Procedure to Uninstall the AMP Connector if the Password is Forgotten

Contents

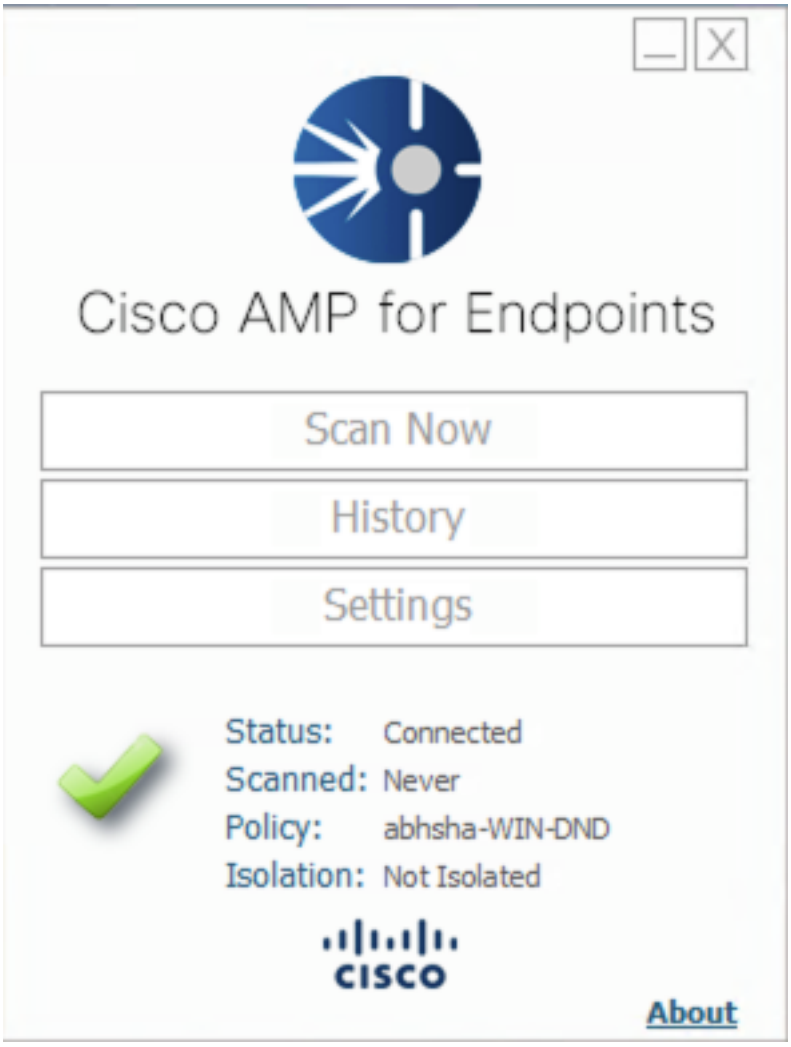
Introduction

This document describes the procedure in order to uninstall the Cisco Advanced Malware Protection (AMP) connector in case the uninstallation is blocked by the connector protection feature that requires a password to be supplied, and that password is forgotten. There are 2 scenarios in this case, and it depends on whether the connector shows "Connected" to the AMP cloud. It applies to the Windows OS only, since Connector Protection is a feature that is available on Windows OS only.

Connector is Connected

Step 1. Click on the tray icon and open the Cisco AMP for Endpoints Connector.

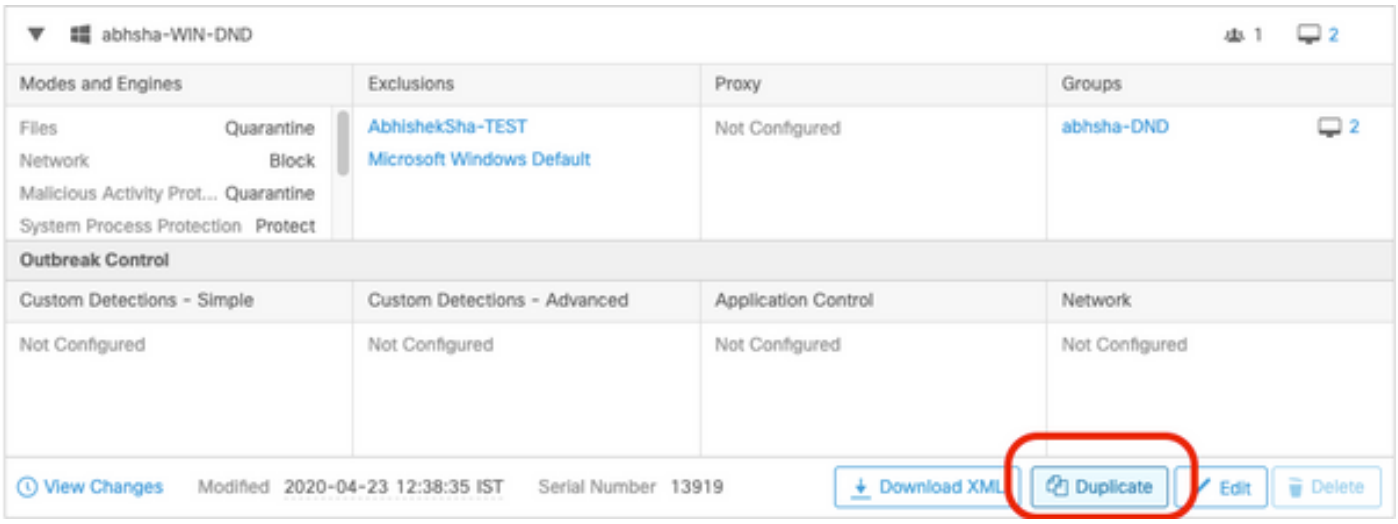
Step 2. Ensure that the Connector is shown as connected.



