Introdução

O rápido crescimento das redes de comunicação nos anos recentes, e especialmente o crescimento extraordinário da Internet, fez o uso do correio eletrônico muito popular.

Uma das maiores vantagens do correio eletrônico é a possibilidade de enviar e receber arquivos. Este também se tornou um novo ponto de entrada para vírus.

Documentos trocados por correio eletrônico são uma prática muito comum. Isto, em grande parte, facilitou a propagação de vírus de Word e Excel. Entretanto, você deve ter em mente que podem ser enviados e recebidos todos os tipos de vírus por correio eletrônico, não apenas vírus de Word e Excel.

Os Antivírus convencionais não são capazes de detectar e desinfectar eficazmente os vírus localizados em mensagens de correio eletrônico pelas seguintes razões:

1. As mensagens de correio eletrônico são normalmente armazenadas em um banco de dados de correio usando formato e compressão específicos e/ou técnicas de criptografia, o torna ineficaz a análise por vírus utilizando antivírus convencionais.

2. No correio eletrônico são armazenadas freqüentemente mensagens e arquivos anexados que estão em servidores que os antivírus convencionais não podem ter acesso.

Pelas razões acima, um antivírus de correio eletrônico deve ser projetado especificamente para descobrir e remover vírus em ambientes de correio eletrônico. Para isto, as principais características que um antivírus de correio eletrônico deve possuir são as seguintes:

- Análise imediata totalmente automática de mensagens recebidas.
- Análise automática ao abrir mensagens.
- Análise automática de cada mensagem a ser enviada. Deste modo, você evita a possibilidade de enviar mensagens infectadas por vírus.
- Análise automática de todas as mensagens salvas em disco.
- Análise a qualquer hora de todas as mensagens de correio eletrônico sob demanda do usuário.
- Integração com o programa de correio eletrônico.
- Possibilidade de analisar arquivos comprimidos.
- Possibilidade de analisar mensagens aninhadas (mensagens dentro de outras mensagens).

O Panda Antivírus para Exchange/Outlook é um antivírus de correio eletrônico que possui todas as características anteriores, e muitas outras, que completam sua efetividade e o converte em uma poderosa ferramenta, embora facilmente configurável, que previne todos os riscos ao se trabalhar com mensagens de correio eletrônico.

NOTA
Os seguintes produtos são explicados neste manual:

- Panda Antivírus para Exchange/Outlook
- Panda Antivírus para Cliente de Rede Exchange/Outlook

O primeiro permite a instalação direta do Panda Antivírus para Exchange/Outlook em um computador. O segundo permite a distribuição do antivírus em todas as estações de uma rede, simplificando assim o trabalho do administrador de rede.

Refira-se sempre à parte do manual que corresponde ao produto você adquiriu.

Instalação

Requisitos

O Panda Antivírus para Exchange/Outlook requer:

- Um computador IBM PC ou compatível capaz de rodar Windows 95, Windows 98 ou Windows NT Workstation 3.51 ou 4.0.
- MS-Exchange e/ou MS-Outlook.
- 3 MB de espaço livre em disco rígido.

Instalação

Para instalar o Panda Antivírus para Exchange/Outlook, insira disco o 1 na unidade de disco flexível e rode o programa SETUP.EXE.

O processo de instalação consiste em uma série de janelas nas quais será requisitada a informação necessária para completar a instalação.

Uma vez concluída a instalação, recomendamos que você reinicie o computador. O antivírus para Exchange/Outlook não será executado até que você reinicie o Exchange/Outlook.

Desinstalação

Para desinstalar Panda Antivírus para Exchange/Outlook, primeiro saia do programa Exchange/Outlook, depois vá para o *Painel de Controle*, escolha a opção *Adicionar ou remover programas* e selecione Panda Antivírus para Exchange/Outlook na lista. Uma vez feito isso, clique em *Adicionar ou Remover*. A desinstalação concluirá em questão de segundos. Não se deve tentar desinstalar esta versão apagando a pasta na qual foi instalada. O produto sempre deve ser desinstalado a partir do procedimento indicado.

Como procurar por vírus com Panda Antivírus para Exchange/Outlook

Análise Sob demanda

Para analisar uma pasta específica, primeiro selecione-a. Se você selecionar uma pasta que contém outras pastas (por exemplo, uma caixa postal), todas as pastas subordinadas serão analisadas. Uma vez escolhida a pasta, clique no botão de Análise dentro da barra de botões padrão do MS-Exchange/Outlook ou selecione *Procurar por vírus* na opção *Ferramentas* dentro do menu principal do MS-Exchange/Outlook.

Uma vez concluída a análise, você poderá ver um relatório de resultados que contém detalhes de qualquer incidente encontrado durante o processo.

O Panda Antivírus para Exchange/Outlook também permite analisar uma ou mais mensagens. Para fazer isto, selecione a mensagem ou mensagens que você quer analisar. Uma vez selecionadas, clique no botão Análise de sob demanda para iniciar a análise.

Para selecionar várias mensagens, clique em cada uma delas enquanto mantém pressionada a tecla Crtl. Se você quiser selecionar um grupo de mensagens, selecione a primeira e então clique na última enquanto mantém pressionada a tecla Shift.

Proteção em tempo real

É a proteção permanente que lhe permite trabalhar com seu correio sem ter que se preocupar com vírus, já que o Panda Antivírus para Exchange/Outlook monitorará todas as operações para você.

A proteção permanente analisa por vírus em:

- Todas as novas mensagens recebidas.
- Todas as mensagens enviadas.
- Todas as mensagens abertas, recebidas antes ou depois da instalação do antivírus.
- Todas as mensagens salvas.

A proteção permanente pode ser habilitada ou desabilitada facilmente selecionando-se o botão correspondente dentro da barra de botões padrão do MS-Exchange/Outlook.

O Panda Antivírus para Exchange/Outlook é capaz de analisar arquivos comprimidos e mensagens aninhadas (mensagens dentro de outras mensagens), oferecendo assim os mais altos níveis de proteção.

Como o Panda Antivírus para Exchange/Outlook trabalha

O Panda Antivírus para Exchange/Outlook é completamente integrado dentro do programa MS-Exchange/Outlook. Toda a manipulação antivírus é executada portanto a partir do próprio programa de correio eletrônico.

O Panda Antivírus para Exchange/Outlook adiciona quatro botões na barra de botões padrão do MS-Exchange/Outlook. Estes quatro botões são:

Análise: Este botão começa a análise da pasta ou das mensagens selecionadas no começo do processo de análise. Serão analisadas todas as pastas subordinadas encontradas abaixo da pasta selecionada. Uma janela lhe permite acompanhar o processo de análise exibindo o conjunto de pastas a serem analisadas, a pasta que está sendo analisada atualmente e uma barra de progresso.

Relatório de resultados: Este botão exibe um relatório de incidentes encontrados pelo antivírus. Este relatório mantém informações de todas as sessões até que o usuário decida apagá-lo.

Habilita ou Desabilita o Antivirus: Este botão lhe permite habilitar ou desabilitar a proteção permanente do Panda Antivírus. Se esta proteção for desabilitada, o programa Panda Antivírus para Exchange/Outlook não analisará as novas mensagens recebidas ou enviadas à procura de vírus. Também não analisará mensagens abertas para leitura. Porém, você poderá analisar uma pasta ou mensagem específica a qualquer hora por meio do botão de Análise. A análise inicial para o programa Exchange/Outlook será executada apesar da proteção permanente estar desabilitada.

