

Procedimento para desinstalar o conector AMP se a senha foi esquecida

Contents

[Introduction](#)

[O conector está conectado](#)

[O conector está desconectado](#)

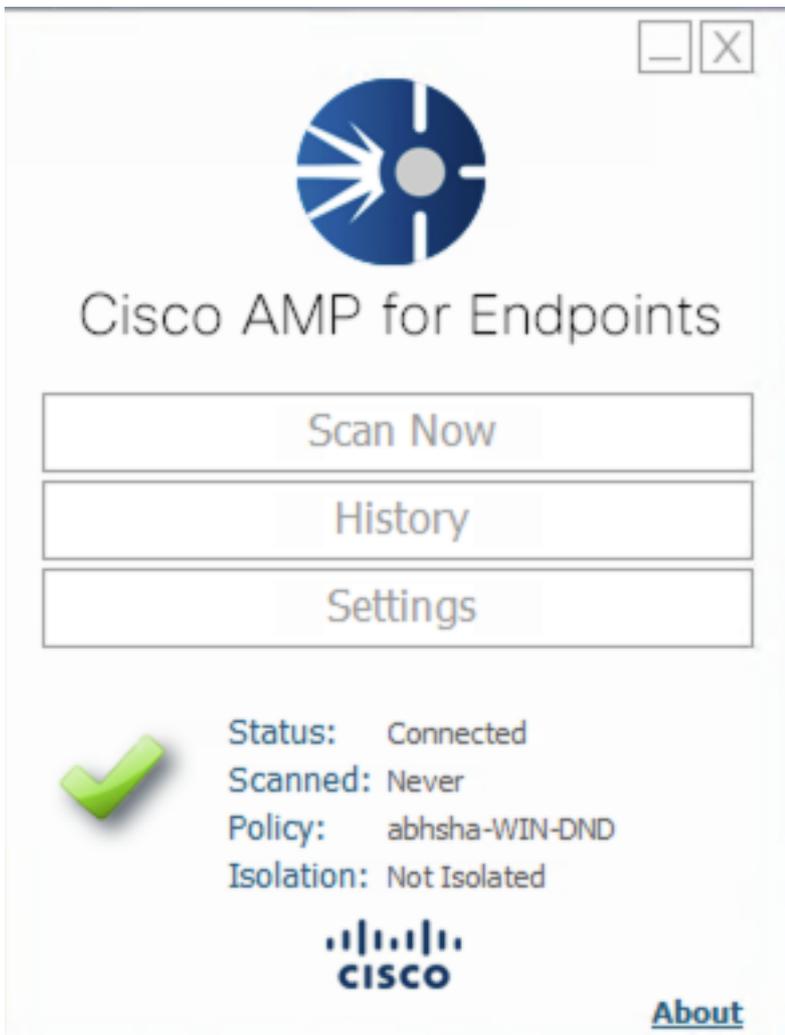
Introduction

Este documento descreve o procedimento para desinstalar o conector Advanced Malware Protection (AMP) da Cisco caso a desinstalação seja bloqueada pelo recurso de proteção do conector que exige que uma senha seja fornecida e essa senha seja esquecida. Há dois cenários nesse caso e depende se o conector mostra "Conectado" à nuvem AMP. Aplica-se apenas ao SO Windows, uma vez que a Proteção de Conector é um recurso disponível somente no SO Windows.

O conector está conectado

Etapa 1. Clique no ícone da bandeja e abra o conector Cisco AMP para endpoints.

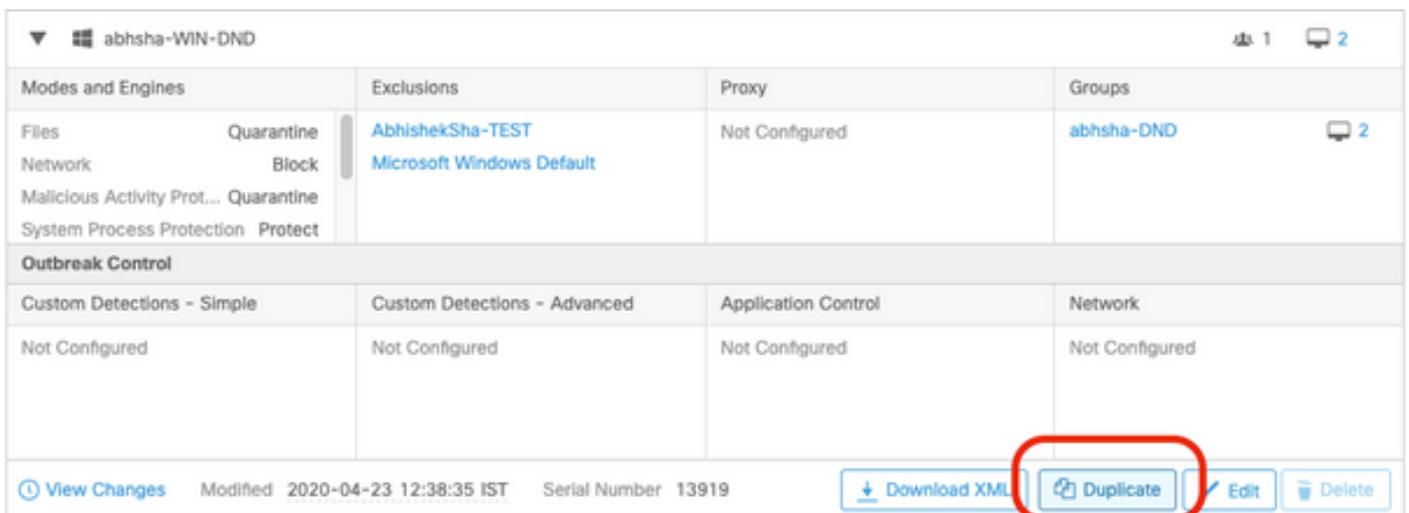
Etapa 2. Verifique se o conector está exibido como conectado.



