Procedimiento para desinstalar el conector de AMP si se ha olvidado la contraseña

Contenido

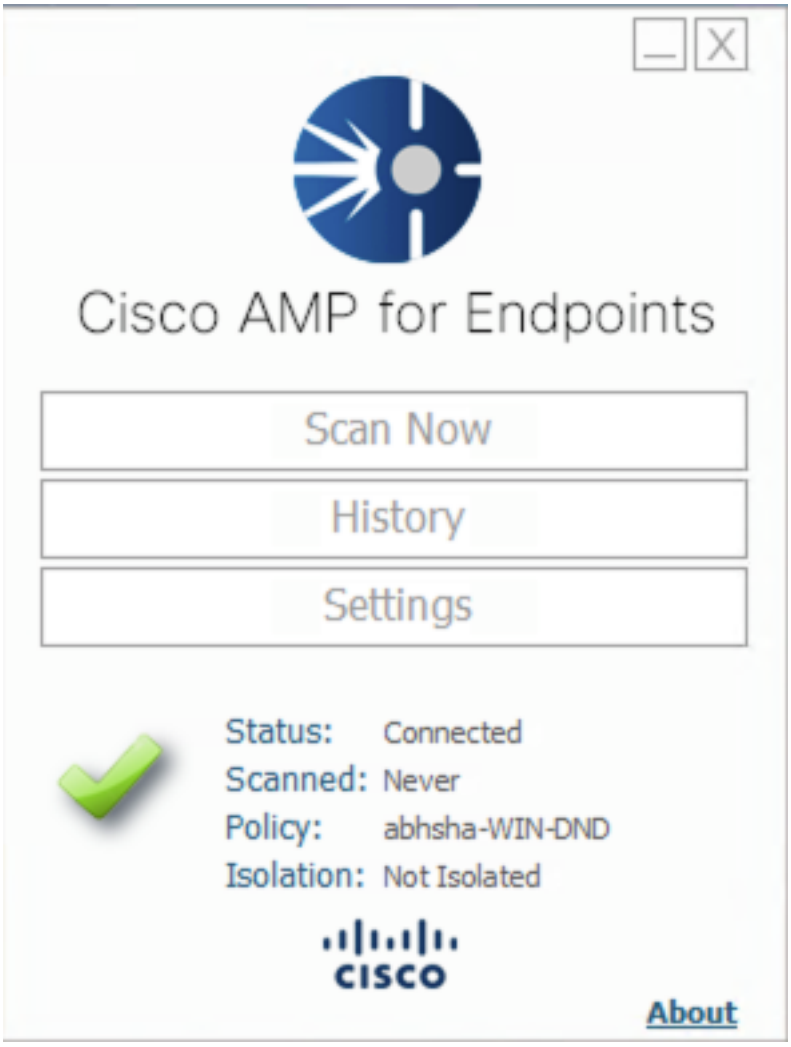
Introducción

Este documento describe el procedimiento para desinstalar el conector Protección frente a malware avanzado de Cisco (AMP) en caso de que la desinstalación se bloquee por la función de protección del conector que requiere que se proporcione una contraseña y dicha contraseña se olvide. En este caso, hay dos escenarios y depende de si el conector muestra "Conectado" a la nube de AMP. Se aplica sólo al sistema operativo Windows, ya que la protección de los conectores es una función que sólo está disponible en el sistema operativo Windows.

El conector está conectado

Paso 1. Haga clic en el icono de la bandeja y abra el conector de Cisco AMP para terminales.

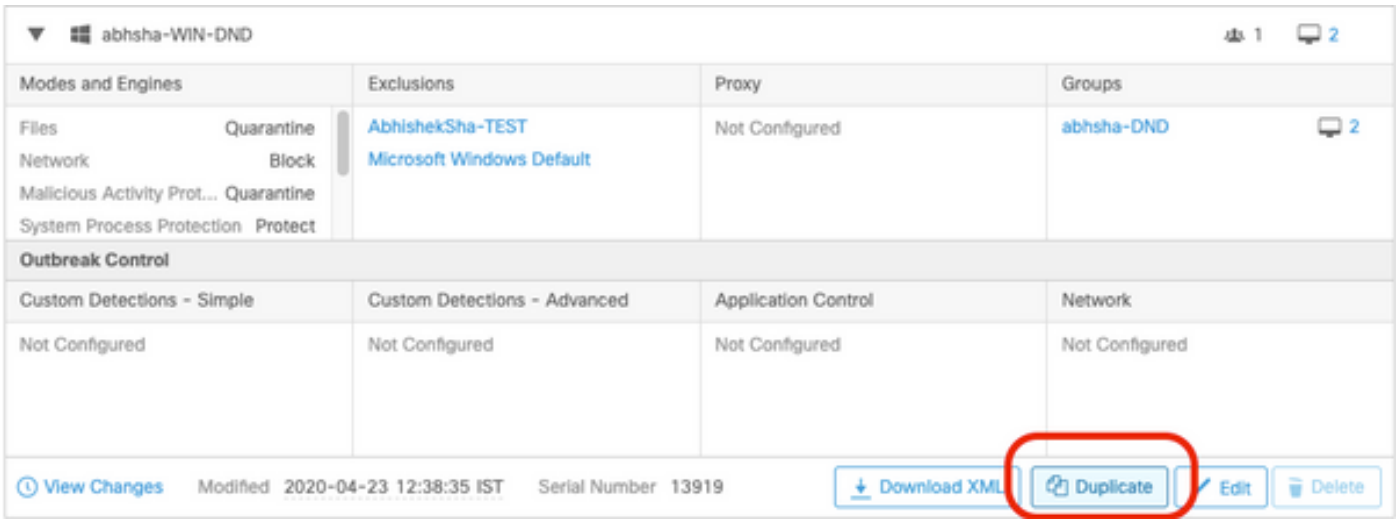
Paso 2. Asegúrese de que el conector se muestra como conectado.



