



Tutorial sobre AVG Antimalware e AVGAdmin

Este tutorial tem como objetivo fornecer orientações e suporte aos administradores de redes na instalação das ferramentas de proteção contra códigos nocivos que foram adquiridas para o parque computacional da UNICAMP, sendo elas AVG Antivírus 7.5 e AVGAdmin 7.5 da empresa Grisoft.

Conforme já foi relatado por e-mail, recentemente conseguimos do fornecedor uma nova licença para podermos utilizar um novo produto da Grisoft conhecido como AVG Antimalware. Como algumas unidades/órgãos da Unicamp relataram problemas durante a instalação deste novo produto, o CCUEC decidiu preparar e distribuir este tutorial com o objetivo de facilitar e esclarecer o processo de instalação.

Se as dúvidas persistirem, pedimos que entrem em contato conosco no ramal 12207, ou diretamente com o suporte da Winco/Grisoft no telefone (11) 4226-3529.



Sobre o AVG Antimalware:

O AVG Antimalware é uma versão do antivírus AVG que integra a funcionalidade de antispymware em seu console. O CCUEC recomenda que seja utilizada esta versão em substituição à versão anterior que é o AVG Antivírus 7.5.

Para isso, orientamos sobre a necessidade da desinstalação completa do AVG 7.5 do sistema operacional de cada equipamento. Em seguida deve ser feito “download” do arquivo de instalação do AVG Antimalware que se encontra disponível no FTP da Unicamp em:

<ftp://ftp2.unicamp.br/pub2/apoio/antivirus/avg75/avg75amw476.exe>

Para instalação do AVG Antimalware deverá ser fornecido o número da licença disponibilizado na documentação destinada às unidades e órgãos que foi distribuída e retirada através da Biblioteca do CCUEC.

Sobre o AVGAdmin 7.5:

O AVGAdmin é uma ferramenta de gerenciamento remoto do programa antivírus AVG. Através dele é possível distribuir a instalação do AVG Antimalware, atualizar e efetuar verificações nas estações por agendamento.

Esta ferramenta é indicada às unidades e órgãos da UNICAMP que tenham uma grande quantidade de computadores que necessitem de atualização e manutenção do antivírus e que desejam fazer a instalação do software via administração remota, o que pode facilitar significativamente o processo de instalação.

Sendo assim recomendamos que os administradores de rede dêem preferência à atualização do antivírus via AVGAdmin, já que isso facilitará não só a instalação da nova versão, mas também a verificação periódica do status de proteção existente no parque computacional sob sua responsabilidade.

A seguir são apresentadas instruções específicas sobre como efetuar a instalação e uso do AVGAdmin.

Instalação da Ferramenta de Administração Remota AVGAdmin 7.5

Para utilizar a ferramenta de Administração Remota do AVG é necessário seguir alguns passos antes de partir para sua efetiva instalação.

Nestes passos são descritos a preparação do pacote de instalação do antivírus e alguns scripts que vão orientar a Administração Remota na distribuição do cliente para as estações Windows do domínio.

Será necessário, preferencialmente, uma estação com Windows Server(2000/2003), ou Windows XP Pro para a instalação do AVGAdmin e a hospedagem do pacote de instalação do AVG Antimalware e suas respectivas atualizações.

Primeiramente baixe o arquivo de instalação do AVGAdmin 7.5 que está disponível em:

<ftp://ftp2.unicamp.br/pub2/apoio/antivirus/avg75/admin/avg75adm.exe>

E em seguida o arquivo de instalação do AVG Antimalware:

<ftp://ftp2.unicamp.br/pub2/apoio/antivirus/avg75/avg75amw476.exe>

Obs.: Esta é a última versão disponibilizada na base da Grisoft. Verifique se existe uma versão mais atual no site da Grisoft para trabalhar sempre com a última versão.

Copie o arquivo setupfiles.zip. Este arquivo contém os scripts de instalação que serão lidos pelo AVGAdmin no processo de distribuição do AVG Antimalware.

<ftp://ftp2.unicamp.br/pub2/apoio/antivirus/avg75/admin/setupfiles.zip>

Preparando o servidor para a instalação do AVGAdmin 7.5

- 1) Crie uma pasta com o nome "avginst" na máquina servidora que será a fonte da instalação remota.
- 2) Descompacte o arquivo de instalação do AVG 7.5 Antimalware (avg75amw476.exe) na pasta "avginst" utilizando o WinRar (botão direito no arquivo - Extrair para...)
- 3) Em seguida compartilhe a pasta "avginst" para "todos".
- 4) Descompacte os arquivos de scripts de instalação também para dentro da pasta "avginst".
- 5) Na pasta "avginst", edite os arquivos avgsetup.bat e avgsetup.ini alterando os números de IP que aparecem para o número do IP da máquina que agora é o seu servidor de administração remota do AVG.
Exemplo:

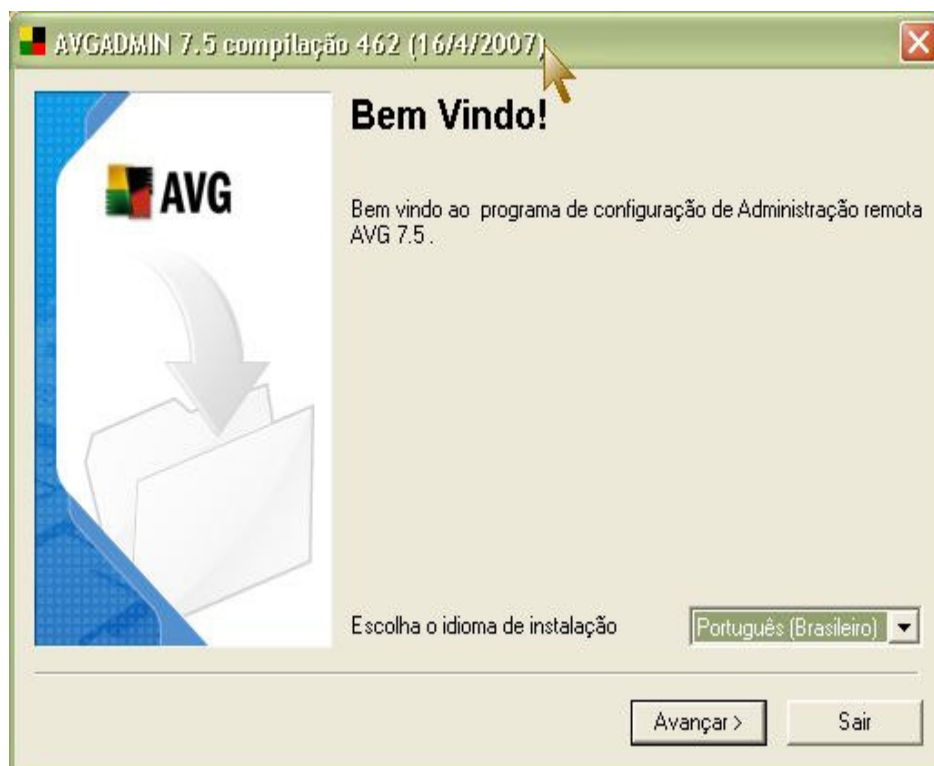
```
@ECHO OFF
REM AVG Setup Batch
SET SETUP="\\143.106.80.224\avginst\Setup.exe"
IF NOT EXIST %SETUP% SET SETUP="\\143.106.80.224\avginst\AvgSetup.exe"
IF NOT EXIST %SETUP% GOTO NoSetup
REM Start AVG Setup
%SETUP% /SCRIPT_FILE "\\143.106.80.224\avginst\AvgSetup.ini" %1 %2 %3 %4 %5 %6 %7 %8 %9
```

- 6) No arquivo avgsetup.ini, além da alteração do IP da máquina servidor, será necessário também a inserção do número de licença do AVG, retirado na Biblioteca do Centro de Computação.
A licença deve ser inserida no campo LICNO, entre as aspas, como no exemplo abaixo:

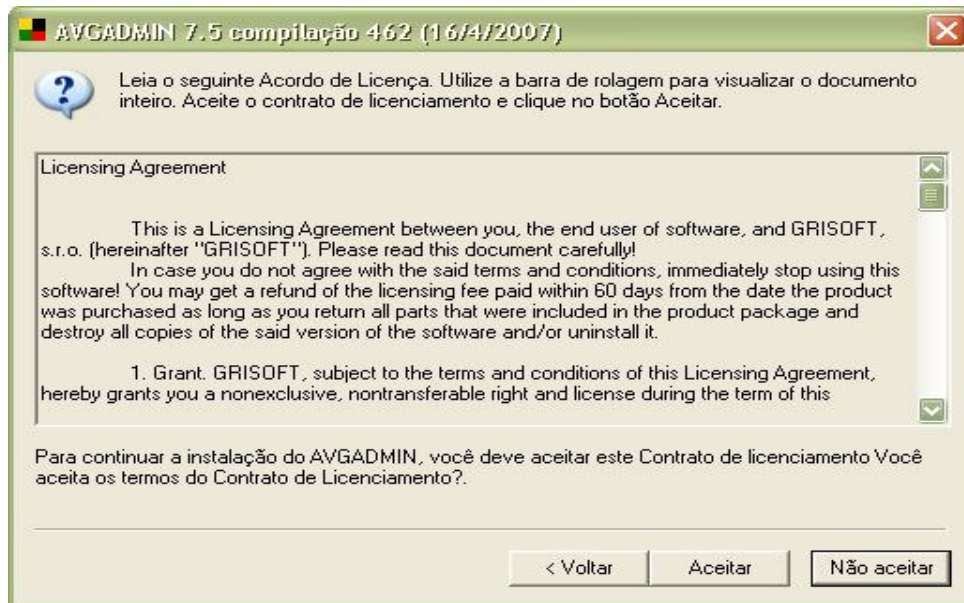
```
HIDE:
RESTART_IF_NEEDED:
KILL_PROCESS_IF_NEEDED:
LOG: "\\143.106.80.224\avginst\AVG7INST.LOG"
LICNO: "
ADD_FEATURE: fea_AVG_ResidentShield
ADD_FEATURE: fea_AVG_Antispy
ADD_FEATURE: fea_AVG EMC
```

Instalando o AVGAdmin 7.5

- 1) Execute o arquivo avg75adm.exe.
- 2) Na janela “Bem Vindo” aceite o idioma Português brasileiro e clique no botão “Avançar”.



