Etapas a clonar ou imagem um computador com o conector AMP instalado

Índice

Introdução

Este original descreve as etapas para clonar ou imagem um computador com o conector avançado da proteção do malware (AMP) instalado, a fim impedir computadores múltiplos para tentar globalmente o uso de mesmos - o identificador exclusivo (GUID), para evitar o computador duplicado objeta para aparecer no painel da nuvem AMP.

Como um administrador de sistema, você quer incluir o conector AMP em suas imagens mestras do PC Windows. O AMP exige que os sistemas podem excepcionalmente ser identificados.

Pré-requisitos

- Conhecimento de navegar e de editar o registro de Windows.
- Usando o comando prompt do SO Windows.
- Usando o terminal de comando do Linux OS.

Para Windows

Verifique que persistência da identidade está ajustada corretamente para o ambiente do desenvolvimento. Os ambientes VDI tendem a clonar endereços MAC assim que a sincronização pelo MAC não é recomendada. O melhor prática para VDI é sincronização pelo hostname através da política. Para a funcionalidade apropriada, toda a persistência da identidade deve ser congruente através do negócio. Se uma política é ajustada para a “sincronização através da política”, todas as políticas que usam a persistência da identidade devem usar a “sincronização através da política”.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

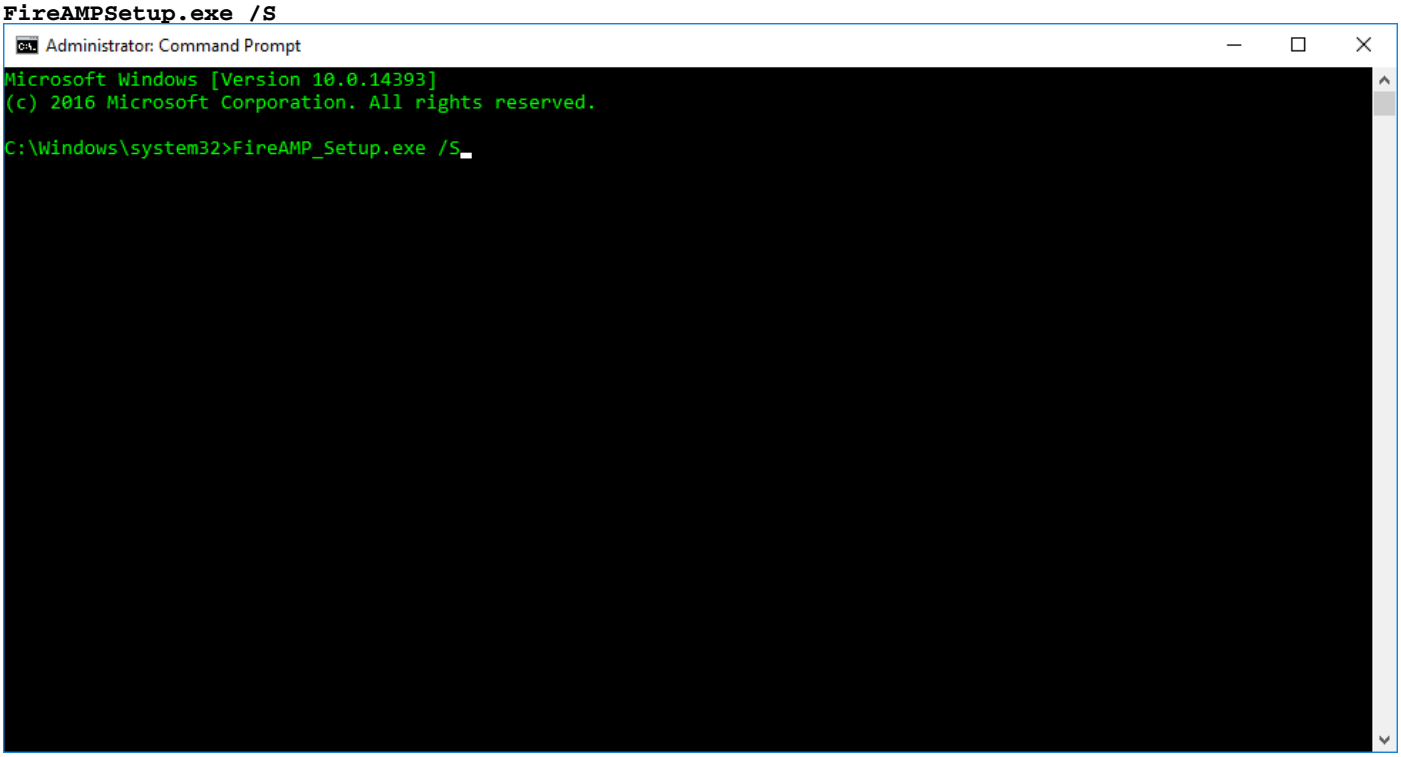
Instalação provisória - Versão 6.2.1+

Execute estas etapas para preparar um computador para a imagem latente:

1. Desabilite o acesso à internet na máquina.

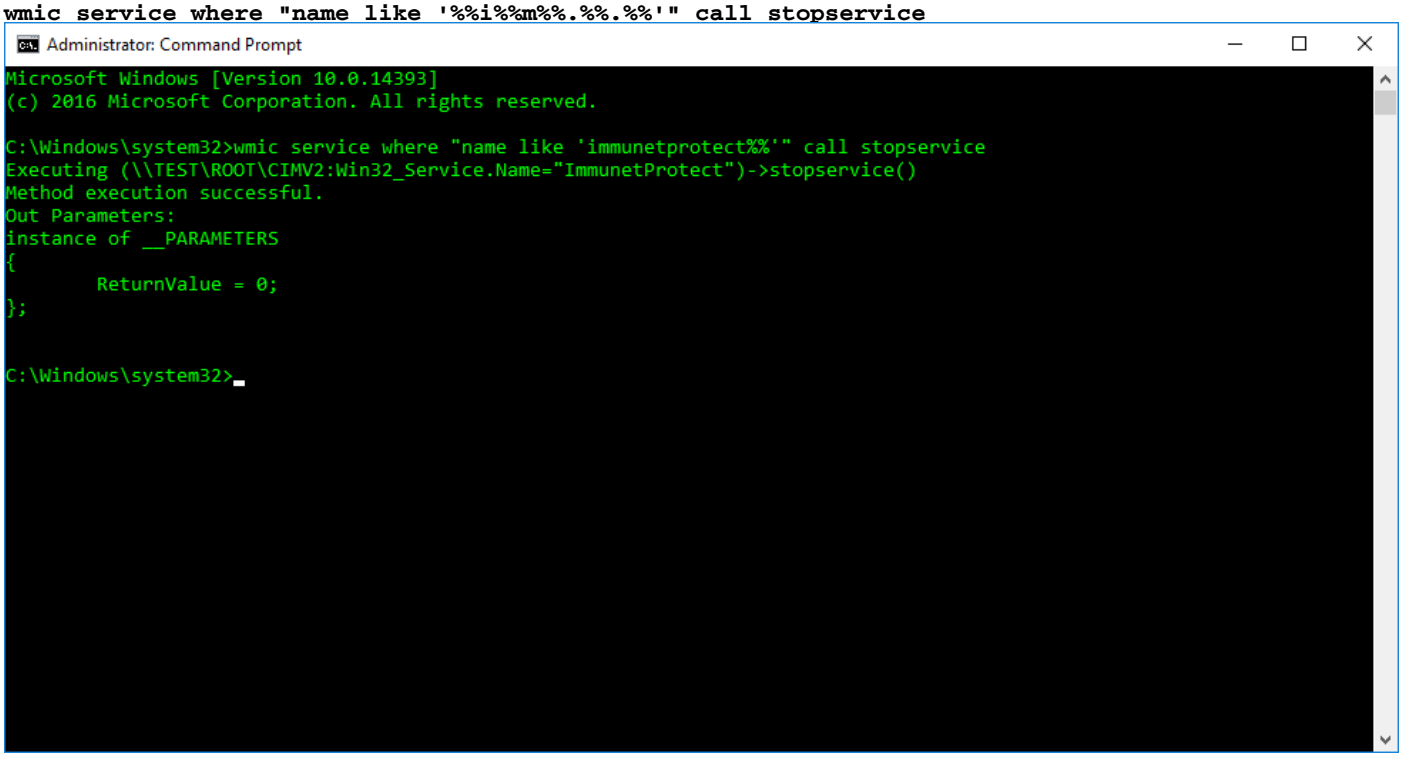
2. Instale o conector AMP em sua imagem mestra.

```
FireAMPSetup.exe /S
```



3. Pare o serviço AMP.

```
wmic service where "name like '%%i%%m%%.%%.%%'" call stopservice
```



Use o comando seguinte **se você tem a proteção do conector permitida.** A senha será visível no comando prompt.

```
"%PROGRAMFILES%\Cisco\AMP\X.X.X\sfc.exe" -k protectionpassword
```

