

Secure ACS para Windows v3.2 com autenticação da máquina do EAP-TLS

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Material de Suporte](#)

[Convenções](#)

[Diagrama de Rede](#)

[Configurando 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](#)

[Reiniciar o serviço e definir as configurações EAP-TLS no ACS](#)

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

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

[Reinicie o serviço](#)

[Configurando a inscrição automática no MS Certificate Machine](#)

[Configurando o Cisco Access Point](#)

[Configurando o cliente Wireless](#)

[Unir ao domínio](#)

[Obter um certificado para o usuário](#)

[Configure a rede Wireless](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar o protocolo extensible authentication – Transport Layer Security (EAP-TLS) com Cisco Secure Access Control System (ACS) para a versão do Windows 3.2.

Nota: A autenticação da máquina não é apoiada com Certificate Authority (CA) de Novell. O ACS pode usar o EAP-TLS para apoiar a autenticação da máquina ao diretório ativo de Microsoft Windows. O cliente do utilizador final pôde limitar o protocolo para a autenticação de usuário ao mesmo protocolo que é usado para a autenticação da máquina. Isto é, o uso do EAP-TLS para a autenticação da máquina pôde exigir o uso do EAP-TLS para a autenticação de usuário. Para obter mais informações sobre a autenticação da máquina, refira a seção da [autenticação da](#)

[máquina do](#) *Guia do Usuário para o Serviço de controle de acesso Cisco Secure 4.1.*

Nota: Quando estabelecer o ACS para autenticar máquinas através do EAP-TLS e do ACS estabelecer-se-á para a autenticação da máquina, o cliente deve ser configurado para fazer a autenticação da máquina somente. Para mais informação, consulte [como permitir a autenticação do computador-somente para uma rede 802.1X-based em Windows Vista, em Windows Server 2008, e em Windows XP Service Pack 3.](#)

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 e hotfix 323172](#)**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 estiver trabalhando em uma rede ativa, certifique-se de que entende o impacto potencial de qualquer comando antes de utilizá-lo.

Material de Suporte

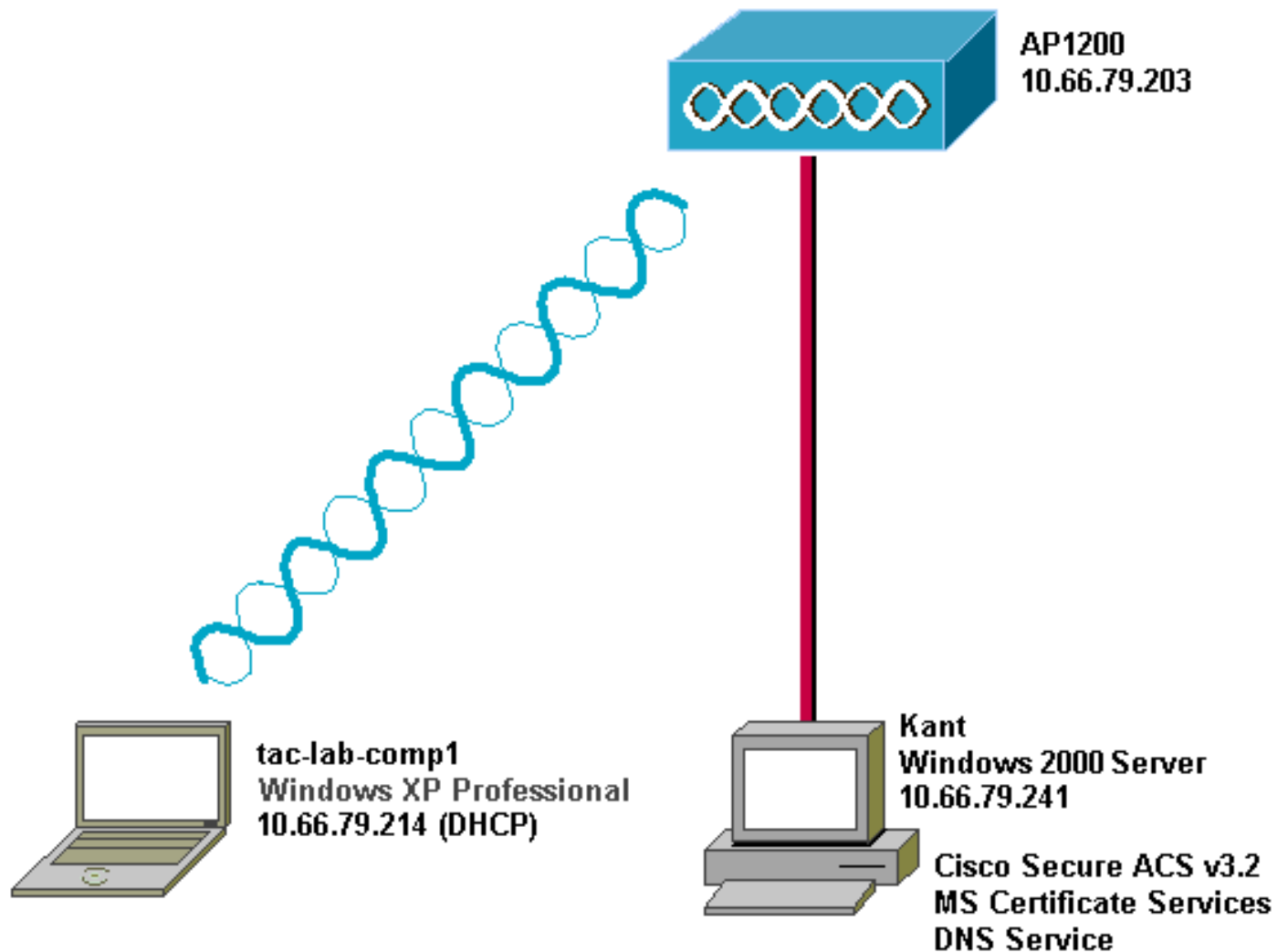
Tanto o EAP-TLS quanto o Protocolo protegido de autenticação extensível (PEAP) criam e utilizam um túnel TLS/Secure Socket Layer (SSL). O EAP-TLS usa a autenticação mútua, na qual tanto o servidor ACS (AAA - autenticação, autorização e relatório) quanto os clientes possuem certificados e comprovam suas identidades uns aos outros. O PEAP, contudo, usa somente a autenticação do lado de servidor; somente o server tem um certificado e prova sua identidade ao cliente.