3) Aceite o termo de licença no botão Aceitar;



4) Na janela "Pasta de destino" clique no botão "Avançar"



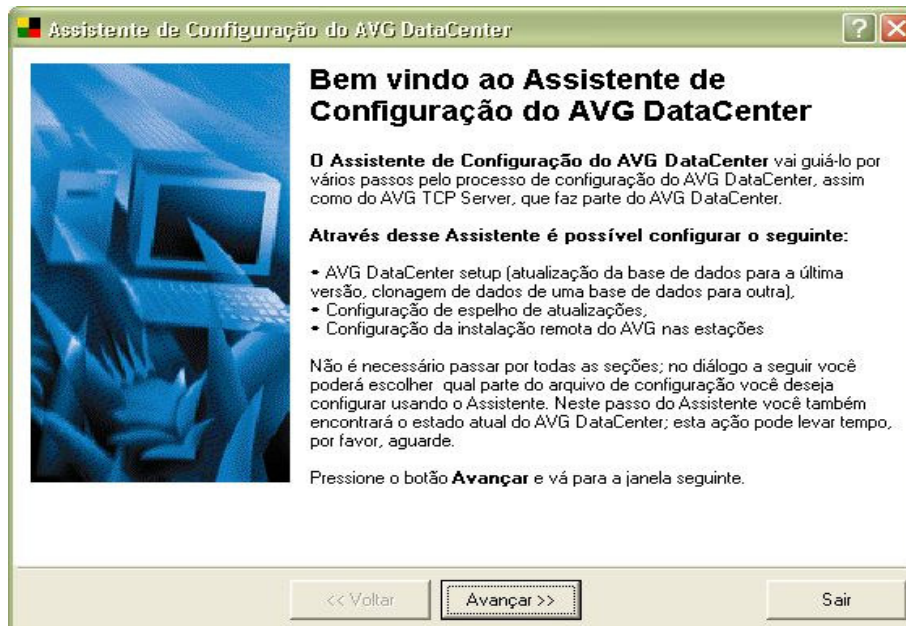
5) Na janela “Seleção de Componentes”, o AVGAdmin adiciona o banco de dados Firebird necessário para gerenciar as estações e suas instalações e atualizações. Clique no botão “Avançar”.



6) Clique em Concluir para finalizar a instalação do AVGAdmin, para em seguida iniciar as configurações da ferramenta.



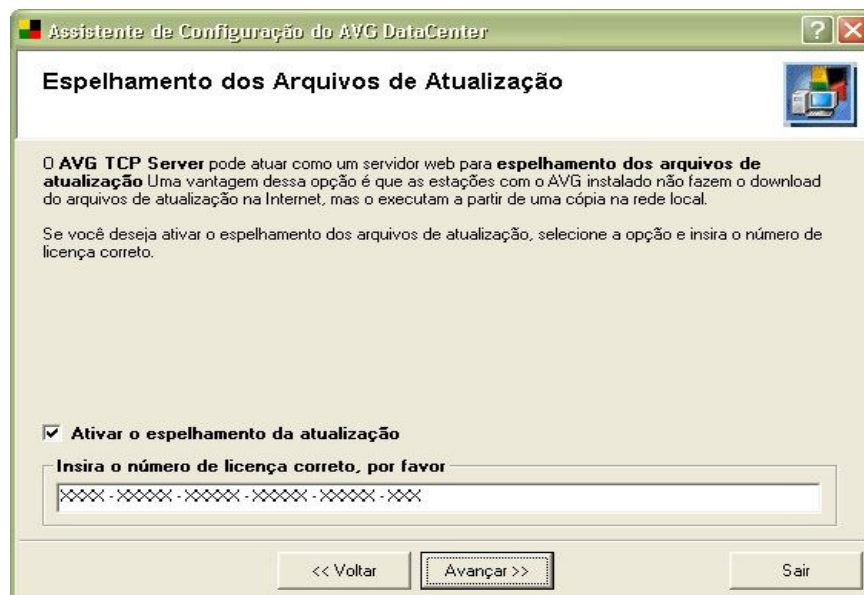
7) Dando início à configuração do AVGAdmin, clique em “Avançar”



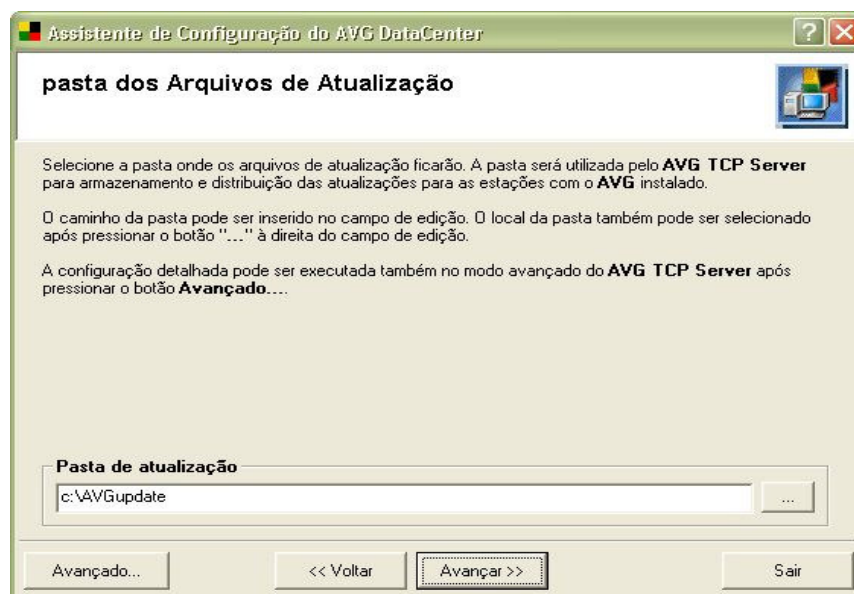
8) Na janela “Estado Atual do AVG Datacenter” selecione as opções Setup de Atualizações e Instalação Remota do AVG e clique em “Avançar”.



