Configurações de Firewall e DCOM no Windows 7 para aplicações Elipse.

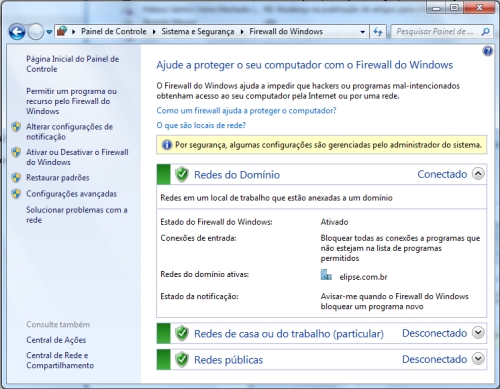
***\* Se o sistema operacional for o Windows XP/2003/Vista/2008, clique*** [***aqui***](http://kb.elipse.com.br/pt-br/questions/17/Configura%C3%A7%C3%B5es+de+Firewall+e+DCOM+no+Windows+XP%7B47%7D2003%7B47%7DVista%7B47%7D2008+para+aplica%C3%A7%C3%B5es+Elipse.) ***\****

**1) Elipse DCOM Wizard**

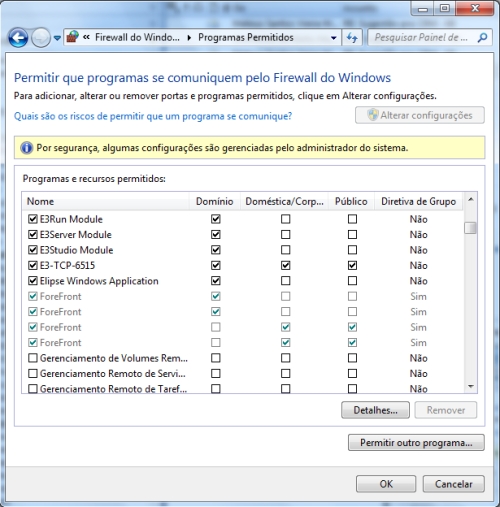
O Elipse DCOM Wizard é um assistente de configuração do DCOM (*Distributed Component Object Model*) e do Firewall do Windows para permitir conexões remotas. Apresenta configurações pré-definidas para os principais produtos da Elipse Software, mas pode ser usado também para configurar produtos de terceiros. **Ao executar o assistente, as configurações descritas abaixo serão aplicadas automaticamente.**

O download do **Elipse DCOM Wizard** está disponível [em nosso site.](http://www.elipse.com.br/port/download_opc.aspx)

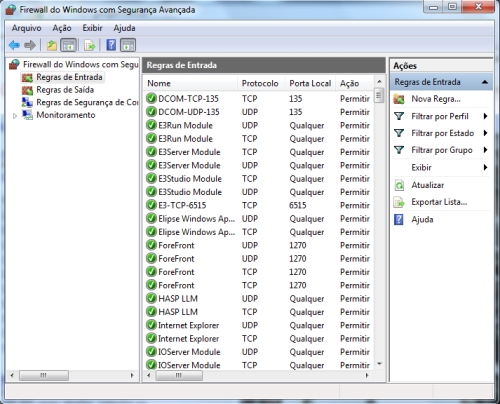
**2) Introdução**  
  
**Firewalls** são barreiras interpostas entre a rede privada e a rede externa com a finalidade de evitar ataques ou invasões; ou seja, são mecanismos (dispositivos) de segurança que protegem os recursos de hardware e software da empresa dos perigos aos quais o sistema está exposto. Estes mecanismos de segurança são baseados em hardware e software, e seguem a política de segurança estabelecida pela empresa.  
  
O **COM** (Component Object Model) da Microsoft é um sistema orientado a objetos, distribuído e independente de plataforma, destinado à criação de componentes de software binários que podem interagir entre si. O **DCOM** (Distributed Component Object Model) permite que os aplicativos sejam distribuídos entre os locais mais relevantes para o usuário e para o aplicativo. O protocolo de conexão DCOM oferece suporte de forma transparente, visando a comunicação confiável e eficiente entre os componentes COM. Por este motivo, os drivers de comunicação OPC utilizam este protocolo.  
  
Para que os sistemas Elipse possam funcionar adequadamente, é necessário fazer alguns ajustes nas configurações do Firewall e do DCOM, como veremos a seguir. Estes ajustes devem ser feitos tanto na máquina servidora quanto na máquina cliente, independentemente da comunicação ocorrer entre módulos do Elipse ou entre cliente e servidor OPC.  
  