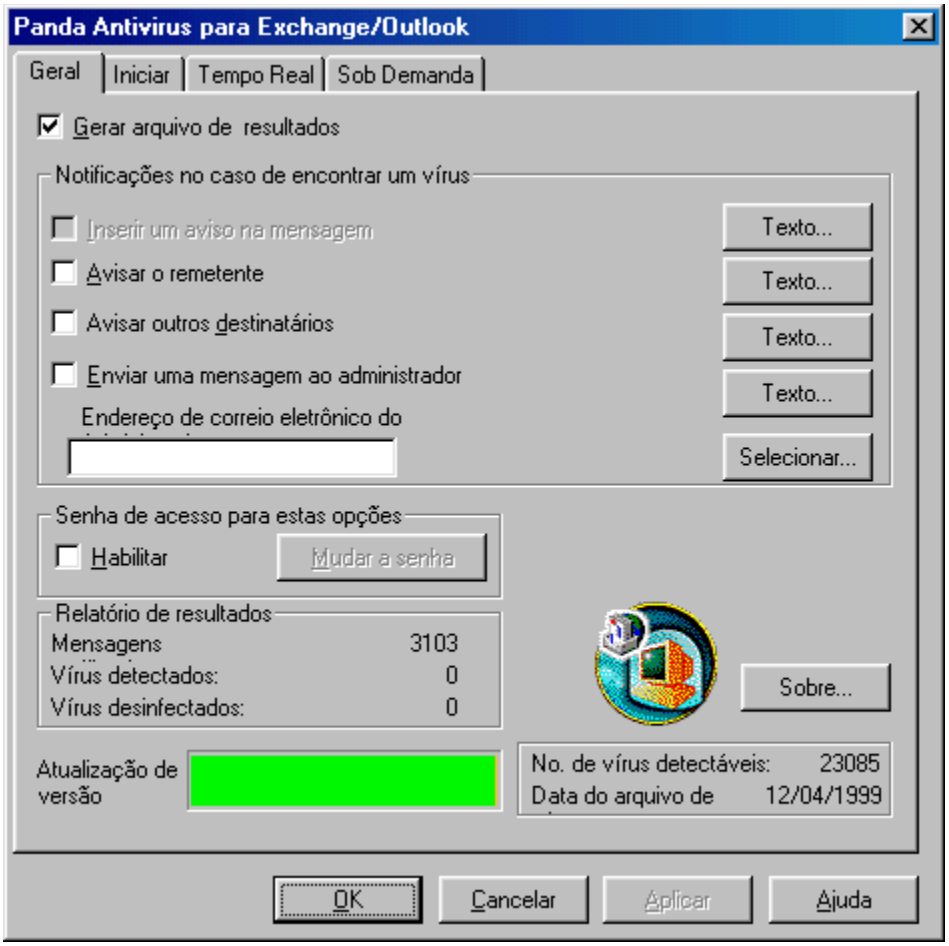
Configurar: Este botão exibe a janela de configuração do Panda Antivírus para Exchange/Outlook. Através desta janela você pode configurar o comportamento geral do antivírus, como seu comportamento ao iniciar o programa de correio, na proteção permanente e sob demanda. Você também pode ter acesso à configuração do Panda Antivírus para Exchange/Outlook selecionando *Ferramentas* e então *Opções* dentro do menu principal do MS-Exchange/Outlook. Uma página chamada Panda Antivírus para Exchange/Outlook aparecerá então na janela de opções, onde você pode configurar o antivírus.

Configuração do Panda Antivírus para Exchange/Outlook

O Panda Antivírus para Exchange/Outlook permite uma configuração detalhada de cada uma de suas funções. A janela de configuração é dividida em várias páginas, cada qual relacionada a uma parte específica do antivírus..

Geral

As opções listadas nesta página são de natureza geral e determinam o comportamento do antivírus em todos os casos, como segue:



Gerar arquivo de resultados: Se esta opção for selecionada, todas as operações de análise do antivírus registrarão os diversos incidentes em um arquivo de resultados.

Insira uma mensagem de aviso: Se esta opção for selecionada, toda vez que um vírus é encontrado em uma mensagem, um texto será acrescentado à mensagem na forma de um aviso. Esta mensagem será adicionada independentemente da ação que você decidiu realizar quando um vírus é encontrado. A mensagem pode ser personalizada, permitindo que o usuário insira qualquer texto que desejar.

Avisar ao remetente: Se esta opção for selecionada, toda vez que um vírus é encontrado em uma mensagem, uma notificação será enviada ao remetente da mensagem infectada para avisá-lo da situação. O texto da mensagem que o remetente receberá pode completamente personalizado.

Avisar outros destinatários: Se esta opção for selecionada, quando um vírus é encontrado em uma mensagem de correio, uma mensagem de notificação é enviada aos outros destinatários da mensagem, se houver. Deste modo, você pode avisar os usuários que podem não estar protegidos contra o vírus. O texto da mensagem que os outros destinatários receberão também pode ser personalizado.

Enviar uma mensagem ao administrador: Se você selecionar esta opção e indicar o endereço de correio eletrônico do administrador, uma mensagem de notificação será enviada ao administrador do sistema cada vez que um vírus for detectado. O texto da mensagem de notificação pode completamente personalizado.

Habilitar Senha: Se esta opção for selecionada, a configuração do Panda Antivírus para Exchange/Outlook será protegida por uma senha. Deste modo, nenhum usuário sem autorização poderá mudar a configuração do antivírus.

Alterar senha: Este botão lhe permite mudar a senha que protege a configuração do Panda Antivírus para Exchange/Outlook.

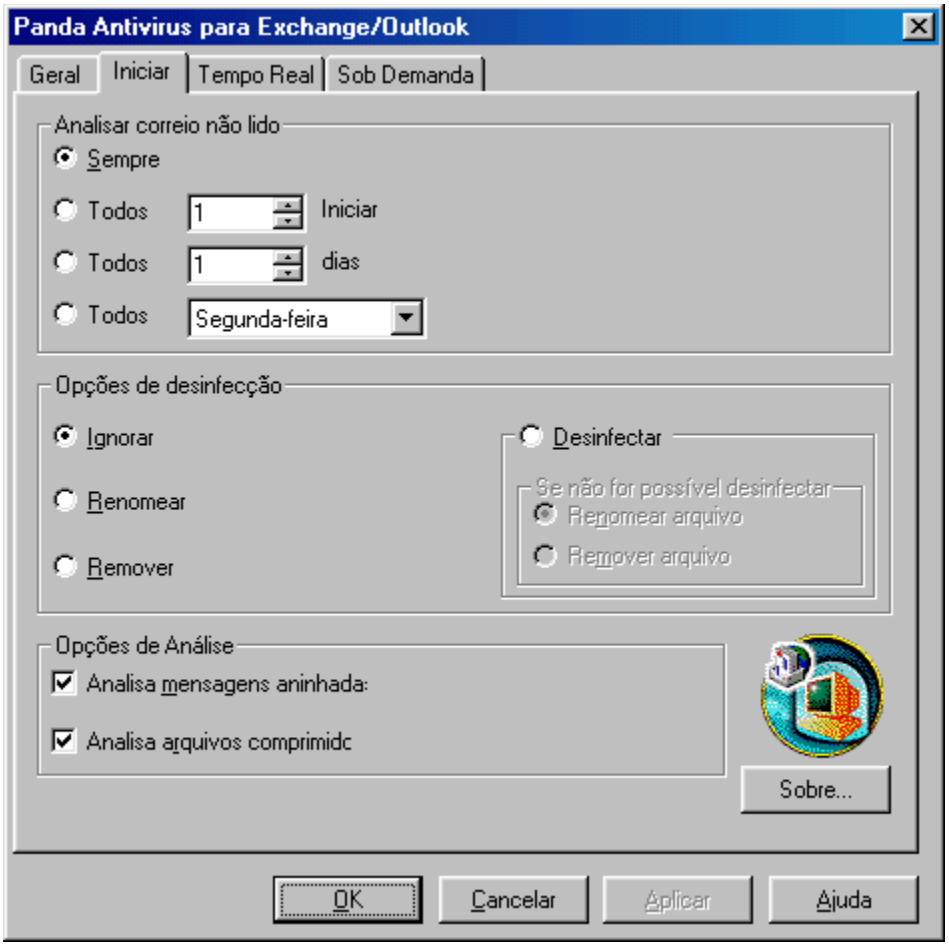
Relatório de resultados: Esta opção exibe a informação sobre quantas mensagens foram analisadas, quantos vírus foram detectados e quantos foram desinfectados.