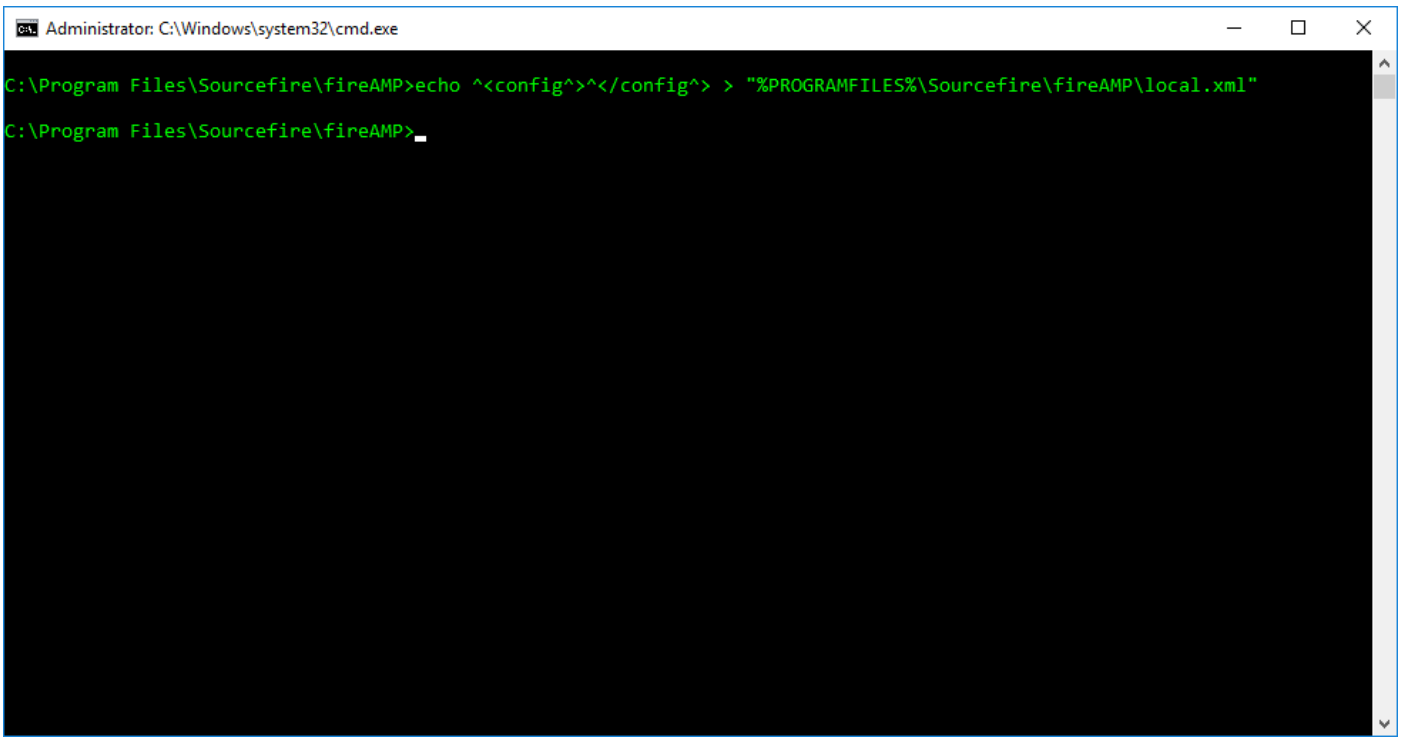
> **Note**: **Recomenda-se altamente** para verificar **Policy.xml (%PROGRAMFILES%** \ Cisco \ AMP \ Policy.xml) e para verificar que há uma entrada para o <Install><Token>. Isto é necessário para que o conector seja registrado no grupo correto/política. O melhor prática seria guardar uma cópia desse arquivo caso que as próximas etapas estão tendo que ser repetidas por qualquer razão.
>
> **Nota:** Se o serviço AMP é começado outra vez, a imagem mestra regenerateslocal.xml**.** **Você** precisa de repetir estas etapas para neutralizar outra vez a imagem mestra. Seja certo incluir estas etapas em seu processo da preparação da imagem mestra.

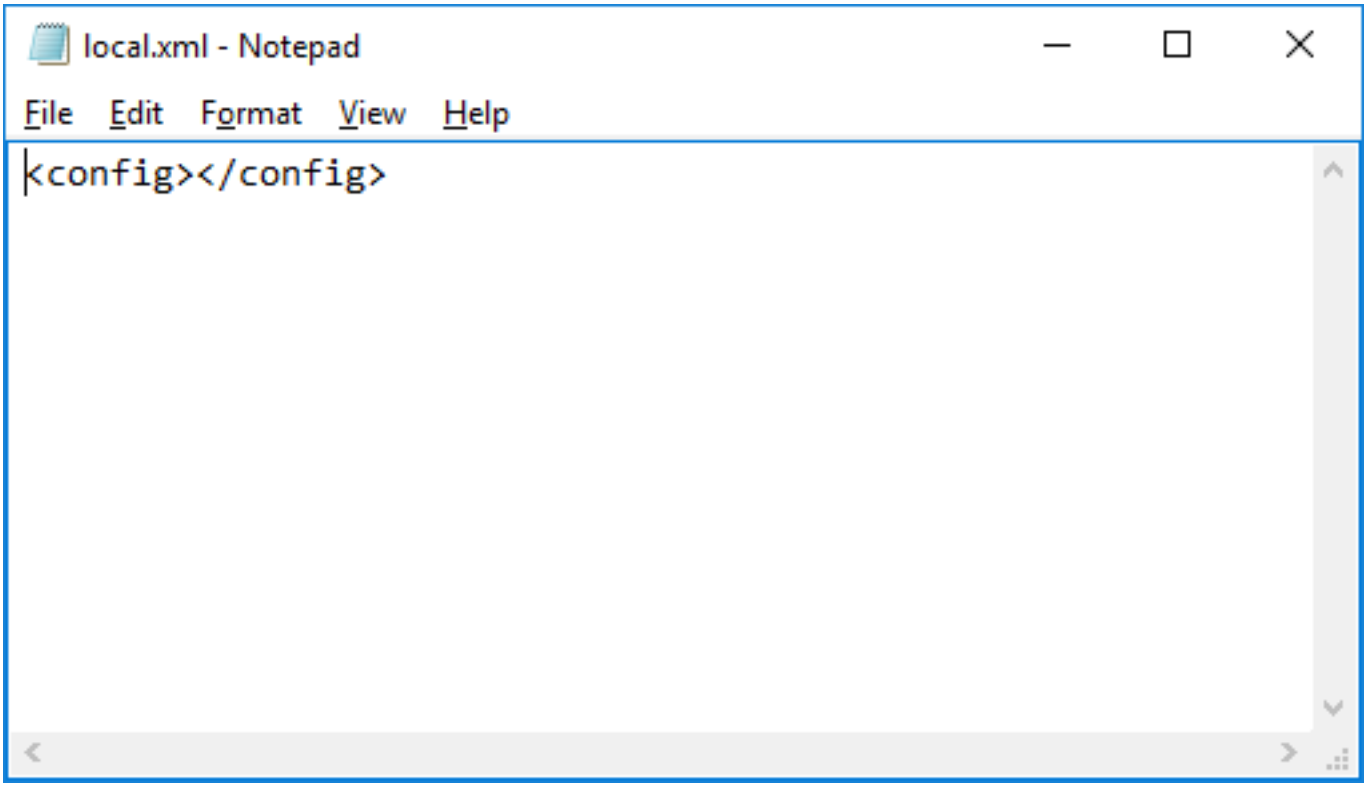
4. Deletelocal.xml**.**

```
del "%PROGRAMFILES%\Cisco\AMP\local.xml"
```