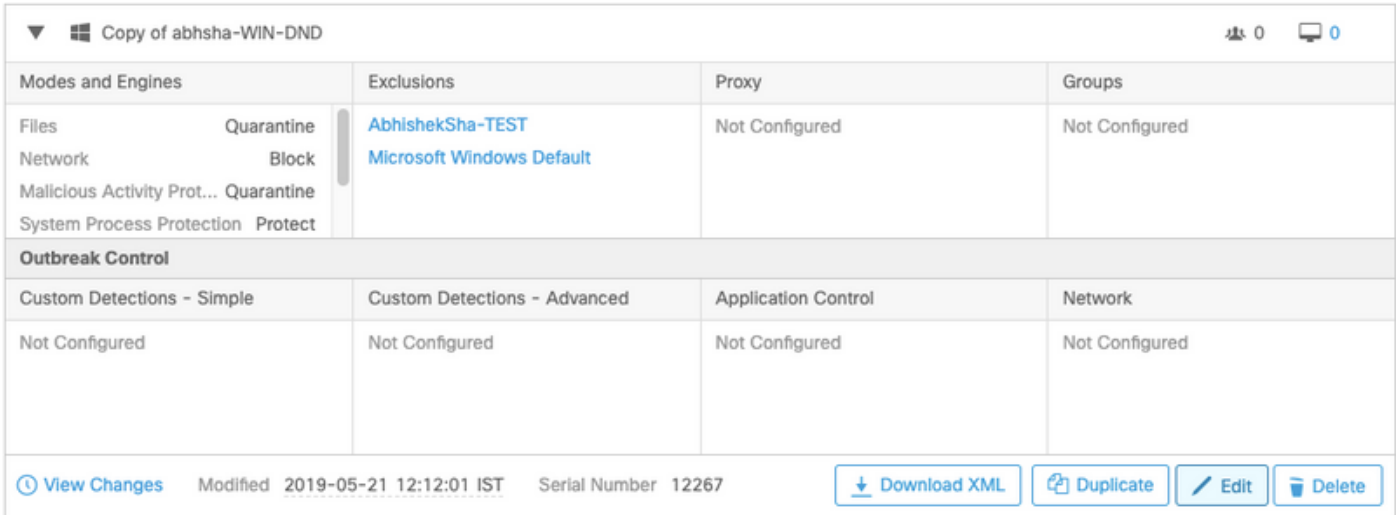
Step 3. Note that the policy has been assigned to that connector.

Step 4. Navigate to your AMP for Endpoints Console and search for the policy that was previously noted.

Step 5. Expand the policy and click **Duplicate** as shown in the image.

