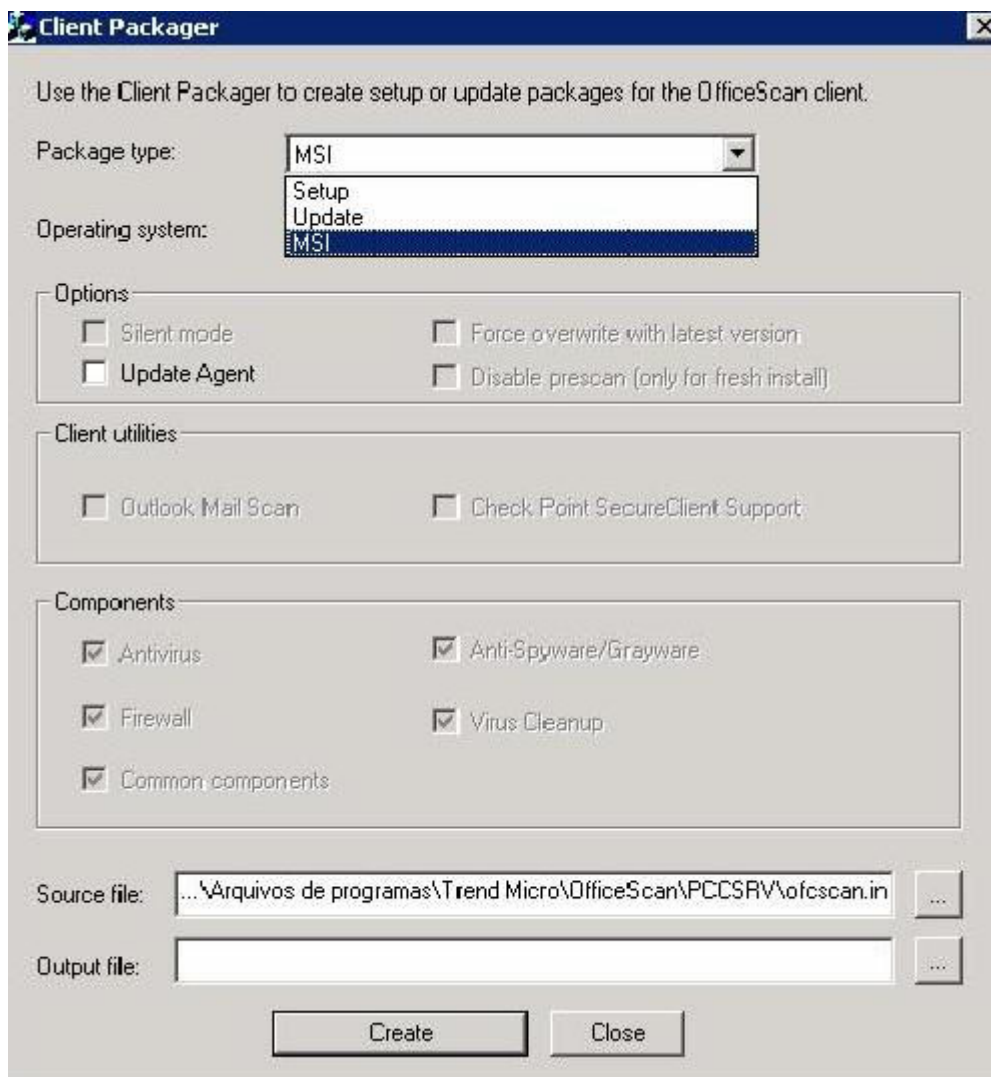


**Instalando e atualizando um Client Remoto
(Servidores na DMZ, Notebooks e Máquinas fora da rede).**


1. Instalação do cliente, utilizando a ferramenta ClientPackager.

- No diretório
... \Arquivos de programas\Trend Micro\OfficeScan\PCCSRV\Admin\Utility\ClientPackager
Obs. Essa ferramenta deve ser executada localmente no servidor ou com a utilização de alguma ferramenta de acesso remoto.
- Duplo clique no arquivo *ClnPack.exe*.