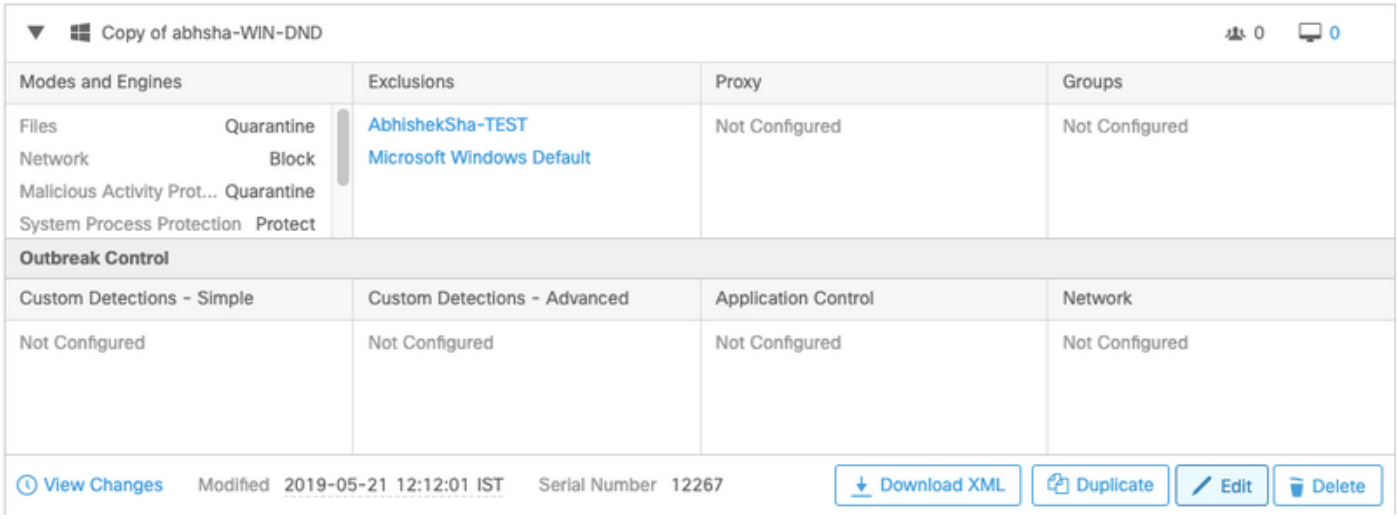
Paso 3. Tenga en cuenta que la política se ha asignado a ese conector.

Paso 4. Navegue hasta la consola de AMP para terminales y busque la política que se ha señalado anteriormente.

Paso 5. Expanda la política y haga clic en **Duplicar** como se muestra en la imagen.

