

Configurando o Cisco Secure ACS for Windows v3.2 com autenticação da máquina PEAP-MS-CHAPv2

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Material de Suporte](#)

[Convenções](#)

[Diagrama de Rede](#)

[Configurar o Cisco Secure ACS for Windows v3.2](#)

[Obtenha um certificado para o servidor ACS](#)

[Configurar o ACS para utilizar um certificado do armazenamento](#)

[Especifique as autoridades de certificado adicionais em que o ACS deve confiar](#)

[Reinicie o serviço e configure as opções de PEAP no ACS](#)

[Especifique e configure o ponto de acesso como um cliente AAA](#)

[Configure o banco de dados de usuário externo](#)

[Reinicie o serviço](#)

[Configurar o ponto de acesso da Cisco](#)

[Configurar o cliente Wireless](#)

[Configurar o registro automático de máquina do certificado MS](#)

[Unir ao domínio](#)

[Instalar manualmente o certificado de raiz no Windows Client](#)

[Configure a rede Wireless](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

[Introdução](#)

Este documento demonstra como configurar Protocolo de autenticação extensível protegida (PEAP) com Cisco Secure ACS for Windows versão 3.2.

Para obter mais informações sobre de como configurar o acesso Wireless seguro usando controladores do Wireless LAN, o software de Microsoft Windows 2003, e o Serviço de controle de acesso Cisco Secure (ACS) 4.0, referem o [PEAP sob redes Wireless unificadas com ACS 4.0 e Windows 2003](#).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nas versões de software e hardware abaixo.

- Cisco Secure ACS para Windows versão 3.2
- Microsoft Certificate Services (instalado como Enterprise root certificate authority [CA])**Nota:** [Para obter mais informações, consulte o Manual passo a passo para configurar uma autoridade de certificação.](#)
- Serviço DNS com Windows 2000 Server com Service Pack 3**Nota:** [Se tiver problemas com o servidor CA, instale a correção dinâmica 323172. O cliente do Windows 2000 SP3 exige o hotfix 313664](#) permitir a autenticação do IEEE 802.1X.
- Cisco Aironet 1200 Series Wireless Access Point 12.01T
- IBM ThinkPad T30 executando Windows XP Professional com Service Pack 1

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 você está trabalhando em uma rede viva, assegure-se de que você compreenda o impacto potencial do comando any antes do usar.

Material de Suporte

o PEAP e o EAP-TLS constroem e usam um túnel da camada de soquete TLS/Secure (SSL). O PEAP usa somente a autenticação do lado de servidor; somente o server tem um certificado e prova sua identidade ao cliente. O EAP-TLS, contudo, usa a autenticação mútua em que o server e os clientes ACS ([AAA] do autenticação, autorização e relatório) têm Certificados e provam suas identidades entre si.