Atualização de versão: Exibe uma representação gráfica do estado de atualização do antivírus.

Detalhes de versão: O número de vírus detectáveis e a data do arquivo de dados fornecem informações sobre a instalação do antivírus.

Iniciar

É onde você pode configurar o comportamento do antivírus ao iniciar o programa de correio eletrônico MS-Exchange/Outlook. As opções disponíveis são as seguintes:



Sempre analise o correio não lido: Se esta opção for selecionada, toda vez que o MS-Exchange/Outlook é iniciado, serão analisadas todas as mensagens não lidas na Caixa de Entrada.

Análise de correio não lido ao atingir um determinado número de inicializações: Se esta opção for selecionada, serão analisadas as mensagens não lidas na Caixa de Entrada toda vez que seu programa de correio eletrônico alcança o número especificado de inicializações.

Análise de correio não lido ao alcançar um determinado número de dias: Se esta opção for selecionada, a análise das mensagens não lidas na Caixa de Entrada só será executada após passar o número especificado de dias.

Análise de Correio em determinados dias: Se esta opção for selecionada, só serão analisadas as mensagens não lidas na Caixa de Entrada no dia da semana especificado.

Desinfecção - Ignorar: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus

não executará nenhuma ação.

Desinfecção - Renomear: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus renomeará o arquivo infectado por vírus.

Desinfecção - Remover: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus removerá o arquivo infectado.

Desinfecção - Desinfectar: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus tentará desinfectar o arquivo infectado.

Desinfecção - Se a desinfecção não for possível, renomeie: Se o antivírus não conseguir desinfectar um arquivo infectado, este será renomeado.

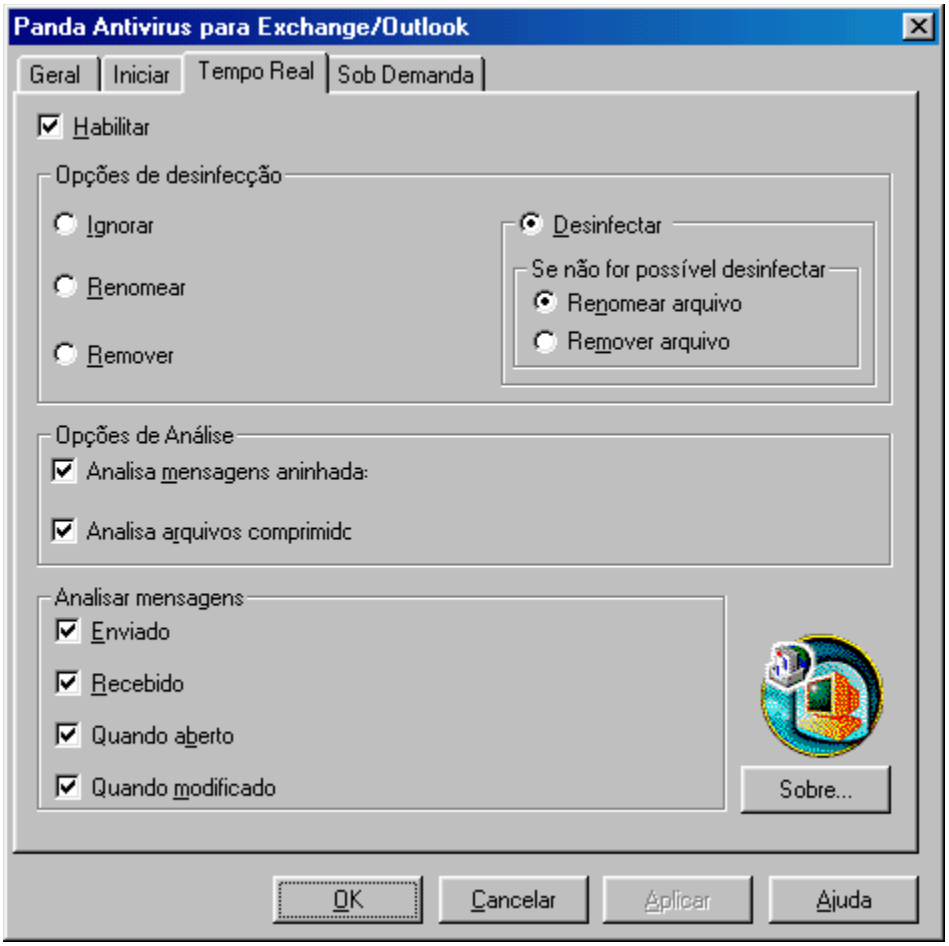
Desinfecção - Se a desinfecção não for possível, remova: Se o antivírus não puder desinfectar um arquivo infectado, este será removido.

Análise de mensagens aninhadas: Se esta opção for selecionada, serão analisadas as mensagens aninhadas. Em outras palavras, se uma mensagem é achada dentro de outra, serão analisadas ambas as mensagens. O número de níveis de mensagens que podem ser analisados dependem dos recursos do computador.

Análise de arquivos comprimidos: Se esta opção for selecionada, quando um arquivo comprimido é encontrado, este será analisado da mesma forma que um arquivo normal.

Tempo Real

É a opção que lhe permite configurar a proteção permanente oferecida pelo antivírus. As opções disponíveis são as seguintes:



Habilitar: Se esta opção for selecionada, a proteção permanente será habilitada. Isto significa que todas as mensagens recebidas serão analisadas, assim como todas as mensagens enviadas, abertas ou comprimidas.

Desinfecção - Ignorar: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus não executará nenhuma ação.

Desinfecção - Renomear: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus renomeará o arquivo infectado por vírus.

Desinfecção - Remover: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus removerá o arquivo infectado.

Desinfecção - Desinfectar: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus tentará desinfectar o arquivo infectado.

Desinfecção - Se a desinfecção não for possível, renomeie: Se o antivírus não conseguir desinfectar um arquivo infectado, este será renomeado.