Etapa 3. Observe que a política foi atribuída a esse conector.

Etapa 4. Navegue até o console do AMP for Endpoints e procure a política anotada anteriormente.

Etapa 5. Expanda a diretiva e clique em **Duplicar** conforme mostrado na imagem.



Etapa 6. Uma nova política chamada "Cópia de..." serão criados. Clique em **Editar** para editar esta política conforme mostrado na imagem.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Mallicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2019-05-21 12:12:01 IST Serial Number 12267
 [Download XML](#) [Duplicate](#) [Edit](#) [Delete](#)

Passo 7. Na página **Editar política**, navegue para **Configurações avançadas > Recursos administrativos**.

Etapa 8. No campo **Proteção por senha do conector**, substitua a senha por uma nova senha que pode ser recuperada conforme mostrado na imagem.

Modes and Engines

Exclusions
2 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

- Administrative Features
- Client User Interface
- File and Process Scan
- Cache
- Endpoint Isolation

Send User Name in Events i

Send Filename and Path Info i

Heartbeat Interval: i

Connector Log Level: i

Tray Log Level: i

Enable Connector Protection i

Connector Protection Password: i

Automated Crash Dump Uploads i

Command Line Capture i

Command Line Logging i

Etapa 9. Clique no botão **Salvar** para salvar esta diretiva.

Etapa 10. Navegue até **Gerenciamento > Grupos** e crie um novo grupo.

Groups [View All Changes](#)

Etapa 11. Insira um nome de grupo e selecione a **Diretiva do Windows** como a diretiva editada anteriormente. Clique no botão **Salvar** como mostrado na imagem.

< New Group

Name	<input type="text" value="TZ-TEST-GROUP"/>
Description	<input type="text"/>
Parent Group	<input type="text"/>
Windows Policy	<input type="text" value="Copy of abhsha-WIN-DND - #1"/>
Android Policy	<input type="text" value="Default Policy (Vanilla Android)"/>
Mac Policy	<input type="text" value="Default Policy (Vanilla OSX)"/>
Linux Policy	<input type="text" value="Default Policy (Vanilla Linux)"/>
Network Policy	<input type="text" value="Default Policy (network_policy)"/>
iOS Policy	<input type="text" value="Default Policy (Audit)"/>

Etapa 12. Navegue até **Gerenciamento > Computadores** e procure o computador no qual você tenta desinstalar o conector AMP.

Etapa 13. Expanda o computador e clique em **Mover para grupo**. Na caixa de diálogo exibida, selecione o Grupo criado anteriormente.

DESKTOP-RESMRDG in group abhsha-DND		Definitions Outdated	
Hostname	DESKTOP-RESMRDG	Group	abhsha-DND
Operating System	Windows 10 Pro	Policy	abhsha-WIN-DND
Connector Version	7.2.7.11687	Internal IP	10.197.225.213
Install Date	2020-04-23 12:35:56 IST	External IP	72.163.220.18
Connector GUID	48838c52-f04f-454a-8c3a-5e55f7366775	Last Seen	2020-04-23 12:49:01 IST
Definition Version	TETRA 64 bit (None)	Definitions Last Updated	None
Update Server	tetra-defs.amp.cisco.com		
Processor ID	0fabfbff000006f2		

[Events](#) [Device Trajectory](#) [Diagnostics](#) [View Changes](#)

Etapa 14. Aguarde a diretiva ser atualizada no endpoint. Geralmente leva de 30 minutos a 1 hora e depende do intervalo configurado.

