Introdução

O auge das redes de comunicação nos últimos anos e especialmente, o vertiginoso crescimento da Internet, popularizaram grandemente o uso do correio electrónico.

Uma das maiores vantagens do correio electrónico é a possibilidade de enviar e receber ficheiros. Esta, que é uma das principais vantagens do correio electrónico, foi também convertida numa nova porta de entrada para vírus.

É muito frequente fazer intercâmbio de documentos através do correio electrónico. Isto possibilitou, em grande parte, a enorme expansão de vírus de Word e Excel. Apesar disto, é preciso não esquecer que através do correio electrónico se podem enviar e receber todo o tipo de vírus e não somente os de Word e Excel.

Os antivírus convencionais não estão preparados para levar a cabo uma detecção e desinfecção eficiente de vírus situados em mensagens de correio electrónico pelas seguintes razões:

1. Habitualmente, as mensagens do correio electrónico são armazenadas numa base de dados de correio com um formato próprio e com técnicas de compressão e/ou encriptação que impossibilitam a análise dos antivírus convencionais.

2. É muito frequente que as mensagens do correio electrónico e os seus ficheiros associados estejam guardados num servidor ao qual um antivírus convencional não irá poder ter acesso.

Pelas razões expostas, um antivírus para correio electrónico deve estar especificamente concebido para detectar e eliminar vírus no âmbito do correio electrónico. Por isso, as características principais com as quais deve contar um antivírus para correio electrónico são:

- Análise das mensagens no mesmo instante da sua recepção de um modo totalmente automático.
- Análise automática de cada mensagem na altura em que esta for aberta.
- Análise automática de cada mensagem que se tente enviar. Deste modo, é evitada a possibilidade de enviar mensagens contaminadas com vírus.
- Análise automática de cada mensagem que se guarde.
- Análise de todas as mensagens de correio em qualquer altura pretendida pelo utilizador.
- Integração com o programa de correio electrónico.
- Possibilidade de analisar ficheiros comprimidos.
- Possibilidade de analisar mensagens anexadas (mensagens dentro de outras mensagens).

O Panda Antivírus para Exchange/Outlook é um antivírus para correio electrónico, o qual conta com todas as características descritas e com muitas outras que completam o seu funcionamento e o convertem numa ferramenta potente embora bastante configurável, que evita todos os riscos no trabalho com mensagens de correio electrónico.

NOTA
Neste manual são explicados os seguintes produtos:

- Panda Antivírus Exchange/Outlook
- Panda Antivírus Exchange/Outlook Network Client

O primeiro permite instalar o Panda Antivírus Exchange/Outlook num computador, de modo directo. O segundo permite a distribuição do referido antivírus a todas as estações de uma rede, simplificando assim a tarefa do administrador da rede.

Consulte a parte do manual correspondente ao produto que foi adquirido.

Instalação

Requisitos

O Panda Antivírus Exchange/Outlook precisa de:

- Computador compatível com IBM, capaz de executar Windows 95, 98 ou Windows NT Workstation 3.51 ou 4.0.
- MS-Exchange e/ou MS-Outlook
- 3 Mb de espaço em disco rígido.

Instalação

Para instalar o Panda Antivírus Exchange/Outlook é necessário introduzir a disquete número 1 na drive e executar o programa SETUP.EXE.

O processo de instalação consta de uma série de janelas nas quais se perguntam os diferentes dados necessários para levar a cabo a instalação.

Uma vez concluída a instalação, recomendamos reiniciar a máquina. O antivírus para o Exchange/Outlook não se irá pôr em funcionamento até que se volte a iniciar o Exchange/Outlook.

Desinstalação

Para desinstalar o Panda Antivírus Exchange/Outlook é preciso fechar o programa de correio Exchange/Outlook, ir ao *Painel de Controlo*, escolher a opção *Adicionar ou Excluir programas* e escolher da lista Panda Antivírus Exchange/Outlook. Feito isto, é necessário premir o botão *Adicionar ou Excluir*. A desinstalação será concluída em alguns momentos. Não se deve tentar desinstalar esta versão apagando a pasta sobre a qual foi instalada, é preciso desinstalar sempre seguindo o procedimento indicado.

Como analisar com o Panda Antivírus Exchange/Outlook

Análise requerida

Para analisar uma determinada pasta, seleccione-a. Se escolher uma pasta que contenha outras pastas (por exemplo, uma caixa de correio), serão analisadas todas as pastas dependentes da pasta escolhida. Uma vez escolhida uma pasta, prima o botão Analisar na barra de botões standard do MS-Exchange/Outlook ou seleccione a opção Analisar em busca de vírus dentro da opção Ferramentas no menu principal do MS-Exchange/Outlook. Irá aparecer a seguinte janela de análise:

Uma vez terminada a análise, poderá ver o relatório de resultados no qual é detalhada qualquer incidência encontrada durante a análise.

O Panda Antivírus Exchange/Outlook também permite analisar uma ou várias mensagens. Para isso, seleccione a mensagem ou mensagens que deseja analisar. Uma vez seleccionadas, prima o botão de análise para que comece a análise.

Para seleccionar várias mensagens, faça clic sobre estas mantendo pressionada a tecla Control. Se quiser seleccionar um conjunto de mensagens, seleccione a primeira e faça clic sobre a último mantendo pressionada a tecla Shift.

Protecção em tempo real

A protecção permanente permite-lhe trabalhar com toda a tranquilidade com o seu correio sem ter que se preocupar com os vírus, visto que o Panda Antivírus Exchange/Outlook irá vigiar todas as operações das quais você suspeita.

A protecção permanente encarrega-se de ir analisando em busca de vírus:

- Todas as mensagens novas que forem recebidas.
- Todas as mensagens que se queiram enviar.
- Todas as mensagens que se abram independentemente de serem recebidas antes ou depois da instalação do antivírus.
- Todas as mensagens que se queiram guardar.

A protecção permanente pode ser activada ou desactivada facilmente activando ou desactivando o botão designado para tal efeito na barra de botões standard do MS-Exchange/Outlook.

O Panda Antivírus Exchange/Outlook é capaz de analisar ficheiros comprimidos e mensagens anexadas (mensagens dentro de outras mensagens) oferecendo assim os maiores níveis de protecção.

Funcionamento do Panda Antivírus Exchange/Outlook

O Panda Antivírus Exchange/Outlook integra-se completamente com o MS-Exchange/Outlook. Portanto, todo o uso do antivírus é levado a cabo a partir do próprio programa de correio.

O Panda Antivírus Exchange/Outlook adiciona quatro botões à barra de botões standard do MS-Exchange/Outlook. Esses quatro botões são:

Analisar: este botão começa uma análise da pasta ou mensagens seleccionadas no momento de começar a análise. Serão analisadas todas as sub-pastas que se encontrem dentro da referida pasta. Uma janela permite o seguimento do processo de análise mostrando o conjunto de pastas que se irão analisar, a pasta que se está a analisar em cada instante e uma barra de progresso.

Relatório de resultados: este botão mostra o relatório de incidências que o antivírus encontrou. Este relatório é conservado de sessão em sessão até que o utilizador decida apagá-lo.

Activar ou desactivar o antivírus: este botão permite activar ou desactivar a protecção permanente do Panda Antivírus. Caso se desactive a referida protecção, o Panda Antivírus Exchange/Outlook não irá analisar em busca de vírus as novas mensagens que se recebam ou se enviem. Nem sequer irá analisar em busca de vírus as mensagens que se abrem para serem lidas. Todavia, será possível analisar uma determinada pasta ou mensagem em qualquer momento através do botão Analisar. A análise no arranque do Exchange/Outlook será levada a cabo ainda que se tenha desconectado a protecção permanente.