  
**3) Firewall**  
  
Para acessar as configurações do Firewall, um atalho está disponível no Painel de Controle (Fig. 1).

  
**Figura 1** - Ativando o Firewall

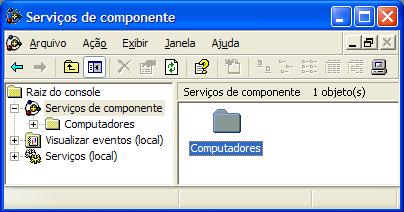
Caso escolha desabilitar o Firewall, nenhuma outra providência a seu respeito deverá ser tomada para o funcionamento do OPC Server ou qualquer outra funcionalidade dos produtos Elipse (note que ainda assim será necessário seguir as instruções contidas na sessão DCOM). Caso seja necessário ativar o Firewall, alguns passos deverão ser seguidos. Em primeiro lugar, deve-se liberar alguns programas do firewall clicando na opção **Permitir que programas se comuniquem pelo Firewall do Windows** (Fig. 2).

  
**Figura 2** - Liberando programas

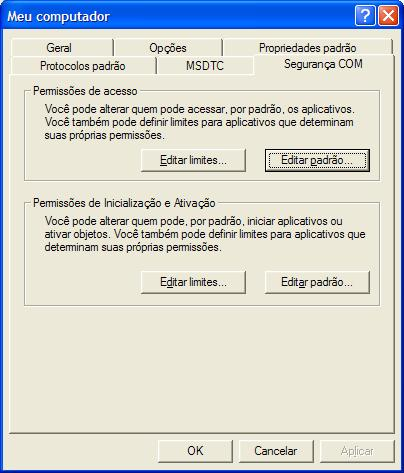
Basicamente, deve-se adicionar o E3OPCClient, o E3Server.exe, o E3Run.exe e o Studio.exe para o E3, e o Elipse32.exe para o Elipse SCADA. No caso do Elipse Drivers OPC, adicione o ED\_OPC.exe. Também deve ser adicionado o Opcenum.exe, que pode ser encontrado nas pastas C:\Windows\system32 (na versão 32 bits do Windows) ou C:\Windows\sysWOW64 (na versão 64 bits do Windows), o que permitirá a conexão remota de clientes OPC.  
  
Além dos programas, é necessário criar novas regras de entrada para liberar as portas TCP e UDP de número 135 e a porta TCP 445, utilizadas pelo DCOM, além da porta TCP de número 6515, responsável pela conexão do Viewer com o E3Server e Hot-Standby, e conexão do Studio a um E3Server remoto. Isto pode ser feito clicando na opção **Configurações Avançadas** da página inicial do Firewall (Fig. 3).

  
**Figura 3** - Liberando portas

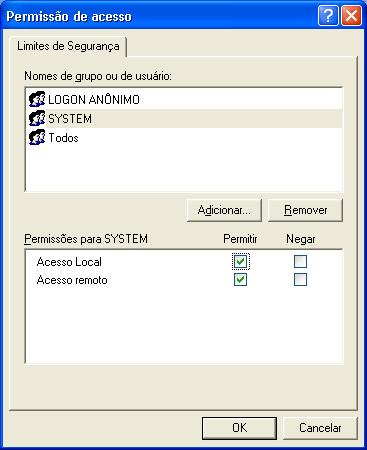
Feito isso, a aplicação está pronta para funcionar com o Firewall.  
  
  
**4) DCOM**  
  
Para configurar esta opção a partir da interface do usuário, o administrador deve abrir o gerenciador de **Serviços de componente** (dcomcnfg) e selecionar **Propriedades** no menu de contexto do computador a ser configurado (Fig. 4).

  
**Figura 4** - Selecionando o computador a ser configurado

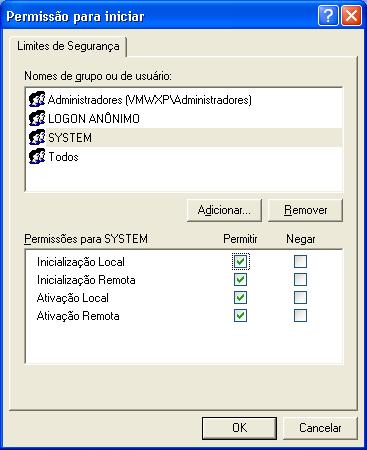
Será exibida uma caixa de diálogo (Fig. 5), e a segurança deverá ser configurada na aba **Segurança COM**.