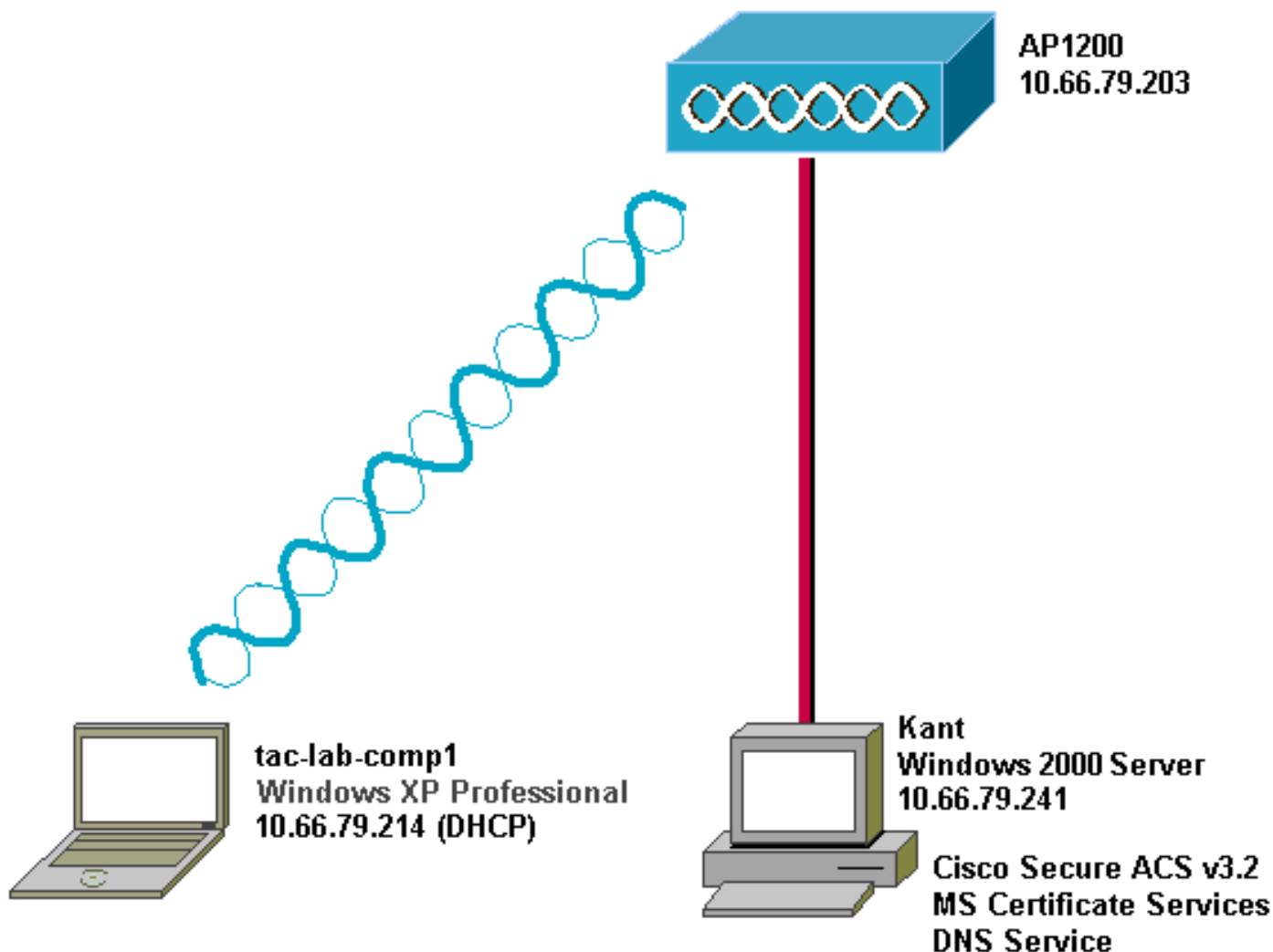
O PEAP é conveniente porque os clientes não exigem certificados. O EAP-TLS é útil para autenticar dispositivos decapitado, porque os Certificados não exigem nenhuma interação do usuário.

Convenções

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

Diagrama de Rede

Este documento utiliza a instalação de rede mostrada no diagrama abaixo.



Configurar o Cisco Secure ACS for Windows v3.2

Siga estas etapas para configurar ACS 3.2.

1. [Obtenha um certificado para o servidor de ACS.](#)
2. [Configure o ACS para utilizar um certificado do armazenamento.](#)
3. [Especifique autoridades de certificação adicionais nas quais o ACS deve confiar.](#)
4. [Reinicie o serviço e configure as definições PEAP no ACS.](#)
5. [Especifique e configure o ponto de acesso como um cliente AAA.](#)
6. [Configure os bancos de dados de usuário externo.](#)
7. [Reinicie o serviço.](#)

Obtenha um certificado para o servidor ACS

Siga estes passos para obter um certificado.

1. No servidor ACS, abra um navegador da Web e navegue até o servidor CA, digitando `http://CA-ip-address/certsrv` na barra de endereços. Efetuar logon no domínio como

Enter Network Password [?] [X]

 Please type your user name and password.

Site: 10.66.79.241

User Name: Administrator

Password: *****

Domain: SEC-SYD

Save this password in your password list

OK Cancel

Administrador.

2. Selecione o **pedido um certificado**, e clique-o então em

Microsoft Certificate Services -- Our TAC CA [Home](#)

Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.

Select a task:

- Retrieve the CA certificate or certificate revocation list
- Request a certificate
- Check on a pending certificate

Next >

seguida.