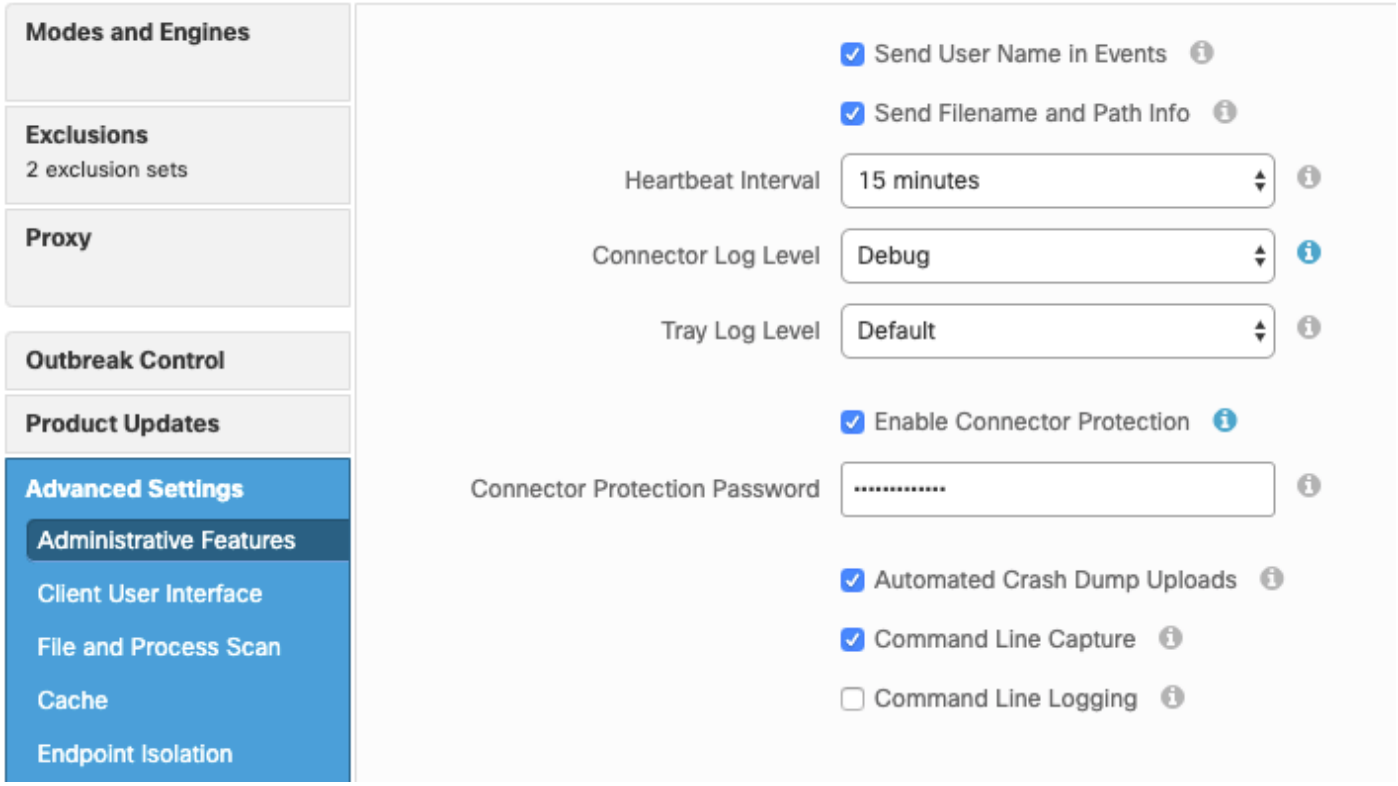


Paso 6. Una nueva política llamada "Copia de..." se creará. Haga clic en **Editar** para editar esta política como se muestra en la imagen.



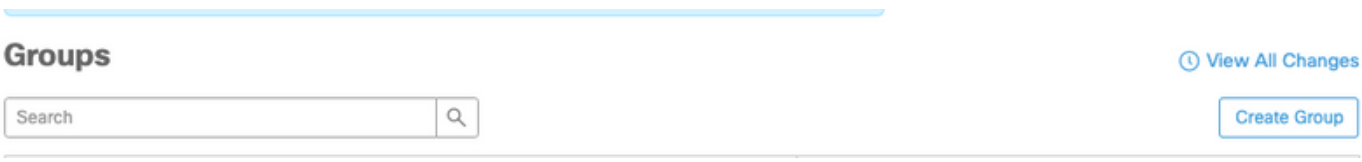
Paso 7. En la página **Editar política**, vaya a **Configuración avanzada > Funciones administrativas.**

Paso 8. En el campo **Connector Password Protection**, reemplace la contraseña por una nueva contraseña que se pueda recuperar como se muestra en la imagen.