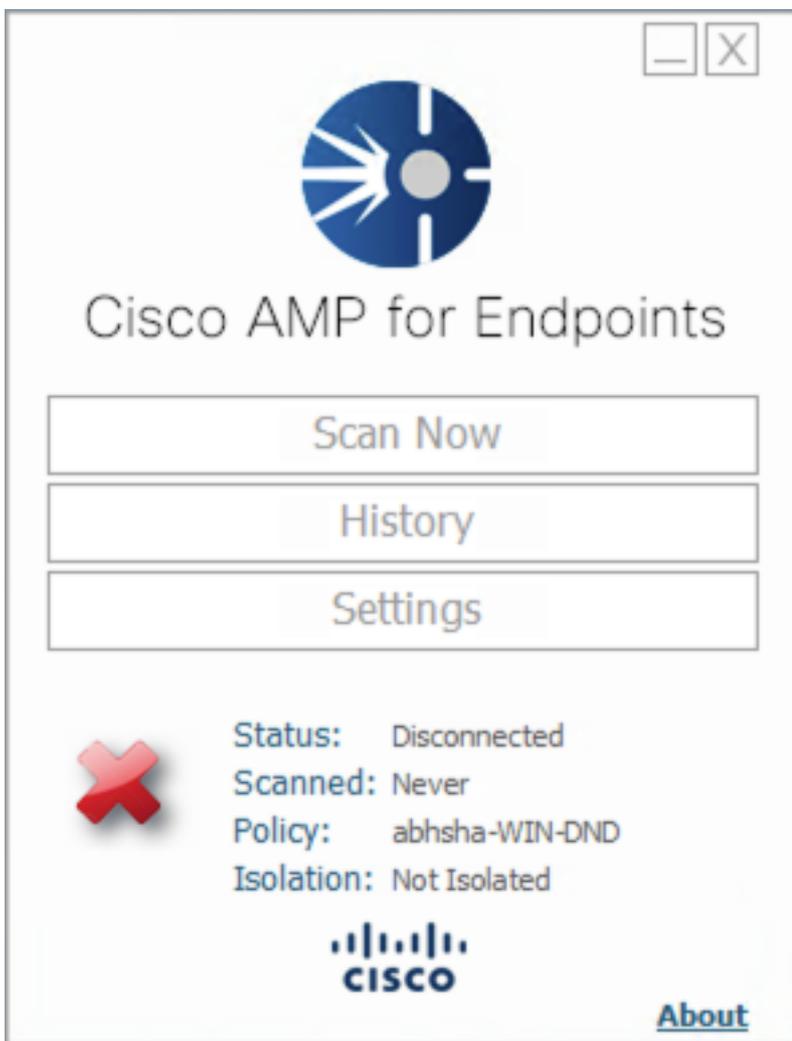
Etapa 15. Depois que a diretiva tiver sido atualizada no endpoint, você poderá desinstalar o conector com o uso da senha que configurou recentemente.

O conector está desconectado

Se o conector estiver desconectado da nuvem AMP, é importante poder inicializar o computador no modo de segurança.

Etapa 1. Clique no ícone da bandeja e abra o conector Cisco AMP para endpoints.

Etapa 2. Verifique se o conector está exibido como desconectado.



Etapa 3. Observe a política atribuída a esse conector.

Etapa 4. Navegue até o console do AMP for Endpoints e procure a política anotada anteriormente.

Etapa 5. Expanda a diretiva e clique em **Duplicar** conforme mostrado na imagem.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	abhsha-DND 2
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced		Network
Not Configured		Not Configured		Not Configured

[View Changes](#) Modified 2020-04-23 12:38:35 IST Serial Number 13919
 [Download XML](#)

[Duplicate](#)
[Edit](#)
[Delete](#)

Etapa 6. Uma nova política chamada "Cópia de..." serão criados. Clique em **Editar** para editar esta diretiva.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced		Network
Not Configured		Not Configured		Not Configured

[View Changes](#) Modified 2019-05-21 12:12:01 IST Serial Number 12267
 [Download XML](#)
[Duplicate](#)
[Edit](#)
[Delete](#)

Passo 7. Na página Editar política, navegue para **Configurações avançadas > Recursos administrativos**.

Etapa 8. No campo **Proteção por senha do conector**, substitua a senha por uma nova senha que pode ser recuperada.

Etapa 9. Clique no botão **Salvar** para salvar esta diretiva.

Etapa 10. Navegue até **Gerenciamento > Políticas** e procure a política que foi duplicada recentemente.