Convenções

Para obter mais informações sobre convenções de documento, consulte as [Convenções de dicas técnicas Cisco](#).

Diagrama de Rede

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



Configurando o Cisco Secure ACS for Windows v3.2

Siga os passos abaixo para configurar o 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 entre em [http:// CA-ip-address/certsrv](http://CA-ip-address/certsrv) a fim alcançar o server de CA.
2. 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.

3. Selecione Solicitar um certificado e, em seguida, clique em Avançar.

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 >

4. 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.

5. 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.

6. Configurar as opções do certificado: Selecione o **servidor de Web** como o molde de certificado, e dê entrada com o nome do servidor

Advanced Certificate Request

Certificate Template:

Web Server

Identifying Information For Offline Template:

Name: OurACS

E-Mail:

Company:

Department:

City:

State:

Country/Region: US

ACS.

Incor

pore **1024** ao campo do tamanho chave, e verifique as **chaves de Mark como exportable** e **use** caixas de seleção da **loja de máquina local**. 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

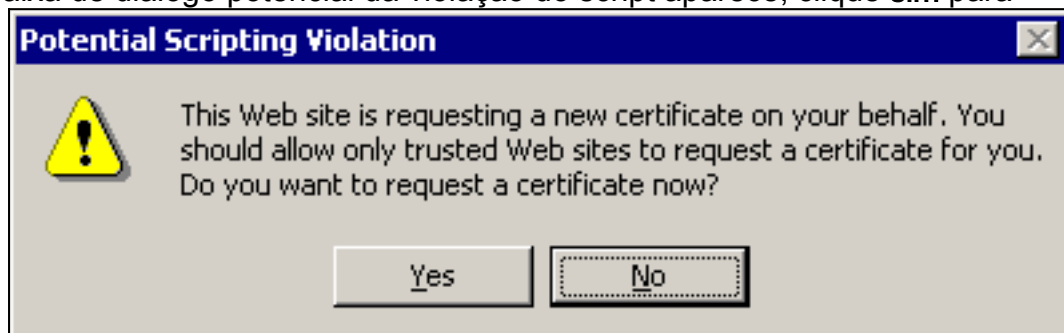
Attributes:

Submit >

Enviar.

No

ta: Se a caixa de diálogo potencial da violação do script aparece, clique **sim** para




continuar.

