Procedimento para desinstalar o conector AMP se a senha foi esquecida

Contents

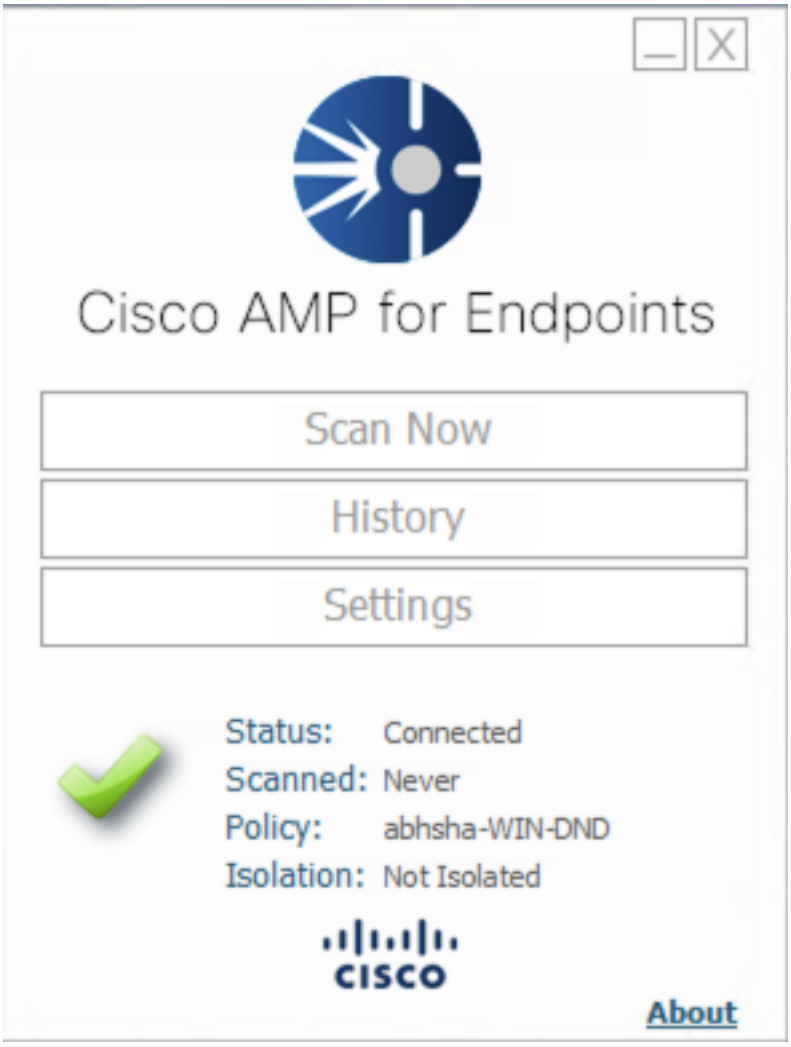
Introduction

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.

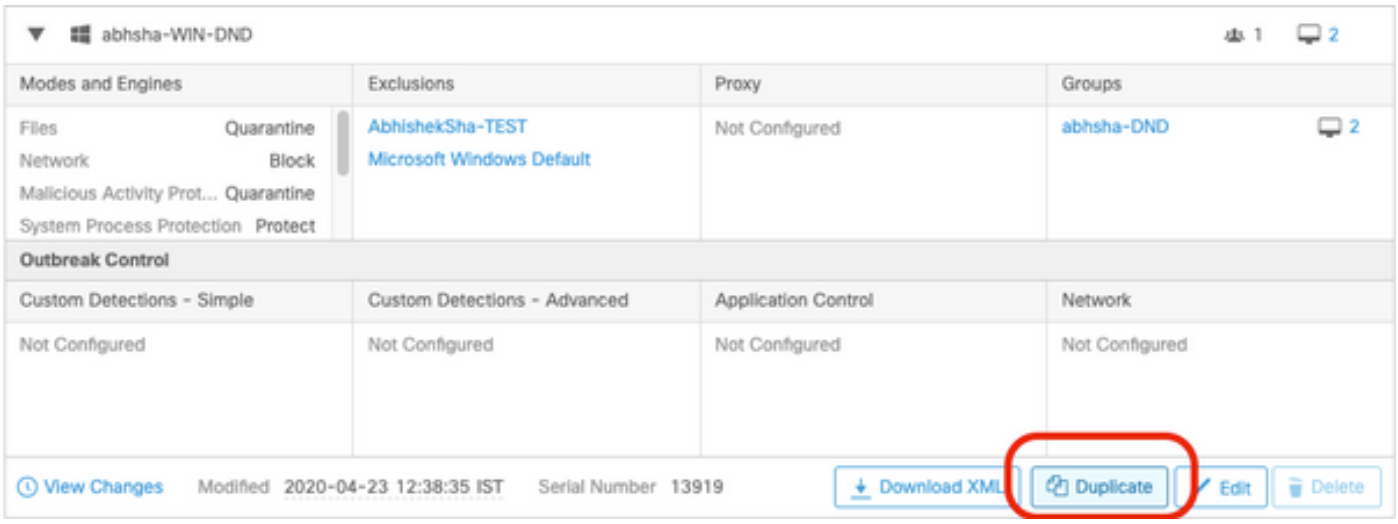
Etapa 2. Verifique se o conector está exibido como conectado.