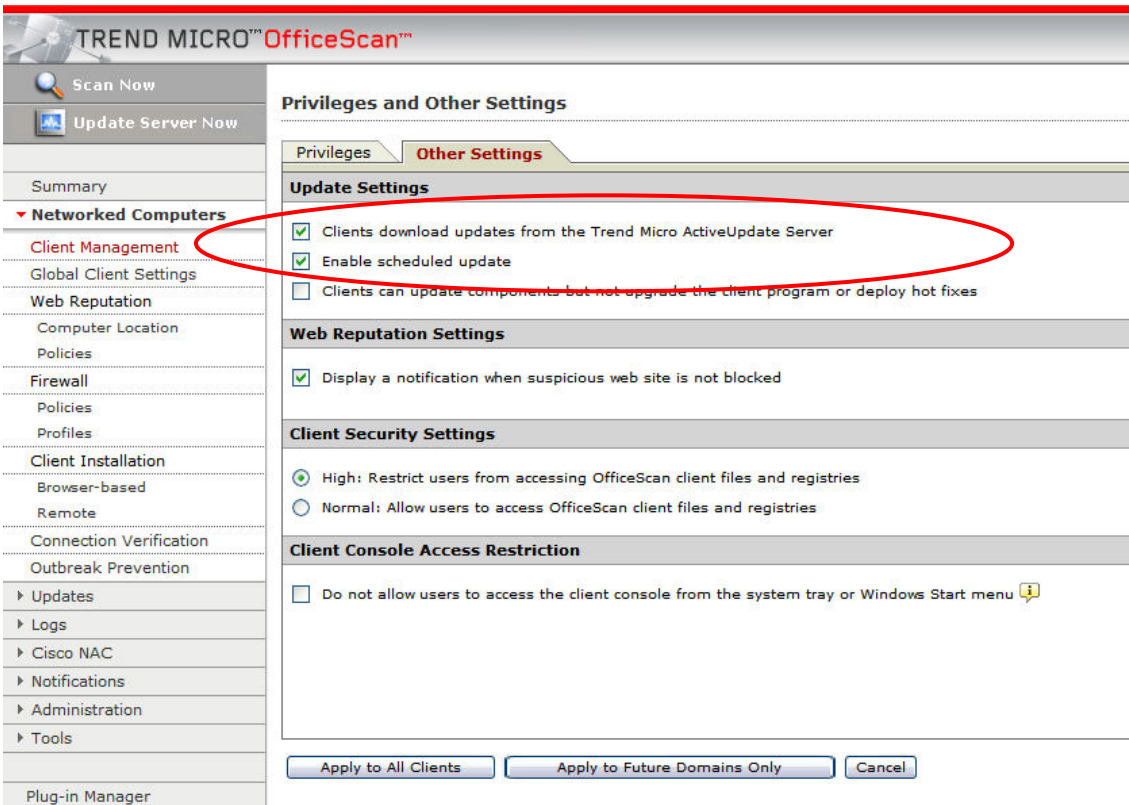
- Selecionar Package Type MSI ou SETUP (EXE).
- Na penúltima linha (Source File) determine o local do arquivo "ofcscan.ini", que a ferramenta usará para criar o cliente com as devidas configurações. Na ultima linha (Output File) determina o local e o nome que será gravado o arquivo final.

Observações e Recomendações:

1. Pode-se utilizar uma “pasta compartilhada” na rede, na qual as máquinas possam acessá-la e executar o *Pacote de Instalação* necessário.
2. Antes de instalar o cliente verifique se possui as devidas permissões de administrador da máquina.
3. Ao término da instalação o cliente estará azul conforme esse ícone .