  
**Figura 5** - Configurando a segurança

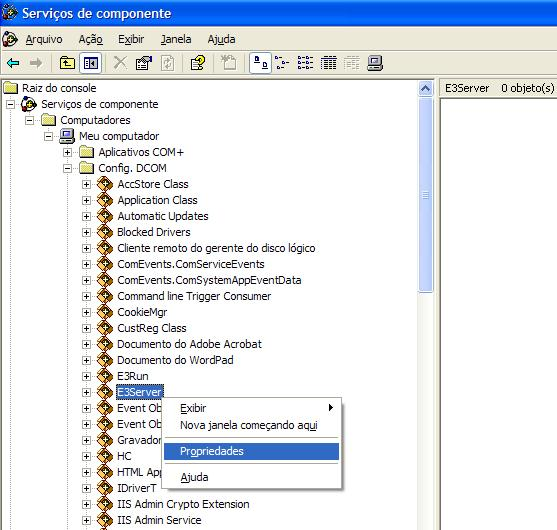
Clique em **Editar Limites...** na área **Permissões de acesso**, adicione os usuários LOGON ANÔNIMO, Todos e SYSTEM, e habilite as opções **Acesso Local** e **Acesso Remoto** de cada um deles (Fig. 6):

  
**Figura 6** - Definindo permissões de acesso

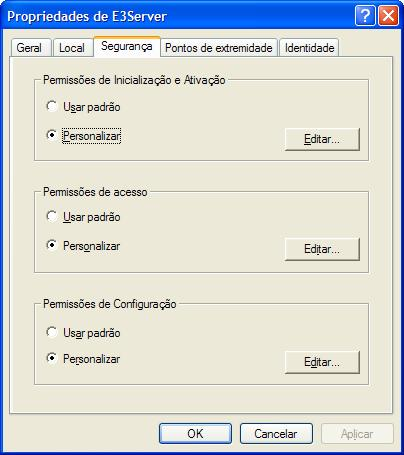
Clique em  **Editar Limites...** na área **Permissões de Inicialização e Ativação**, adicione os usuários LOGON ANÔNIMO e SYSTEM, e habilite as opções **Inicialização Remota** e **Ativação Remota**. Deve-se também marcar as opções **Inicialização Remota** e **Ativação Remota** do usuário Todos (Fig. 7):

  
**Figura 7** - Definindo permissões de acesso em Permissão para iniciar

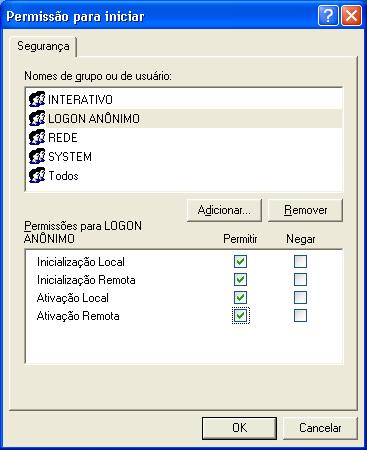
Também é necessário dar permissões de acesso, inicialização e ativação remota do **E3Server** para o usuário LOGON ANÔNIMO. Para isto, selecione as propriedades através do menu de contexto do E3Server, clicando com o botão direito do mouse sobre o E3Server (Fig. 8):

  
**Figura 8** - Selecionando as propriedades do E3Server

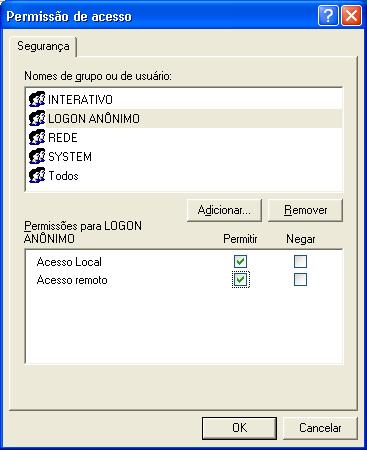
As configurações deverão ser feitas na aba **Segurança** (Fig. 9):

