

O acesso sem fios é feito através do SSID **minedu**.

3.6. Configuração de clientes Windows para 802.1x

No caso de um acesso sem fios verifique se tem a placa Wireless ligada, se a placa Wireless é compatível com a norma IEEE802.1x, se tem o(s) driver(s) da placa correctamente instalados (software da placa) e se possui dados de autenticação válidos (login/password).¹

Verifique também se o serviço relativo à autenticação 802.1x está activo. O serviço a activar depende do sistema operativo usado.

3.7. Configuração no Windows Vista

CONFIGURAÇÃO DA INTERFACE DE REDE

Para configurar um PC terminal com o sistema operativo Windows Vista, podem fazer-se os seguintes passos:

1. CONFIGURAR UMA LIGAÇÃO OU REDE

Activar o serviço “Configuração Automática com fios” e configurar como “Automático”;

No menu “Iniciar”, clique em “Ligar a”.

Na janela “Ligar a uma rede” clicar na ligação pretendida.

¹ *NOTA: Foi detetado que alguns antivírus (ex. Panda), firewalls e aplicativos de gestão Wireless prejudicam o processo de autenticação 802.1x., pelo que aconselhamos a sua desativação durante o processo de configuração da rede.*

Nesta janela escolha a opção “Ligar manualmente a uma rede sem fios”.

2. INFORMAÇÕES DA REDE

Defina o Nome de Rede (SSID - identificador de ligação). Selecciona a opção 802.1x no tipo de segurança, coloque um visto em “Iniciar automaticamente esta ligação” e “ligar mesmo que a rede não esteja a difundir”.

Clique em OK.

Clique na opção Alterar as definições da ligação:

3. PROPRIEDADES DA REDE

Na janela seguinte seleccione o separador Segurança. Escolha o método de autenticação EAP protegido (PEAP). Depois clique em Definições do método de autenticação. ²

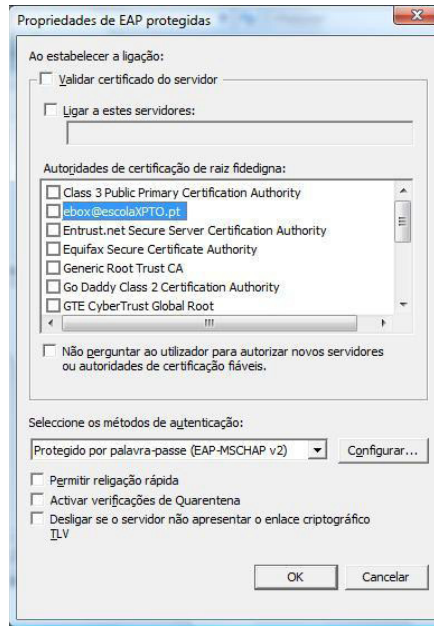
4. DEFINIÇÕES DO MÉTODO DE AUTENTICAÇÃO

Não é obrigatório seleccionar a opção “validar certificado do servidor” mas pode fazê-lo. Para isso é necessário que tenha instalado o certificado que valida o servidor. Esta opção aumenta a segurança do serviço porque garante que o servidor é de facto o servidor ao qual pretende ligar-se.

5. MÉTODO DE AUTENTICAÇÃO SEM VALIDAÇÃO DO CERTIFICADO

Se preferir não validar o certificado do servidor, desmarque a opção Validar certificado do servidor, de acordo com a figura.

² *NOTA: Deverá ajustar a configuração de “Tipo de Segurança” e “Tipo de encriptação” de forma a satisfazer os requisitos da rede da escola. Para exemplo foram usados WPA-Enterprise e TKIP, mas outras combinações poderão ser suportadas, nomeadamente 802.1x + WEP e WPA2-Enterprise + AES.*



6. MÉTODO DE AUTENTICAÇÃO COM VALIDAÇÃO DO CERTIFICADO

Selecione a opção Validar certificado do servidor. Em Autoridades de certificação de raiz fidedigna procure e selecione a autoridade de certificação que instalou (se não a encontrar, verifique os passos de instalação do certificado). Seleccione o método de autenticação EAP-MSCHAPv2.