Desinfecção - Se a desinfecção não for possível, remova: Se o antivírus não puder desinfectar um arquivo infectado, este será removido.

Análise de mensagens aninhadas: Se esta opção for selecionada, serão analisadas as mensagens aninhadas. Em outras palavras, se uma mensagem é achada dentro de outra, serão analisadas ambas as mensagens. O número de níveis de mensagens que podem ser analisados dependem dos recursos do computador.

Análise de arquivos comprimidos: Se esta opção for selecionada, quando um arquivo comprimido é encontrado, este será analisado da mesma forma que um arquivo normal.

Análise de mensagens enviadas: Se esta opção for selecionada, serão analisadas todas as mensagens que você pretende enviar antes mesmo do envio. Isto impede o envio de arquivos infectados.

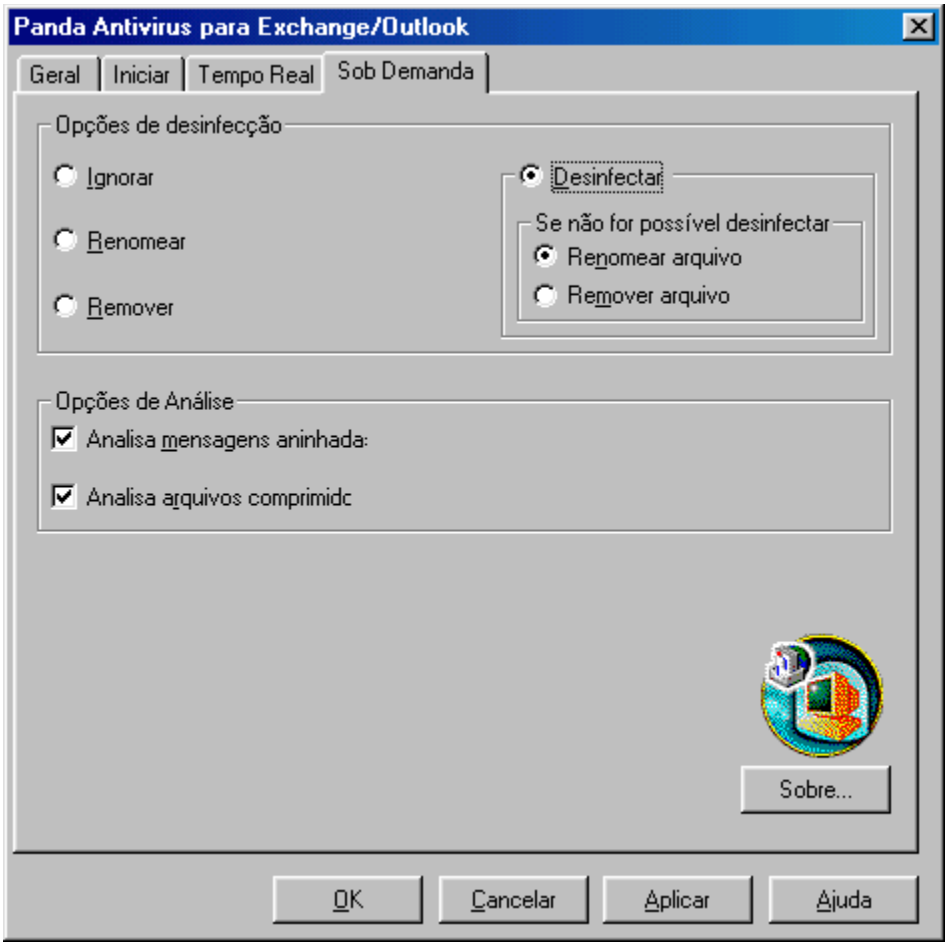
Análise de mensagens recebidas: Se esta opção for selecionada, serão analisadas todas as mensagens recebidas imediatamente durante a chegada, até mesmo antes de serem abertas.

Análise de mensagens abertas: Se esta opção for selecionada, serão analisadas todas as mensagens abertas, não importa quando foram recebidas.

Análise de mensagens modificadas: Se esta opção for selecionada, todas as mensagens salvas serão analisadas.

Sob demanda

É onde você pode configurar a análise sob demanda oferecida pelo antivírus. As opções disponíveis são as seguintes:



Desinfecção - Ignorar: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus não executará nenhuma ação.

Desinfecção - Renomear: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus renomeará o arquivo infectado por vírus.

Desinfecção - Remover: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus removerá o arquivo infectado.

Desinfecção - Desinfectar: Se esta opção for selecionada, quando um vírus é encontrado, o antivírus tentará desinfectar o arquivo infectado.

Desinfecção - Se a desinfecção não for possível, renomeie: Se o antivírus não conseguir desinfectar um arquivo infectado, este será renomeado.

Desinfecção - Se a desinfecção não for possível, remova: Se o antivírus não puder desinfectar

um arquivo infectado, este será removido.

Análise de mensagens aninhadas: Se esta opção for selecionada, serão analisadas as mensagens aninhadas. Em outras palavras, se uma mensagem é achada dentro de outra, serão analisadas ambas as mensagens. O número de níveis de mensagens que podem ser analisados dependem dos recursos do computador.

Análise de arquivos comprimidos: Se esta opção for selecionada, quando um arquivo comprimido é encontrado, este será analisado da mesma forma que um arquivo normal.

Introdução à distribuição através de uma rede

A idéia por trás de distribuir o antivírus através de uma rede é simplificar o trabalho de um administrador de rede, que quer proteger uma série de estações, do modo mais rápido e mais confortável possível.

É executado do seguinte modo:

1. O administrador de rede copia o antivírus em um diretório do servidor ou um diretório compartilhado para o qual todos os usuários têm acesso. Esta cópia é executada por um programa de instalação projetado para este propósito. Você deve ter em mente que o antivírus NÃO está sendo instalado no servidor. Você está apenas copiando os arquivos necessários para instalar o antivírus nas estações.

2. Cada vez que um usuário se conecta à rede o programa verificará se a estação tem o antivírus instalado e atualizado. Em caso positivo, não executará nada, mas se o antivírus não está instalado ou atualizado, procederá com a instalação automática ou atualização do programa antivírus.

Como vimos, o servidor (quem compartilhou o recurso) só é usado como meio para distribuir o antivírus às estações.

Este procedimento geral é usado para praticamente todos tipos de redes. Porém, é executado de modo ligeiramente diferentemente para cada tipo. O procedimento para os tipos mais comuns de redes em uso atualmente será explicado neste manual.

Como distribuir o antivírus através de uma rede

Requisitos

Para distribuir o Panda Antivírus para Exchange/Outlook através de uma rede, você precisa de:

- Um computador IBM PC ou compatível capaz de rodar Windows 95, Windows 98 ou Windows NT Workstation 3.51 ou 4.0.
- 3 MB de espaço em disco rígido no servidor que será usado como o meio de distribuição.
- 3 MB de espaço em disco rígido em cada computador no qual o antivírus será instalado.

Como distribuir o antivírus facilmente para todas as estações de uma rede

O processo de distribuir o antivírus para todas as estações de rede consiste em duas partes:

1. Copiar o antivírus em um diretório ao qual todos os usuários podem ter acesso.

2. Distribuir o antivírus para todas as estações assim que estas se conectarem à rede por meio do programa RINSTALL.

Abaixo temos uma descrição detalhada de como executar os dois passos anteriores. Alguns aspectos deste processo de instalação requerem conhecimento do tipo de rede na qual o antivírus será distribuído. Toda essa informação é explicada em detalhes para cada um dos tipos principais de rede nas seções correspondentes. Consulte estas seções se você tiver qualquer dúvida.