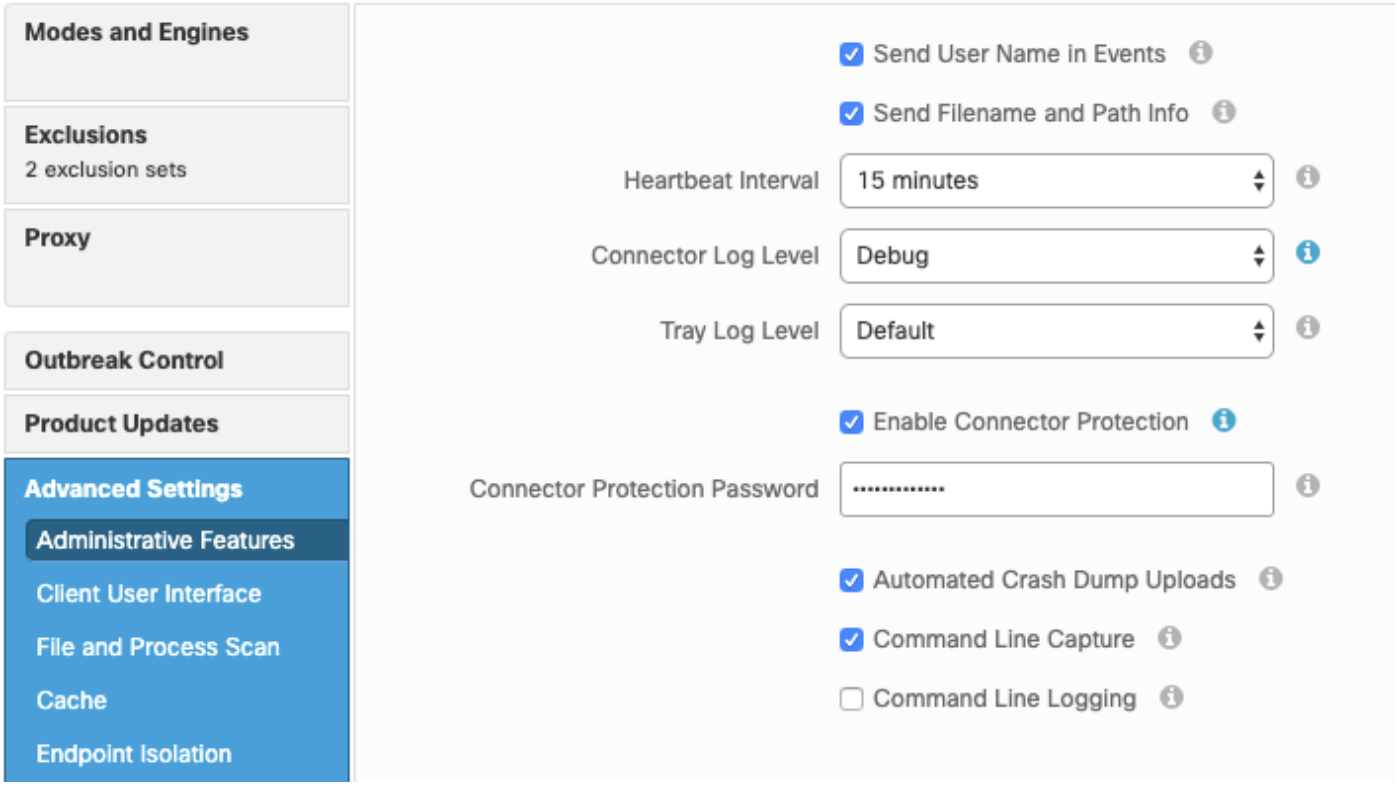


Step 6. A new policy called "Copy of.." will be created. Click on **Edit** in order to edit this policy as shown in the image.



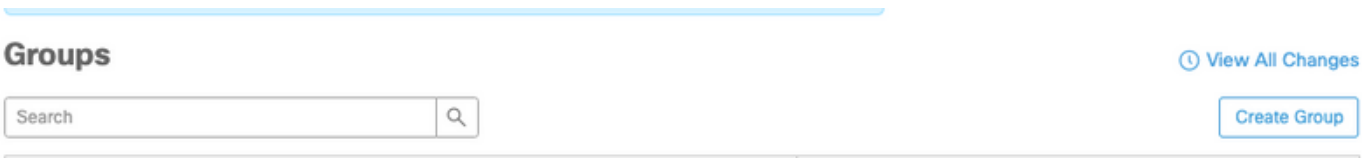
Step 7. At the **Edit Policy** page, navigate to **Advanced Settings > Administrative Features.**

Step 8. At the **Connector Password Protection** field, replace the password with a new password that can be recalled as shown in the image.