2. Atualizando o cliente remoto via privilégios.

- 2.1. Abra uma conexão momentânea no seu firewall para as portas do officescan (porta WebServer, exemplo:8080 e porta Client/Server, exemplo:12345), assim, você pode configurar na console do OfficeScan Server: -> *Network Computers* -> *Client Management* -> **(Selecione o cliente)** -> *Settings* -> *Privileges other Settings* -> *Other Settings* -> **Clients download updates from the Trend Micro ActiveUpdate Server** e **Enable Scheduled Update**



The screenshot displays the Trend Micro OfficeScan console interface. The left sidebar shows a navigation menu with categories like 'Scan Now', 'Update Server Now', 'Summary', 'Networked Computers', 'Client Management', 'Global Client Settings', 'Web Reputation', 'Firewall', 'Client Installation', 'Connection Verification', 'Outbreak Prevention', 'Updates', 'Logs', 'Cisco NAC', 'Notifications', 'Administration', 'Tools', and 'Plug-in Manager'. The main content area is titled 'Privileges and Other Settings' and has two tabs: 'Privileges' and 'Other Settings'. The 'Other Settings' tab is active, showing the 'Update Settings' section with three options: 'Clients download updates from the Trend Micro ActiveUpdate Server' (checked), 'Enable scheduled update' (checked), and 'Clients can update components, but not upgrade the client program or deploy hot fixes' (unchecked). Below this are sections for 'Web Reputation Settings' (with 'Display a notification when suspicious web site is not blocked' checked) and 'Client Security Settings' (with 'High: Restrict users from accessing OfficeScan client files and registries' selected). At the bottom, there is a 'Client Console Access Restriction' section with 'Do not allow users to access the client console from the system tray or Windows Start menu' unchecked. At the very bottom of the console, there are three buttons: 'Apply to All Clients', 'Apply to Future Domains Only', and 'Cancel'.

Depois de realizar as configurações, “feche” novamente as portas abertas no firewall

3. Atualizando o client remoto via registro.

Atenção! As configurações a seguir são feitas no registro do windows, recomendamos que seja feito um back-up do registro antes de iniciarmos as configurações.

- **INICIAR -> Executar** , digite **regedit**.
- No Regedit, selecione, **HKEY_LOCAL_MACHINE -> SOFTWARE -> Trend Micro -> PcCillinNTCorp -> Current Version -> Misc**.
- Na pasta **Misc.**, do lado direito da tela, clique com o botão direito e crie uma nova CHAVE “**Valor da sequência**” com o valor **UpdateFrom**, conforme o Sistema Operacional.