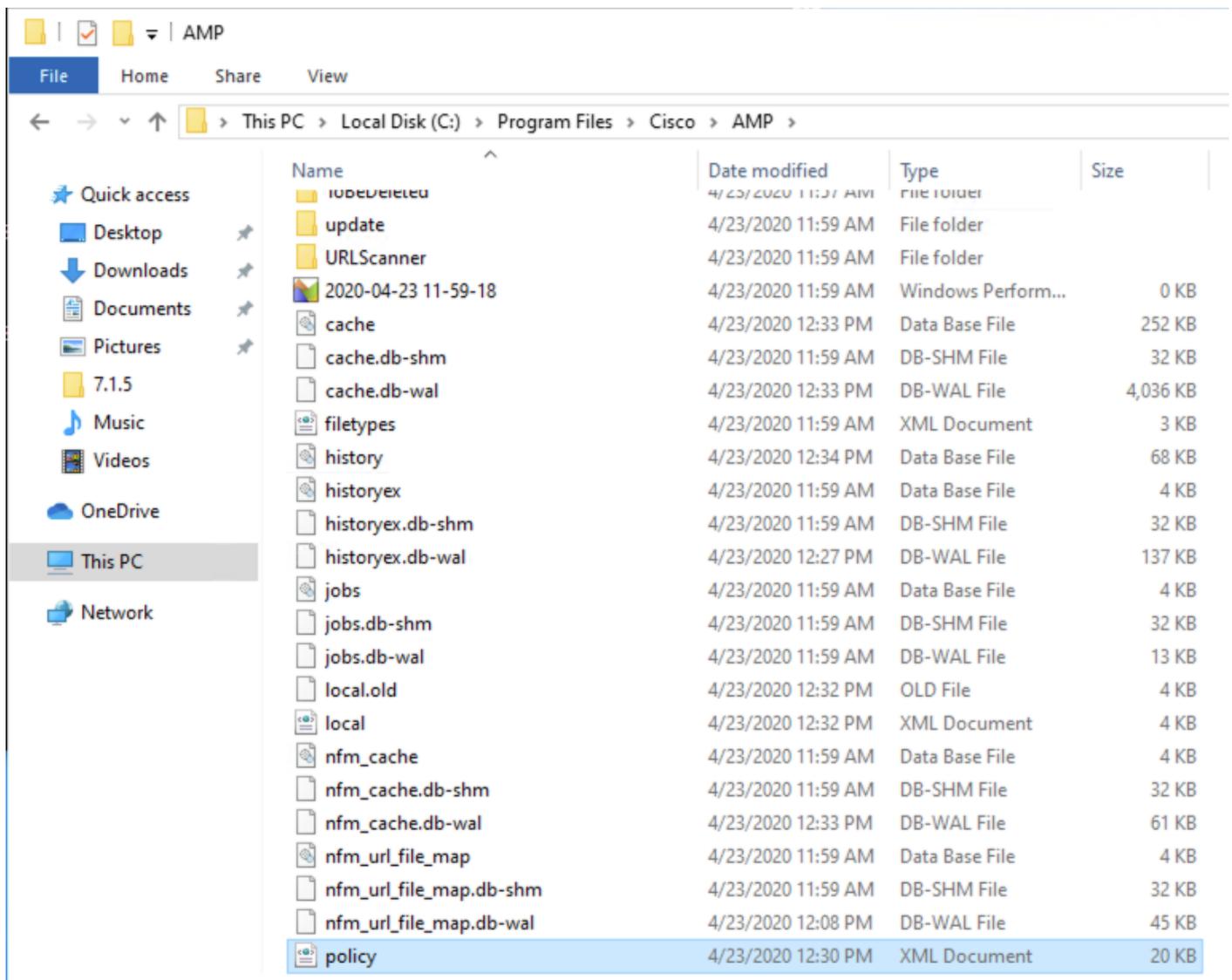
Etapa 11. Expanda a diretiva e clique em **Download XML**. Um arquivo chamado **policy.xml** será salvo na sua máquina.

Etapa 12. Copie este **policy.xml** para o ponto final afetado.

Etapa 13. Reinicie o endpoint afetado no **modo de segurança**.

Etapa 14. Quando o endpoint afetado estiver no **modo de segurança**, navegue até **C:\Program Files\Cisco\AMP**.

Etapa 15. Nesta pasta, procure um arquivo chamado **policy.xml** e renomeie-o para **policy_old.xml**.



Etapa 16. Agora, cole o **policy.xml** copiado anteriormente nesta pasta.

Etapa 17. Depois que o arquivo tiver sido copiado, a desinstalação poderá ser executada normalmente e, no prompt de senha, a senha recém-configurada deverá ser inserida.

Etapa 18. Esta é uma etapa opcional. Como o conector foi desinstalado quando a máquina foi desconectada, a entrada do computador permanecerá no console. Portanto, você pode navegar para **Gerenciamento > Computadores** e expandir o endpoint afetado. Clique em **Excluir** para excluir o ponto final.