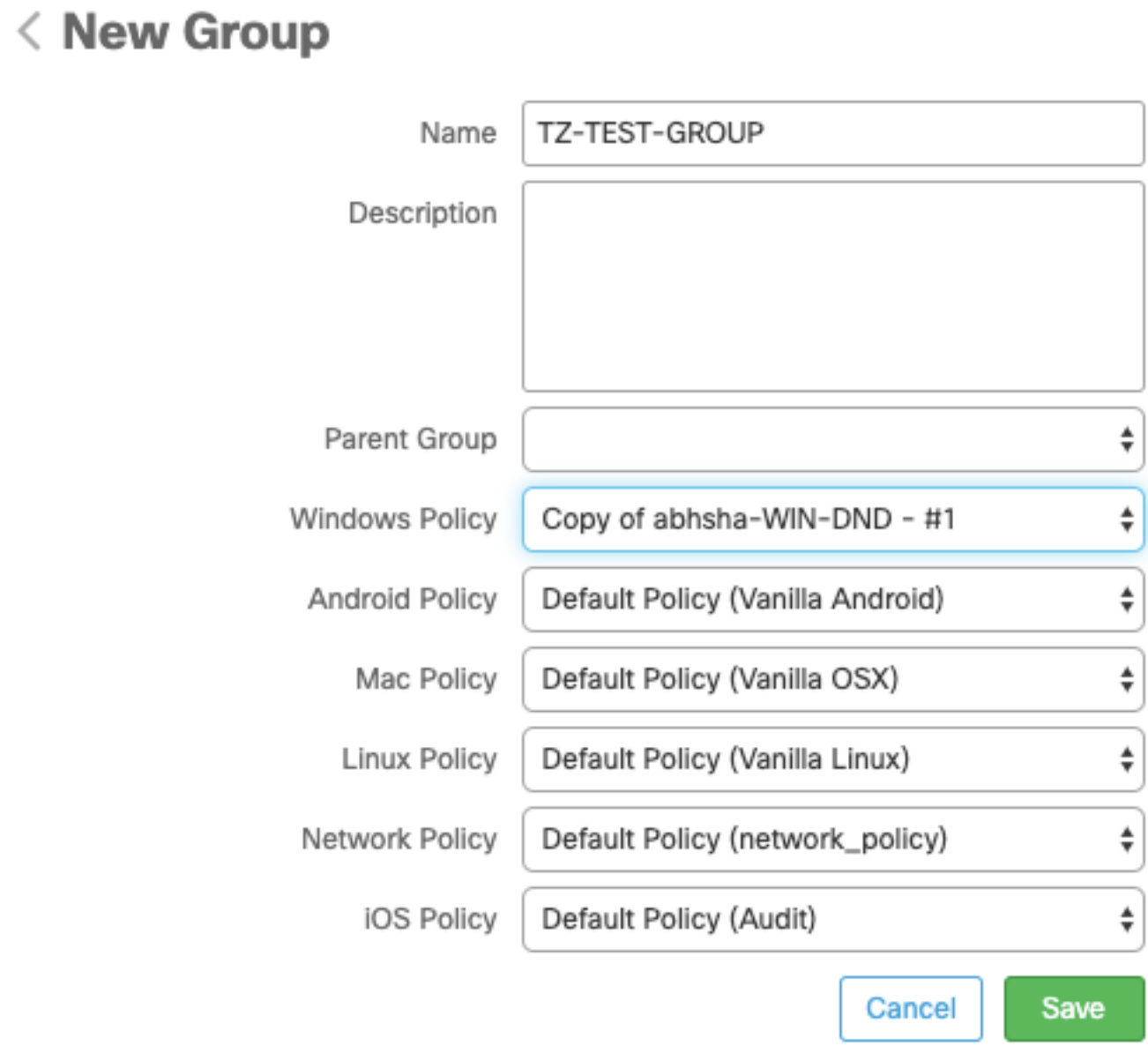


Step 9. Click the **Save** button in order to save this policy.

Step 10. Navigate to **Management > Groups** and create a new group.

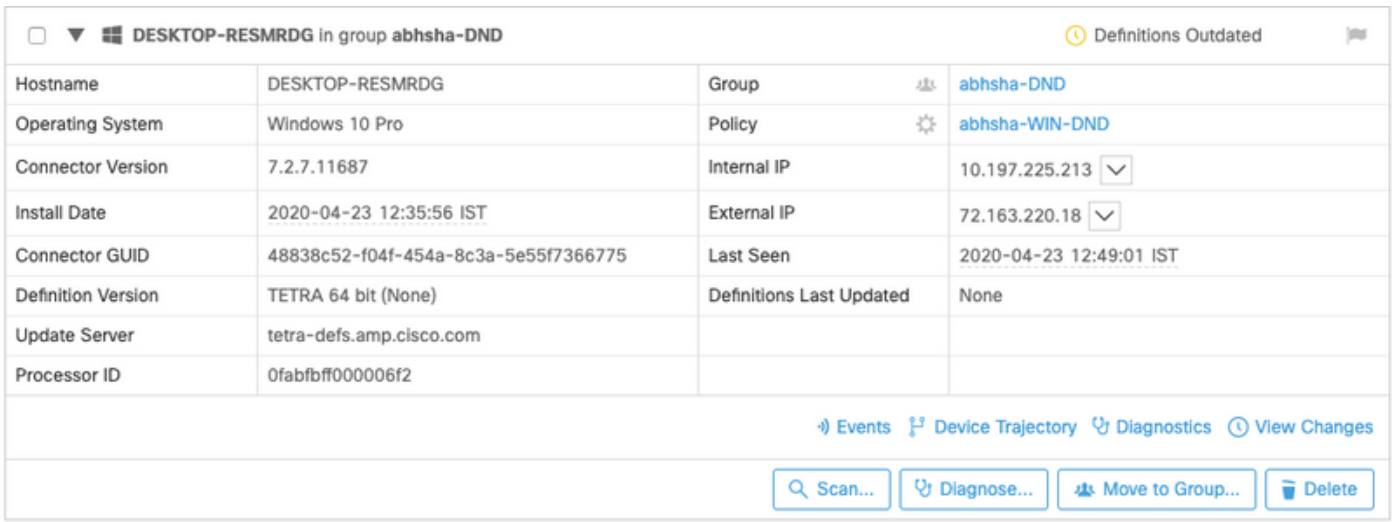


Step 11. Enter a group name and select the **Windows Policy** as the previously edited policy. Click the **Save** button as shown in the image.