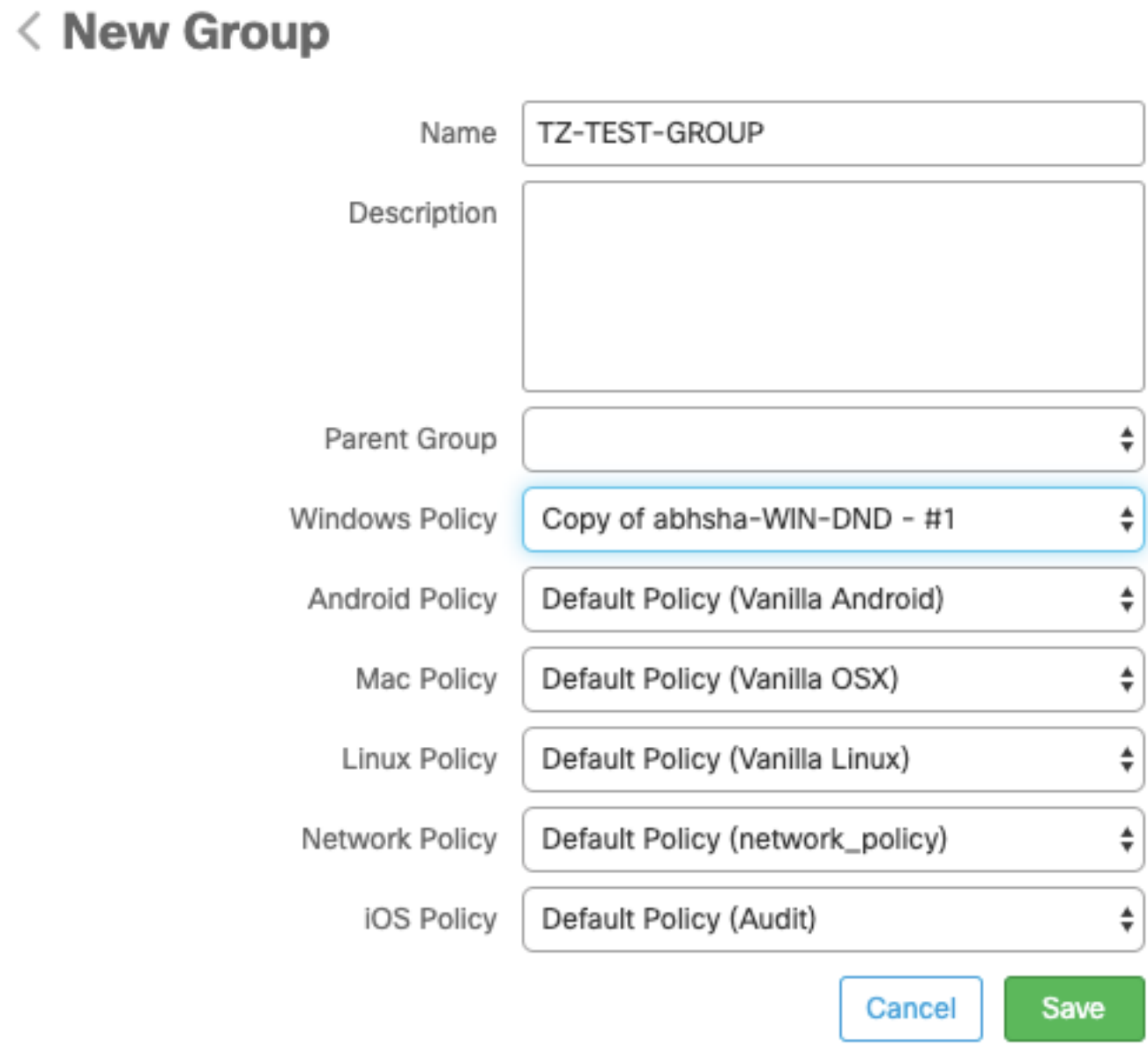


Paso 9. Haga clic en el botón **Guardar** para guardar esta política.

Paso 10. Navegue hasta **Administración > Grupos** y cree un nuevo grupo.

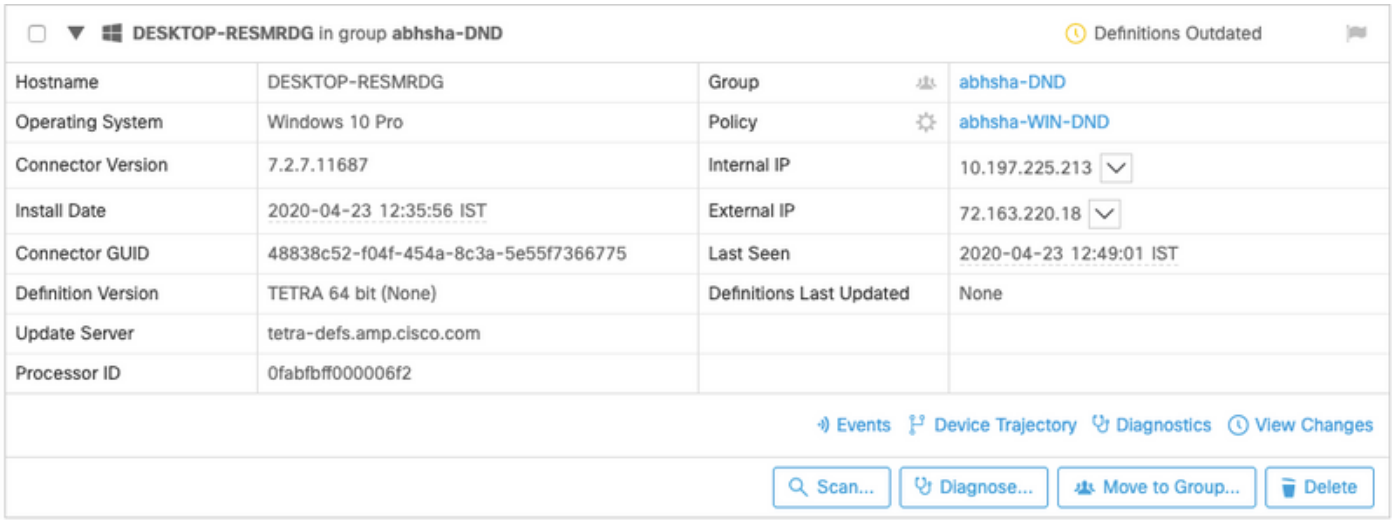


Paso 11. Introduzca un nombre de grupo y seleccione la **directiva de Windows** como directiva editada anteriormente. Haga clic en el botón **Guardar** como se muestra en la imagen.



Paso 12. Vaya a **Management > Computers** y busque el equipo en el que intenta desinstalar el conector de AMP.