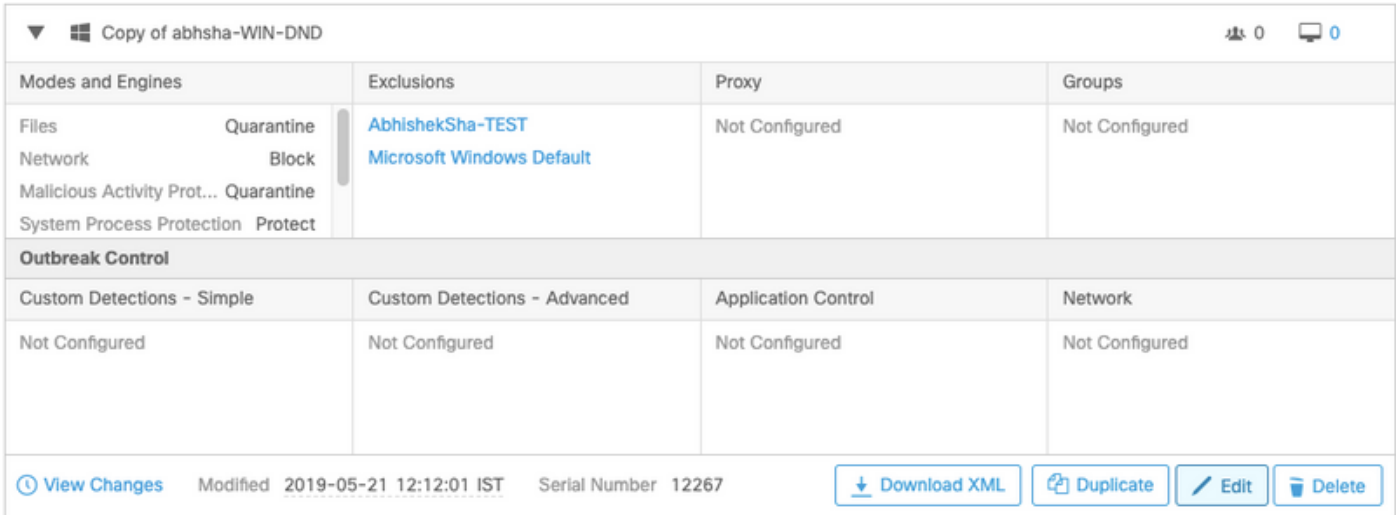
Etapa 3. Observe que a política foi atribuída a esse conector.

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.