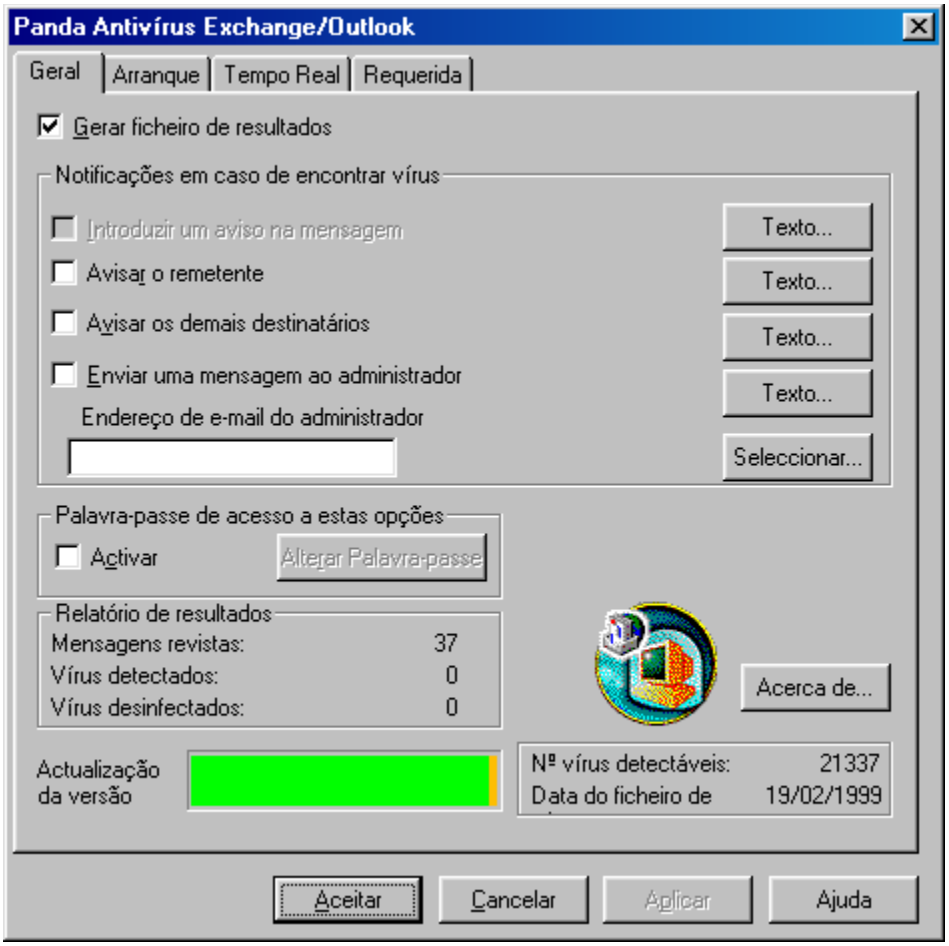
Configurar: este botão mostra a janela de configuração do Panda Antivírus Exchange/Outlook. Através desta janela, é possível configurar o comportamento geral do antivírus, o seu comportamento no arranque do programa de correio e o seu comportamento como protecção permanente e como protecção requerida. Também é possível aceder à configuração do Panda Antivírus Exchange/Outlook escolhendo Opções dentro de Ferramentas no menu principal do MS-Exchange/Outlook. Nessa janela de opções aparece uma página chamada Panda Antivírus Exchange/Outlook através da qual é possível configurar o antivírus.

Configuração do Panda Antivírus Exchange/Outlook

O Panda Antivírus Exchange/Outlook permite uma ampla configuração para cada uma das suas funções. A janela de configuração está dividida em várias páginas, cada uma delas referente a uma determinada parte do antivírus.

Geral

As opções agrupadas nesta página são de âmbito geral e condicionam o comportamento do antivírus em todos os casos. As opções são as seguintes:



Gerar ficheiro de resultados. Caso se escolha esta opção, todas as operações de análise do antivírus irão registar as diferentes incidências num ficheiro de resultados.

Introduzir um aviso na mensagem. Caso se escolha esta opção, cada vez que um vírus for encontrado numa mensagem, será anexado um texto a essa mensagem como forma de advertência. Essa mensagem será anexada independentemente da acção que se tenha decidido levar a cabo ao encontrar um vírus. A mensagem é personalizável, permitindo a cada utilizador transmitir o que desejar.

Avisar ao remetente. Caso se escolha esta opção, cada vez que um vírus for encontrado numa mensagem, será enviada uma mensagem ao remetente da mensagem infectada para o avisar dessa circunstância. O texto da mensagem que o remetente irá receber é totalmente configurável podendo, portanto, ser personalizado.

Avisar outros destinatários. Caso se escolha esta opção e se encontre um vírus numa mensagem, será enviada uma mensagem aos restantes destinatários da mensagem infectada, se os houver. Desta forma, é possível avisar a utilizadores que, porventura não estejam protegidos contra os vírus. O texto da mensagem que irão receber os restantes destinatários pode ser personalizado.

Enviar uma mensagem ao administrador. Caso se escolha esta opção e se indique o endereço de correio electrónico do administrador, cada vez que se detecte um vírus numa mensagem, será enviada uma mensagem de advertência ao administrador do sistema. O texto da referida mensagem de advertência é totalmente personalizável.

Activar a palavra-passe. Caso se escolha esta opção, a configuração do Panda Antivírus Exchange/Outlook ficará protegida com uma palavra-passe. Desta forma, nenhum utilizador não autorizado poderá alterar a configuração do antivírus.

Alterar a palavra-passe. Este botão permite alterar a palavra-passe com a qual se protegeu a configuração do Panda Antivírus Exchange/Outlook.

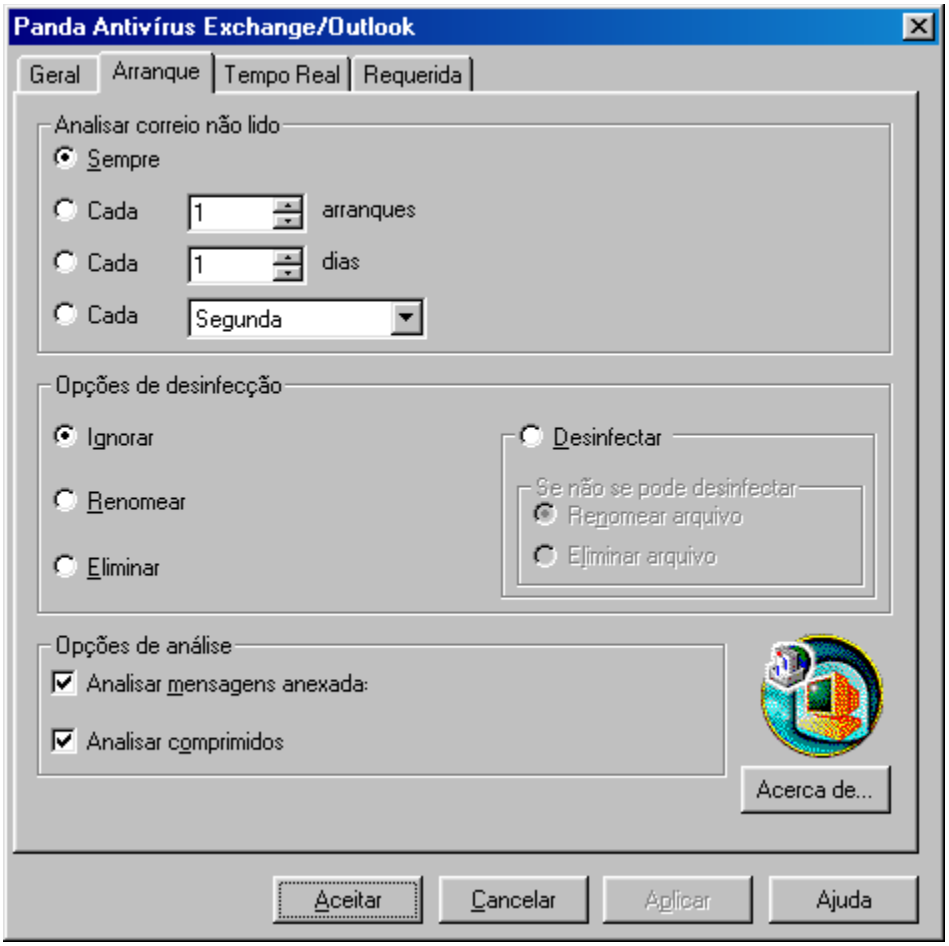
Relatório de resultados. Nessa opção é mostrada informação acerca de quantas mensagens foram analisadas, quantos vírus se detectaram e quantos foram desinfectados.

