Executar Switches de Linha de Comando de Ponto de Extremidade Seguro

Contents

Introduction

Este documento descreve os switches de Linha de Comando (CLI) disponíveis para uso com o Cisco Secure Endpoint e o ipsupporttool.exe.

Informações de Apoio

A interação com endpoints, tanto fisicamente quanto através da Interface Gráfica do Usuário (GUI), nem sempre está disponível para acessibilidade em ambientes específicos. O Cisco Secure Endpoint oferece várias abordagens para interação. Este documento pode fornecer os switches para a CLI.

> **Observação**: os switches CLI do instalador estão disponíveis aqui Switches de linha de comando para o Cisco Secure Endpoint Installer. A matriz de requisitos de reinicialização é apresentada aqui AMP for Endpoints Atualização do conector do Windows Requisitos de reinicialização.

Switches de linha de comando Cisco Secure Endpoint

Switches sfc.exe de ponto de extremidade seguro

1. Abra o prompt de comando no Windows.
2. Navegue até a pasta no prompt de comando. Caminho padrão: **C:\Program Files\Cisco\AMP\X.X.X**, o X.X.X denota o número da versão).
   <#root>

   ```
   cd C:\Program Files\Cisco\AMP\7.5.1\
   ```

3. Execute os switches disponíveis fornecidos.

> **Observação**: na execução de switches, não pode haver saída ecoada de volta.

Switches disponíveis para serem usados com o **sfc.exe**.

- **-s** : iniciar o serviço de Proteção Imunet (Conector do Windows). O serviço já deve ter sido registrado

com o SCM para ser iniciado.

<#root>

```
sfc.exe -s
```

- **-k** : serviço Parar Proteção Imunet (Conector do Windows). Se a Proteção do Conector estiver habilitada, você poderá interromper o serviço usando: **sfc.exe -k _password_**

<#root>

```
sfc.exe -k
```

```
sfc.exe -k examplepassword
```

- **-i** : Instalar o serviço Immunet Protect (Conector do Windows). Ele também define a ação padrão a ser tomada se o serviço falhar.

<#root>

```
sfc.exe -i
```

- **-u** : Desinstalar o serviço Immunet Protect (Conector do Windows). Cancele o registro do serviço com o Windows Service Control Manager (SCM). Esta opção é usada pelo desinstalador para desinstalar o serviço do conector do Windows.

<#root>

```
sfc.exe -u
```

- **-r** : Redefine o serviço de Proteção Imunet (Conector do Windows). Isso é muito semelhante à opção -i, mas não instala o serviço. Isso é útil para corrigir corrupção de local.xml.

<#root>

```
sfc.exe -r
```

- **-l começa** a ativar e **-l pára** a desativar. (O disparador é um L minúsculo) - Alterna o registro de depuração e do kernel dinamicamente. Esse estado pode continuar até que seja desativado, o serviço seja reiniciado ou uma nova política seja configurada para alterar o nível de log.

<#root>

```
sfc.exe -l start
```

```
sfc.exe -l stop
```

- **-unblock SHA_of_the_file** : Essa opção desbloqueia a execução de um processo. Depois que a opção de comando é executada, o aplicativo pode ser removido do cache de kernel local da lista de bloqueio de aplicativos.

A situação para usar esta opção de comando é quando um aplicativo é bloqueado por causa de falso positivo ou erro, e queremos desbloquear rapidamente o aplicativo sem esperar 30 minutos ou reinicializar a máquina.

<#root>

```
sfc.exe -unblock f5b6ab29506d5818a2f8d328029bb2fcb5437695702f3c9900138140f3cd980c
```

- **-reregister** (a partir do Connector v.6.2.1): essa opção pode limpar o uuid e os certificados do local.xml e do Registro enquanto o serviço está em execução e aciona um novo registro. Local.xml e o registro são atualizados com novos valores. No entanto, isso será bloqueado se a Sincronização de ID estiver habilitada e o conector obtiver o UUID existente novamente. Isso pode colocar o conector no grupo/política padrão após o novo registro se o pacote de instalação usado para a instalação inicial tiver sido modificado. Se a Proteção do Conector estiver habilitada, será necessário inserir o seguinte: **sfc.exe -reregister _password_**

<#root>

```
sfc.exe -reregister
```

```
sfc.exe -reregister examplepassword
```

- **-forceupdate** (a partir do Connector v.7.2.7): essa opção pode forçar o conector a atualizar as definições TETRA.

<#root>

```
sfc.exe -forceupdate
```

Switches Ipsupporttool.exe de Ponto de Extremidade Seguro

1. Abra o prompt de comando no Windows.
2. Navegue até a pasta no prompt de comando. Caminho padrão:**C:\Program Files\Cisco\AMP\X.X.X**, o X.X.X denota o número da versão).
   <#root>

```
cd C:\Program Files\Cisco\AMP\6.1.7\
```

3. Execute os switches disponíveis fornecidos.

Observação: na execução de switches, não pode haver saída ecoada de volta.

Switches disponíveis com **ipsupporttool.exe**:

Cuidado: qualquer switch que faça referência a uma opção de pasta requer que as pastas sejam criadas antes da especificação.

- **-d** : especifica a pasta da qual a Ferramenta de Suporte do Windows pode recuperar arquivos.
  - Se não for especificado, a Ferramenta de Suporte poderá recuperar arquivos do diretório do conector atual.

<#root>

```
ipsupporttool.exe -d C:\Program Files\Cisco\AMP\6.1.7\TestFolder\
```

- **-o**: Especifica a pasta de saída para a Ferramenta de Suporte. O padrão é a área de trabalho se esta opção não for especificada.

<#root>

```
ipsupporttool.exe -o C:\Program Files\Cisco\AMP\6.1.7\TestFolder\
```

- **-t**: executa um diagnóstico de nível de depuração com tempo na Ferramenta de Suporte do Windows para o tempo especificado. A duração é especificada em minutos.

<#root>

```
ipsupporttool.exe -t 5
```

Comutadores IPTray.exe de ponto de extremidade seguro

- **-f** : Permite que a interface de usuário do cliente se torne ativa a partir da linha de comando. Isso só será necessário se um endpoint tiver a GUI desativada por meio da política com a opção Iniciar interface de usuário do cliente desmarcada.

<#root>

```
iptray.exe -f
```

Informações Relacionadas

- **Suporte Técnico e Documentação - Cisco Systems**
- **Endpoint seguro da Cisco - Notas técnicas**
- **Endpoint Cisco Secure - Guia do usuário**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.