3. Selecione a solicitação Avançado e clique em

Choose Request Type

Please select the type of request you would like to make:

User certificate request:

User Certificate



Advanced request

Next >

Avançar.

4. Selecione Enviar uma solicitação de certificado para este CA, utilizando um formulário e, em seguida, clique em

Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Note that the policy of the certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Station.
You must have an enrollment agent certificate to submit a request for another user.

Next >

Avançar.

5. Configure as opções de certificado. Selecione o servidor da Web como modelo de certificado. Digite o nome do servidor de

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS

E-Mail:

Company:

Department:

City:

State:

Country/Region: US

ACS.

Defi

na o tamanho da chave como 1024. Selecione as opções para Mark keys as exportable e Use local machine store. Configure outras opções, conforme necessário e, em seguida, clique em

Key Options:

CSP: Microsoft Base Cryptographic Provider v1.0

Key Usage: Exchange Signature Both

Key Size: Min: 384 Max: 1024 (common key sizes: [512](#) [1024](#))

- Create new key set
 - Set the container name
- Use existing key set
- Enable strong private key protection
- Mark keys as exportable
 - Export keys to file

Use local machine store

You must be an administrator to generate a key in the local machine store.

Additional Options:

Hash Algorithm:

Only used to sign request.

Save request to a PKCS #10 file

Attributes:

Submit >

Enviar.

No

ta: Se você visualizar uma janela de advertência relacionada à violação de script (dependendo de suas configurações de segurança/privacidade do navegador), clique em Yes para




continuar.

6. Clique em Instalar este certificado.

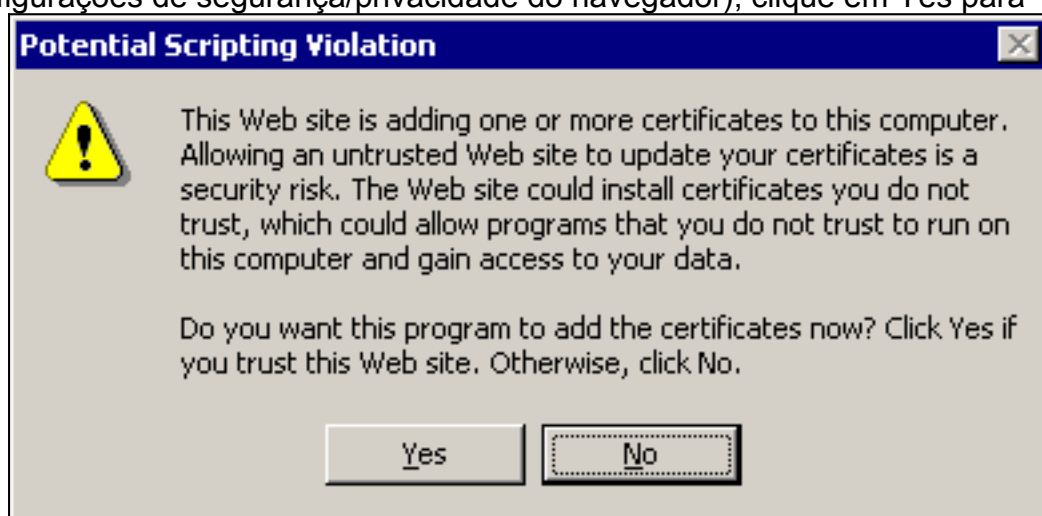
Microsoft Certificate Services -- Our TAC CA [Home](#)

Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

Nota: Se você visualizar uma janela de advertência relacionada à violação de script (dependendo de suas configurações de segurança/privacidade do navegador), clique em Yes para



continuar.

7. Se a instalação foi concluída com sucesso, você verá uma mensagem de confirmação.

Microsoft Certificate Services -- Our TAC CA [Home](#)

Certificate Installed

Your new certificate has been successfully installed.

[Configurar o ACS para utilizar um certificado do armazenamento](#)

Siga estas etapas para configurar o ACS a fim de utilizar o certificado em armazenamento.