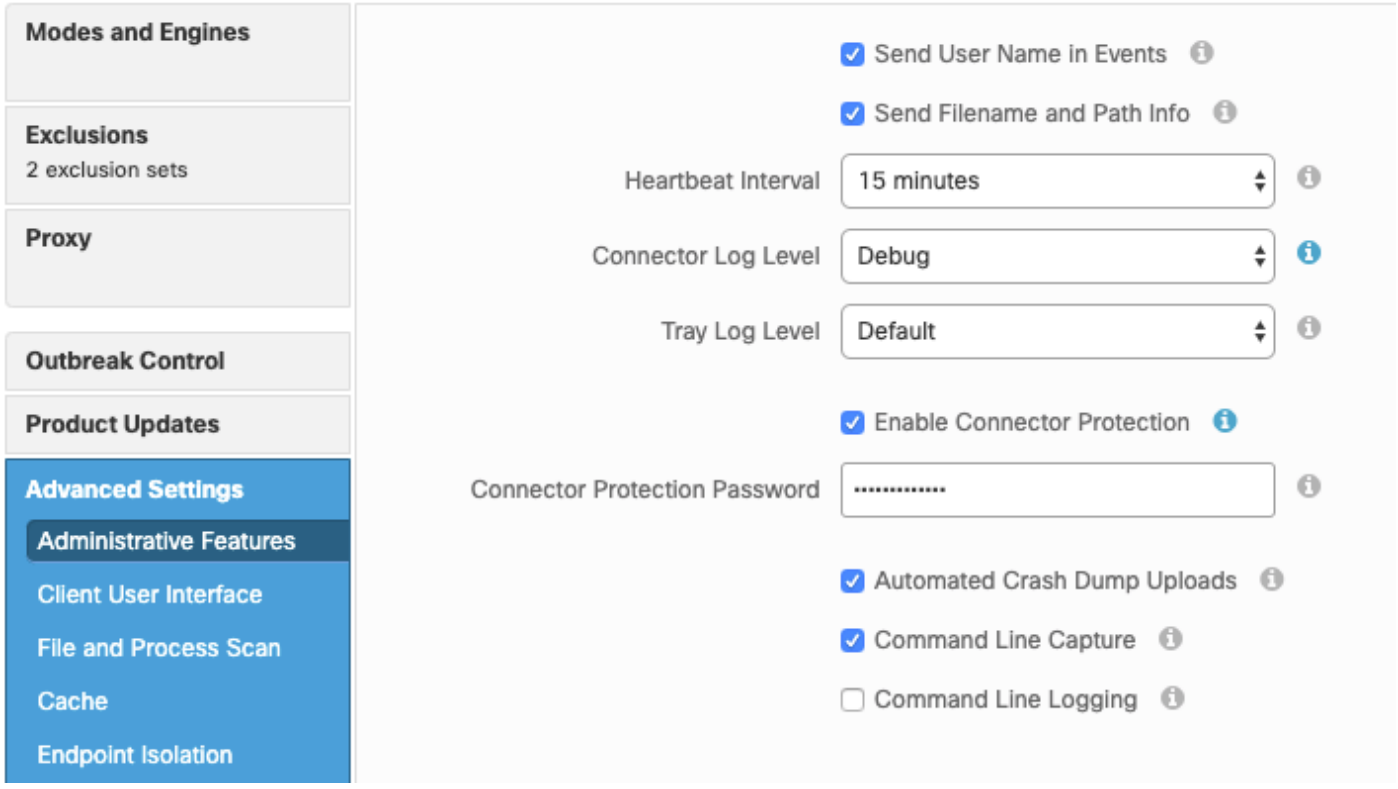


Etapa 6. Uma nova política chamada "Cópia de..." serão criados. Clique em **Editar** para editar esta política conforme mostrado na imagem.



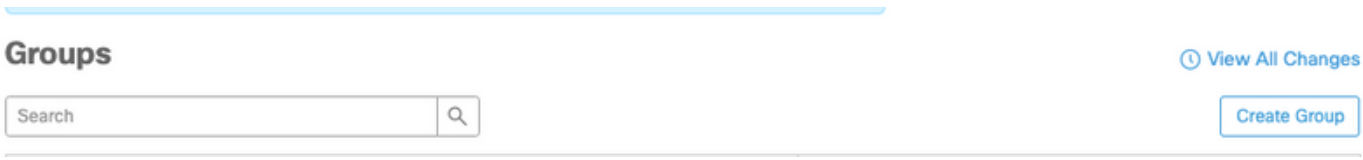
Passo 7. Na página **Editar política**, navegue para **Configurações avançadas > Recursos administrativos.**