  
**Figura 9** - Configurando a segurança do E3Server

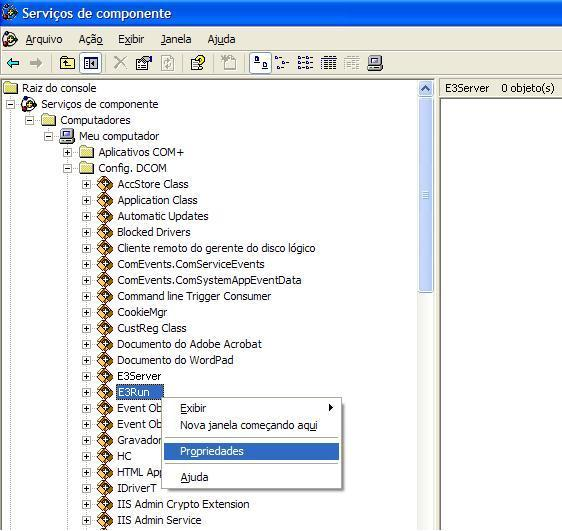
Clique em **Editar** na área **Permissões de Inicialização e Ativação**, adicione o usuário LOGON ANÔNIMO, e habilite as opções **Inicialização Remota** e **Ativação Remota** (Fig. 10):

  
**Figura 10** - Definindo permissões para iniciar o E3Server

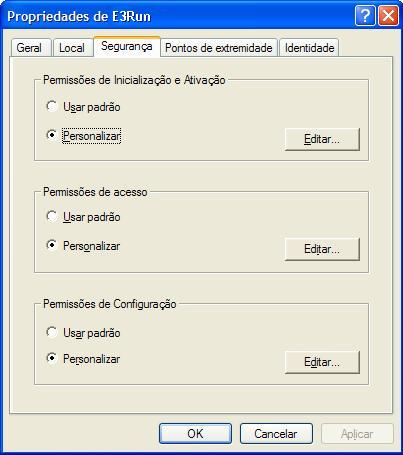
Clique em **Editar** na área **Permissões de acesso**, adicione o usuário LOGON ANÔNIMO, e habilite a opção **Acesso Remoto** (Fig. 11):

  
**Figura 11** - Definindo permissões de acesso para o E3Server

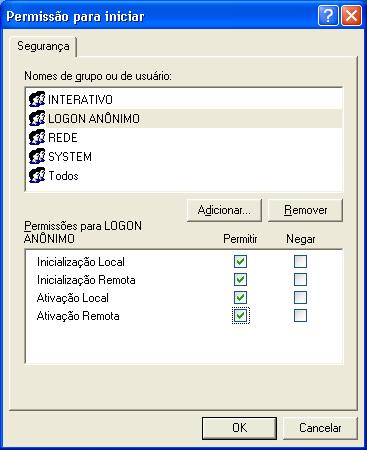
Logo após, é necessário dar permissões de acesso, inicialização e ativação remota do **E3Run** para o usuário LOGON ANÔNIMO. Para isto, selecione as propriedades através do menu de contexto do E3Run, clicando com o botão direito do mouse sobre o E3Run (Fig. 12):

  
**Figura 12** - Selecionando as propriedades do E3Run

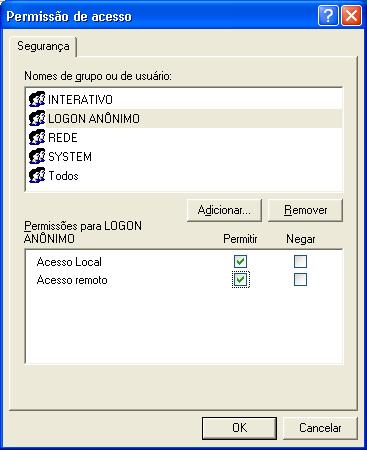
As configurações deverão ser feitas na aba **Segurança** (Fig. 13):

  
**Figura 13** - Configurando a segurança do E3Run

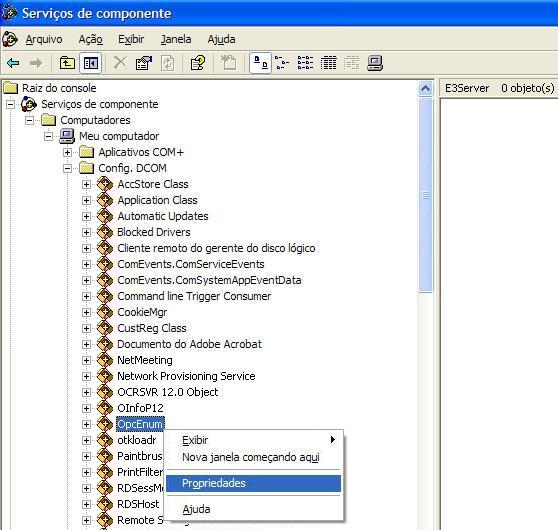
Clique em **Editar** na área **Permissões de Inicialização e Ativação**, adicione o usuário LOGON ANÔNIMO, e habilite as opções **Inicialização Remota** e **Ativação Remota** (Fig. 14):