Paso 13. Expanda el equipo y haga clic en **Mover al grupo**. En el cuadro de diálogo que aparece, seleccione el grupo creado anteriormente.



Paso 14. Espere a que se actualice la política en el terminal. Normalmente, tarda de 30 minutos a 1 hora y depende del intervalo configurado.

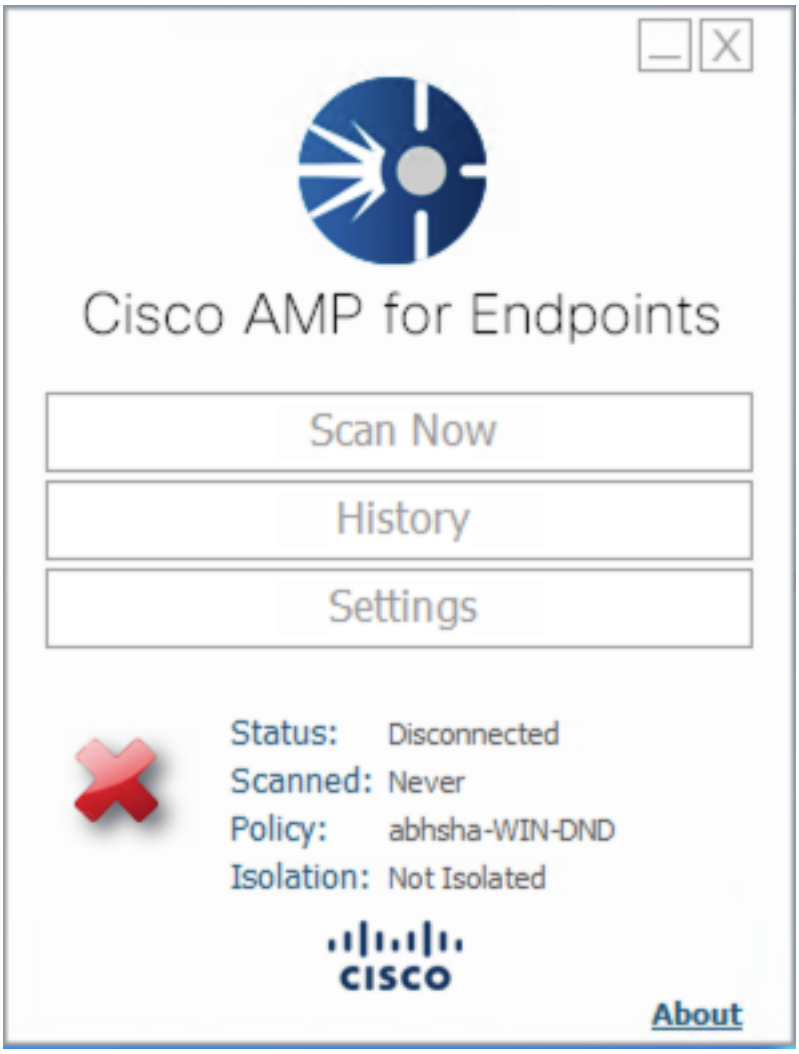
Paso 15. Una vez que la política se haya actualizado en el terminal, podrá desinstalar el conector con el uso de la contraseña que ha configurado recientemente.

El conector está desconectado

Si el conector se desconecta de la nube de AMP, es importante poder iniciar el ordenador en el modo seguro.

Paso 1. Haga clic en el icono de la bandeja y abra el conector de Cisco AMP para terminales.

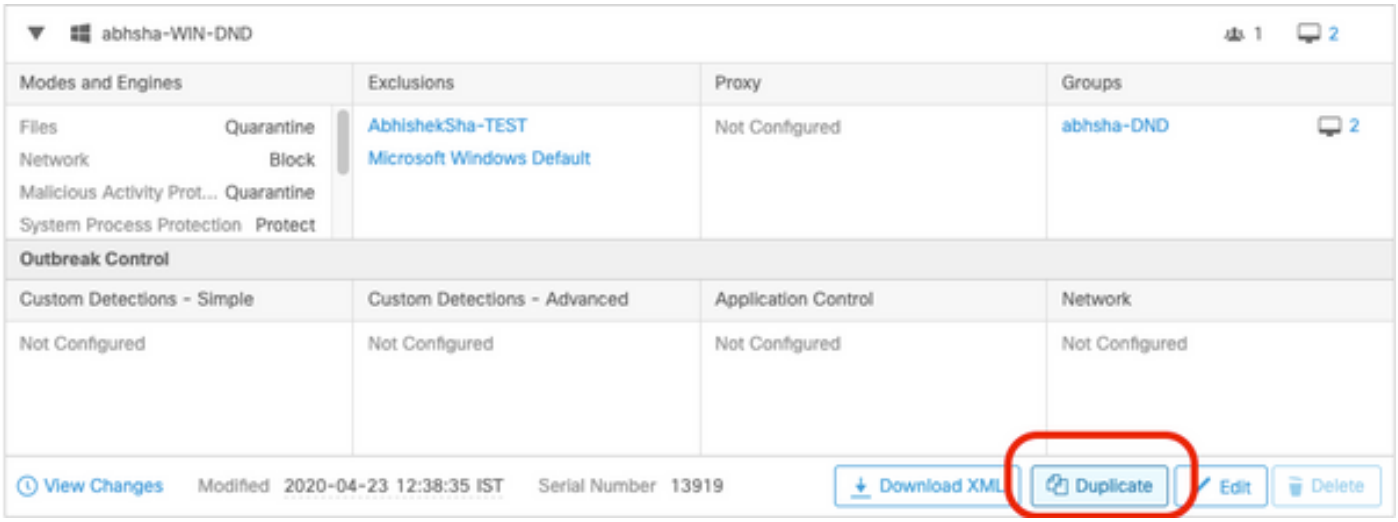
Paso 2. Asegúrese de que el conector se muestra como desconectado.



