:

1. Feche o computador de cliente.
2. Desligue o computador de cliente do segmento de rede do intranet.
3. Reinicie o computador de cliente, e entre então usando a conta do administrador local.
4. Instale o adaptador de rede Wireless. **Nota:** Não instale o software de configuração do

fabricante para o adaptador Wireless. Instale os direcionadores do adaptador de rede Wireless que usam o wizard de hardware adicionar. Também, quando alertado, forneça o CD fornecido pelo fabricante ou por um disco os direcionadores actualizados para o uso com o profissional de Windows XP com o SP2.

Configurar a conexão de rede Wireless

Execute estas etapas:

1. Termine e entre então usando a conta de **WirelessUser no domínio demo.local**.
2. Escolha o **começo** > o **Control Panel**, fazer duplo clique **conexões de rede**, e clicar com o botão direito então a **conexão de rede Wireless**.
3. Clique **propriedades**, vá à aba das **redes Wireless**, e certifique-se que o **uso Windows configurar meus ajustes da rede Wireless** está verificado.
4. Clique em **Add**.
5. Sob a aba da associação, inscreva o *empregado* no campo do nome de rede (SSID).
6. Escolha o **WPA** para a autenticação de rede, e certifique-se de que a criptografia de dados está ajustada ao **TKIP**.
7. Clique a aba da **autenticação**.
8. Valide que o tipo EAP está configurado para usar **EAP protegido (PEAP)**. Se não é, escolha o do menu suspenso.
9. Se você quer a máquina ser autenticado antes do início de uma sessão (que permite scripts do início de uma sessão ou política do grupo empurra para ser aplicado), a verificação **autentica como o computador quando a informação de computador está disponível**.
10. Clique em **Propriedades**.
11. Como o PEAP envolve a autenticação do server pelo cliente, assegure-se de que o **certificado de servidor da validação** esteja verificado. Também, certifique-se que CA que emitiu o certificado ACS está verificado sob o menu das Autoridades de certificação de raiz confiável.
12. Escolha a **senha fixada (EAP-MSCHAP v2)** sob o método de autenticação como é usado para a autenticação interna.
13. Certifique-se que a **possibilidade rapidamente para reconectar** a caixa de verificação está verificada. Então, **APROVAÇÃO** do clique três vezes.
14. Clicar com o botão direito o ícone da conexão de rede Wireless em systray, e clique então **redes Wireless disponíveis da vista**.
15. Clique a rede Wireless do empregado, e clique-a então **conectam**. O cliente Wireless mostrará **conectado** se a conexão é bem sucedida.
16. Depois que a autenticação é bem sucedida, verifique a configuração TCP/IP para ver se há o adaptador Wireless usando conexões de rede. Deve ter uma escala de endereço de 10.0.20.100-10.0.20.200 do escopo de DHCP ou do espaço criado para os clientes Wireless de CorpNet.
17. A fim testar a funcionalidade, abra um navegador e consulte a **http://10.0.10.10** (ou ao endereço IP de Um ou Mais Servidores Cisco ICM NT do server de CA).

Pesquise defeitos a autenticação wireless com ACS

Execute estas etapas:

1. Vão ao **ACS** > a **monitoração e os relatórios**, e clicam a **monitoração do lançamento & relatam o visor**.
2. Uma janela de ACS separada abrirá. **Painel do clique**.
3. Em minha seção de relatórios favorita, **autenticações do clique – RAIO – hoje**.
4. Um log mostrará todas as autenticações RADIUS porque passagem ou falha. Dentro de uma entrada registrada, clique sobre o **ícone da lupa na coluna dos detalhes**.
5. O detalhe da autenticação RADIUS fornecerá muita informação sobre as tentativas registradas.
6. A contagem da batida do serviço ACS pode fornecer uma vista geral das tentativas que combinam as regras criadas no ACS. Vão ao **ACS** > as **políticas de acesso** > os **serviços do acesso**, e clicam **regras de seleção do serviço**.

[A autenticação de PEAP falha com servidor ACS](#)

Quando seu cliente falha a autenticação de PEAP com um servidor ACS, verifique se você encontra o Mensagem de Erro `duplicado NAS da tentativa de autenticação` na opção das **falhas de tentativa** sob o menu do **relatório e da atividade do ACS**.

Você pôde receber este Mensagem de Erro quando o Microsoft Windows XP SP2 está instalado na máquina cliente e Windows XP SP2 autentica contra um server da terceira parte a não ser um server do Microsoft IAS. Em particular, o server do Cisco RADIUS (ACS) usa um método diferente para calcular o tipo de protocolo extensible authentication: Comprimento: Formato do valor (EAP-TLV) ID do que os usos de Windows XP do método. Microsoft identificou este como um defeito no suplicante de XP SP2.

Para um hotfix, o contato Microsoft e refere a [autenticação de PEAP do artigo não é bem sucedido quando você conecta a um servidor Radius da terceira](#) . [A questão subjacente é aquela no lado do cliente, com utilitário de windows, o rápido reconecta a opção é desabilitada para o PEAP à revelia. Contudo, esta opção é permitida à revelia no lado de servidor \(ACS\). A fim resolver esta edição, desmarcar o rápido reconectam a opção no servidor ACS \(sob opções do sistema global\). Alternativamente, você pode permitir o rápido reconecta a opção no lado do cliente para resolver a edição.](#)

Perorm estas etapas a fim permitir rapidamente reconecta no cliente que executa Windows XP usando o utilitário de windows:

1. Vá ao **começo** > aos **ajustes** > ao **Control Panel**.
2. Fazer duplo clique o ícone das **conexões de rede**.
3. Clicar com o botão direito o ícone da **conexão de rede Wireless**, e clique então **propriedades**.
4. Clique a aba das **redes Wireless**.
5. Escolha o **uso Windows configurar minha opção de configuração da rede Wireless** a fim permitir indicadores de configurar o adaptador cliente.
6. Se você tem configurado já um SSID, escolha o SSID e clique **propriedades**. Se não, clique **novo** a fim adicionar um WLAN novo.
7. Incorpore o SSID sob a aba da associação. Certifique-se de que a autenticação de rede está **aberta** e criptografia de dados é ajustado ao **WEP**.
8. Clique a **autenticação**.
9. Escolha a **autenticação do IEEE 802.1X** da possibilidade para esta opção de rede.
10. Escolha o **PEAP** como o tipo EAP, e clique **propriedades**.

11. Escolha a **possibilidade reconectam rapidamente** a opção na parte inferior da página.

Informações Relacionadas

- [PEAP sob redes Wireless unificadas com ACS 4.0 e Windows 2003](#)
- [Controlador de LAN do Cisco Wireless \(WLC\) e exemplo de configuração de Cisco ACS 5.x \(TACACS+\) para a autenticação da Web](#)
- [A instalação e guia da elevação para o Cisco Secure Access Control System 5.1](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)