7. Clique em Instalar este certificado.

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

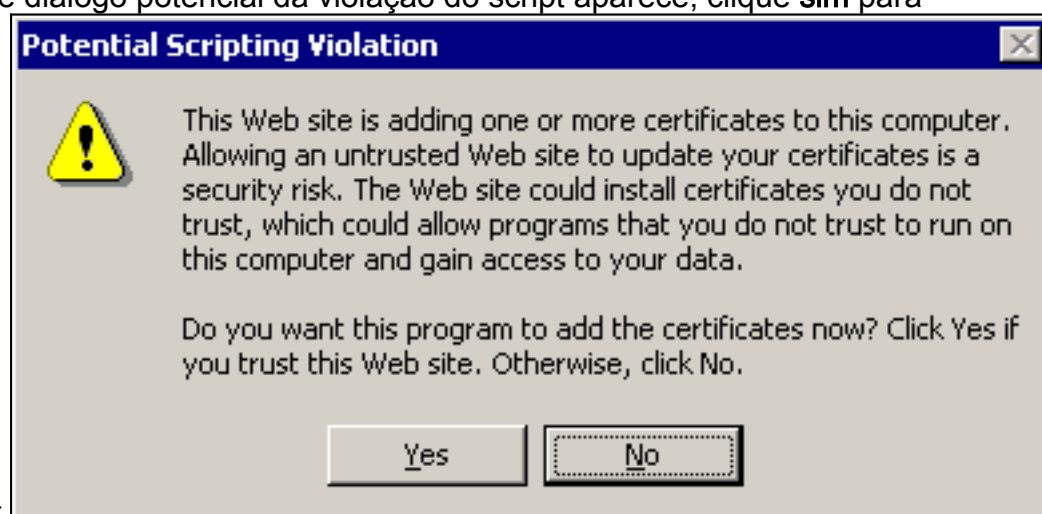
Certificate Issued

The certificate you requested was issued to you.

 [Install this certificate](#)

Nota: Se

a caixa de diálogo potencial da violação do script aparece, clique **sim** para



continuar.

8. Se a instalação é bem sucedida, a mensagem instalada certificado

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

Certificate Installed

Your new certificate has been successfully installed.

aparece.

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

Termine estas etapas a fim configurar o ACS para usar o certificado no armazenamento.

1. Abra um navegador da Web, e entre em **http:// ACS-ip-address:2002/** a fim alcançar o servidor ACS.
2. Clique em System Configuration e, em seguida, em ACS Certificate Setup.
3. Clique em Install ACS Certificate (Instalar certificado ACS).
4. Clique o **certificado do uso do** botão de rádio do **armazenamento**.
5. No campo do CN do certificado, dê entrada com o nome do certificado que você atribuiu na

etapa 5a de [obter um certificado do ACS Serversection](#) deste documento.

6. Clique em

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 with a red border), 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. A sub-section titled "Install new certificate" contains two radio button options: "Read certificate from file" and "Use certificate from storage". The "Use certificate from storage" option is selected and circled in red. Below it, a text box labeled "Certificate CN" contains the value "OurACS". Further down are text boxes for "Private key file" and "Private key 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 "Submit" and "Cancel" buttons.

Submit.

Um a vez que a configuração está completa, um mensagem de confirmação aparece que indique que a configuração do servidor ACS esteve mudada. **Nota:** Você não precisa reiniciar o ACS desta

vez.

The screenshot shows the Cisco System Configuration interface. On the left is a navigation menu with options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main area is titled 'System Configuration' and 'Edit'. A dialog box titled 'Install ACS Certificate' is open, showing 'Installed Certificate Information' with the following details:

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

Below the information is a red warning message: **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.** At the bottom of the dialog are two buttons: 'Install New Certificate' and 'Cancel'.

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

O ACS confia automaticamente CA que emitiu seu próprio certificado. Se os certificados de cliente são emitidos por CA adicionais, você deve terminar estas etapas:

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.
3. No campo para o arquivo do certificado de CA, digite a localização do certificado e, em seguida, clique em

The screenshot shows the Cisco System Configuration interface. At the top left is the Cisco Systems logo. The main title is "System Configuration". Below the title is a black bar with the word "Edit" in white. On the left side, there is a vertical navigation menu with icons and labels for: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration (highlighted in purple), Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "ACS Certification Authority Setup" and contains a section for "CA Operations" with a help icon. Below this, it says "Add new CA certificate to local certificate storage" and features a text input field labeled "CA certificate file". At the bottom of the main content area is a yellow button with a question mark icon and the text "Back to Help".

Submit.

4. Clique em Edit Certificate Trust List.
5. Selecione todas as CAs nas quais o ACS deve confiar e desmarque todas as CAs nas quais o ACS não deve confiar.
6. 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 Naciona
- 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.

[Reiniciar o serviço e definir as configurações EAP-TLS no ACS](#)

Termine estas etapas a fim reiniciar o serviço e configurar ajustes do EAP-TLS:

1. Clique em System Configuration e, depois, em Service Control.
2. Clique o **reinício** a fim reiniciar o serviço.
3. A fim configurar ajustes do EAP-TLS, clique a **configuração de sistema**, e clique então a **instalação da autenticação global**.
4. Marque Allow EAP-TLS e, em seguida, marque uma ou mais comparações de certificado.
5. Clique em