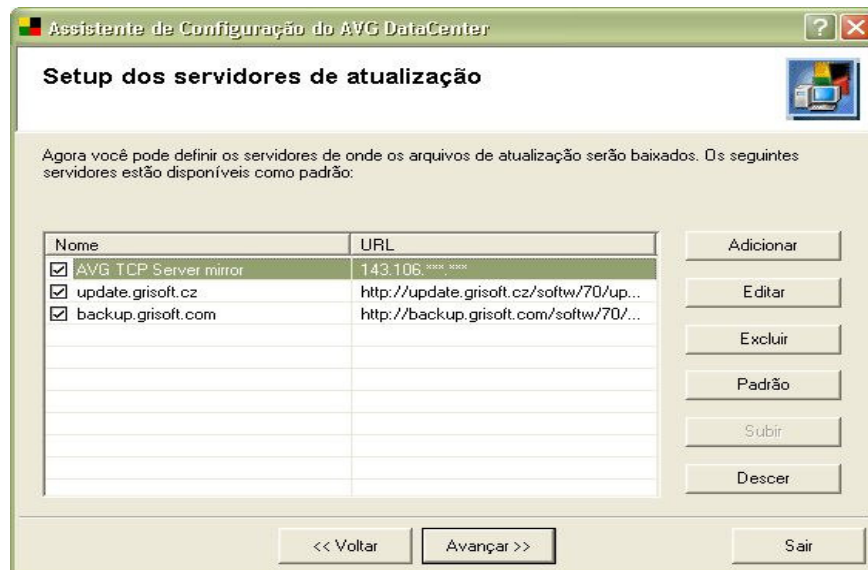
9) Na janela Espelhamento dos Arquivos de Atualização selecione a opção Ativar o espelhamento da atualização e insira o número da licença do AVG que foi retirada na Biblioteca do Centro de Computação.



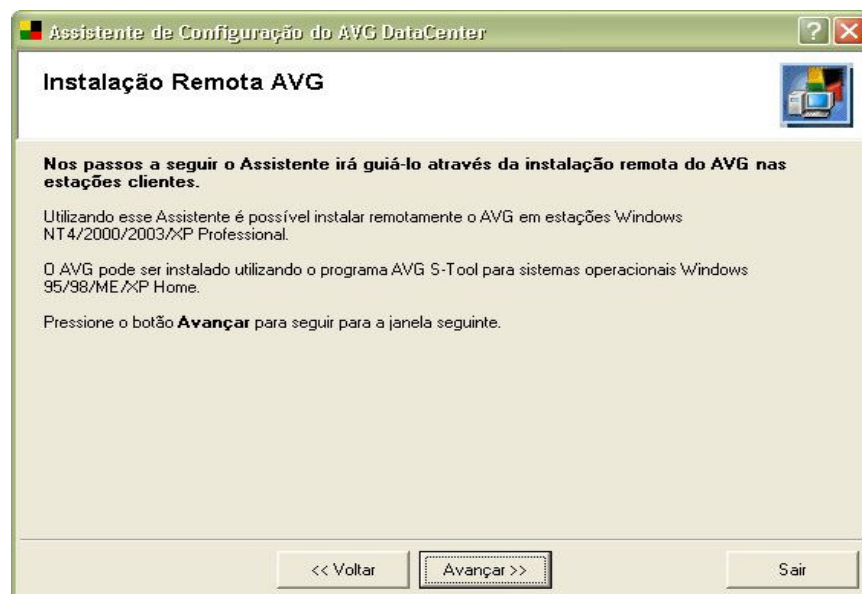
10) Verifique se a pasta AVGUpdate está selecionada como na janela “Pasta dos Arquivos de Atualização” abaixo e clique em Avançar.