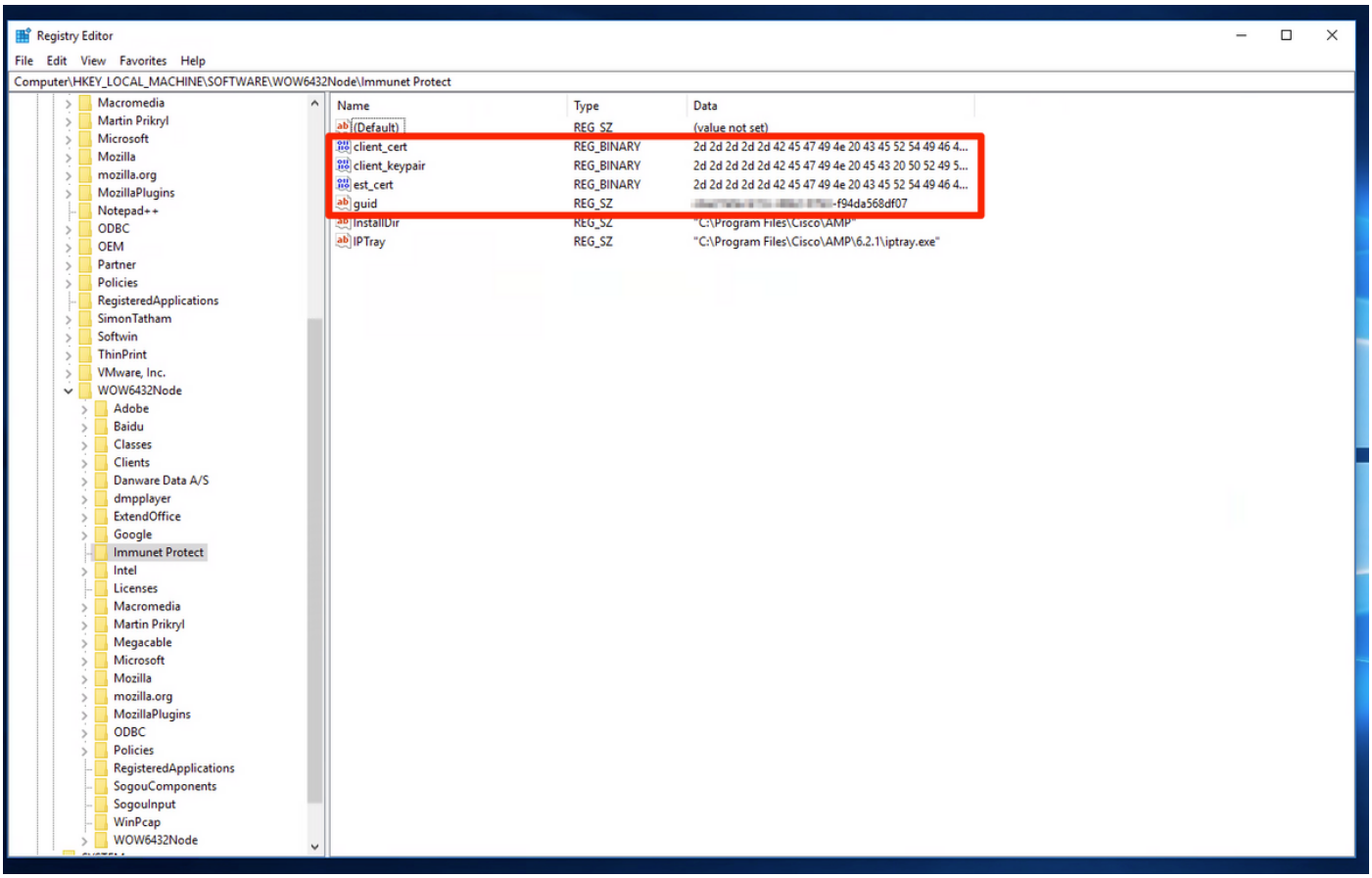
5. Crie um **`local.xmlfile`** vazio.

```
echo ^<config^>^</config^> > "%PROGRAMFILES%\Cisco\AMP\local.xml"
```



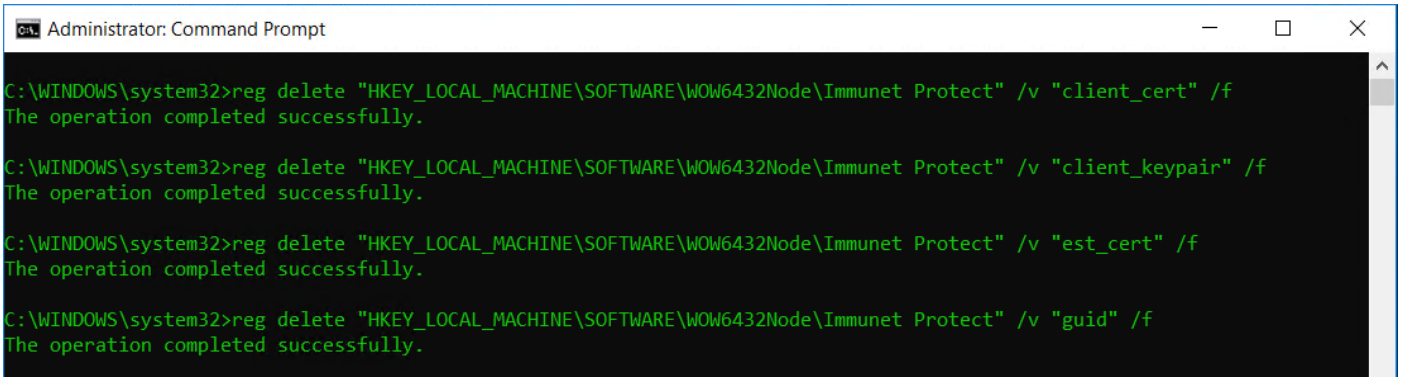


6. Cancele o GUID e a informação do certificado do registro de *KEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Immunet protegem*.