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

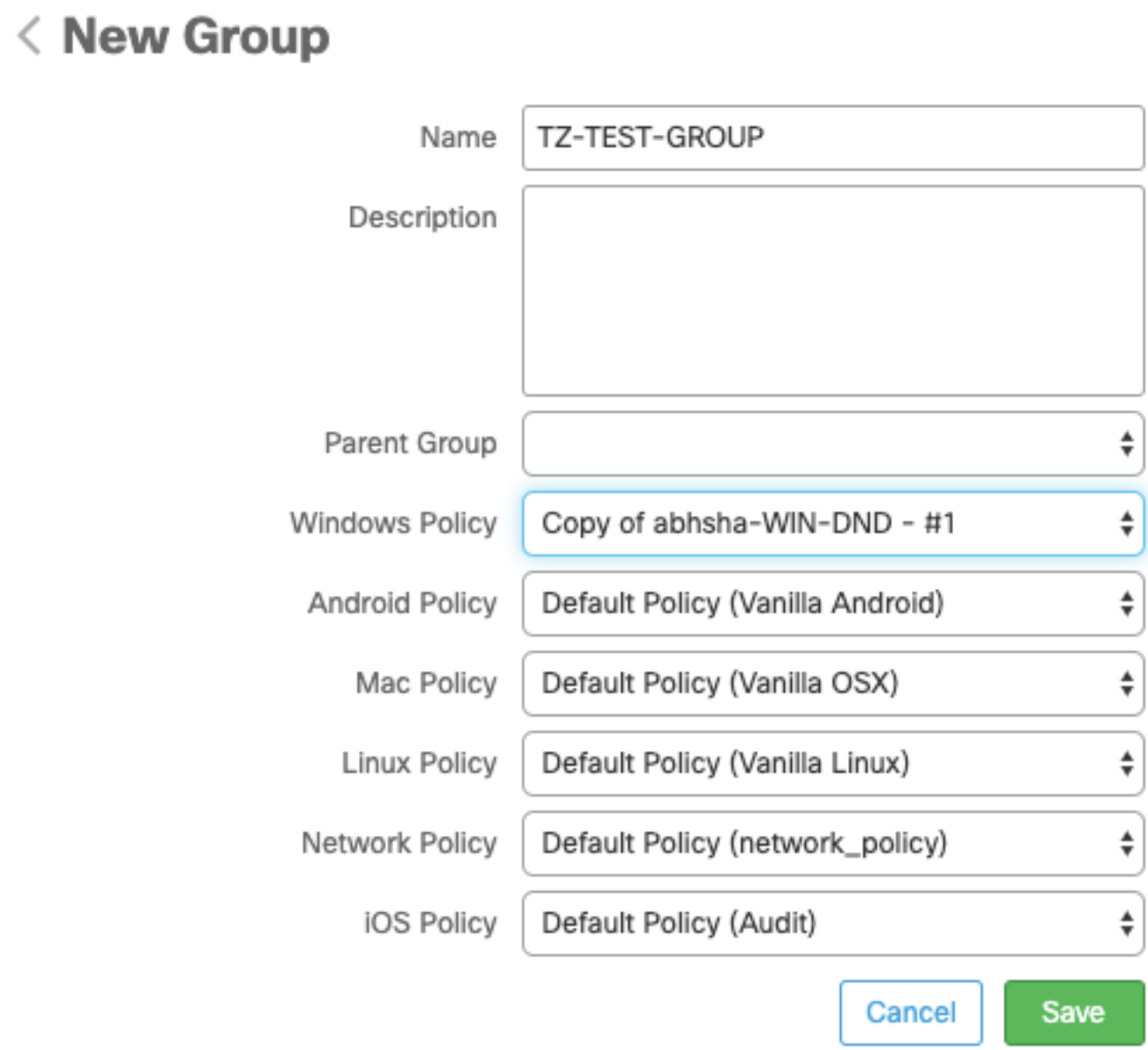


Etapa 9. Clique no botão **Salvar** para salvar esta diretiva.

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

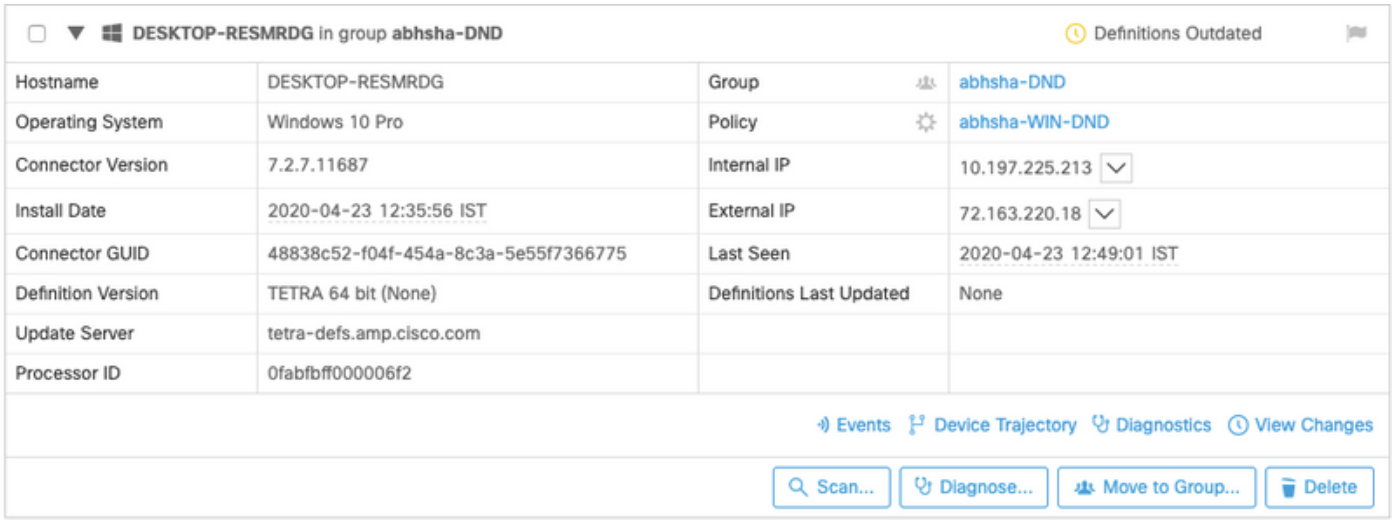


Etapa 11. Insira um nome de grupo e selecione a **Diretiva do Windows** como a diretiva editada anteriormente. Clique no botão **Salvar** como mostrado na imagem.