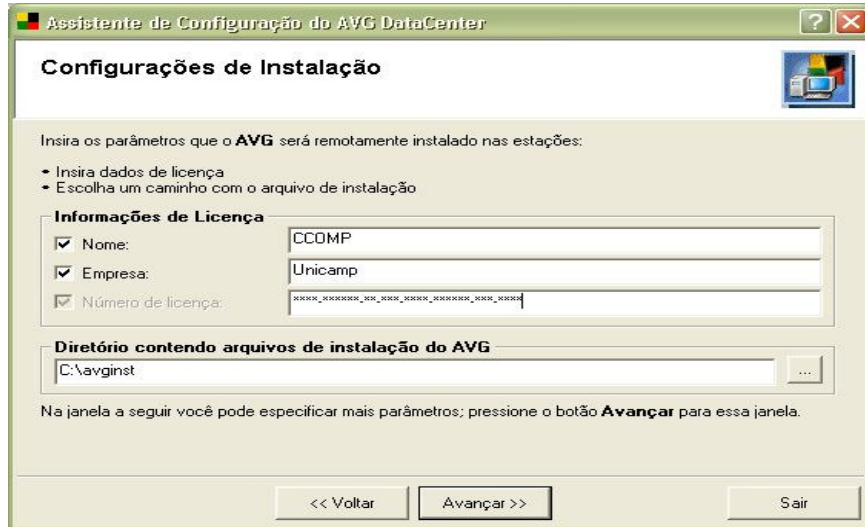
11) Na janela Setup dos Servidores de Atualização, selecione o campo AVG TCP Server mirror e clique no botão Editar. No Campo URL, insira o número IP da máquina onde está sendo instalado o AVGAdmin.



12) Na janela Instalação Remota do AVG, clique em Avançar para dar início ao processo de instalação remota do AVG Antimalware.



13) Na janela Configurações de Instalação, no campo Nome digite o nome de sua unidade, no campo Empresa digite Unicamp e insira novamente o número da licença do AVG Antimalware e clique em avançar.



Assistente de Configuração do AVG DataCenter

Configurações de Instalação

Insira os parâmetros que o **AVG** será remotamente instalado nas estações:

- Insira dados de licença
- Escolha um caminho com o arquivo de instalação

Informações de Licença

Nome: CCOMP

Empresa: Unicamp

Número de licença: xxxxx-xxxxxxx-xxx-xxxx-xxxxxxxx-xxxx-xxxx

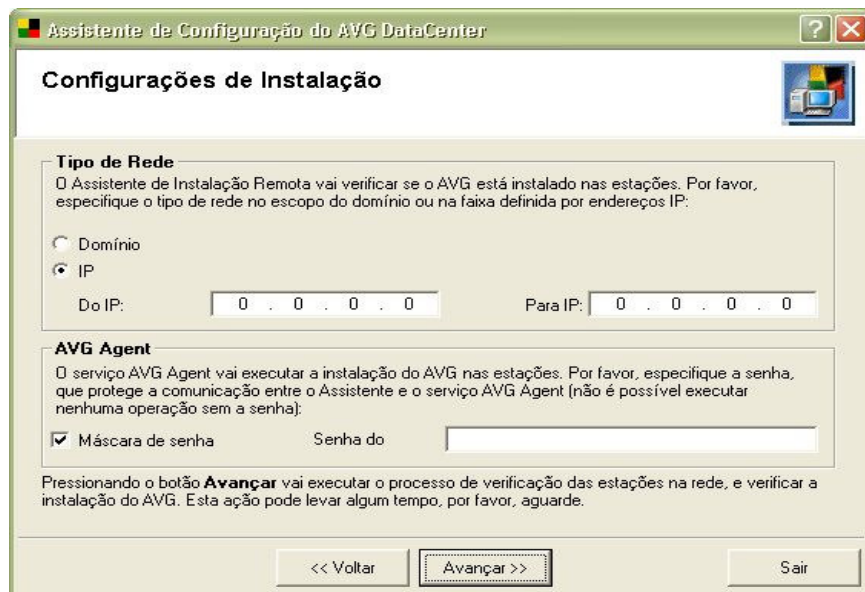
Diretório contendo arquivos de instalação do AVG

C:\avginst

Na janela a seguir você pode especificar mais parâmetros; pressione o botão **Avançar** para essa janela.

<< Voltar Avançar >> Sair

14) Neste próximo passo, será possível definir se a varredura pela rede será através do escopo do domínio ou pela faixa de IP que fará uma consulta no DNS e trará todas as estações dentro da faixa especificada.



Assistente de Configuração do AVG DataCenter

Configurações de Instalação

Tipo de Rede

O Assistente de Instalação Remota vai verificar se o AVG está instalado nas estações. Por favor, especifique o tipo de rede no escopo do domínio ou na faixa definida por endereços IP:

Domínio

IP

Do IP: 0 . 0 . 0 . 0 Para IP: 0 . 0 . 0 . 0

AVG Agent

O serviço AVG Agent vai executar a instalação do AVG nas estações. Por favor, especifique a senha, que protege a comunicação entre o Assistente e o serviço AVG Agent (não é possível executar nenhuma operação sem a senha):