Note: **Começando com 6.2.1**, os GUID e os Certificados são armazenados igualmente no registro como a remediação para o erro [CSCvi92800](#) .

```
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Immunet Protect" /v "client_cert" /f
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Immunet Protect" /v "client_keypair" /f
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Immunet Protect" /v "est_cert" /f
reg delete "HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Immunet Protect" /v "guid" /f
```



7. **Não comece o serviço outra vez ou você será forçado a repetir etapas 3-6.** O serviço deve começar na bota.

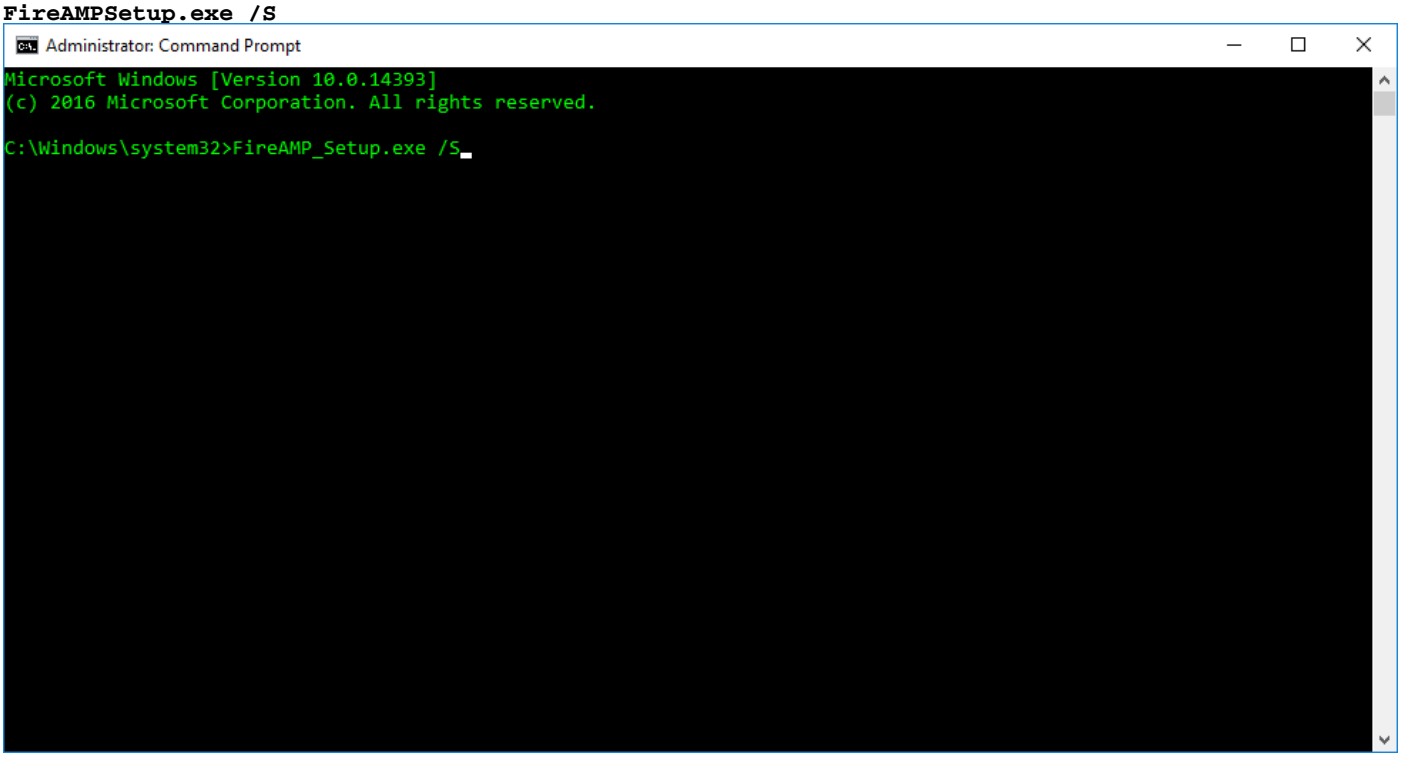
Instalação provisória - Versões 4.1.4 à 6.1.7

Execute estas etapas para preparar um computador para a imagem latente:

1. Desabilite o acesso à internet na máquina.

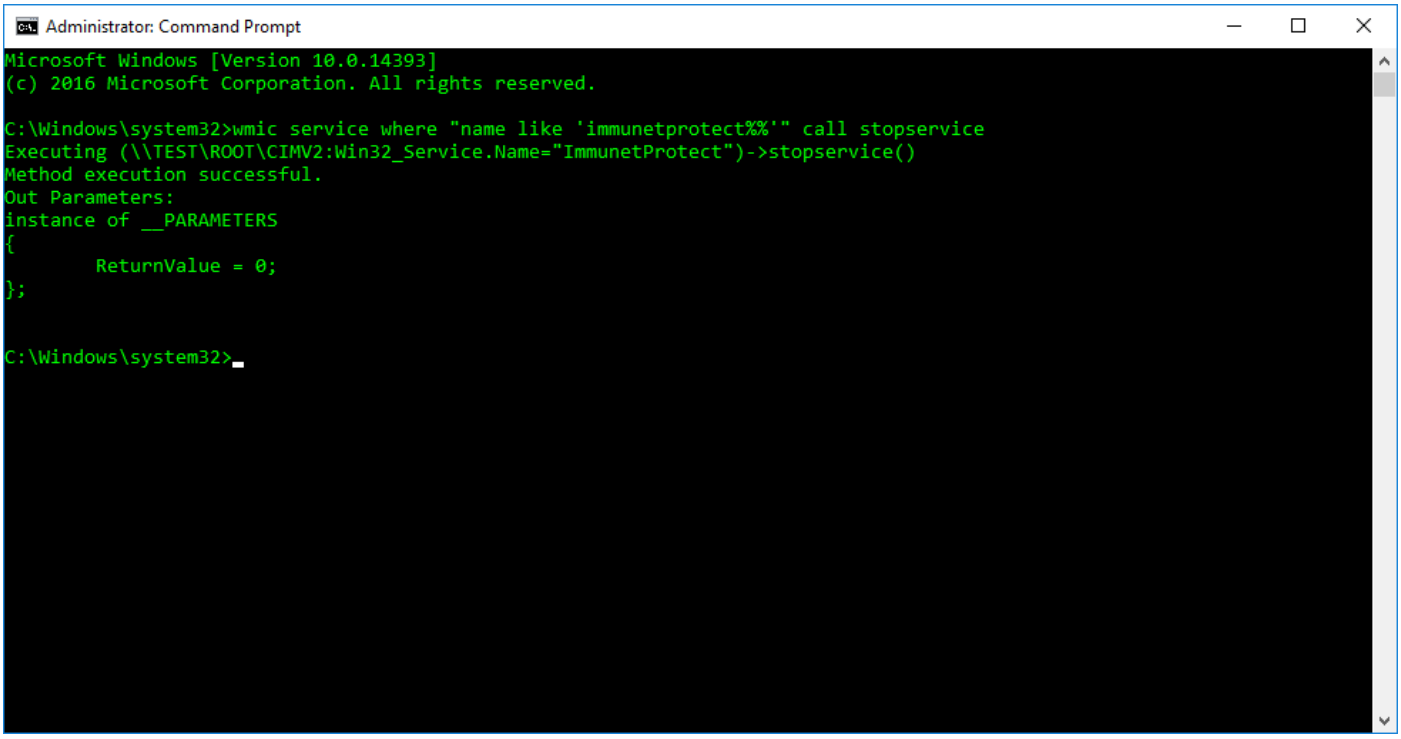
2. Instale o conector AMP em sua imagem mestra.

```
FireAMPSetup.exe /S
```



3. Pare o serviço AMP.

```
wmic service where "name like '%%i%%m%%.%%.%%'" call stopservice
```



Use o comando seguinte **se você tem a proteção do conector permitida.** A senha será visível no comando prompt.

```
4.2 and Lower: Not Available
4.3 to 5.0: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\sfc.exe" -k protectionpassword
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\sfc.exe" -k protectionpassword
```

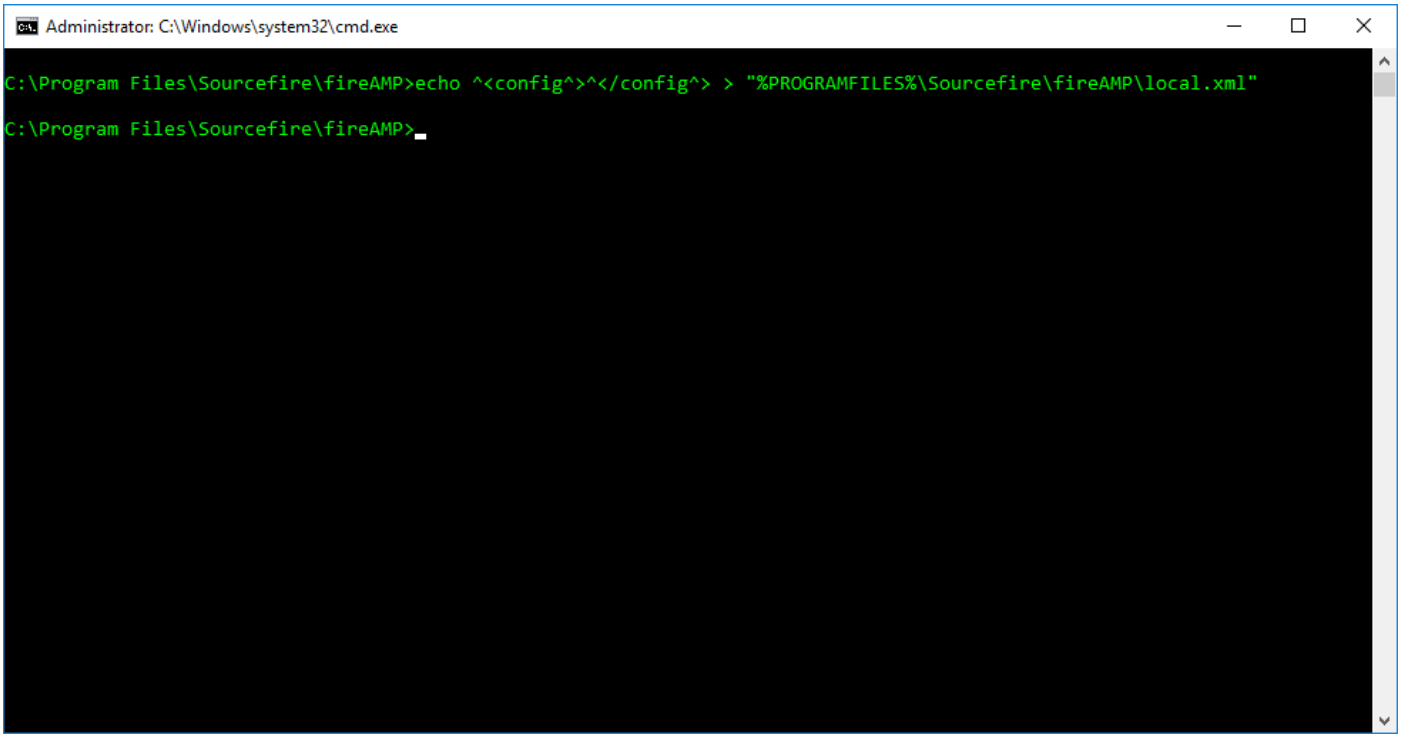
> **Nota:** É altamente a verificação **Policy.xml do advisedto (%PROGRAMFILES%** \ Cisco \ AMP \ Policy.xml) e verifica que há uma entrada para o <Install><Token>. Isto é necessário para que o conector seja registrado no grupo correto/política. O melhor prática seria guardar uma cópia desse arquivo caso que as próximas etapas estão tendo que ser repetidas por qualquer razão.
>
> **Note**: Se o serviço AMP é começado outra vez, a imagem mestra regenera **local.xml. Você** precisa de repetir estas etapas para neutralizar outra vez a imagem mestra. Seja certo incluir estas etapas em seu processo da preparação da imagem mestra.