7. PROPRIEDADE DE EAP MSCHAPV2

Clique no botão "Configurar..." do método de autenticação. Verifique que está seleccionado o método EAP-MSCHAPv2.

Nas propriedades do EAP-MSCHAPv2 tem de desactivar a opção de usar automaticamente o login/password do Windows.

8. CONCLUIR A CONFIGURAÇÃO

Confirme as configurações efectuadas clicando em OK em todas as janelas abertas usadas para a configuração da rede.

Ativar antivírus e firewalls. Este passo é necessário caso tenha desactivado algum software que estivesse a bloquear o processo de autenticação.

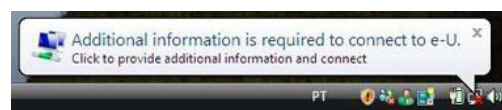
9. INICIAR A LIGAÇÃO

O Windows pesquisa a rede configurada e ao detectá-la pede os dados de autenticação.

Clique na mensagem que pede as credenciais.

Os dados necessários são apenas o nome de utilizador (no formato utilizador@domínio) e a palavra-chave.

Atenção: NÃO se deve preencher o campo domínio. A figura serve apenas de exemplo.



10. INTRODUZIR CREDENCIAIS

Introduza o seu username e password. Coloque o seu login no formato user@escola.pt.

Clique OK.

Se usar o formato user@escola.pt, quando se deslocar para instituições que tenham aderido ao Projeto, não precisa de fazer qualquer alteração para se autenticar e obter ligação de rede.



11. INSTALAÇÃO DO CERTIFICADO

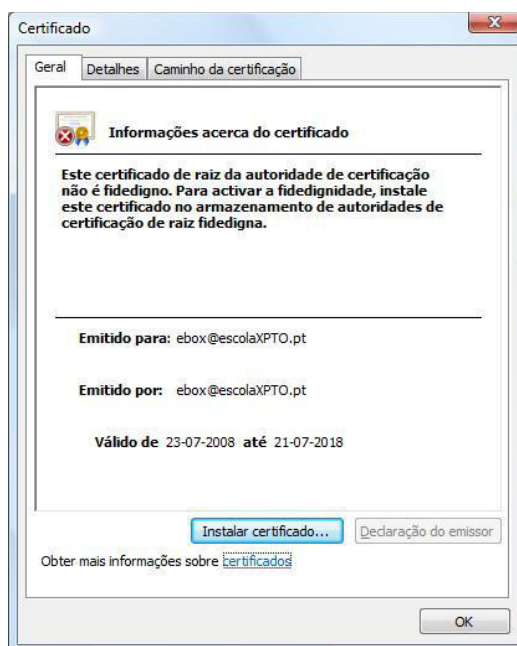
O certificado serve para validar o servidor de autenticação. Deste modo quando se liga à rede as suas credenciais só são entregues ao servidor se a validação dos certificados for positiva. Este processo é semelhante para as várias versões do Windows XP e Windows Vista.

12. CERTIFICADO

Depois de obter o ficheiro zip, abra-o e clique duas vezes em cacert.der. Deverá aparecer uma mensagem com informações sobre o certificado. Seleccione "Instalar certificado..." para proceder à sua instalação.

Use o assistente, escolha a opção "Colocar todos os certificados no seguinte arquivo", clique em "Procurar..." e seleccione "Autoridade de certificação de raiz fidedigna".

Para terminar aceite o aviso de segurança.