Actualização da versão. Aqui é mostrada de forma gráfica quão actualizado está o antivírus.

Dados sobre a versão. O número de vírus detectáveis e a data do ficheiro de vírus dão informação sobre a versão do antivírus instalada.

Arranque

Nesta página é possível configurar o comportamento do antivírus no momento do arranque do programa de correio electrónico MS-Exchange/Outlook. As opções disponíveis são as seguintes:



Analisar sempre o correio não lido. Caso seleccione esta opção, cada vez que o MS-Exchange/Outlook arranque, serão analisadas todas as mensagens não lidas da pasta de entrada.

Analisar o correio não lido em cada determinado número de arranques. Caso seleccione esta opção, as mensagens não lidas da pasta de entrada serão analisadas cada vez que se cumpra o número indicado de arranques do programa de correio.

Analisar o correio não lido em cada espaço de tempo. Caso seleccione esta opção, a análise das mensagens não lidas da pasta de entrada será levada a cabo somente de cada vez que passe o prazo de dias indicado.

Analisar o correio em determinados dias. Caso se seleccione esta opção, só serão analisadas as mensagens não lidas da pasta de entrada no dia da semana escolhido.

Desinfecção - Ignorar: caso escolha esta opção e um vírus for encontrado, o antivírus não levará a cabo nenhuma acção além de apenas mostrar uma janela avisando de que um vírus foi encontrado.

Desinfecção - Renomear: caso seleccione esta opção e um vírus for encontrado, o antivírus irá proceder à renomeação do ficheiro contaminado com vírus.

Desinfecção - Eliminar: caso seleccione essa opção e um vírus for encontrado, o antivírus irá proceder à eliminação do ficheiro infectado.

Desinfecção - Desinfectar: caso seleccione esta opção e um vírus for encontrado, o antivírus irá tentar desinfectar o ficheiro infectado.

Desinfecção – Se não se pode desinfectar, renomear: se o antivírus não pode desinfectar um ficheiro infectado, irá proceder à renomeação desse ficheiro.

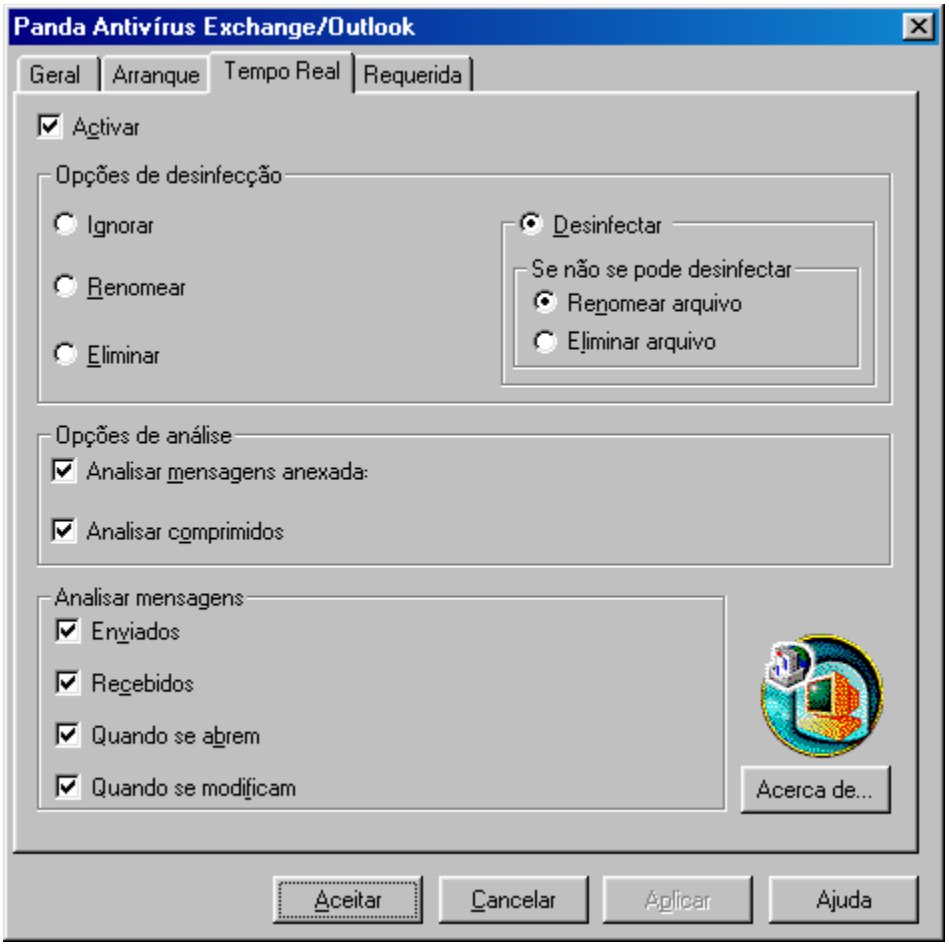
Desinfecção - Se não se pode desinfectar, eliminar: se o antivírus não pode desinfectar um ficheiro infectado, irá proceder à eliminação do referido ficheiro.

Analisar mensagens anexadas: caso seleccione esta opção, serão analisadas as mensagens anexadas. Ou seja, caso se encontre uma mensagem dentro de outra, será feita uma análise a ambas as mensagens. O número de níveis de mensagens que se podem analisar depende dos recursos da máquina.

Analisar ficheiros comprimidos: caso seleccione esta opção e um vírus for encontrado num ficheiro comprimido, será feita a sua análise como se de um ficheiro normal se tratasse.

Tempo real

Nesta página é possível configurar a protecção permanente oferecida pelo antivírus . As opções disponíveis são as seguintes:



Activar: caso seleccione esta opção, será activada a protecção permanente. Isto quer dizer que serão analisadas automaticamente todas as mensagens que cheguem, bem como todas as mensagens que se enviem, abram ou guardem.

Desinfecção - Ignorar: caso seleccione esta opção e um vírus for encontrado, o antivírus não irá levar a cabo nenhuma acção além de mostrar uma janela avisando de que um vírus foi encontrado.

Desinfecção - Renomear: caso seleccione esta opção e um vírus for encontrado, o antivírus irá proceder à renomeação do ficheiro contaminado com vírus.

Desinfecção - Eliminar: caso seleccione esta opção e um vírus for encontrado, o antivírus irá proceder à eliminação do ficheiro infectado.

Desinfecção - Desinfectar: caso seleccione esta opção e um vírus for encontrado, o antivírus irá tentar desinfectar o ficheiro infectado.

Desinfecção - Se não se pode desinfectar, renomear: se o antivírus não pode desinfectar um ficheiro contaminado, irá proceder à renomeação desse ficheiro.

Desinfecção - Se não se pode desinfectar, eliminar: se o antivírus não pode desinfectar um ficheiro infectado, irá proceder à eliminação do referido ficheiro.

Analisar mensagens anexadas: caso seleccione esta opção, serão analisadas as mensagens anexadas. Ou seja, caso se encontre uma mensagem dentro de outra, será feita uma análise a ambas as mensagens. O número de níveis de mensagens que se podem analisar depende dos recursos da máquina.

Analisar ficheiros comprimidos: caso seleccione esta opção e se encontre um ficheiro comprimido, será feita a sua análise como se de um ficheiro normal se tratasse.

Analisar mensagens enviados: caso seleccione esta opção, serão analisadas as mensagens que se querem enviar antes do seu envio. Desta forma, evita-se o envio de ficheiros infectados.