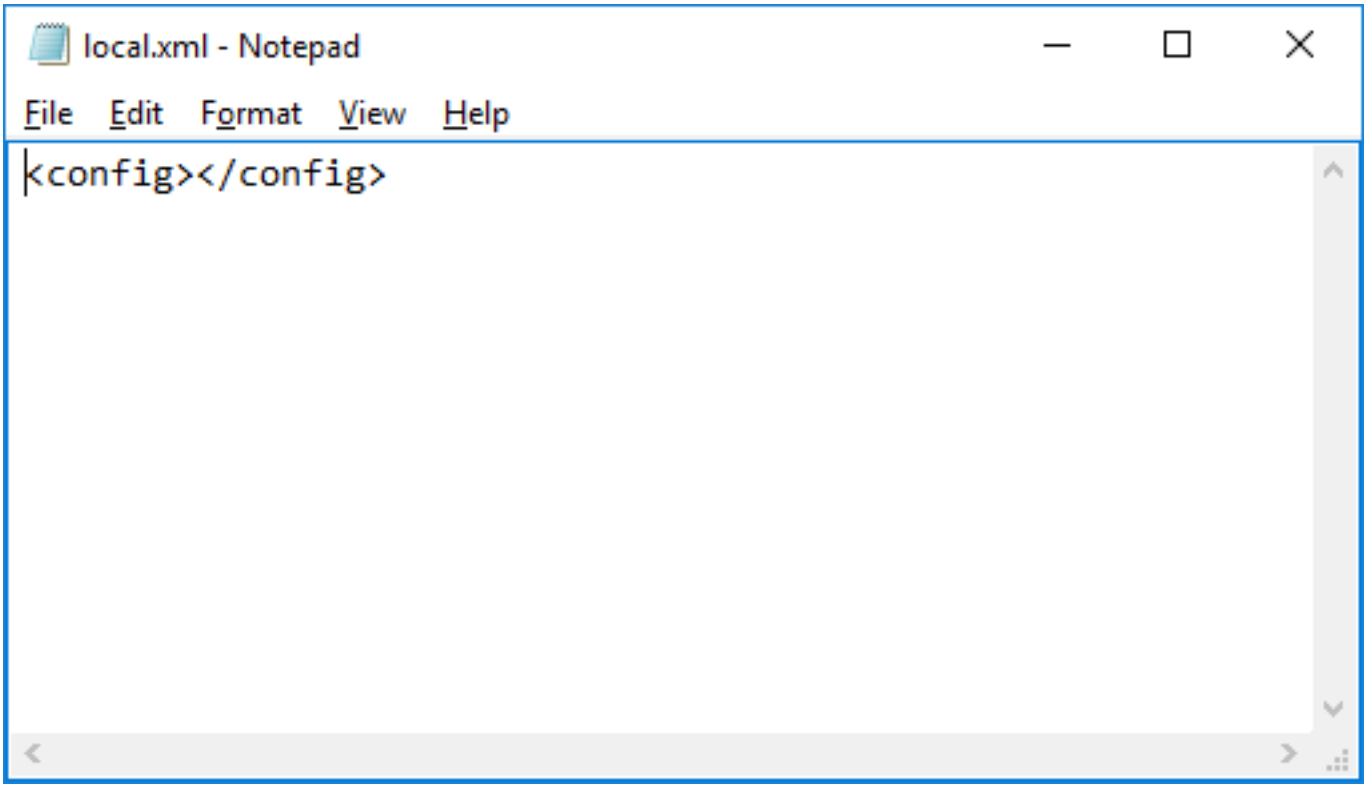
4. Suprima de **`local.xml`**.

```
5.0 and Lower: del "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
5.1 and Above: del "%PROGRAMFILES%\Cisco\AMP\local.xml"
```