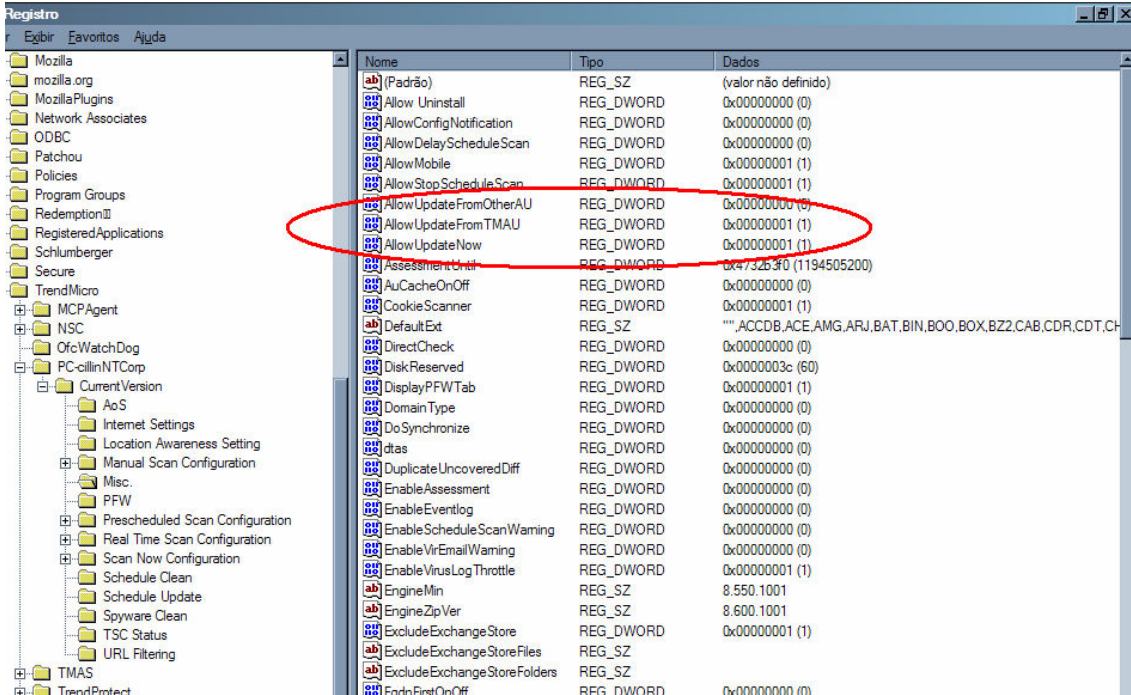
Officescan 7.3

Clique em **UpdateFrom** com o botão direito -> Modificar e insira o seguinte link:
<http://officescan-p.activeupdate.trendmicro.com/activeupdate>

Officescan 8.0

Clique em **UpdateFrom** com o botão direito -> Modificar e insira o seguinte link:
<http://osce8-p.activeupdate.trendmicro.com/activeupdate>

- Clique com o botão direito em **AllowUpdateFromOtherAU**, opção modificar e insira o valor 1.
- Clique com o botão direito em **AllowUpdateFromTMAU**, opção modificar e insira o valor 1.
- Clique com o botão direito **AllowUpdateNow**, opção modificar e insira o valor 1



Nome	Tipo	Dados
(ab) (Padrão)	REG_SZ	(valor não definido)
(ab) Allow_Uninstall	REG_DWORD	0x00000000 (0)
(ab) AllowConfigNotification	REG_DWORD	0x00000000 (0)
(ab) AllowDelayScheduleScan	REG_DWORD	0x00000000 (0)
(ab) AllowMobile	REG_DWORD	0x00000001 (1)
(ab) AllowStopScheduleScan	REG_DWORD	0x00000001 (1)
(ab) AllowUpdateFromOtherAU	REG_DWORD	0x00000000 (0)
(ab) AllowUpdateFromTMAU	REG_DWORD	0x00000001 (1)
(ab) AllowUpdateNow	REG_DWORD	0x00000001 (1)
(ab) AssessmentURL	REG_DWORD	0x473263f0 (1194505200)
(ab) AuCacheOnOff	REG_DWORD	0x00000000 (0)
(ab) CookieScanner	REG_DWORD	0x00000001 (1)
(ab) DefaultExt	REG_SZ	"";_ACCDB;ACE;AMG;ARJ;BAT;BIN;BOO;BOX;BZ2;CAB;CDR;COT;C...
(ab) DirectCheck	REG_DWORD	0x00000000 (0)
(ab) DiskReserved	REG_DWORD	0x0000003c (60)
(ab) DisplayPFWTab	REG_DWORD	0x00000001 (1)
(ab) DoSynchronize	REG_DWORD	0x00000000 (0)
(ab) dtas	REG_DWORD	0x00000000 (0)
(ab) DuplicateUncoveredDiff	REG_DWORD	0x00000000 (0)
(ab) EnableAssessment	REG_DWORD	0x00000000 (0)
(ab) EnableEventlog	REG_DWORD	0x00000000 (0)
(ab) EnableScheduleScanWarning	REG_DWORD	0x00000000 (0)
(ab) EnableVirEmailWarning	REG_DWORD	0x00000000 (0)
(ab) EnableVirusLogThrottle	REG_DWORD	0x00000001 (1)
(ab) EngineMin	REG_SZ	8.550.1001
(ab) EngineZipVer	REG_SZ	8.600.1001
(ab) ExcludeExchangeStore	REG_DWORD	0x00000001 (1)
(ab) ExcludeExchangeStoreFiles	REG_SZ	
(ab) ExcludeExchangeStoreFolders	REG_SZ	
(ab) ForInFirstOnOff	REG_DWORD	0x00000000 (0)

- Utilize a ferramenta **SucTool** para programar as atualizações automáticas do client, assim o Update não precisara ser manual.

Segue compactada a ferramenta.



SucTool.zip