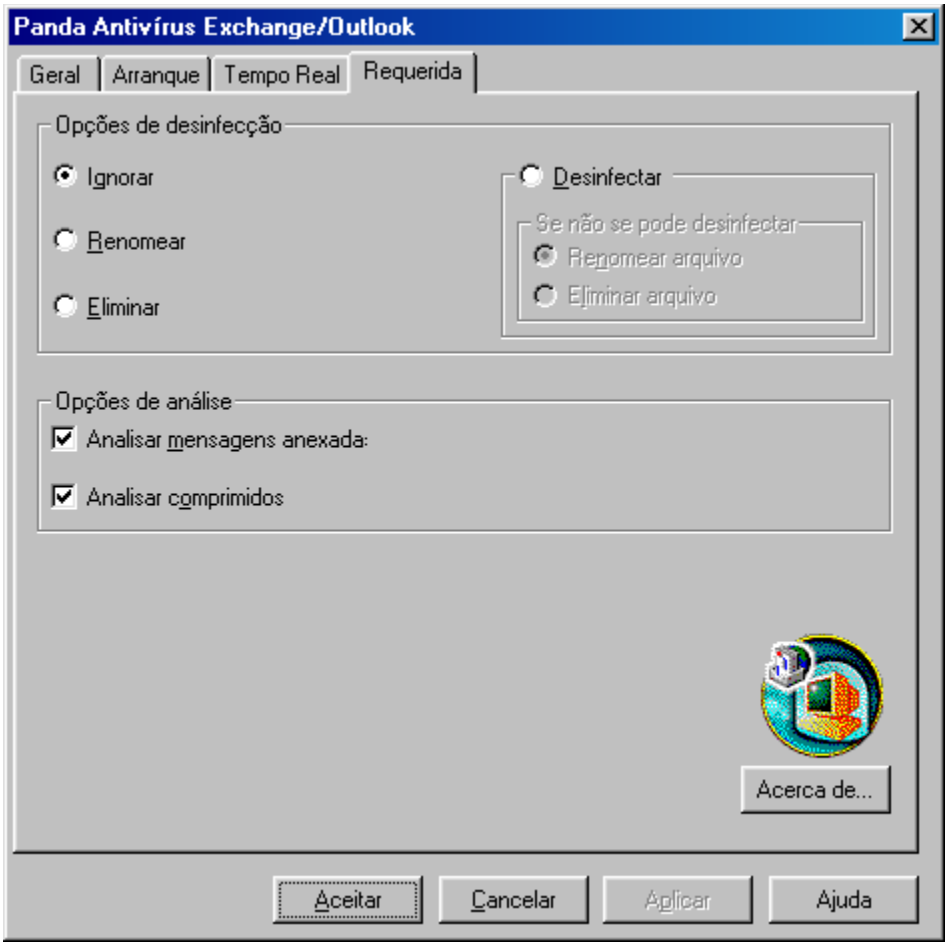
Analisar mensagens recebidas: caso seleccione esta opção, serão analisadas todas as mensagens que se recebam no mesmo instante da sua recepção, mesmo antes de serem abertas.

Analisar mensagens quando se abrem: caso seleccione esta opção, serão analisadas todas as mensagens que se abram independentemente de quando tenham sido recebidas.

Analisar mensagens quando se modificam: caso seleccione esta opção, serão analisadas todas as mensagens que sejam guardadas.

Análise Imediata

Nesta página é possível configurar a análise imediata oferecida pelo antivírus. As opções disponíveis são as seguintes:



Desinfecção - Ignorar: caso seleccione esta opção e um vírus for detectado, o antivírus não irá levar a cabo nenhuma acção além de apenas mostrar uma janela avisando de que foi encontrado um vírus.

Desinfecção - Renomear: caso seleccione esta opção e um vírus for detectado, o antivírus irá proceder à renomeação do ficheiro infectado com vírus.

Desinfecção - Eliminar: caso seleccione esta opção e um vírus for detectado, o antivírus irá proceder à eliminação do ficheiro infectado.

Desinfecção - Desinfectar: caso seleccione esta opção e um vírus for detectado, o antivírus irá tentar desinfectar o ficheiro infectado.

Desinfecção - Se não se pode desinfectar, renomear: se o antivírus não pode desinfectar um ficheiro contaminado, irá proceder à renomeação desse ficheiro.

Desinfecção - Se não se pode desinfectar, eliminar: se o antivírus não pode desinfectar um

ficheiro infectado, irá proceder à eliminação do referido ficheiro.

Analisar mensagens anexadas: caso seleccione esta opção, serão analisadas as mensagens anexadas. Ou seja, caso se encontre uma mensagem dentro de outra, será feita uma análise de ambas as mensagens. O número de níveis de mensagens que se podem analisar depende dos recursos da máquina.

Analisar ficheiros comprimidos: caso seleccione esta opção e se encontre um ficheiro comprimido, será feita a sua análise como se de um ficheiro normal se tratasse.

Introdução à distribuição através de uma rede

A ideia de distribuir o antivírus através de uma rede, surge para facilitar o trabalho de um administrador de rede que queira proteger um conjunto de postos de uma forma cómoda e rápida.

O funcionamento é como se segue:

1. O administrador da rede copia o antivírus para um directório no servidor ou para um directório compartilhado ao qual tenham acesso todos os utilizadores. Esta cópia é levada a cabo através de um programa instalador concebido para tal efeito. É preciso ter em conta que NÃO se está a instalar o antivírus no servidor, senão que, somente estão a ser copiados os ficheiros necessários para instalar o antivírus nos postos.

2. Cada vez que um posto se conecte à rede, será comprovado se tem o antivírus instalado e actualizado. Se assim for, não se fará nada, mas se não tem o antivírus instalado ou actualizado, será procedida a instalação ou actualização do mesmo de forma totalmente automática.

Como foi visto, o servidor (ou recurso compartilhado) somente serve de meio para distribuir o antivírus aos postos.

Este procedimento global serve para praticamente todo o tipo de redes. Ora bem, em cada uma delas é levada a cabo de uma forma ligeiramente diferente. Nesta documentação irá proceder-se à explicação desse procedimento para os tipos de redes mais comuns hoje em dia.

Como distribuir o antivírus através de uma rede

Requisitos

Para a distribuição do Panda Antivírus Exchange/Outlook através de uma rede, é preciso:

- Um computador compatível com IBM capaz de executar o Windows 95, 98 ou Windows NT Workstation 3.51 ou 4.0.
- 3 Mb de espaço no disco rígido do servidor que venha a servir como meio de distribuição.
- 3 Mb de espaço no disco rígido de cada computador no qual se venha a instalar o antivírus.

Como distribuir facilmente o antivírus a todos os postos da rede

O processo de distribuição do antivírus a todos os postos da rede consta de duas partes:

1. Cópia do antivírus para um directório ao qual possam aceder todos os utilizadores.

2. Distribuição do antivírus a todos os postos à medida que se vão conectando à rede através do programa RINSTALL.

Em seguida é explicado em detalhe como realizar os dois passos mencionados. Alguns aspectos deste processo de instalação requerem conhecimentos do tipo de rede através da qual se vai distribuir o antivírus. Todos estes conhecimentos são explicados em detalhe para os principais tipos de rede nos compartimentos correspondentes, consulte-os se tiver alguma dúvida.

Cópia do antivírus para um directório ao qual possam aceder todos os utilizadores

O primeiro passo na distribuição do antivírus através da rede, é a cópia de ficheiros para um directório num dos discos rígidos do servidor. É muito importante ter em conta que a cópia dos ficheiros para o servidor deve ser realizada num ambiente livre de vírus. Caso contrário, os ficheiros do antivírus poderiam ser infectados. Como esses ficheiros vão ser distribuídos a todas os posto que se conectem à rede, o vírus seria distribuído juntamente com eles. Para conseguir uma cópia de ficheiros segura e para se certificar de que esses ficheiros não se irão contaminar a partir de nenhum posto no futuro, deve ser levada a cabo a cópia de acordo com os seguintes passos:

1. O administrador deve assegurar-se de que o seu computador esteja livre de vírus. Seria conveniente que o administrador instalasse o antivírus adequado da Panda Software no seu computador e activasse a protecção permanente correspondente. Não deveria continuar com a instalação a não ser que esteja seguro de que o computador a partir do qual se esteja a instalar o antivírus está livre de vírus.