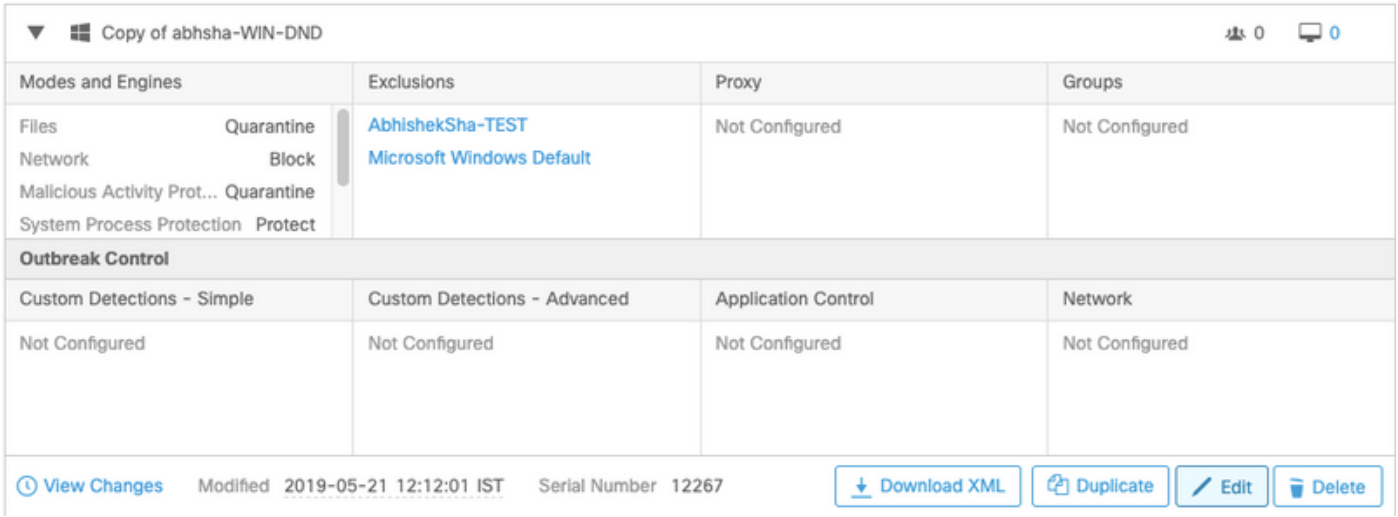
Paso 3. Observe la política que se ha asignado a ese conector.

Paso 4. Navegue hasta la consola de AMP para terminales y busque la política que se ha señalado anteriormente.

Paso 5. Expanda la política y haga clic en **Duplicar** como se muestra en la imagen.