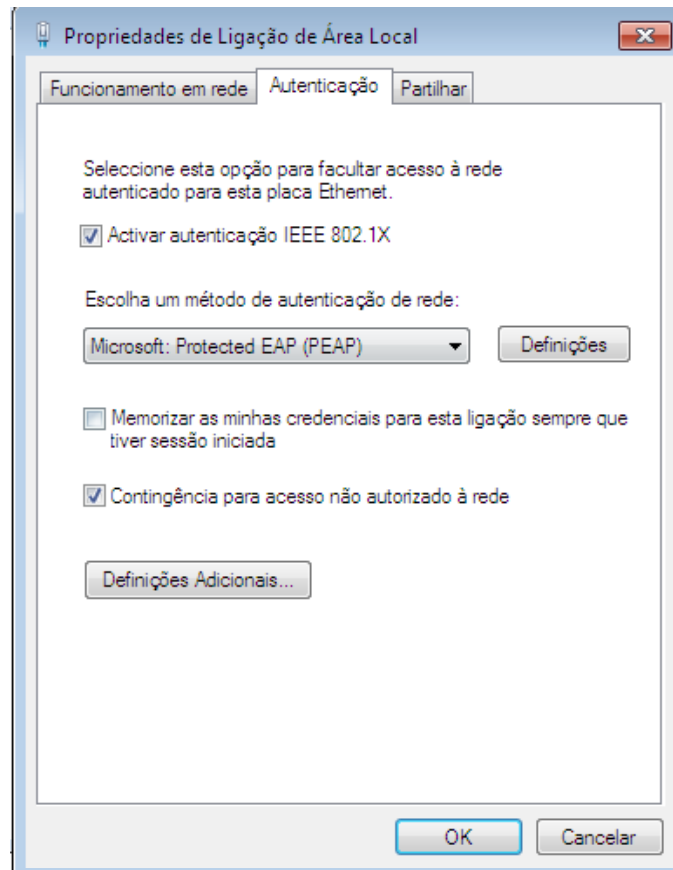
3.8. Configuração no Windows 7

CONFIGURAÇÃO DA INTERFACE DE REDE

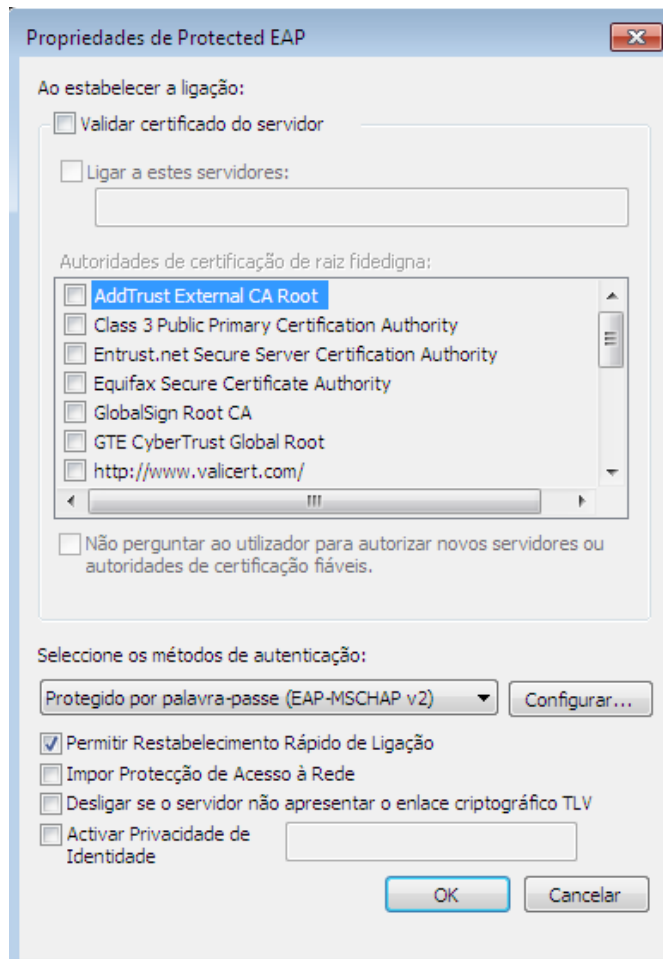
Para configurar um PC terminal com o sistema operativo Windows 7, podem fazer-se os seguintes passos:

13. CONFIGURAR UMA LIGAÇÃO OU REDE

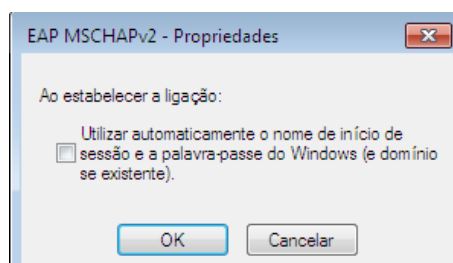
Activar o serviço “Configuração Automática com fios” e configurar como “Automático”;
Abrir o “Centro de Rede e Partilha”;
Selecione a placa de rede a configurar e clique com botão do lado direito do rato;
Escolha a opção “Propriedades” e o separador “Autenticação”;
Confira que as opções configuradas estão de acordo com a figura apresentada:



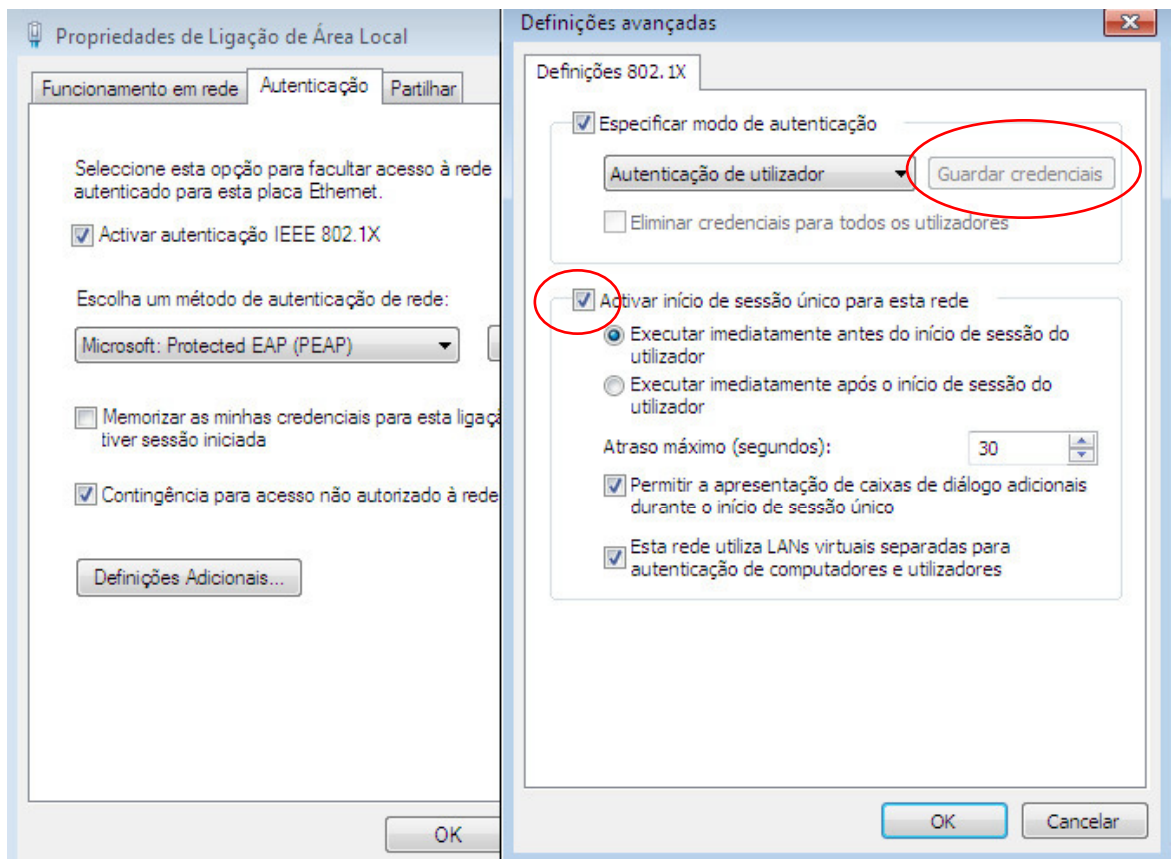
Nesta janela escolha a opção “Definições”
Confira que as opções configuradas estão de acordo com a figura apresentada:



Nesta janela escolha a opção “Configurar”
Confira que as opções configuradas estão de acordo com a figura apresentada, caso o servidor radius não esteja integrado com uma *Active Directory*.



Voltando ao separador “Autenticação”, clique em Definições Adicionais e aplique as configurações visíveis na figura:



14. INICIAR A LIGAÇÃO

○ Windows pesquisa a rede configurada e ao detecta-la pede os dados de autenticação.

Clique na mensagem que pede as credenciais.

Os dados necessários são apenas o nome de utilizador (no formato utilizador@domínio) e a palavra-chave.

Atenção: NÃO se deve preencher o campo domínio. A figura serve apenas de exemplo.