Copiando o antivírus em um diretório onde todos os usuários podem ter acesso

O primeiro passo na distribuição do antivírus pela rede é a copia de arquivos em um diretório num dos discos rígidos do servidor. É essencial que ao copiar estes arquivos, o servidor esteja rodando em um ambiente livre de vírus. Se isto não for feito, os arquivos antivírus podem ser infectados. Como estes arquivos são distribuídos para todas as estações que se conectam à rede, o vírus seria distribuído junto com eles. Para obter uma cópia de arquivo segura e ter certeza que estes arquivos não irão infectar qualquer estação no futuro, a cópia deve ser executada de acordo com os passos seguintes:

1. O administrador deve ter certeza que o seu computador está livre de vírus. Seria aconselhável para o administrador instalar o Panda Software Antivírus em seu computador e ativar a proteção permanente correspondente. Você não deve continuar com a instalação até que esteja seguro que o computador a partir do qual você está instalando o antivírus está completamente livre de vírus.

2. Escolha um diretório no servidor correspondente onde você vai copiar os arquivos. Nós recomendamos que você crie um diretório novo chamado PAVEXCLI para o qual todos os usuários tem direito de leitura. É importante que nenhum usuário tenha direito de escrever ou apagar neste diretório. Caso contrário, qualquer usuário pode, acidental ou deliberadamente, infectar ou apagar os arquivos do antivírus, tendo como implicação sérias conseqüências.

3. Uma vez criado o diretório designado, apenas insira o disco 1 ou o CD-ROM, e rode o programa SETUP.EXE a partir do drive correspondente.

O processo de instalação consiste em uma série de janelas nas quais serão requisitados os dados

necessários para executar a instalação em seu computador. Um dos detalhes solicitados é o diretório destino. Você deve selecionar o diretório criado para este propósito de modo que os arquivos antivírus serão copiados neste local.

Distribuição do antivírus

Aqui é onde a vantagem de nosso antivírus para computadores em rede pode ser vista claramente. Em lugar de ter que ir de estação em estação instalando o antivírus, este será instalado automaticamente assim a estação se conecte à rede.

Quando uma estação se conecta à rede, uma série de comandos ou programas são executados para preparar a operação normal em rede, da mesma maneira como uma série de comandos ou programas são executados quando um computador inicia (boot). Esta série de programas e/ou comandos é conhecida como um *Login Script*.

Nosso antivírus com capacidade de distribuição em rede vem com um programa chamado **RINSTALL**, que executa a distribuição automática do antivírus. Assim, executar a distribuição automática do antivírus é tão fácil quanto colocar a execução do **RINSTALL** no *Login Script*.

O **RINSTALL** será executado toda vez que uma estação se conecta à rede. O **RINSTALL** primeiro verifica se a estação conectada já tem o antivírus instalado. Se o antivírus está instalado e atualizado, nada é executado, e o restante dos comandos do Login Script são executados normalmente. Se a estação não tem o antivírus instalado ou se este não está atualizado, o **RINSTALL** instalará o antivírus. Uma vez terminado este processo, a execução dos comandos de Login Script restantes continuam normalmente.

Como a execução do **RINSTALL** é completamente automática, o administrador de rede só precisa copiar os arquivos e modificar o *Login Script* para instalar a proteção antivírus que será distribuída para as estações quando estas se conectarem ao servidor.

Distribuição do antivírus em rede através de um Novell NetWare

Para distribuir o antivírus automaticamente para todas as estações quando estas se conectarem a um Novell NetWare, você deve inserir a seguinte linha no *Login Script de sistema* (ou *container*):

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

Consulte a seção Novell NetWare para obter uma explicação mais detalhada deste assunto.

Como pode ser visto no exemplo, você deve indicar o local no servidor onde os arquivos antivírus podem ser encontrados. Esta linha deve estar *depois* dos mapeamentos, deixando esta parte do *Login Script* como a seguir:

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

(assumindo que o nome do servidor é ALFA e que os arquivos estão localizados no volume SYS).

Distribuição do antivírus em uma rede Windows NT

Para distribuir o antivírus automaticamente para todas as estações assim que estas conectarem à rede, você deve acrescentar a seguinte linha no *Logon Script* e utilizá-lo através do programa Gerenciador de Perfis:

Consulte a seção Windows NT para obter uma explicação mais detalhada deste assunto.

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

Como pode ser visto no exemplo, você deve indicar onde os arquivos antivírus estão copiados. Esta linha deve estar antes do mapeamento dos recursos compartilhados, deixando esta parte do *Logon Script* como segue:

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

(assumindo que o nome de servidor é Alfa e o recurso compartilhado é chamado Sys).

Distribuição do antivírus em uma rede OS/2

Para distribuir o antivírus automaticamente para todas as estações assim que estas se conectem à rede, você deve acrescentar a seguinte linha no arquivo PROFILE.BAT (ou PROFILE.CMD):

Consulte a seção OS/2 para obter uma explicação mais detalhada deste assunto.

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

Como pode ser visto no exemplo, você deve indicar onde os arquivos antivírus estão copiados. Esta linha deve estar antes do mapeamento dos recursos compartilhados, deixando esta parte do arquivo de PROFILE.BAT como a seguir:

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

(assumindo que o nome de servidor é Alfa e o recurso compartilhado é chamado Sys).

Distribuição do antivírus em uma rede Pathworks

Para distribuir o antivírus automaticamente para todas as estações assim que estas se conectem à rede, você deve acrescentar a linha seguinte à seqüência de conexão do grupo de usuários dos computadores onde o antivírus será instalado:

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

Como pode ser visto no exemplo, você deve indicar onde os arquivos antivírus foram copiados. Desta forma, é aconselhável definir o mapeamento de rede antes rodar o **RINSTALL**.

Distribuição do antivírus em uma rede Banyan-Vines

Para distribuir o antivírus automaticamente para todas as estações assim que estas se conectem à rede, você deve acrescentar a seguinte linha ao perfil de cada usuário cujo computador será protegido. O perfil de usuário é a sucessão de comandos que são executados cada vez que um usuário se conecta à rede.

Basta editar este perfil com o comando de MUSER e adicionar a seguinte linha de comando:

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

(assumindo o mapeamento para o servidor como F: e que os arquivos foram copiados para o diretório **PAVEXCLI**).

É aconselhável definir o mapeamento de rede antes de rodar o RINSTALL e ter certeza que o disco rígido do servidor é referenciado da mesma maneira por todas as estações.

Mudar o perfil de todos os usuários, um a um, pode ser uma tarefa muito tediosa se houver muitos usuários. Normalmente, há um perfil comum usado por todos os usuários. Este perfil é chamado então dentro dos vários perfis de usuário. O comando usado para chamar um perfil dentro de outro é:

```
USE Sample_Profile@group@organization
```

onde *Sample_Profile* é um usuário fictício, e *group* e *organization* correspondem à estrutura da empresa.