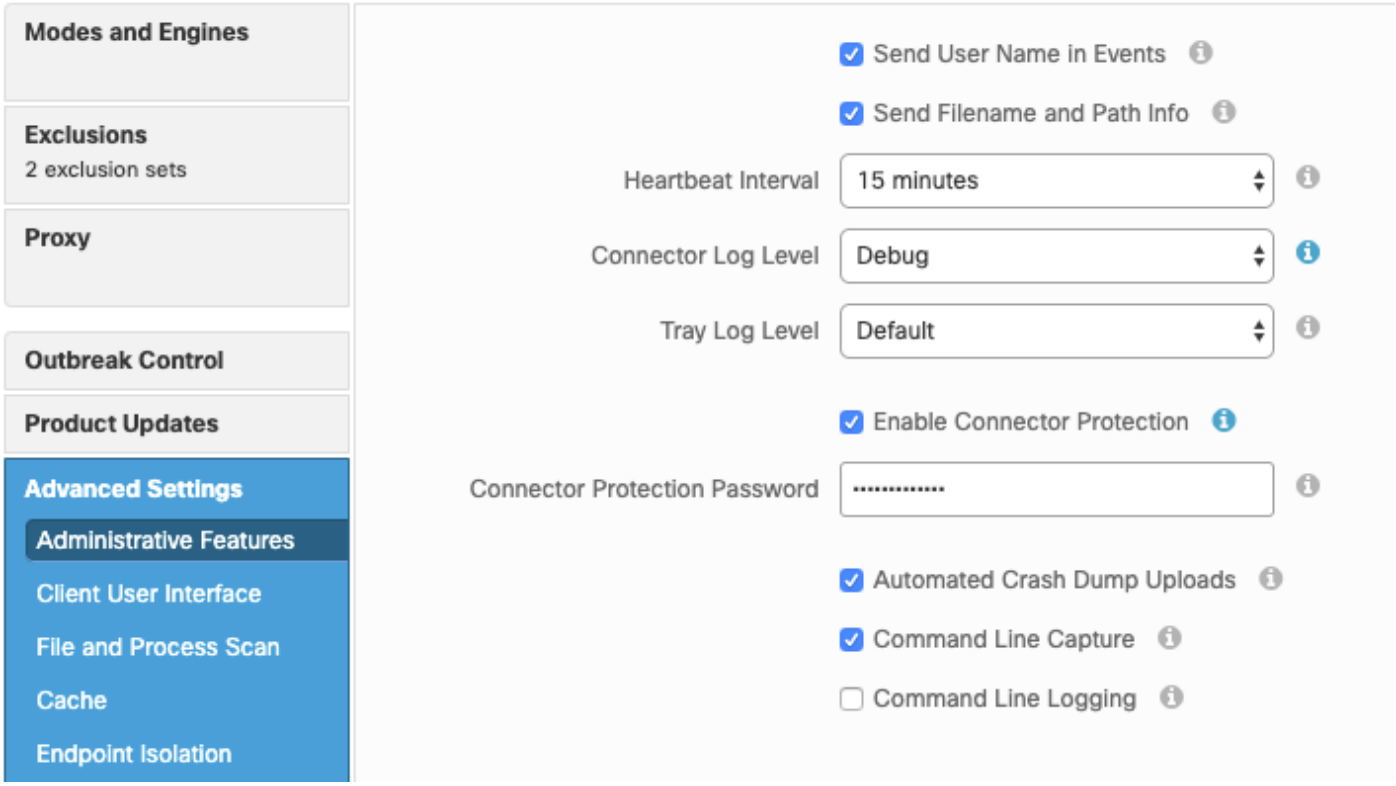


Paso 6. Una nueva política llamada "Copia de..." se creará. Haga clic en **Editar** para editar esta política.



Paso 7. En la página Editar directiva, navegue hasta **Configuración avanzada > Funciones administrativas**.

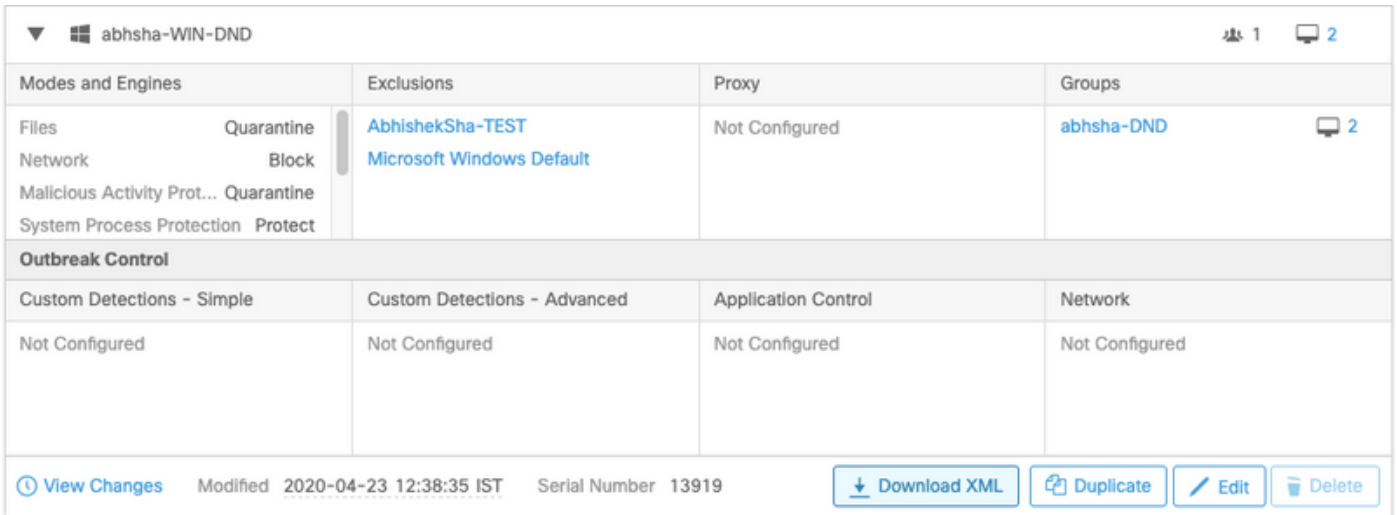
Paso 8. En el campo **Connector Password Protection**, reemplace la contraseña por una nueva que se pueda recuperar.



Paso 9. Haga clic en el botón **Guardar** para guardar esta política.