Step 12. Navigate to **Management > Computers** and search for the computer on which you try to uninstall the AMP connector.

Step 13. Expand the computer and click **Move to Group**. From the dialog box that appears, select the previously created Group.



Step 14. Wait for the policy to be updated on the endpoint. It usually takes about 30 minutes to 1 hour and depends upon the configured interval.

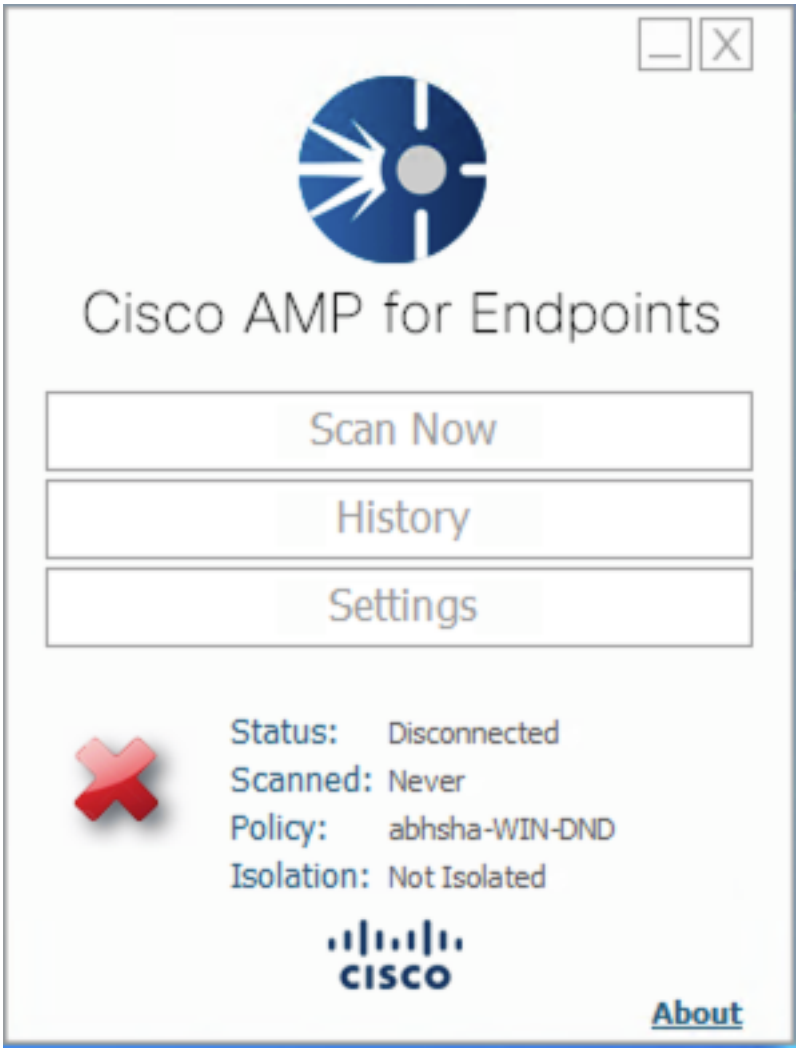
Step 15. Once the policy has been updated on the endpoint, you will be able to uninstall the connector with the use of the password that you've newly configured.

Connector is Disconnected

If the Connector is disconnected from the AMP cloud, then it is important to be able to boot the computer in Safe Mode.

Step 1. Click on the tray icon and open the Cisco AMP for Endpoints Connector.

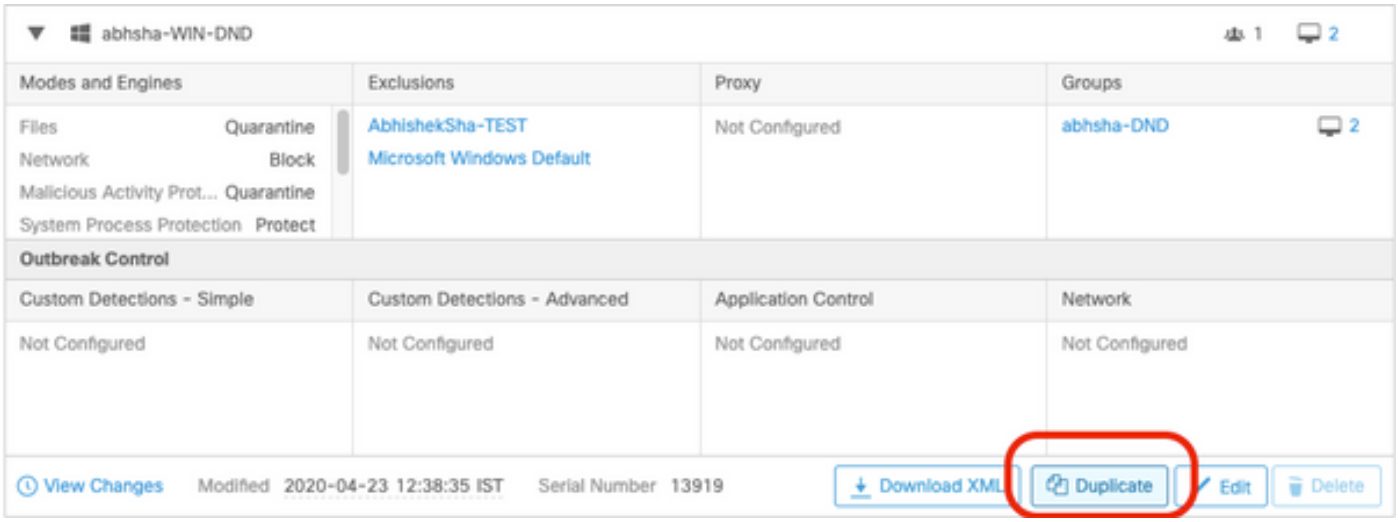
Step 2. Ensure that the Connector is shown as disconnected.