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.



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

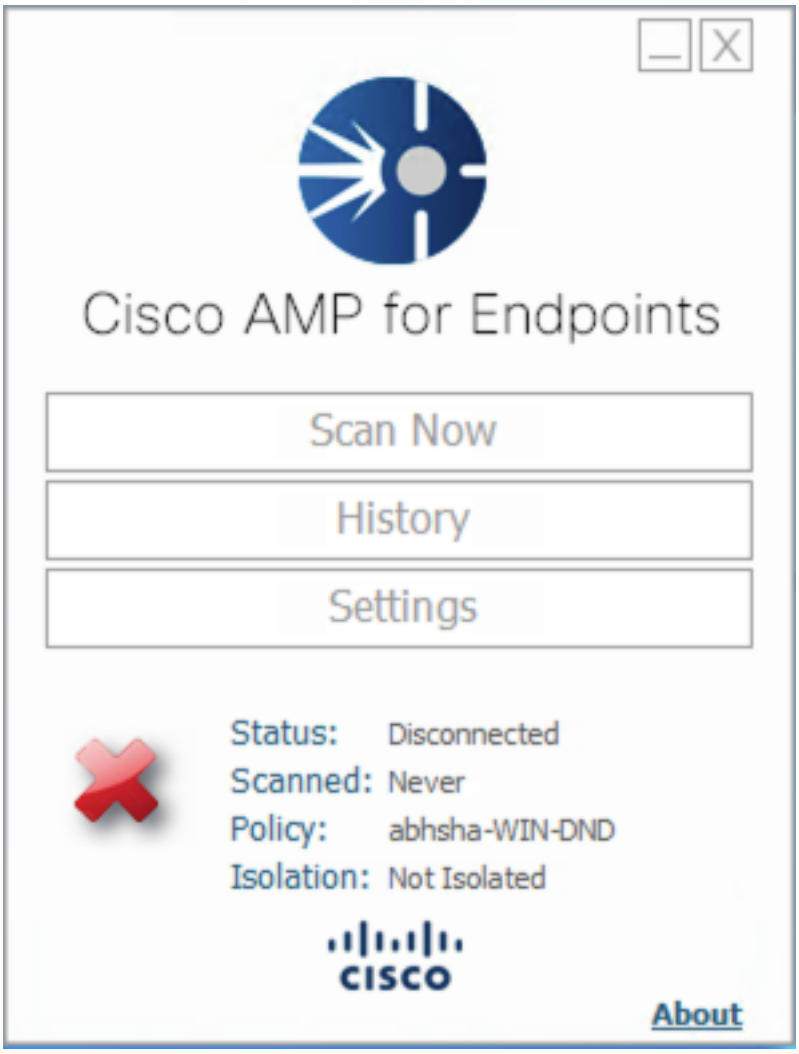
Etapa 15. Depois que a diretiva tiver sido atualizada no endpoint, você poderá desinstalar o conector com o uso da senha que configurou recentemente.

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.

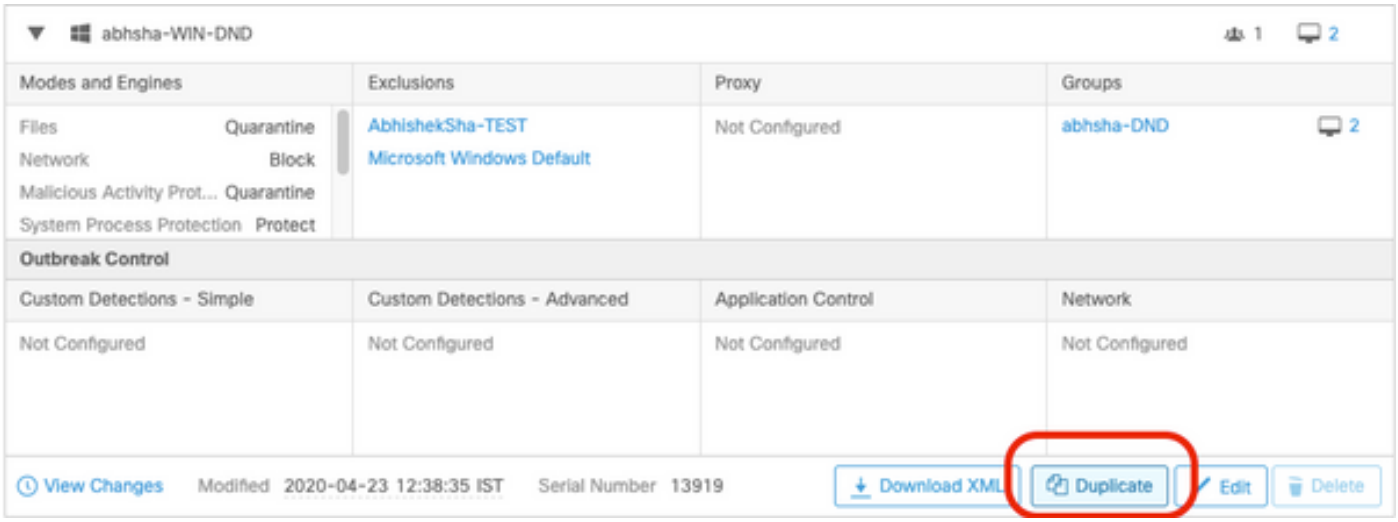
Etapa 2. Verifique se o conector está exibido como desconectado.