1. Abra um navegador da Web e vá até o servidor ACS digitando `http://ACS-ip-address:2002/` na barra de endereços. Clique em System Configuration e, em seguida, em ACS Certificate Setup.
2. Clique em Install ACS Certificate (Instalar certificado ACS).
3. Selecione Use certificate from storage. No campo NC do certificado, dê entrada com o nome

do certificado que você atribuiu na etapa 5a da seção [obtem um certificado para o servidor ACS](#). Clique em Submit. Esta entrada deve combinar o nome que você datilografou no campo de nome durante o pedido do certificado avançado. É o nome NC no campo de assunto do certificado de servidor; você pode editar o certificado de servidor para verificar para ver se há este nome. Neste exemplo, o nome é "OurACS". Não digite o nome CN do

The screenshot shows the Cisco System Configuration web interface. On the left is a navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "System Configuration" and "Edit". Below this is the "Install ACS Certificate" section. It contains a sub-section "Install new certificate" with a help icon. There are two radio button options: "Read certificate from file" and "Use certificate from storage" (which is selected and circled in red). Below the selected option is a text input field for "Certificate CN" containing the text "OurACS". Below this are three more text input fields: "Private key file", "Private key", and "password". At the bottom of the form area is a yellow button with a question mark icon and the text "Back to Help". At the very bottom of the page are two buttons: "Submit" and "Cancel".

emissor.

4. Quando a configuração estiver concluída, você verá uma mensagem de confirmação indicando que a configuração do servidor ACS foi alterada. **Nota:** Você não precisa reiniciar o ACS desta

vez.

CISCO SYSTEMS

System Configuration

Edit

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

Install ACS Certificate

Installed Certificate Information ?

Issued to: OurACS
Issued by: Our TAC CA
Valid from: June 23 2003 at 02:19:56
Valid to: June 18 2005 at 00:52:30
Validity: OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Install New Certificate Cancel

[Especifique as autoridades de certificado adicionais em que o ACS deve confiar](#)

O ACS confiará automaticamente no CA que emitiu seu próprio certificado. Se os certificados do cliente forem emitidos por CAs adicionais, será necessário concluir os seguintes passos.

1. Clique em System Configuration e, em seguida, em ACS Certificate Setup.
2. Clique em ACS Certificate Authority Setup para adicionar CAs à lista de certificados confiáveis. No campo para o arquivo do certificado de CA, digite a localização do certificado e, em seguida, clique em

CISCO SYSTEMS

System Configuration

Edit

ACS Certification Authority Setup

CA Operations 

Add new CA certificate to local certificate storage

CA certificate file

 Back to Help

User Setup

Group Setup

Shared Profile Components

Network Configuration

System Configuration

Interface Configuration

Administration Control

External User Databases

Reports and Activity

Online Documentation

Submit.

3. Clique em Edit Certificate Trust List. Selecione todas as CAs nas quais o ACS deve confiar e desmarque todas as CAs nas quais o ACS não deve confiar. Clique em

CISCO SYSTEMS

System Configuration

Edit

Edit Certificate Trust List

Edit the Certificate Trust List (CTL)

Display Name (Friendly Name)

- ABA.ECOM Root CA
(DST (ABA.ECOM) CA)
- Autoridad Certificadora de la Asociacion Na
(Autoridad Certificadora de la Asociacion N)
- Autoridad Certificadora del Colegio Nacional
- Baltimore EZ by DST
(DST (Baltimore EZ) CA)
- Belgacom E-Trust Primary CA
- C&W HKT SecureNet CA Class A
(CW HKT SecureNet CA Class A)
- C&W HKT SecureNet CA Class B
(CW HKT SecureNet CA Class B)

Submit

[Reinicie o serviço e configure as opções de PEAP no ACS](#)

Siga estas etapas para reiniciar o serviço e para configurar ajustes PEAP.

1. Clique em System Configuration e, depois, em Service Control.
2. Clique em Restart (Reiniciar) para reiniciar o serviço.
3. Para configurar ajustes PEAP, clique a **configuração de sistema**, e clique então a **instalação global da autenticação**.
4. Verifique as duas configurações indicadas abaixo e deixe as demais como padrão. Se desejar, poderá especificar configurações adicionais, por exemplo, Enable Fast Reconnect. Quando terminar, clique em Enviar. **Permitir o EAP-MSCHAPv2 Permitir a autenticação do MS-CHAP versão 2** Nota: [Para obter mais informações sobre Fast Connect, consulte "Opções de configuração de autenticação" na configuração de sistema: Autenticação e certificados.](#)