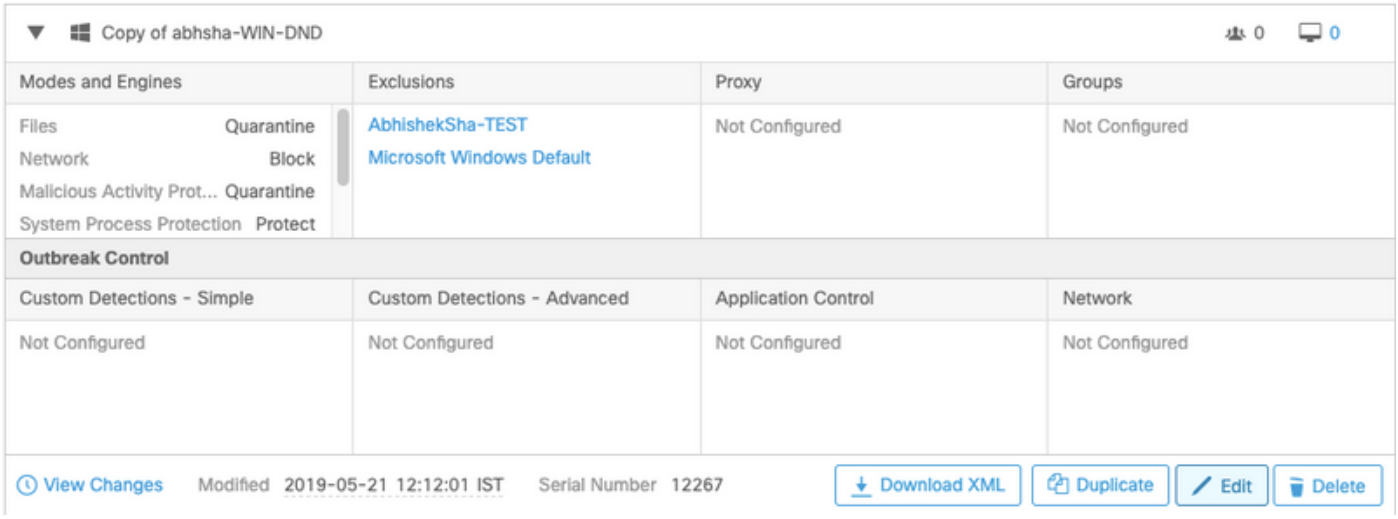
Step 3. Note the policy that has been assigned to that connector.

Step 4. Navigate to your AMP for Endpoints Console and search for the policy that was previously noted.

Step 5. Expand the policy and click **Duplicate** as shown in the image.