Paso 10. Navegue hasta **Administración > Políticas** y busque la política que se duplicó recientemente.

Paso 11. Expanda la política y haga clic en **Descargar XML.** Un archivo denominado **policy.xml** se guardará en su equipo.

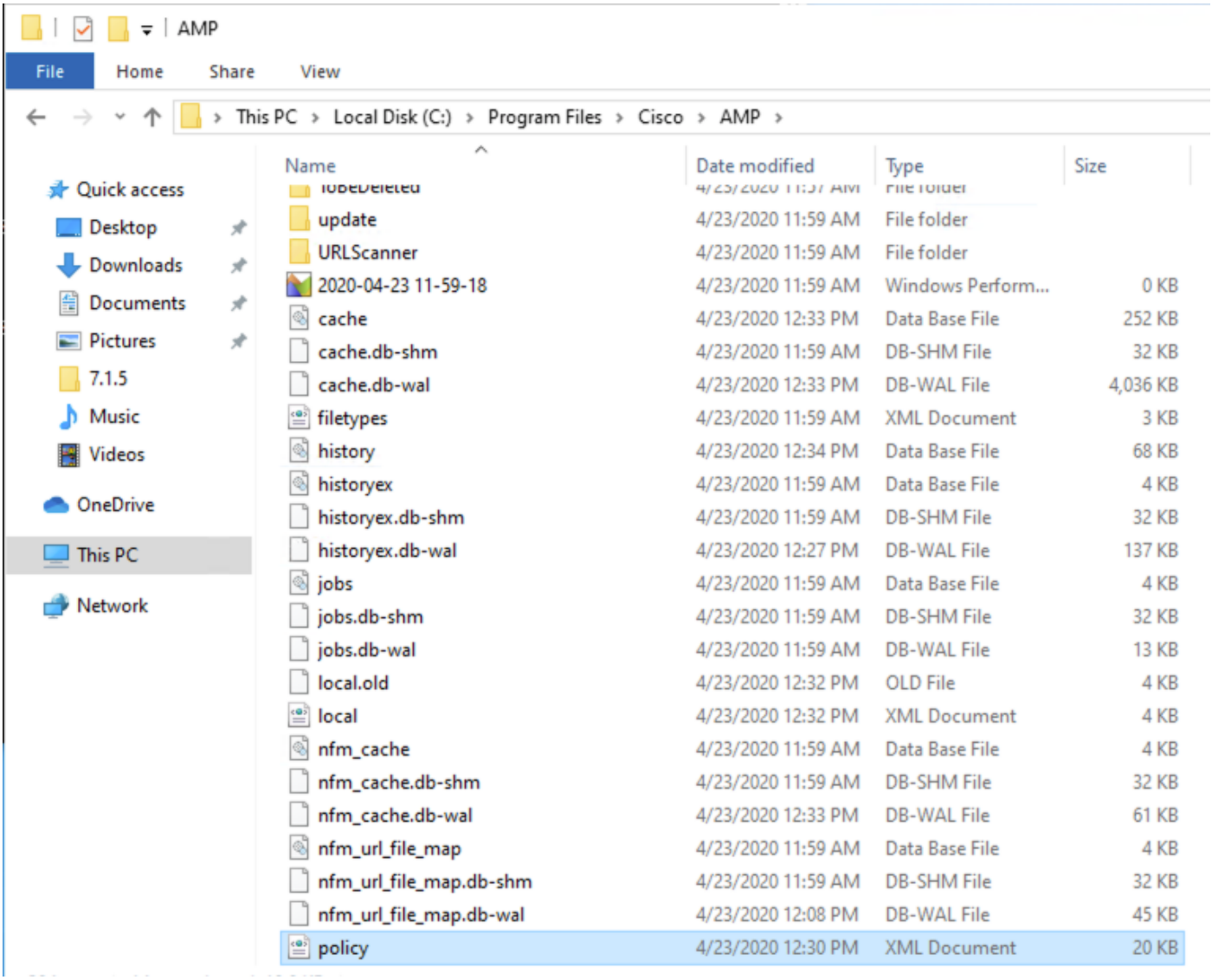


Paso 12. Copie este archivo **policy.xml** al terminal afectado.

Paso 13. Reinicie el punto final afectado en el **modo seguro**.

Paso 14. Una vez que el terminal afectado esté en **Modo seguro**, navegue a **C:\Program Files\Cisco\AMP**.

Paso 15. En esta carpeta, busque un archivo denominado **policy.xml** y renombrelo como **policy_old.xml**.



Paso 16. Ahora, pegue el archivo **policy.xml** previamente copiado en esta carpeta.

Paso 17. Una vez copiado el archivo, la desinstalación se puede realizar normalmente y en el mensaje de contraseña, se debe ingresar la contraseña recién configurada.

Paso 18. Este es un paso opcional. Dado que el conector se desinstaló cuando se desconectó la máquina, la entrada del ordenador permanecerá en la consola. Por lo tanto, puede navegar a **Management > Computers** y expandir el extremo afectado. Haga clic en **Eliminar** para eliminar el punto final.