Máscara de senha Senha do: _____

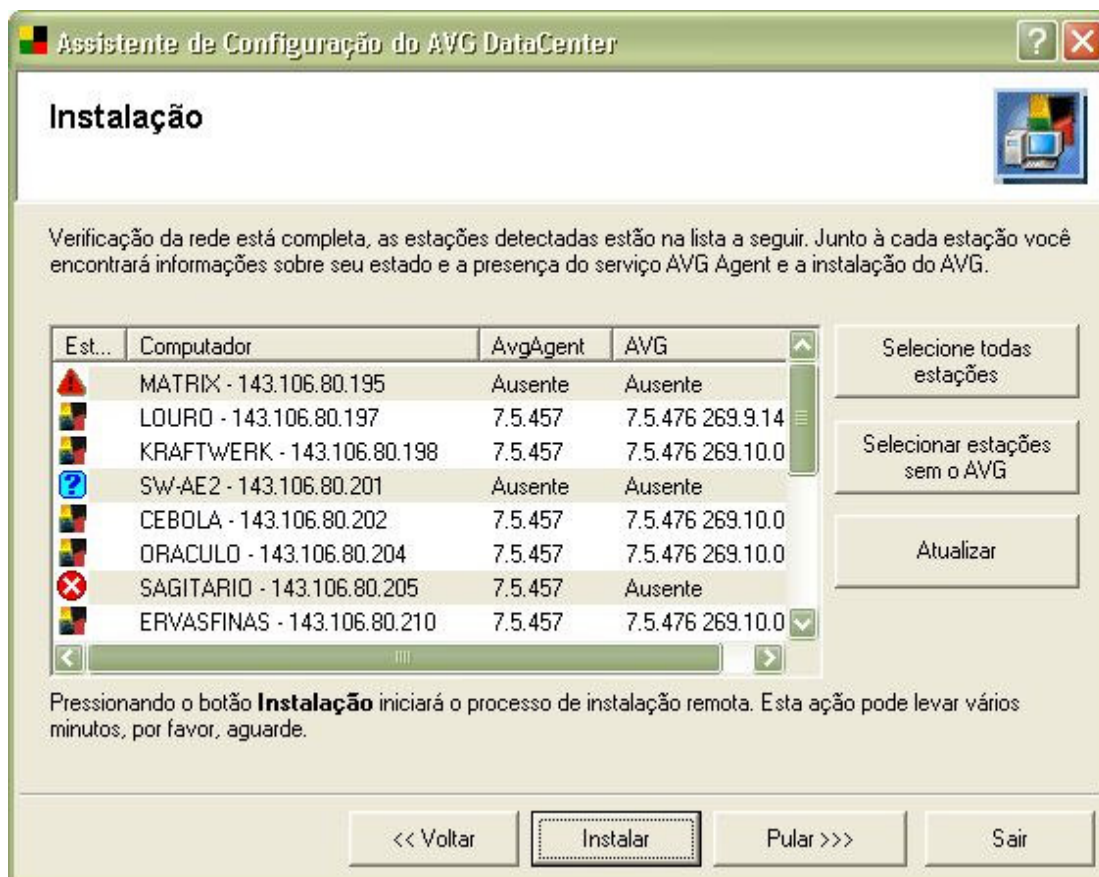
Pressionando o botão **Avançar** vai executar o processo de verificação das estações na rede, e verificar a instalação do AVG. Esta ação pode levar algum tempo, por favor, aguarde.

<< Voltar Avançar >> Sair

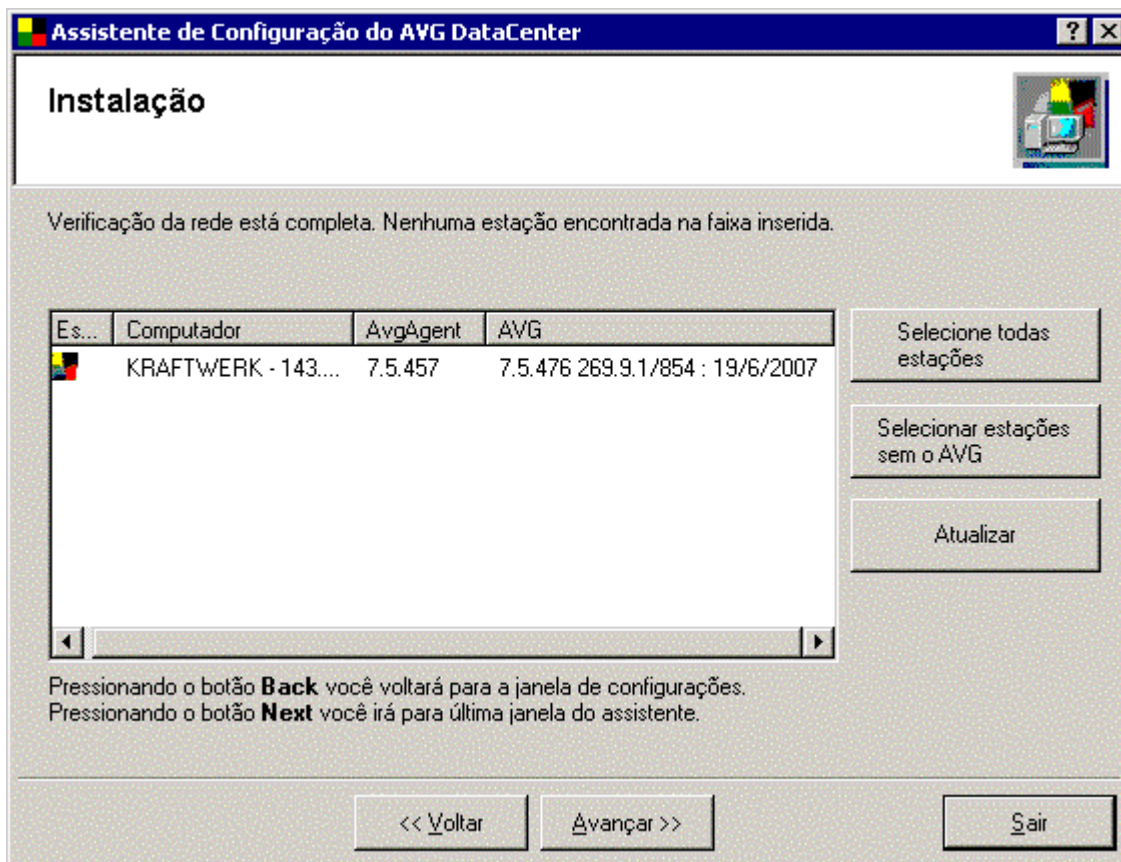
15) A janela “Instalação” descreve o resultado da varredura na rede, onde é possível verificar quais estações já possuem o antivírus e quais necessitam de instalação.