  
**Figura 14** - Definindo permissões para iniciar o E3Run

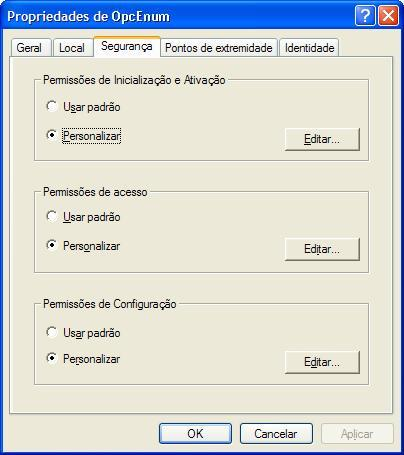
Clique em **Editar** na área **Permissões de acesso**, adicione o usuário LOGON ANÔNIMO, e habilite a opção **Acesso Remoto** (Fig. 15):

 **Figura 15** - Definindo permissões de acesso para o E3Run

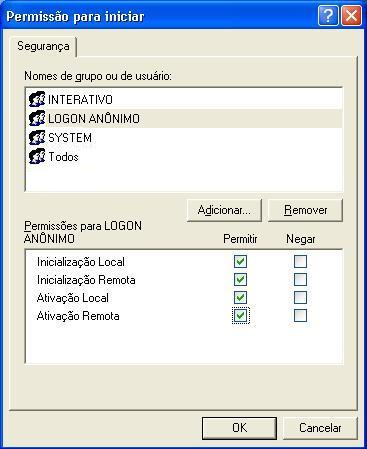
Caso a aplicação também utilize o OPC, é necessário dar permissões de acesso, inicialização e ativação remota do **OpcEnum** para o usuário LOGON ANÔNIMO, em procedimento semelhante aos utilizados com o E3Server e o E3Run. Para isto, selecione as propriedades através do menu de contexto do OpcEnum, clicando com o botão direito do mouse sobre o OpcEnum (Fig. 16):

  
**Figura 16** - Selecionando as propriedades do OpcEnum

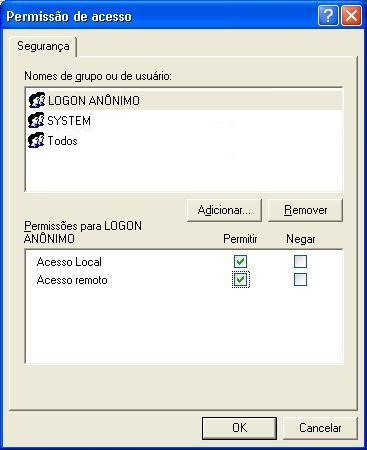
As configurações deverão ser feitas na aba **Segurança** (Fig. 17):

  
**Figura 17** - Configurando a segurança do OpcEnum

Clique em **Editar** na área **Permissões de Inicialização e Ativação**, adicione os usuários LOGON ANÔNIMO e SYSTEM, e habilite  as opções **Inicialização Remota** e **Ativação Remota** (Fig. 18):

  
**Figura 18** - Definindo permissões para iniciar o OpcEnum

Clique em **Editar** na área **Permissões de acesso**, adicione os usuários LOGON ANÔNIMO e SYSTEM, e habilite  a opção **Acesso Remoto** (Fig. 19):

  
**Figura 19** - Definindo permissões de acesso para o OpcEnum

A partir da **versão 4.6** do Elipse E3, também é necessário dar permissões de acesso, inicialização e ativação remota do **E3OpcClient** para o usuário LOGON ANÔNIMO.

**5) Rede**  
  
Para estabelecer a comunicação OPC com as configurações deste artigo, os computadores envolvidos precisam estar em um mesmo domínio Microsoft, ou pelo menos em Grupos de Trabalho com necessariamente mesmo usuário e a mesma senha em todos os computadores (o usuário não precisa necessariamente estar logado, bastando apenas ter sido criado).   
  
É necessário que ambos os computadores sejam capazes de se "enxergar" pelos seus nomes na rede para a troca de informações, não sendo suficiente apenas o IP ou uma pasta compartilhada.  
  
**Importante**: É indispensável que todos os computadores da rede com o Windows 7 instalado sejam configurados do mesmo modo, do contrário eles  também recusarão a conexão com o Servidor OPC.