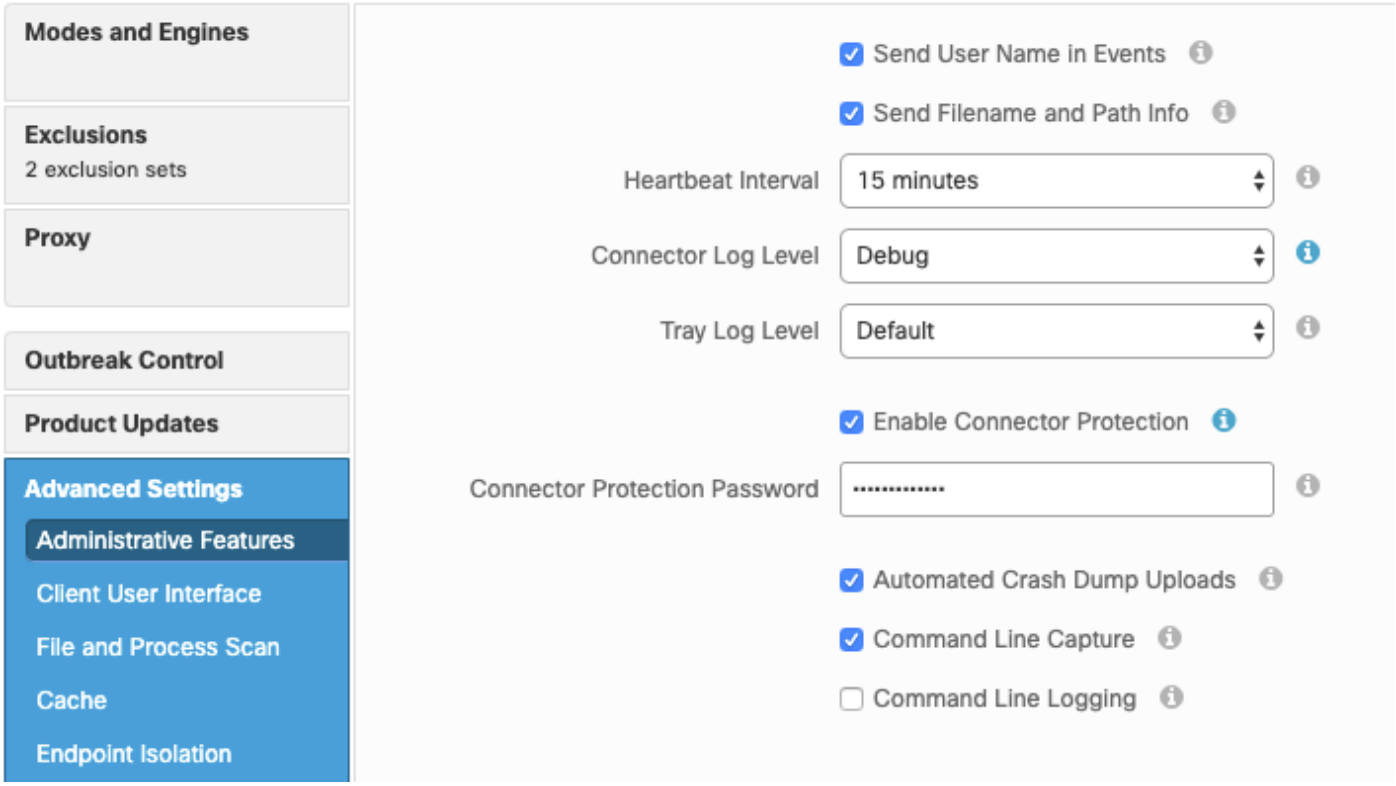


Step 6. A new policy called "Copy of.." will be created. Click on **Edit** to edit this policy.



Step 7. At the Edit Policy page, navigate to **Advanced Settings > Administrative Features**.

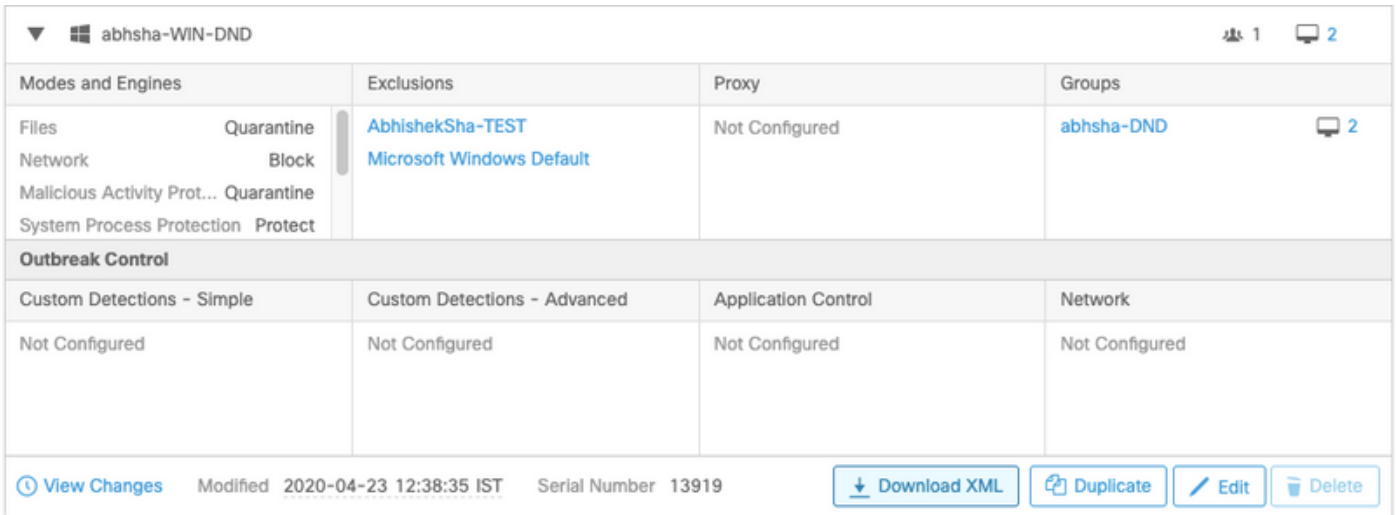
Step 8. At the **Connector Password Protection** field, replace the password with a new password that can be recalled.