Para assegurar que a instalação da nova versão Antimalware será feita integralmente, recomendamos que seja removida a instalação anterior do AVG. Certifique, também, que nas estações com Windows XP o firewall do sistema esteja desativado para que o AVGAdmin possa identificá-las. Selecione as estações as quais deseja instalar a nova versão e clique em Instalar.

O processo envia o avgagent para a estação a qual passa a ser instruída a buscar os pacotes de instalação no servidor. Este processo pode levar de 5 a 7 minutos por estação.



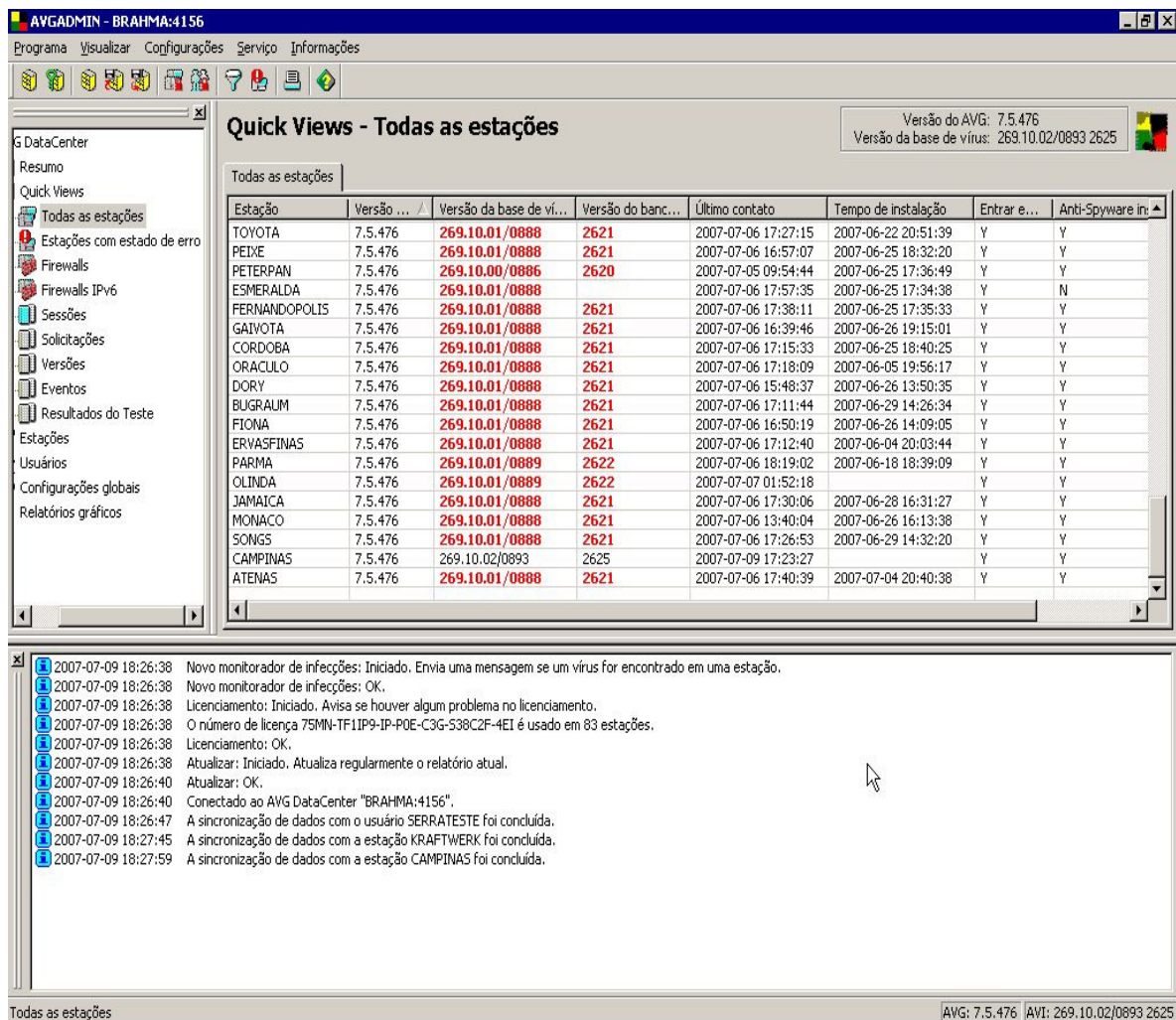
Concluída a instalação nas estações definidas (como exemplo da janela abaixo) pode-se voltar ao passo anterior através do botão Voltar para definir uma nova faixa de IP's que receberão o processo de instalação. Nesta janela temos as informações de estado da estação, nome e IP, versão do avgagent e a informação completa da versão do AVG Antimalware.