Deste modo, você só precisa fazer as mudanças necessárias no Sample_Profile para que isto afete todos os usuários que chamam este perfil dentro de seu próprio perfil de usuário.

Instalação do antivírus em uma estação não conectada à rede

Se você quiser instalar Panda Antivírus para Exchange/Outlook em uma estação que não está conectada à rede, você deve executar o procedimento seguinte:

1. Insira disco 1 ou o CD-ROM do Panda Antivírus para Exchange/Outlook, vá para o caminho correspondente e rode o programa SETUP.EXE. O processo de instalação consiste em uma série de janelas, onde serão solicitadas as informações necessárias para executar a instalação em seu computador. Um dos detalhes solicitados é o diretório destino. Você deve selecionar um diretório no computador onde você está instalando o antivírus, e não um diretório de servidor como descrito anteriormente.

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

   C:\PAVEXCLI\RINSTALL PAVEX.SCR

   (se você instalou o antivírus em outro caminho ou diretório, indique as mudanças apropriadas).

3. Quando este processo estiver concluído, o programa antivírus para MS-Exchange/Outlook estará instalado em seu computador.

4. Apague o diretório onde você instalou o antivírus no passo 1, pois ele não será mais necessário.

Resolvendo problemas de distribuição

Se o antivírus não foi distribuído corretamente para um ou mais computadores, verifique o seguinte:

1. Tenha certeza o computador pode conectar-se ao servidor onde o antivírus foi copiado.

2. Tente rodar o **RINSTALL** diretamente no computador. Vá para o diretório do servidor onde o

antivírus foi copiado e rode **RINSTALL** PAVEX.SCR.

Se as duas verificações acima executarem corretamente, confira o *login script* e certifique-se que o *script* correto foi alterado e que a linha adicionada corresponde ao que foi previamente detalhado neste manual.

Características avançadas

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

Se você deseja evitar que os usuários que irão instalar automaticamente o Panda Antivírus para Exchange/Outlook alterem sua configuração, siga o procedimento descrito abaixo:

1. Instale o Panda Antivírus para Exchange/Outlook no computador do administrador de rede.

2. Abra o programa de correio MS-Exchange/Outlook e configure o antivírus do modo desejado.

3. Proteja a configuração com uma senha. Isto é executado através da janela de configuração do antivírus.

4. Copie o arquivo de PAVEXCLI.CFG encontrado no diretório WINDOWS\SYSTEM do computador do administrador para o diretório de rede a partir de onde o antivírus será ser distribuído.

5. Modifique o *login script* para distribuir o antivírus em todas as estações de rede.

É essencial que este procedimento seja executado antes da distribuição do antivírus através da rede.

Informação necessária sobre Novell NetWare

A distribuição do antivírus em uma rede Novell NetWare requer um certo conhecimento deste sistema. Os conceitos que você precisa entender são descritos abaixo, junto com exemplos de como preparar o sistema corretamente.

Comandos que são executados no início de uma sessão de rede

Normalmente, quando um computador inicia, uma série de comandos definida em um arquivo é executada. No caso do MS-DOS ou Windows, este é o arquivo AUTOEXEC.BAT.

Da mesma forma, também é normal que quando um computador se conecta a uma rede, uma série de comandos seja executada. Esta série de programas e/ou comandos é conhecida como *login script*.

O *login script* pode ser geral (o mesmo para todos os usuários) ou específico (um diferente para cada usuário). Também pode haver uma solução mista, com um *login script* geral comum a todos os usuários, e outro login script para cada usuário em particular.

Como o login script é executado cada vez que um usuário se conecta à rede, é o local ideal para atingir a distribuição do antivírus para todas as estações. Você só precisa rodar o programa de distribuição do Panda Software Antivírus no login script para distribuir o antivírus para todas as estações assim que estas se conectarem à rede.

Login script de sistema

No caso do Novell NetWare, o login script geral comum a todos os usuários é conhecido como o *Login script* de sistema. Você deve editar este arquivo para adicionar a execução do programa de distribuição do Panda Software Antivírus. Para editar o *Login script* de sistema, execute os passos seguintes:

1. Se você tiver um Novell NetWare versão 3.x, você deve usar o programa de SYSCON. Se você tiver um Novell NetWare versão 4.x, você precisa usar o programa NETADMIN. Todo servidor Novell NetWare tem normalmente um volume chamado SYS dentro de qual sempre há um diretório chamado o PUBLIC. Os dois programas (SYSCON e NETADMIN) pode ser encontrados neste diretório.

2. Para editar o *Login script* de sistema com SYSCON, rode o programa, selecione *Opções do Supervisor* e então *Login script de sistema.*

3. Para editar o Login script de sistema com NETADMIN, rode o programa e repetidamente selecione os dois pontos (..) na caixa na esquerda até esta opção não mais estar disponível. Você terá apenas uma opção então (à direita descrita como uma organização). Selecione esta opção e clique a tecla F10. No menu que se aparecerá, selecione a de opção Visualizar ou Editar Propriedades do Objeto e no menu seguinte selecione a opção Login Script. A partir deste ponto, você pode modificar o Login script de sistema.

Você deve inserir duas linhas no *Login script de sistema*: a linha relativa ao *mapeamento* (este conceito é explicado na próxima seção) e a linha que executa a distribuição automática do antivírus.

Associando uma letra de drive

Esta seção explica o conceito de *mapeamento*. Em um computador, o disco rígido é identificado

normalmente com a letra C, a unidade de disco flexível com a letra A ou B e o CD-ROM como drive D, E, e assim por diante, dependendo do número de dispositivos instalados.

Os volumes de um servidor Novell NetWare também precisam ser identificados com uma letra de drive para que os diretórios e arquivos nestes volumes possam ser acessados a partir das estações conectadas. A operação de associar uma letra de drive a um volume é conhecida como *mapeamento.*

É aconselhável que todas as estações possuam os mesmos mapeamentos para assegurar que os diferentes volumes sejam determinados pela mesma letra em cada caso. Fazer isto, você precisa colocar o comando de mapeamento no Login script de sistema. Geralmente os volumes são mapeados com letras a partir de F, mas qualquer outra letra de drive pode ser usada, contanto que já não esteja sendo usada. Considerando isto, o comando de mapeamento seria como segue:

```
MAP ROOT F:=SERVER_NAME\VOLUME_NAME
```

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

```
MAP ROOT F:=ALPHA\SYS:
```

Informação necessária sobre Windows NT

A distribuição do antivírus através de uma rede de Windows NT requer um certo conhecimento deste sistema. Os conceitos que você precisa entender são descritos abaixo, junto com exemplos de como preparar o sistema corretamente.

Comandos que são executados no início de uma sessão de rede

Normalmente, quando um computador inicia, uma série de comandos definida em um arquivo é executada. No caso do MS-DOS ou Windows, este é o arquivo AUTOEXEC.BAT.

Da mesma forma, também é normal quando um computador se conecta a uma rede, que uma série de comandos seja executada. No Windows NT esta série de programas e/ou comandos é conhecida como o *logon script*.

No Windows NT, cada usuário tem seu próprio logon script. Isto significa que você deveria modificar os logon scripts de todos os usuários para os quais você vai distribuir o antivírus. Para evitar esta tarefa tediosa, a Panda Software desenvolveu um utilitário chamado Gerenciador de Perfil, cujo funcionamento é explicado abaixo.