Step 9. Click the **Save** button in order to save this policy.

Step 10. Navigate to **Management > Policies** and search for the policy that was newly duplicated.

Step 11. Expand the policy and click **Download XML.** A file named **policy.xml** will be saved to your machine.

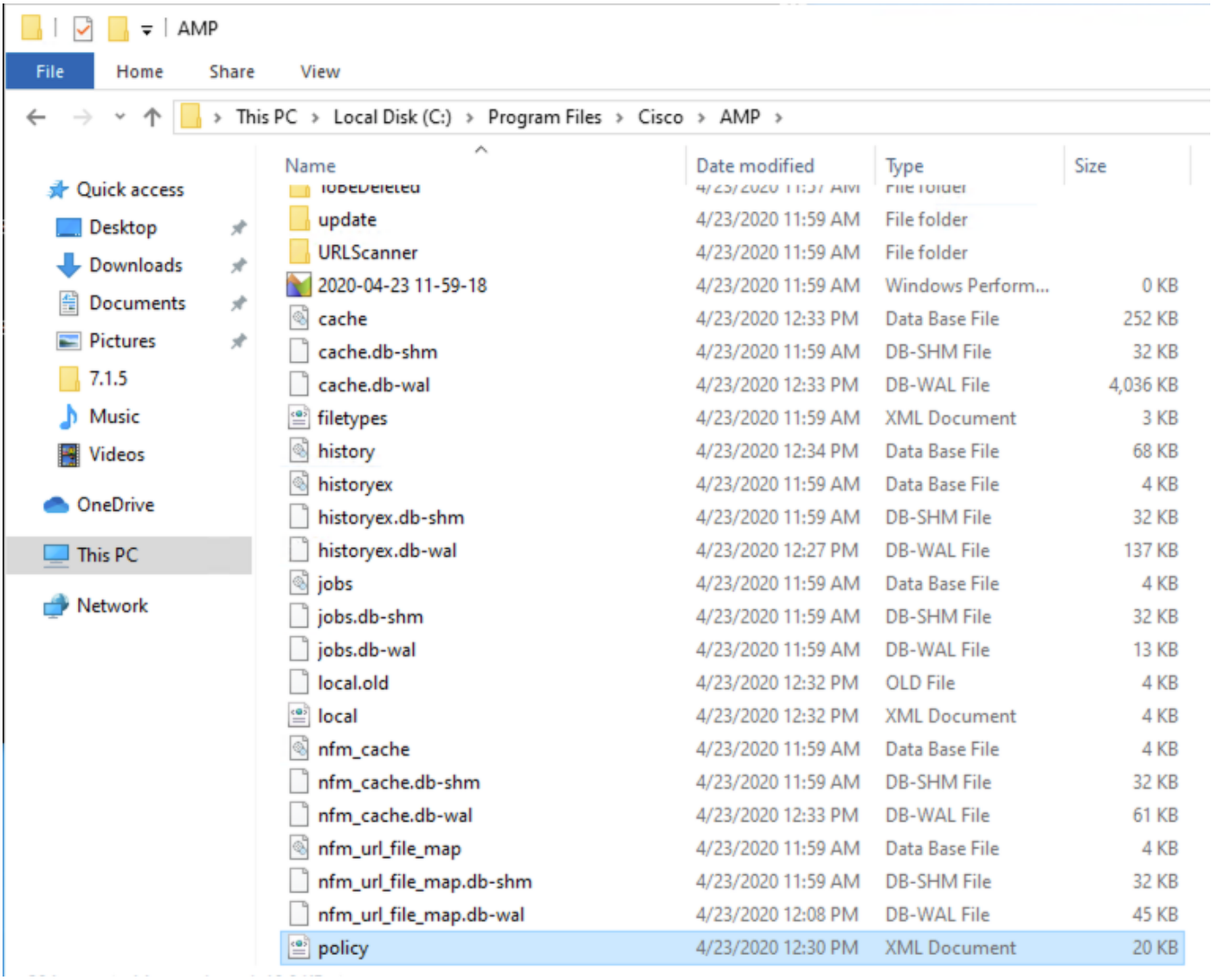


Step 12. Copy this **policy.xml** to the affected endpoint.

Step 13. Reboot the affected endpoint in **Safe Mode**.

Step 14. Once the affected endpoint is in **Safe Mode**, navigate to **C:\Program Files\Cisco\AMP**.

Step 15. In this folder, search for a file named **policy.xml** and rename this to **policy_old.xml**.



Step 16. Now, paste the previously copied **policy.xml** to this folder.

Step 17. After the file has been copied, the uninstallation can be performed normally and at the password prompt, the newly configured password must be entered.

Step 18. This is an optional step. Since the connector was uninstalled when the machine was disconnected, the computer entry will remain on the console. Therefore, you can navigate to **Management > Computers** and expand the affected endpoint. Click **Delete** in order to delete the endpoint.