5. Crie um **`arquivo`** vazio **`local.xml`**.

```
5.0 and Lower: echo ^<config^>^</config^> > "%PROGRAMFILES%\Sourcefire\fireAMP\local.xml"
5.1 and Above: echo ^<config^>^</config^> > "%PROGRAMFILES%\Cisco\AMP\local.xml"
```





6. Donotstart o serviço outra vez ou você será forçado para repetir etapas 3-5. O serviço deve começar na bota.

A Cargo-instalação - Versões 4.1.4 ou mais recente

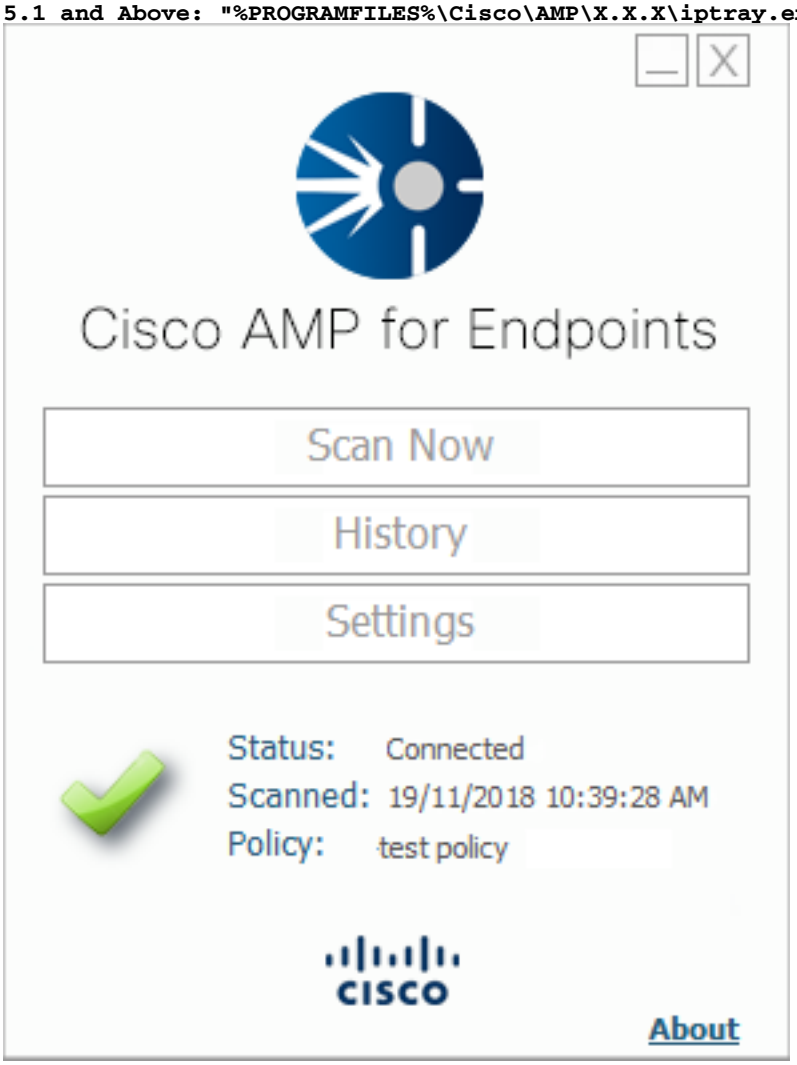
A versão 4.1.4 e mais recente do conector AMP gerencie automaticamente um regisration novo e um identificador exclusivo universal (UUID) quando o serviço do conector detecta um **`arquivo`** vazio **`local.xml`**.

Note: Espera-se que as máquinas que se registram com um **`arquivo`** vazio **`local.xml`** é

colocado no grupo padrão das suas organizações. Você deve decidir se você quer mover manualmente estas máquinas ou mudar seu grupo padrão para ser o grupo desejado para aquelas máquinas.

Neste momento o cliente AMP deve ser em serviço. Você pode usar a interface do utilizador para verificar a Conectividade e que o serviço está sendo executado. Se sua interface do utilizador não é ajustada para começar, pode manualmente ser começada com estes comando. Seja certo atualizar atualmente o número de versão para sua versão instalada.

```
5.0 and Lower: "%PROGRAMFILES%\Sourcefire\fireAMP\X.X.X\iptray.exe" -f
5.1 and Above: "%PROGRAMFILES%\Cisco\AMP\X.X.X\iptray.exe" -f
```



Linux

As etapas gerais para clonar uma máquina para Linux e têm uma identidade nova são similares a Windows. Estão aqui as etapas e os comandos:

1. Instale o AMP em sua imagem mestra

```
$ (sudo) yum install filename.rpm
```

2. Pare o serviço AMP

```
$ (sudo) initctl stop cisco-amp
```

3. Suprima de local.xml

```
$ (sudo) rm /opt/cisco/amp/etc/local.xml
```

Quando as botas diferentes de uma máquina acima com a imagem clonada, o serviço AMP começarão automaticamente acima e gerarão uma identidade nova. Deve ser original através de todos os conectores de comunicação em um grupo na nuvem (se público, ou privado).

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems
- Cisco AMP para valores-limite - TechNotes
- Cisco AMP para valores-limite - Guia do Usuário