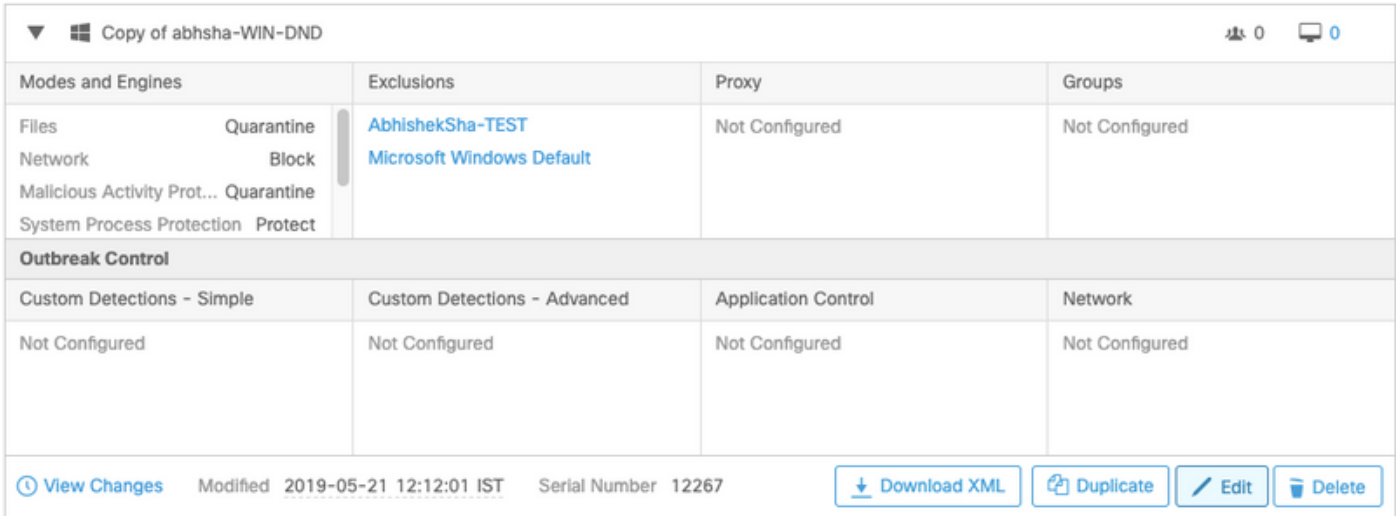
Etapa 3. Observe a política atribuída a esse conector.

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.