Esta é uma visão geral do console do AVGAdmin 7.5.

No console podemos obter uma lista completa de todas as estações com instalação do AVG, como sua versão, versão da base de vírus, versão do banco de dados do antispymware, último contato da estação com o AVGAdmin e a coluna com informações de qual estação está possivelmente infectada, seja com vírus, worms, trojans, spywares, adwares, etc. Geralmente o número apresentado será mais voltado aos spywares e adwares encontrados, uma vez que todo acesso a uma URL através de qualquer estação pode receber pelo menos um cookie.

No campo inferior são informadas as últimas ações das estações em relação ao AVGAdmin e vice-versa.



AVGADMIN - BRAHMA:4156

Programa Visualizar Configurações Serviço Informações

Quick Views - Todas as estações

Versão do AVG: 7.5.476
 Versão da base de vírus: 269.10.02/0893.2625

Estação	Versão ...	Versão da base de ví...	Versão do banc...	Último contato	Tempo de instalação	Entrar e...	Anti-Spyware in:
TOYOTA	7.5.476	269.10.01/0888	2621	2007-07-06 17:27:15	2007-06-22 20:51:39	Y	Y
PEIXE	7.5.476	269.10.01/0888	2621	2007-07-06 16:57:07	2007-06-25 18:32:20	Y	Y
PETERPAN	7.5.476	269.10.00/0886	2620	2007-07-05 09:54:44	2007-06-25 17:36:49	Y	Y
ESMERALDA	7.5.476	269.10.01/0888		2007-07-06 17:57:35	2007-06-25 17:34:38	Y	N
FERNANDOPOLIS	7.5.476	269.10.01/0888	2621	2007-07-06 17:38:11	2007-06-25 17:35:33	Y	Y
GAIVOTA	7.5.476	269.10.01/0888	2621	2007-07-06 16:39:46	2007-06-26 19:15:01	Y	Y
CORDOBA	7.5.476	269.10.01/0888	2621	2007-07-06 17:15:33	2007-06-25 18:40:25	Y	Y
ORACULO	7.5.476	269.10.01/0888	2621	2007-07-06 17:18:09	2007-06-05 19:56:17	Y	Y
DORY	7.5.476	269.10.01/0888	2621	2007-07-06 15:48:37	2007-06-26 13:50:35	Y	Y
BUGRAUM	7.5.476	269.10.01/0888	2621	2007-07-06 17:11:44	2007-06-29 14:26:34	Y	Y
FIONA	7.5.476	269.10.01/0888	2621	2007-07-06 16:50:19	2007-06-26 14:09:05	Y	Y
ERVASFINAS	7.5.476	269.10.01/0888	2621	2007-07-06 17:12:40	2007-06-04 20:03:44	Y	Y
PARMA	7.5.476	269.10.01/0889	2622	2007-07-06 18:19:02	2007-06-18 18:39:09	Y	Y
OLINDA	7.5.476	269.10.01/0889	2622	2007-07-07 01:52:18		Y	Y
JAMAICA	7.5.476	269.10.01/0888	2621	2007-07-06 17:30:06	2007-06-28 16:31:27	Y	Y
MONACO	7.5.476	269.10.01/0888	2621	2007-07-06 13:40:04	2007-06-26 16:13:38	Y	Y
SONGS	7.5.476	269.10.01/0888	2621	2007-07-06 17:26:53	2007-06-29 14:32:20	Y	Y
CAMPINAS	7.5.476	269.10.02/0893	2625	2007-07-09 17:23:27		Y	Y
ATENAS	7.5.476	269.10.01/0888	2621	2007-07-06 17:40:39	2007-07-04 20:40:38	Y	Y

2007-07-09 18:26:38 Novo monitorador de infecções: Iniciado. Envia uma mensagem se um vírus for encontrado em uma estação.
 2007-07-09 18:26:38 Novo monitorador de infecções: OK.
 2007-07-09 18:26:38 Licenciamento: Iniciado. Avisa se houver algum problema no licenciamento.
 2007-07-09 18:26:38 O número de licença 75MN-TF1IP9-IP-POE-C3G-538C2F-4EI é usado em 83 estações.
 2007-07-09 18:26:38 Licenciamento: OK.
 2007-07-09 18:26:38 Atualizar: Iniciado. Atualiza regularmente o relatório atual.
 2007-07-09 18:26:40 Atualizar: OK.
 2007-07-09 18:26:40 Conectado ao AVG DataCenter "BRAHMA:4156".
 2007-07-09 18:26:47 A sincronização de dados com o usuário SERRATESTE foi concluída.
 2007-07-09 18:27:45 A sincronização de dados com a estação KRAFTWERK foi concluída.
 2007-07-09 18:27:59 A sincronização de dados com a estação CAMPINAS foi concluída.

Todas as estações

AVG: 7.5.476 | AVI: 269.10.02/0893.2625



UNICAMP

Universidade Estadual de Campinas
UNICAMP
Centro de Computação
CCUEC



Em caso de dúvidas na instalação ou customização da ferramenta AVGAdmin, entre em contato no ramal 12207, ou entre em contato diretamente com o suporte da Winco/Grisoft no telefone (11) 4226-3529.