Como o *logon script* é executado cada vez que um usuário se conecta à rede, é o local ideal para executar a distribuição do antivírus para todas as estações. Você só precisa rodar o programa de distribuição do Panda Software Antivírus no logon script para distribuir o antivírus para todas as estações assim que estas se conectem à rede.

Logon scripts - Gerenciador de Perfil

Para instalar o programa de Gerenciador de Perfil, que lhe permite modificar todos os logon scripts simultaneamente, insira o disco com a etiqueta *Editor de Logon Script do Windows NT* ou vá para o diretório correspondente no CD-ROM e rode o programa **SETUP.EXE**. Por exemplo:

```
A:\SETUP
```

Uma vez instalado, execute os passos seguintes:

1. Rode o programa.
2. Selecione modo simplificado.
3. Selecione *Edite logon scripts de domínio* no menu Arquivo.
4. Um editor de texto aparecerá no na parte inferior da janela. Este é o local onde as alterações apropriadas são feitas de forma a afetar todos os *logon scripts*.
5. Encerre o programa, salvando as alterações.

Você deve inserir duas linhas no *Logon script*: a linha relativa ao *mapeamento* (este conceito é explicado na próxima seção) e a linha que se refere à execução da distribuição automática do antivírus.

Associando uma letra de drive

Esta seção explica o conceito de mapeamento. Em um computador, o disco rígido é identificado normalmente com a letra C, a unidade de disco flexível com a letra A ou B e o CD-ROM como o drive D, E, e assim por diante, dependendo do número de dispositivos instalados.

No caso de uma rede Windows NT, o conceito de *mapeamento* é relacionado ao conceito de um *recurso compartilhado*. O todo ou uma parte do disco rígido do servidor (ou discos se há vários) pode ser compartilhado, tornando-se assim um recurso compartilhado. Estes recursos compartilhados são aqueles que podem ser mapeados, de forma a poder serem referenciados depois pelas estações.

É aconselhável que todas as estações tenham os mesmos mapeamentos para assegurar que os recursos diferentes compartilhados no servidor sejam localizados do mesmo modo em cada caso. Para fazer isto, você precisa apenas colocar o comando de mapeamento no Logon script. Geralmente são mapeados os recursos compartilhados com letras a partir de F, mas qualquer outra letra pode ser utilizada, desde que já não esteja sendo em uso. Tendo isto em mente, o comando de mapeamento seria como segue:

```
NET USE  F: \\SERVER_NAME\RESOURCE_NAME
```

Se o nome de servidor for ALFA e o nome do recurso DIR, o comando seria:

```
NET USE F: \\ALPHA\DIR
```

Informação necessária sobre OS/2

A distribuição do antivírus através de uma rede OS/2 requer um certo conhecimento deste sistema. Os conceitos que você precisa entender são descritos abaixo, junto com exemplos de como preparar o sistema corretamente.

Comandos que são executados no início de uma sessão de rede

Normalmente, quando um computador inicia, uma série de comandos definida em um arquivo é executada. No caso do MS-DOS ou Windows, este é o arquivo AUTOEXEC.BAT.

Da mesma forma, também é normal que quando um computador se conecta a uma rede, uma série de comandos seja executada. Esta série de programas e/ou comandos é conhecida como o *login script*. No caso do OS/2, cada usuário tem um arquivo chamado PROFILE.BAT (ou PROFILE.CMD) que é executado cada vez o usuário se conecta à rede.

Como cada usuário tem seu próprio login script, você deve modificar os arquivos PROFILE.BAT para todos os usuários para os quais você queira distribuir o antivírus. A desvantagem é que as modificações futuras seriam realizadas também editando todos os arquivos PROFILE.BAT. Isto pode ser evitado criando um arquivo de BAT que contém as linhas necessárias para a distribuição do antivírus, e chamá-lo dentro dos arquivos PROFILE.BAT correspondentes. Deste modo, qualquer modificação futura pode ser feita neste arquivo de BAT de modo a afetar todos os usuários.

Como o login script é executado cada vez que um usuário se conecta à rede, é o local ideal para realizar a distribuição do antivírus para todas as estações. Você só precisa executar o programa de distribuição do Panda Software Antivírus no login script para distribuir o antivírus para todas as estações assim que estas se conectem à rede.

Associando uma letra de drive

Esta seção explica o conceito de *mapeamento*. Em um computador, o disco rígido é identificado normalmente com a letra C, a unidade de disco flexível com a letra A ou B e o CD-ROM como drive D, E, e assim por diante, dependendo do número de dispositivos instalados.

No caso de uma rede OS/2, o conceito de *mapeamento* é relacionado ao conceito de um *recurso compartilhado*. O todo ou uma parte do disco rígido do servidor (ou discos se há vários) pode ser compartilhado, tornando-se assim um recurso compartilhado. Estes recursos compartilhados são aqueles que podem ser mapeados, de forma que eles pode se referenciados depois pelas estações.

É aconselhável que todas as estações tenham os mesmos mapeamentos para assegurar que os recursos diferentes compartilhados no servidor sejam localizados do mesmo modo em cada caso. Você precisa apenas colocar o comando de mapeamento no arquivo PROFILE de cada usuário fazer isto. Geralmente são mapeados recursos compartilhados com letras a partir de F, mas qualquer outra letra de drive pode ser usada, desde que já não esteja em uso. Tendo isto em mente, o comando de mapeamento seria como segue:

```
NET USE  F: \\SERVER_NAME\RESOURCE_NAME
```

Se o nome de servidor é ALFA e o nome de compartilhamento é DIR, o comando seria:

```
NET USE F: \\ALPHA\DIR
```

Sintaxe do comando de script (.SCR)

Você deve ter observado através desta documentação que ao programa **RINSTALL** sempre está associado um parâmetro. Este parâmetro é o nome de um arquivo com extensão SCR (um arquivo de script). Um arquivo de script é um arquivo texto que está dividido em seções, nas quais cada linha contém um comando. O arquivo de script determina o comportamento do programa **RINSTALL**.

Os arquivos de SCR compatíveis com o **RINSTALL** podem ter 6 seções diferentes:

Seção comum **[COMMON]**: Estes comandos sempre são executados.

Seção DOS **[DOS]**: Os comandos desta seção são executados no DOS, Windows 3.1x e Windows 95.

Seção Windows 3.1x **[WIN]**: Os comandos desta seção são executados no DOS, Windows 3.1x e Windows 95, mas apenas se o diretório do Windows 3.1x for encontrado no disco rígido da estação.

Seção Windows 95 **[WIN95]**: Os comandos desta seção são executados no DOS, Windows 3.1x e Windows 95, mas apenas se o diretório do Windows 95 for encontrado no disco rígido da estação.

Seção Windows NT **[WINNT]**: Os comandos desta seção são executados no Windows NT.

Seção OS/2 **[OS/2]**: Os comandos desta seção são executados apenas no OS/2.

Há três tipos de comandos:

1. **Arquivos a serem copiados**: Todas as linhas que não iniciam com um sinal de cerquilha (#) indicam um arquivo que deve estar presente no diretório de origem, e que deve ser copiado para o diretório destino. Por default, estes são copiados quando não existem no diretório destino ou se o arquivo no diretório destino for mais antigo que o no diretório origem.