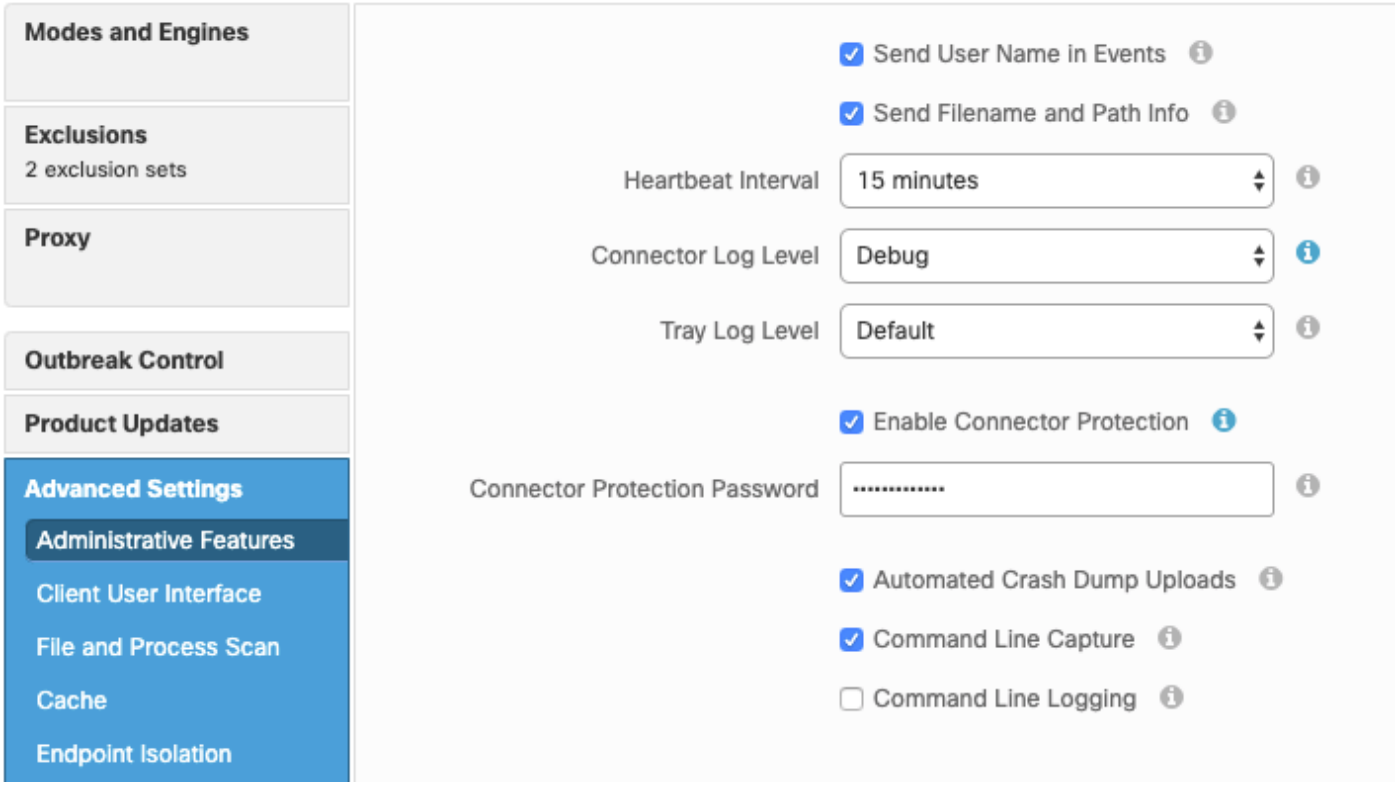


Etapa 6. Uma nova política chamada "Cópia de..." serão criados. Clique em **Editar** para editar esta diretiva.



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

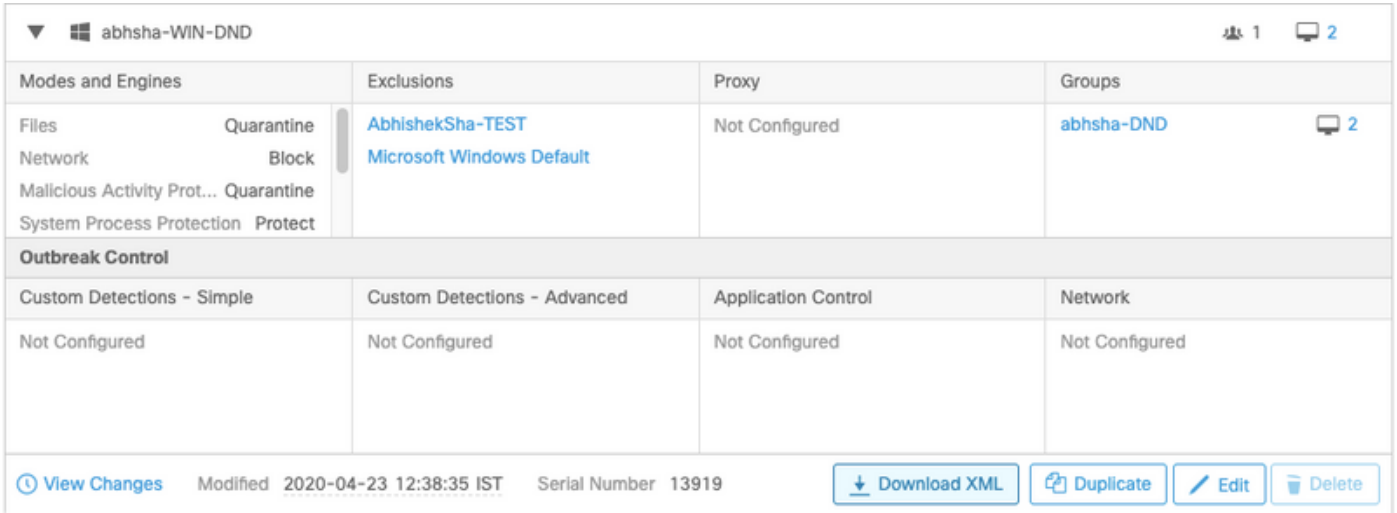
Etapa 8. No campo **Proteção por senha do conector**, substitua a senha por uma nova senha que pode ser recuperada.