2. Deve-se escolher um directório no servidor para onde copiar os ficheiros. Recomendamos que se crie um novo directório chamado PAVEXCLI sobre o qual todos os utilizadores tenham direitos de leitura. É importante que nenhum utilizador tenha direitos de *escrita* ou *apagar* sobre esse directório, caso contrário qualquer utilizador poderia, acidental ou voluntariamente, infectar ou apagar os ficheiros do antivírus com as graves consequências que daí poderiam advir.

3. Uma vez criado o directório de destino, basta introduzir a disquete número 1 ou o CD-ROM, situar-se na unidade correspondente e executar o programa SETUP.EXE.

O processo de instalação consta de uma série de janelas nas quais lhe vão perguntando os diferentes dados necessários para levar a cabo a instalação na sua máquina. Um dos dados que lhe

irão pedir será o directório destino. Deverá escolher o directório criado para esse efeito, para que se possam copiar os ficheiros do antivírus.

Distribuição do antivírus

É nesta etapa onde se comprova a vantagem do nosso antivírus para PCs em rede. Em vez de ter que ir posto a posto instalando o antivírus, este instala-se automaticamente enquanto um posto se conecta à rede.

Habitualmente, quando um posto se conecta a uma rede, são executados uma série de comandos ou programas para preparar o trabalho em rede da mesma forma que são executados uma série de comandos ou programas cada vez que se arranca um computador. Esta série de comandos e/ou programas é conhecida como *Login Script* (ou guião de entrada).

O nosso antivírus com capacidade de distribuição através de uma rede, vem acompanhado de um programa chamado **RINSTALL** o qual se encarrega da distribuição automática do antivírus. Portanto, conseguir a distribuição automática do antivírus é tão fácil como colocar no *Login Script* a execução do **RINSTALL**.

O **RINSTALL** será executado cada vez que um posto se conecte à rede. A primeira coisa que comprova o **RINSTALL,** é que o posto conectado tenha instalado o antivírus. Se o tiver instalado e actualizado, não faz nada, prosseguindo a execução dos restantes comandos do *Login Script* normalmente. Se a estação não tem instalado o antivírus ou o tem desactualizado, o **RINSTALL** irá instalar o antivírus. Uma vez feito isto, a execução dos restantes comandos do *Login Script* continua normalmente.

Como o funcionamento do **RINSTALL** é totalmente automático, o administrador da rede só tem que copiar os ficheiros e modificar o *Login Script* para instalar a protecção antivírus que se irá propagando aos postos à medida que se vão conectando.

Distribuição do antivírus numa rede Novell NetWare

Para que o antivírus se distribua automaticamente a todas os postos à medida que se vão conectando a uma rede Novell NetWare, é necessário introduzir a seguinte linha no *System Login Script*:

```
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Consulte a secção Novell NetWare para obter uma explicação mais detalhada sobre estes aspectos.

Como se pode ver no exemplo, é preciso indicar o local do servidor no qual residem os ficheiros do antivírus. Por isso, a referida linha deverá ir *depois* do mapear das unidades ficando esta parte do *System Login Script* como se segue:

```
   MAP ROOT F:=ALFA\SYS:
#F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(supondo que o servidor tenha por nome Alfa e que os ficheiros residem no volume SYS).

Distribuição do antivírus numa rede Windows NT

Para que o antivírus se distribua automaticamente aos postos da rede à medida que estes se vão

conectando, é necessário acrescentar a seguinte linha ao *Ficheiro de comandos de início de sessão* usando o programa Profile Manager:

Consulte a secção Windows NT para obter uma explicação mais detalhada sobre estes aspectos.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Como se pode ver no exemplo, é necessário indicar o lugar de onde se copiaram os ficheiros do antivírus. Por isso, a referida linha deverá ir *depois* do mapear de recursos compartilhados ficando esta parte do *Ficheiro de comandos de início de sessão* como se segue:

```
NET USE F: \\ALFA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(supondo que o servidor tenha por nome Alfa e que o recurso compartilhado se chame Sys).

Distribuição do antivírus numa rede OS/2

Para que o antivírus se distribua automaticamente às estações da rede à medida que estas se vão conectando, é necessário acrescentar a seguinte linha ao ficheiro PROFILE.BAT (ou PROFILE.CMD):

Consulte a secção OS/2 para obter uma explicação mais detalhada sobre estes aspectos.

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Como se pode ver no exemplo, é necessário indicar o local de onde se copiaram os ficheiros do antivírus. Por isso, a referida linha deverá ir *depois* do mapear de recursos compartilhados ficando esta parte do ficheiro PROFILE.BAT como se segue:

```
NET USE F: \\ALFA\SYS
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

(supondo que o servidor tenha por nome Alfa e que o recurso compartilhado se chame Sys).

Distribuição do antivírus numa rede Pathworks

Para que o antivírus se distribua automaticamente aos postos da rede à medida que estas se vão conectando, é necessário acrescentar a seguinte linha na sequência de conexão de um grupo no qual se encontrem todos os utilizadores aos quais se queira instalar o antivírus:

```
F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

Como se pode ver no exemplo, é necessário indicar o local de onde se copiaram os ficheiros do antivírus. Por isso, é conveniente ter definido o mapa de unidades antes de se executar o RINSTALL.

Distribuição do antivírus numa rede Banyan-Vines

Para que o antivírus se distribua automaticamente aos postos da rede à medida que estes se vão conectando, é necessário acrescentar a seguinte linha no perfil de cada utilizador cuja máquina queira proteger. O perfil de um utilizador é a sequência de ordens que se executam de cada vez que

esse utilizador se conecta à rede.

Basta editar o mencionado perfil com o comando MUSER e acrescentar a linha:

```
POSTLOGIN F:\PAVEXCLI\RINSTALL PAVEX.SCR
```

caso a unidade do servidor esteja *mapeada* como F e se copiaram os ficheiros dentro do directório **PAVEXCLI**.

É bastante conveniente ter definido o mapa de unidades antes que se execute o **RINSTALL** para se assegurar de que o disco rígido do servidor se referencia de igual modo a partir de todas os postos.

A modificação uma a uma de todos os perfis de utilizador pode chegar a ser uma tarefa muito trabalhosa caso hajam muitos utilizadores. Habitualmente costuma haver um perfil comum utilizado por todos os utilizadores. Esse perfil é chamado a partir dos diferentes perfis dos utilizadores. O comando que é preciso usar para chamar um perfil a partir de outro é:

```
USE Sample_Profile@grupo@organização
```

de onde o *Sample_Profile* é um utilizador fictício e o grupo e a organização são os correspondentes na estrutura de cada empresa.

Desta forma, basta efectuar as modificações oportunas sobre o perfil *Sample_Profile* para que afectem todos os utilizadores que chamem a esse perfil a partir do seu próprio.

Instalação do antivírus num posto não conectado à rede

Caso se queira instalar o Panda Antivírus Exchange/Outlook num posto não conectado à rede, é necessário levar a cabo o seguinte procedimento:

1. Introduzir a disquete número 1 ou o CD-ROM de Panda Antivírus Exchange/Outlook, situar-se na unidade correspondente e executar o programa SETUP.EXE. O processo de instalação consta de uma série de janelas nas quais lhe vão perguntando os diferentes dados necessários para levar a cabo a instalação na sua máquina. Um dos dados que lhe será pedido será o directório destino. Deverá escolher um directório na máquina na qual está a instalar e não um directório do servidor tal como foi descrito anteriormente.

2. Uma vez terminado o processo de instalação, execute o seguinte comando:

   ```
   C:\PAVEXCLI\RINSTALL PAVEX.SCR
   ```

   (se instalou o antivírus noutra unidade ou directório, indique o adequado).

3. Logo que termine o processo de distribuição, o programa antivírus para o MS-Exchange/Outlook estará instalado na sua máquina.

4. Elimine o directório de onde instalou o antivírus no passo 1 visto não mais ser necessário.

Solução de problemas de distribuição

Se o antivírus não se distribui adequadamente numa ou mais máquinas, vá a essa máquina ou

máquinas e comprove o seguinte:

1. Que a partir dessa máquina pode conectar-se ao servidor no qual se copiou o antivírus.

2. Prove executar o **RINSTALL** directamente. Situe-se no directório do servidor no qual copiou o antivírus e execute o **RINSTALL** PAVEX.SCR.

Se as duas comprovações anteriores foram correctas, reveja o guião de entrada certificando-se de que modificou o guião adequado e de que a linha corresponde com a que se viu neste manual.

Características avançadas

Como evitar que os utilizadores modifiquem a configuração do Panda Antivírus Exchange/Outlook

Caso se deseje evitar que os utilizadores aos quais se vai instalar automaticamente o Panda Antivírus Exchange/Outlook possam variar a configuração do mesmo, deve-se seguir o procedimento que se descreve em seguida:

1. Instalar o Panda Antivírus Exchange/Outlook no computador do administrador da rede.

2. Abrir o programa de correio MS-Exchange/Outlook e configurar o antivírus da maneira desejada.

3. Proteger a configuração com a palavra-passe. Isto é feito na janela de configuração de antivírus.

4. Copiar o ficheiro PAVEXCLI.CFG situado no directório WINDOWS\SYSTEM no computador do administrador para o directório da rede a partir do qual se vai distribuir o antivírus.

5. Proceder à modificação do *login script* para que comece a distribuição do antivírus a todos os postos da rede.

É importante ter em conta que o procedimento descrito deve levar-se a cabo antes de começar a distribuição do antivírus através da rede.

Conhecimentos necessários sobre o Novell NetWare

A distribuição do antivírus através de uma rede Novell NetWare precisa de uns conhecimentos mínimos sobre este sistema. Em seguida serão descritos os conceitos que é preciso conhecer ilustrando-os com exemplos de como preparar o sistema de maneira adequada.

Comandos que são executados quando se inicia uma sessão de rede

Habitualmente, quando um computador arranca, são executados uma série de comandos definidos num ficheiro. No caso do MS-DOS ou Windows, esse ficheiro é o AUTOEXEC.BAT.

De igual modo, também é habitual que, quando um computador se conecta a uma rede, se executem uma série de comandos. Esta série de comandos e/ou programas é conhecida como *login script* ou guião de entrada.

O *login script* pode ser geral (o mesmo para todos os utilizadores) ou particular (um diferente para cada utilizador). Também se pode dar uma solução mista com um login script geral comum a todos os utilizadores e um login script particular de cada utilizador.

Dado que o *login script* é executado cada vez que um utilizador se conecta à rede, é o local adequado para conseguir a distribuição do antivírus aos postos. Bastará executar no *login script* o programa de distribuição do antivírus da Panda Software para que o mencionado antivírus vá sendo distribuído a todos os postos à medida que se vão conectando à rede.

System Login Script

No caso do Novell NetWare, o login script geral comum a todos os utilizadores é conhecido como *System Login Script*. Deve-se editar este ficheiro para acrescentar nele a execução do programa de distribuição do antivírus da Panda Software. Para editar o *System Login Script* é preciso levar a cabo os seguintes passos:

1. Caso se tenha uma versão Novell NetWare 3.x é preciso usar o programa SYSCON. Caso se tenha uma versão Novell NetWare 4.x é preciso usar o programa NETADMIN. Todos os servidores Novell NetWare têm um volume chamado SES e dentro deste volume existe sempre um directório PUBLIC. Os dois programas referidos (SESCON e NETADMIN) encontram-se nesse directório.

2. Para editar o *System Login Script* com o programa SESCON, é necessário executar o programa, seleccionar a opção *Supervisor Options* e depois a opção *System Login Script*.

3. Para editar o *System Login Script* com o programa NETADMIN, é necessário executar o programa e ir seleccionando os dois pontos (..) no quadro da esquerda até que já não apareça tal opção. Nesse momento, será vista uma única opção (à direita irá estar descrita como uma *organização*). Feito isto, é preciso seleccionar essa única opção e premir a tecla F10. No menu que aparece é preciso seleccionar a opção *Ver ou editar propriedades do objecto* e no seguinte menu que aparece é preciso seleccionar a opção *Guião de entrada*. Feito isto, já se pode modificar o *System Login Script*.

No *System Login Script* devem-se introduzir duas linhas: a linha referente ao *mapear* (é explicado este conceito na secção seguinte) e a linha referente à distribuição automática do antivírus.

Associação de uma letra de unidade

Nesta secção irá proceder-se à explicação do conceito de *mapear*. Num computador, o disco rígido costuma identificar-se com a letra C, a drive com a letra A ou B e o CD-ROM com a D, a E, etc. dependendo dos discos rígidos instalados.

Os volumes ("discos rígidos") do servidor Novell NetWare devem também identificar-se com uma letra de unidade para assim poder referir-se a directórios e ficheiros nestes volumes a partir dos postos sem problemas. A operação de associar uma letra de unidade a um volume é conhecida como *mapear*.

É de todo o interesse mapear todos os postos da mesma forma para assim se assegurar que, para todos els, os diferentes volumes do servidor são referenciados de igual forma. Para isso, basta colocar o comando de mapear no *System Login Script*. Geralmente, os volumes começam a ser nomeados a partir da letra F, embora se possa usar qualquer outra letra de unidade que não está a ser usada. O comando de mapear, tendo isto em conta, seria:

```
MAP ROOT F:=NOME_SERVIDOR\NOME_VOLUMEN
```

Se o nome do servidor é ALFA e o nome do volume é SYS, o comando seria:

```
MAP ROOT F:=ALFA\SES:
```

Conhecimentos necessários sobre o Windows NT

A distribuição do antivírus através de uma rede Windows NT precisa de alguns conhecimentos mínimos sobre esse sistema. Em seguida são descritos os conceitos que é preciso conhecer, sendo estes ilustrados com exemplos de como preparar o sistema de forma adequada.

Comandos que se executam quando se inicia uma sessão de rede

Habitualmente, quando um computador arranca, são executados uma série de comandos definidos num ficheiro. No caso do MS-DOS ou Windows, esse ficheiro é o AUTOEXEC.BAT.

Da mesma forma, também é habitual que, quando um computador se conecta a uma rede, sejam executados uma série de comandos. Esta série de comandos e/ou programas é conhecida como *login script* ou guião de entrada. No caso do Windows NT é usado o nome de *Ficheiro de comandos de inicio de sessão*.

No caso do Windows NT, cada utilizador tem o seu próprio ficheiro de comandos de inicio de sessão. Isto faz com que, no início, seja necessário modificar os ficheiros de comandos de início de sessão de todos os utilizadores aos quais se queira distribuir o antivírus. Para evitar esta pesada tarefa, a Panda Software desenvolveu um utilitário chamado Profile Manager cujo funcionamento se explica em seguida.

Dado que o ficheiro de comandos de início de sessão é executado cada vez que um utilizador se conecta à rede, é o local adequado para conseguir a distribuição do antivírus aos postos. Bastará apenas executar no ficheiro de comandos de início de sessão o programa de distribuição de antivírus da Panda Software para que o referido antivírus seja distribuído a todos os postos à medida que se vão conectando à rede.

Ficheiros de comandos de início de sessão - Profile Manager

Para instalar o programa Profile Manager o qual permite modificar de forma conjunta todos os ficheiros de comandos de início de sessão, é preciso inserir o disco etiquetado como *Editor de comandos de início para o Windows NT* ou situar-se no directório correspondente do CD-Rom e executar o programa **SETUP.EXE**. Por exemplo:

```
A:\SETUP
```

Uma vez instalado, realize os seguintes passos:

1. Execute o programa.
2. Seleccione o modo simplificado.
3. Seleccione *Editar comandos de início de domínio* dentro do menu Ficheiro.
4. Na parte inferior da janela poderá ver um editor de texto. É nesse editor onde se fazem as modificações pertinentes que irão afectar a todos os ficheiros de comandos de início de sessão.
5. Sair do programa gravando as modificações.

No *Ficheiro de comandos de início de sessão* devem ser introduzidas duas linhas: a linha referente ao *mapear* (este conceito é explicado no separador seguinte) e a linha referente à distribuição automática do antivírus.

Associação de uma letra de unidade

Neste separador irá proceder-se à explicação do conceito de *mapear*. Num computador, o disco rígido é identificado com a letra C, a drive com a letra A ou B e o CD-ROM com a D, a E, etc. dependendo dos discos rígidos instalados.

No caso de uma rede Windows NT, o conceito *mapear* está relacionado com o conceito de *recurso compartilhado*. A totalidade ou qualquer parte do disco rígido do servidor (ou dos discos caso hajam vários) pode ser repartido e convertido assim num *recurso compartilhado*. Estes recursos compartilhados são os que se devem mapear para depois poder referir-se a eles a partir dos postos.

É de todo o interesse que todos os postos tenham o mesmo *mapear* para assim ser possível assegurar que, para todos eles, os diferentes recursos compartilhados do servidor são referenciados de forma igual. Para isso, basta apenas colocar a comando de mapear no *Ficheiro de comandos de início de sessão*. Geralmente, os recursos compartilhados começam a ser nomeados a partir da letra F, embora seja possível usar qualquer outra letra de unidade que não esteja a ser usada. O comando de mapear, tendo isto em conta, seria:

```
NET USE  F: \\NOME_SERV\NOME_RECURSO
```

Se o nome do servidor é ALFA e o nome do recurso compartilhado é SYS, o comando seria:

```
NET USE F: \\ALFA\SYS
```

Conhecimentos necessários sobre o OS/2

A distribuição do antivírus através de uma rede OS/2 precisa de alguns conhecimentos mínimos sobre este sistema. Em seguida serão descritos os conceitos que é preciso conhecer sendo estes ilustrados com exemplos de como preparar o sistema de uma forma adequada.

Comandos que são executados quando se inicia uma sessão de rede

Habitualmente, quando um computador arranca, são executados uma série de comandos definidos num ficheiro. No caso do MS-DOS ou Windows, esse ficheiro é o AUTOEXEC.BAT.

De igual modo, também é habitual que, quando um computador se conecta a uma rede, são executados uma série de comandos. Esta série de comandos e/ou programas é conhecida como *login script* ou guião de entrada. No caso do OS/2, cada utilizador tem um ficheiro chamado PROFILE.BAT (ou PROFILE.CMD) que é executado cada vez que o utilizador se conecta à rede.

Como cada utilizador tem o seu próprio ficheiro de comandos de início de sessão, é necessário modificar o ficheiro PROFILE.BAT de cada um dos utilizadores aos quais se queira distribuir. O inconveniente é que as futuras modificações também supõem a edição de todos os ficheiros PROFILE.BAT. Isto pode ser evitado criando um ficheiro BAT que contenha as linhas necessárias para a distribuição do antivírus e chamando esse ficheiro a partir dos correspondentes ficheiros PROFILE.BAT. Desta forma, qualquer modificação futura, basta faze-la sobre o ficheiro BAT criado, afectando assim todos os utilizadores.

Dado que o login script é executado cada vez que um utilizador se conecta à rede, é o local adequado para conseguir a distribuição do antivírus aos postos. Bastará apenas executar no login script o programa de distribução de antivírus da Panda Software, para que o referido antivírus seja distribuído a todos os postos à medida que se vão conectando à rede.

Associação de uma letra de unidade

Neste separador será dada uma explicação sobre o conceito de *mapear*. Num computador, o disco rígido é identificado com a letra C, a drive com a letra A ou B e o CD-ROM com a D, a E, etc. dependendo dos discos rígidos instalados.

No caso de uma rede OS/2, o conceito *mapear* está relacionado com o conceito de *recurso compartilhado*. A totalidade ou qualquer parte do disco rígido do servidor (ou dos discos caso hajam vários) pode ser repartido e convertido assim num *recurso compartilhado*. Estes recursos compartilhados são os que se devem mapear para depois poder referir-se a eles a partir das estações.

É de todo o interesse que todos os postos tenham o mesmo *mapear* para assim ser possível assegurar que, para todas eles, os diferentes recursos compartilhados do servidor são referenciados de forma igual. Para isso, basta apenas colocar o comando de mapear no ficheiro PROFILE de cada utilizador. Geralmente, os recursos compartilhados começam a ser nomeados a partir da letra F, embora seja possível usar qualquer outra letra de unidade que não esteja a ser usada. O comando de mapear, tendo isto em conta, seria:

```
NET USE  F: \\NOME_SERV\NOME_RECURSO
```

Se o nome do servidor é ALFA e o nome do recurso compartilhado é SYS, o comando seria:

```
NET USE F: \\ALFA\SYS
```

Sintaxe dos comandos dos scripts (.SRC)

Ao longo desta documentação, foi observado que é sempre passado um parâmetro ao programa **RINSTALL**. Este parâmetro é o nome de um ficheiro de extensão SCR (ficheiros de script). Um ficheiro de script é um ficheiro de texto dividido em secções onde é indicado um comando por cada linha. O ficheiro de script é o que determina o comportamento do programa **RINSTALL**.

Os ficheiros SCR adequados para o **RINSTALL** podem ter 6 secções diferentes:

Secção comum **[COMMON]**: estas ordens são sempre executadas.

Secção DOS **[DOS]**: as ordens desta secção são executadas sobre o DOS, Windows 3.1x e Windows 95.

Secção Windows 3.1x **[WIN]**: as ordens desta secção são executadas sobre o DOS, Windows 3.1x e Windows 95 embora só no caso de se localizar o directório do Windows 3.1x no disco rígido da estação de trabalho.

Secção Windows 95 **[WIN95]**: as ordens desta secção são executadas sobre o DOS, Windows 3.1x e Windows 95 embora só no caso de se localizar o directório do Windows 95 no disco rígido da estação de trabalho.

Secção Windows NT **[WINNT]**: as ordens desta secção são executadas somente sobre o Windows NT.

Secção OS/2 **[OS/2]**: as ordens desta secção são executadas somente sobre o OS/2.

Existem três tipos de ordens:

1. **Ficheiros a copiar:** todas as linhas que NÃO comecem com o caracter #, indicam um ficheiro que deverá estar presente no directório de origem e que deverá ser copiado ao directório destino. Por defeito, os ficheiros só serão copiados caso não existam no directório destino ou caso o ficheiro presente no directório de destino for mais antigo que o ficheiro que se encontra no directório de origem.

2. **Atribuições:** estes comandos começam pelo caracter # e têm a seguinte estrutura: #Variável = valor. Servem para atribuir um determinado valor a uma variável. Em seguida são descritas as diferentes variáveis disponíveis nos ficheiros script (SCR).

Nome da variável	**Descrição**
Win3xDir	Directório do Windows 3.1x
Win95Dir	Directório do Windows 95
WinNTDir	Directório do Windows NT

BaseSourcePath	Directório de origem base
BaseTargetPath	Directório de destino base
RelSourcePath	Directório de origem relativa
RelTargetPath	Directório de destino relativo
SourcePath	BaseSourcePath + RelSourcePath
TargetPath	BaseTargetPath + RelTargetPath

CopeMode — Indica as condições de cópia dos ficheiros. Pode tomar três valores. COPE indica que só serão copiados os ficheiros que não existem no directório destino. UPDATE indica que os ficheiros só serão copiados se a versão a copiar for mais recente que a versão existente no directório destino. OVERWRITE indica que os ficheiros serão sempre copiados.

ErrorMode — Indica se devem ou não ser mostradas as mensagens de erro. Épossível atribuir um valor 0 (as mensagens não serão mostradas) ou um valor 1 (as mensagens serão mostradas).

3. **Funções:** estes comandos também começam com o caracter #, e servem para levar a cabo determinadas operações. A sua sintaxe é a seguinte: #Função parâmetro1, parâmetro2, ... As diferentes funções disponíveis são:

AddProfileEntry

Esta função acrescenta uma entrada numa secção de um ficheiro tipo INI. Recebe 4 parâmetros:

Parâmetro 1:	indica a secção na qual criar a entrada.
Parâmetro 2:	indica o campo (a 1ª parte da entrada).
Parâmetro 3:	indica o valor (a 2ª parte da entrada).
Parâmetro 4:	indica o caminho ao ficheiro INI.

Exemplo:

```
#AddProfileEntry Windows, Load,
f:\pavfn\winkir.exe, c:\windows\win.ini
```

AppendLine

Esta função acrescenta uma linha a um ficheiro de texto. Recebe 3 parâmetros:

Parâmetro 1:	indica o caminho ao ficheiro de texto.
Parâmetro 2:	indica a linha de texto a acrescentar.
Parâmetro 3:	LITERAL (é opcional). Indicando este parâmetro, asseguramo-nos de que a linha de texto figure tal e qual foi escrita, eliminando qualquer modificação que possa ter sido introduzida.

Exemplo:

```
#AppendLine c:\autoexec.bat,
```

```
c:\pavfn\sentinel.com
```

AppendLineBefore
Esta função acrescenta uma linha a um ficheiro de texto embora sempre antes outra linha especificada. Recebe 4 parâmetros:

Parâmetro 1: indica o caminho ao ficheiro de texto.
Parâmetro 2: indica a linha de texto a acrescentar.
Parâmetro 3: indica a linha de texto posterior à que se insere.
Parâmetro 4: LITERAL (é opcional). Indicando este parâmetro, asseguramo-nos de que a linha de texto figure tal e qual foi escrita eliminando qualquer modificação que possa ter sido introduzida.

Exemplo:

```
#AppendLineBefore c:\autoexec.bat,
c:\pavfn\sentinel.com, win, LITERAL
```

DeleteLine
Esta função serve para apagar uma linha de um ficheiro de texto. Recebe 2 parâmetros:

Parâmetro 1: indica o caminho ao ficheiro de texto.
Parâmetro 2: indica a linha de texto a apagar.

Exemplo:

```
#DeleteLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

InsertLine
Esta função serve para inserir uma linha no princípio de um ficheiro de texto. Recebe 3 parâmetros:

Parâmetro 1: indica o caminho ao ficheiro de texto.
Parâmetro 2: indica a linha de texto a inserir.
Parâmetro 3: LITERAL (é opcional). Indicando este parâmetro, asseguramo-nos de que a linha de texto figure tal e qual foi escrita, eliminando qualquer modificação que possa ter sido introduzida.

Exemplo:

```
#InsertLine c:\autoexec.bat,
c:\pavfn\sentinel.com
```

MakeDir
Esta função cria um directório. Recebe um parâmetro:

Parâmetro 1: indica o caminho ao directório a criar.

Exemplo:

```
#MakeDir c:\pavfn
```

NoWinLoad

Dentro do ficheiro WIN.INI existe uma secção [Windows] que tem uma entrada chamada Load. Este comando faz com que sejam carregados uma série de programas ao entrar no Windows. Pode haver mais de um programa no mesmo comando Load. O comando NoWinLoad elimina o programa que se deseja do comando Load. Recebe um parâmetro:

Parâmetro 1: indica o programa que não se queira carregar.

Exemplo:

```
#NoWinLoad c:\pavfn\winkir.exe
```

ReplaceLine

Esta função repõe uma linha de um ficheiro de texto. Recebe 3 parâmetros:

Parâmetro 1: indica o caminho ao ficheiro de texto.
Parâmetro 2: indica a linha de texto a substituir.
Parâmetro 3: indica a nova linha de texto.

Exemplo:

```
#ReplaceLine c:\autoexec.bat,
«TargetPath»SENTINEL.COM,
«TargetPath»SENTINEL.COM /OE
```

SetProfileEntre

Esta função atribui um valor a uma entrada numa determinada secção de um ficheiro INI. A função tenta encontrar a referida secção. Caso a encontre, atribui-lhe o valor. Caso contrário, cria a entrada e atribui-lhe o valor. Em caso de não existir a secção, também seria criada. Recebe 4 parâmetros:

Parâmetro 1: indica a secção do ficheiro INI
Parâmetro 2: indica o campo (a 1ª parte da entrada)
Parâmetro 3: indica o valor (a 2ª parte da entrada)
Parâmetro 4: indica o caminho ao ficheiro INI.

Exemplo:

```
#SetProfileEntry Windows, Load,
c:\pavfn\winkir.exe, c:\windows\win.ini
```

WinLoad

Dentro do ficheiro WIN.INI existe uma secção [Windows] que tem uma entrada chamada Load. Este comando faz com que sejam carregados uma série de programas ao entrar no Windows. Pode haver mais de um programa no mesmo comando Load. O comando WinLoad acrescenta o programa que

se deseje ao comando Load. Recebe um parâmetro:

Parâmetro 1: indica o programa que se queira carregar.

Exemplo:

```
#WinLoad c:\pavfn\winkir.exe
```

AdminRequired
Através desta função indica-se que a partir desse momento e até que não apareça uma linha com a função EndAdminRequired, é necessário ser administrador para poder executar todo o bloco de comandos (os que se encontram entre #AdminRequired e #EndAdminRequired). A função só tem efeito quando o RInstall é executado com o parâmetro /Local. Esta função não admite parâmetros.

Exemplo:

```
#AdminRequired
```

EndAdminRequired
Quando aparece esta função indica-se que todos os comandos seguintes poderão ser executados sem necessidade de se ser administrador. Somente tem efeito quando o RInstall é executado com o parâmetro /Local. Esta função não admite parâmetros.

Exemplo:

```
#EndAdminRequired
```

ResetMode
Indica se o computador se deve reiniciar nesse momento, no caso de ser necessário, senão reinicia-se-á. O valor 0 significa que não se efectua o reiniciar, enquanto que o 1 significa que este debe-se produzir nesse mesmo instante. Em qualquer dos casos é apresentado um aviso.

CheckSpace
Mediante este comando comprova-se a existência de espaço (em Mb) existente no destino. Em caso de não o encontrar, apresenta um aviso e não se efectua a copia dos ficheiros.

Parâmetro 1: indica o tamanho necessário em Mb.

Exemplo:

```
#CheckSpace 8
```

CopyFileAs
Realiza a copia de um ficheiro desde uma origem até ao seu destino indicando o modo de copia e torna possível que o ficheiro mude de nome no destino. Admite três parâmetros:

Parâmetro 1: indica o caminho original do ficheiro.
Parâmetro 1: indica o caminho do ficheiro destino.
Parâmetro 1: indica o modo de copia, mediante as seguintes possibilidades: COPY (o ficheiro só será copiado se este não existe no destino), UPDATE (o ficheiro só se copia se a

versão a copiar é mais recente que a existente no destino), OVERWRITE (o ficheiro será sempre copiado, mesmo que a origem e o destino sejam iguais) e ONCHANGE (indica que se realizará a copia só se o ficheiro origem é distinto do ficheiro destino, não tendo em conta se este é mais antigo ou não).

DeteleDirDelayed

Quando finaliza a execução de RInstall (depois dos comandos #Run), este comando apaga um directório completo, incluindo os subdirectórios.

Parâmetro 1: indica o directório a apagar.

Exemplo:

```
#DeleteDirDelayed c:\pavfn
```

ExchangeRequired

Mediante tal comando indica-se a necessidade de ter instalado um cliente de Exchange/Outlook para continuar processando a secção na qual se encontra. Não admite nenhum parâmetro.

Exemplo:

```
#ExchangeRequired
```

EndExchangeRequired

Mediante tal comando indica-se que já não é necessário ter instalado um cliente de Exchange/Outlook para continuar a processar a secção na qual se encontra. Não admite nenhum parâmetro.

Exemplo:

```
#EndExchangeRequired
```