2. **Atribuições**: Estes comandos começam com um sinal de cerquilha (#) e tem a seguinte estrutura: #Variavel = valor. São usados para atribuir um certo valor a uma variável. As diferentes variáveis disponíveis em arquivo de script (SCR) estão detalhadas abaixo.

Variable name	**Description**
Win3xDir	diretório do Windows 3.1x
Win95Dir	diretório do Windows 95
WinNTDir	diretório do Windows NT
BaseSourcePath	Diretório base origem
BaseTargetPath	Diretório base destino
RelSourcePath	Diretório relativo origem
RelTargetPath	Diretório relativo destino
SourcePath	BaseSourcePath + RelSourcePath

TargetPath — BaseTargetPath + RelTargetPath

CopyMode — Indica a condição para copiar arquivos. Pode conter três valores. COPY indica que só serão copiados arquivos que não existem no diretório destino. UPDATE indica que só serão copiados arquivos se a versão da cópia for mais recente que o arquivo existente no diretório destino. OVERWRITE indica que os arquivos sempre serão copiados.

ErrorMode — Indica se devem ser exibidas ou não mensagens de erro. Pode ser atribuído o valor 0 (não serão exibidas mensagens) ou o valor 1 (serão exibidas mensagens).

3. **Funções**: estes comandos também começam com um sinal de cerquilha (#), e são usados para executar certas operações. Sua sintaxe é a seguinte: #Funcao Parametro1, parametro2, etc. As diferentes funções disponíveis são:

AddProfileEntry
Esta função acrescenta uma entrada a uma seção de um arquivo INI. Possui 4 parâmetros:

Parâmetro 1: indica em qual seção 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 do arquivo INI.

Exemplo:

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

AppendLine
Esta função acrescenta uma linha a um arquivo texto. Possui 3 parâmetros:

Parâmetro 1: indica o caminho do arquivo texto.
Parâmetro 2: indica a linha de texto a adicionar.
Parâmetro 3: LITERAL (opcional). Quando este parâmetro é especificado, você tem a garantia que a linha de texto aparecerá exatamente como escrita, eliminando qualquer possível modificação.

Exemplo:

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

AppendLineBefore
Esta função acrescenta uma linha a um arquivo texto, mas sempre antes de alguma outra linha específica. Possui 4 parâmetros:

Parâmetro 1: indica o caminho do arquivo texto.

Parâmetro 2: indica a linha de texto a adicionar.
Parâmetro 3: indica a linha de texto antes da qual a nova linha será inserida.
Parâmetro 4: LITERAL (opcional). Quando este parâmetro é especificado, você tem a garantia que a linha de texto aparecerá exatamente como escrita, eliminando qualquer possível modificação.

Exemplo:

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

DeleteLine
Esta função apaga uma linha de um arquivo texto. Possui 2 parâmetros:

Parâmetro 1: indica o caminho do arquivo texto.
Parâmetro 2: indica a linha de texto a apagar.

Exemplo:

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

InsertLine
Esta função insere uma linha no começo de um arquivo texto. Possui 3 parâmetros:

Parâmetro 1: indica o caminho do arquivo texto.
Parâmetro 2: indica a linha de texto para inserir.
Parâmetro 3: LITERAL (opcional). Quando este parâmetro é especificado, você tem a garantia que a linha de texto aparecerá exatamente como escrita, eliminando qualquer possível modificação.

Exemplo:

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

MakeDir
Esta função cria um diretório. Possui um parâmetro:

Parâmetro 1: indica o caminho do diretório a criar.

Exemplo:

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

NoWinLoad
O arquivo WIN.INI contém uma seção [Windows] que tem uma entrada chamada Load. Este comando carrega uma série de programas ao iniciar o Windows. Mais de um programa pode ser

especificado na mesma linha de Load. O comando NoWinLoad remove o programa selecionado do comando de Load. Possui um parâmetro:

Parâmetro 1: indica o programa que não será executado.

Exemplo:

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

ReplaceLine
Esta função substitui uma linha em um arquivo texto. Possui 3 parâmetros:

Parâmetro 1: indica o caminho do arquivo 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
```

SetProfileEntry
Esta função atribui um valor a uma entrada em uma seção especificada de um arquivo INI. A função tenta achar a seção especificada. Se achou, um valor é atribuído. Se não, cria a entrada e atribui o valor. Se a seção não existir, esta também será criada. Possui 4 parâmetros:

Parâmetro 1: indica a seção do arquivo 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 arquivo INI.

Exemplo:

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

WinLoad
O arquivo de WIN.INI contém uma seção [Windows] que tem uma entrada chamada Load. Este comando carrega uma série de programas ao iniciar o Windows. Mais de um programa pode ser especificado na mesma linha de Load. O comando WinLoad acrescenta o programa especificado ao comando de Load. Possui um parâmetro:

Parâmetro 1: indica o programa a ser executado.

Exemplo:

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

AdminRequired
Através desta função se indica que a partir deste momento, e desde que não apareça uma linha com a função EndAdminRequired, é necessário ser administrador para poder executar todo o bloqueio de comandos (os que se encontrem entre #AdminRequired e #EndAdminRequired). A função apenas tem efeito quando o Rinstall é executado com o parâmetro /Local. Esta função não admite parâmetros adicionais.

Exemplo:

```
#AdminRequired
```

EndAdminRequired
Esta função indica que todos os comandos seguintes podem ser executados sem a necessidade de ser administrador. Apenas tem efeito quando o Rinstall se executa com o parâmetro /Local. Esta função não admite parâmetros.

Exemplo:

```
#EndAdminRequired
```

ResetMode
Indica se deve-se reiniciar o computador nesse momento, em caso de ser necessário, ou se não se reiniciará. O valor 0 significa que não se reinicia, enquanto que o 1 significa que deve-se reiniciar agora. Em qualquer um dos casos se apresentará um aviso.

CheckSpace
Mediante este comando será comprovada a existência de espaço (em Mb) existente no destino. Em caso de não haver espaço suficiente, será apresentado um aviso, e os arquivos não serão copiados.

Parâmetro 1: indica o tamanho necessário em Mb.

Exemplo:

```
#CheckSpace 8
```

CopyFileAs
Realiza a cópia de um arquivo desde a origem até o destino, indicando o modo de cópia, e torna possível que o arquivo mude de nome no destino. Admite três parâmetros:

Parâmetro 1: indica a rota original do arquivo.
Parâmetro 1: indica o destino do arquivo.
Parâmetro 1: indica o modo da cópia, mediante as seguintes possibilidades: COPY (o arquivo apenas será copiado se não existir no destino), UPDATE (o arquivo apenas será copiado se a versão a copiar é mais recente que a já existente no destino), OVERWRITE (o arquivo sempre será copiado, ainda que origem e destino sejam iguais) e ONCHANGE (será copiado sempre que os arquivos origem e destino sejam distintos). ONCHANGE indica que se realizará a copia apenas se o arquivo origem é diferente do arquivo destino, não tendo em conta se este é mais antigo ou não.

DeteleDirDelayed

Quando finalizar a execução do RInstall (depois dos comandos #Run), este comando apaga o diretório completo, incluindo os subdiretórios.

Paramêtro 1: indica o diretório a apagar.

Exemplo:

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

ExchangeRequired

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

Exemplo:

```
#ExchangeRequired
```

EndExchangeRequired

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

Exemplo:

```
#EndExchangeRequired
```