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.

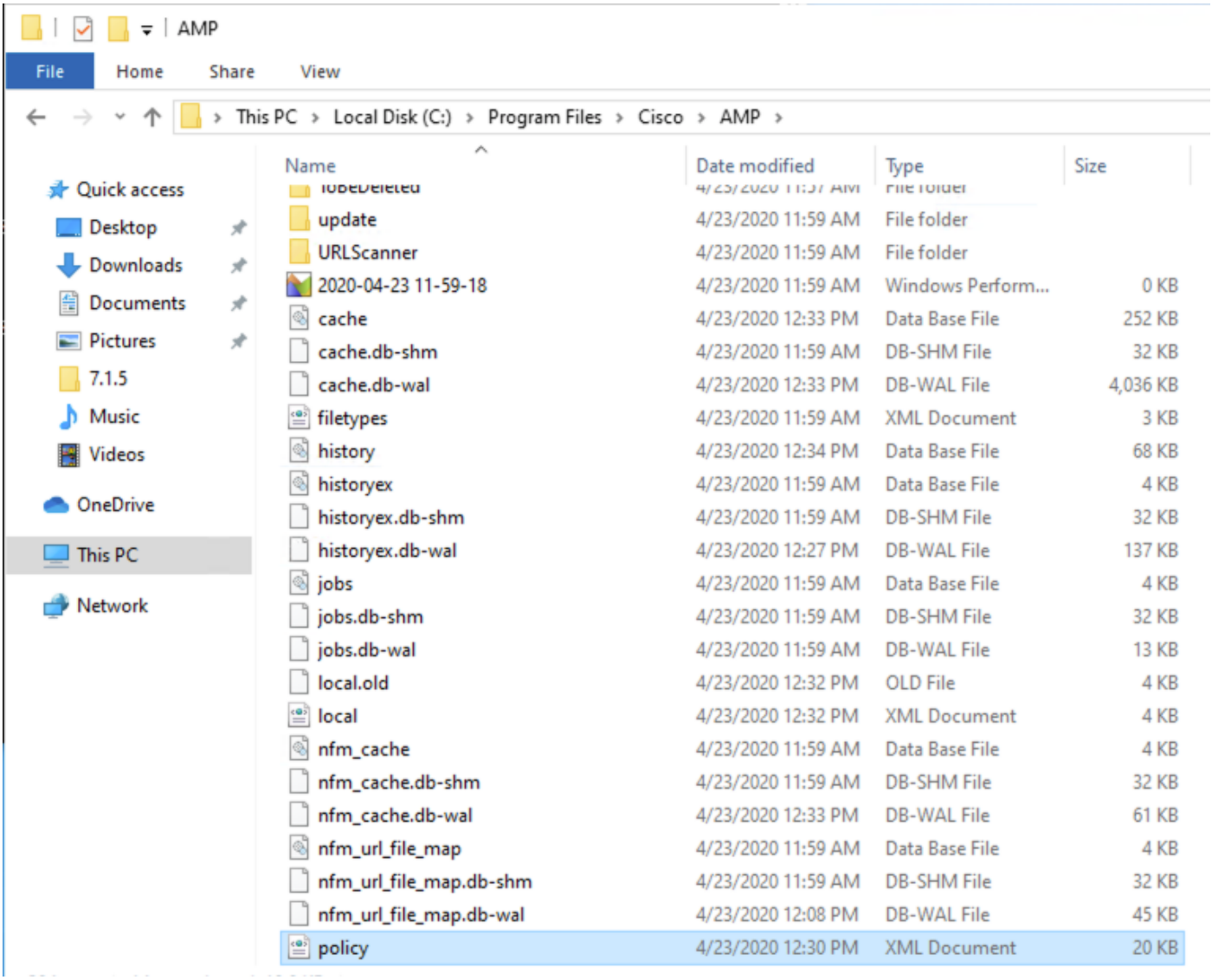


Etapa 12. Copie este **policy.xml** para o ponto final afetado.

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.