Verfahren zur Deinstallation des AMP Connectors bei vergessenem Kennwort

Inhalt

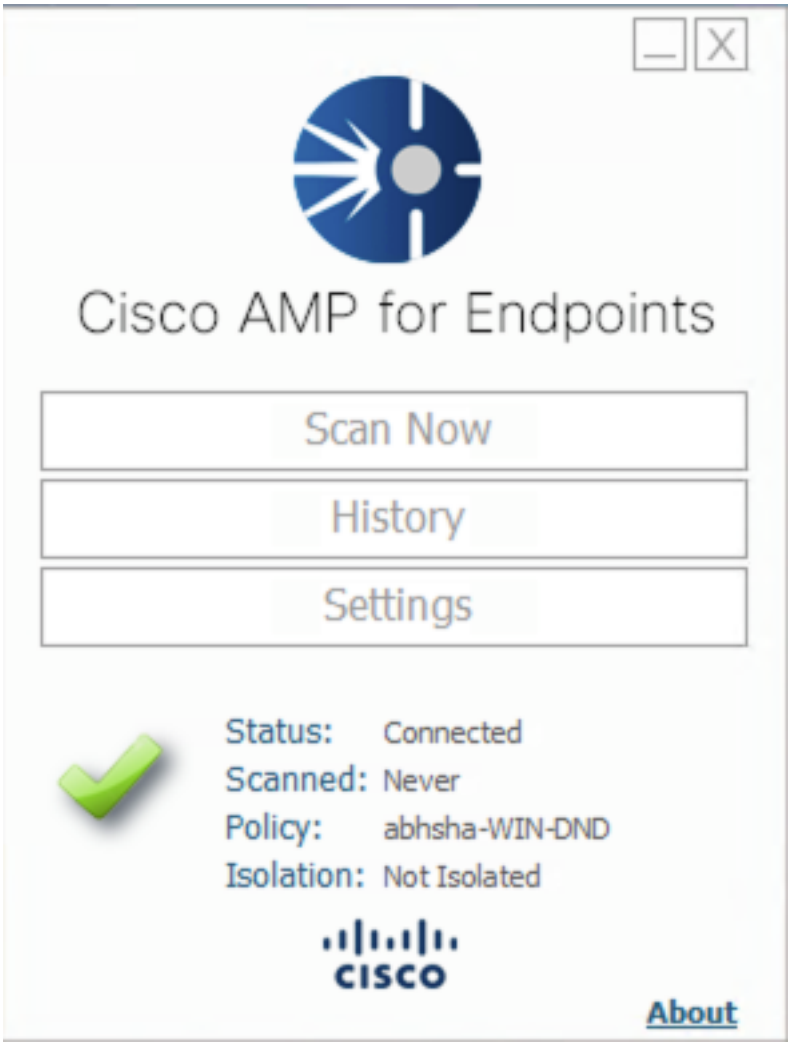
Einführung

In diesem Dokument wird das Verfahren zur Deinstallation des Cisco Advanced Malware Protection (AMP)-Connectors beschrieben, falls die Deinstallation durch die Anschlussschutzfunktion blockiert wird, für die ein Kennwort eingegeben werden muss und dieses Kennwort vergessen wird. In diesem Fall gibt es zwei Szenarien, die davon abhängen, ob der Connector "Connected" (Verbunden) zur AMP-Cloud anzeigt. Sie gilt nur für das Windows-Betriebssystem, da der Connector-Schutz eine Funktion ist, die nur unter Windows verfügbar ist.

Anschluss ist verbunden

Schritt 1: Klicken Sie auf das Taskleistensymbol, und öffnen Sie den Cisco AMP für Endpoints-Connector.

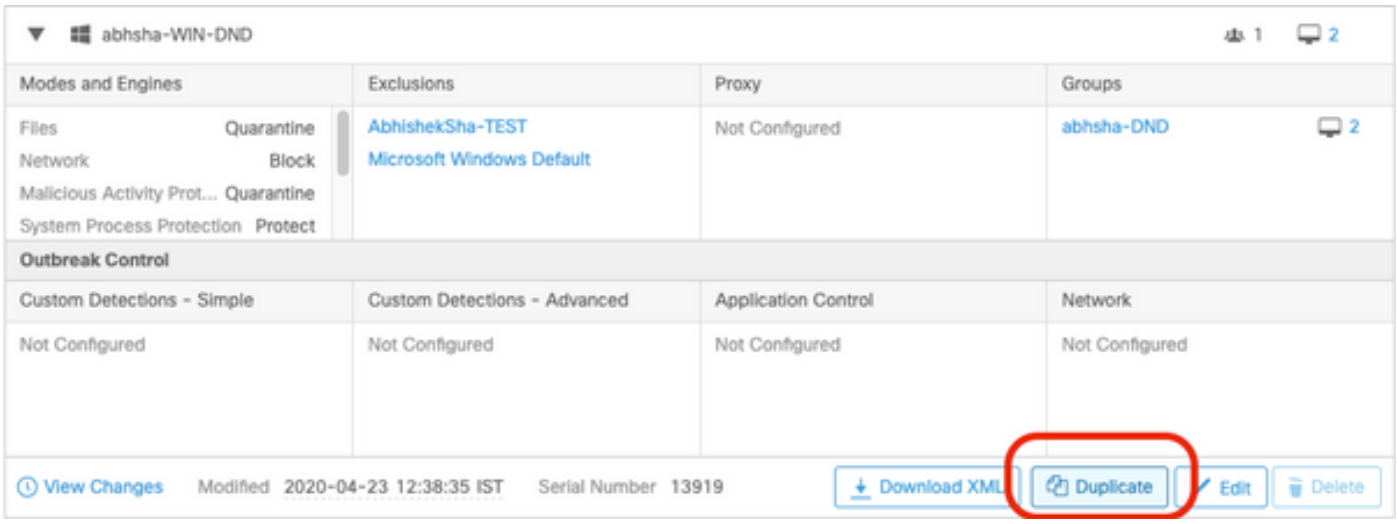
Schritt 2: Stellen Sie sicher, dass der Connector als verbunden angezeigt wird.



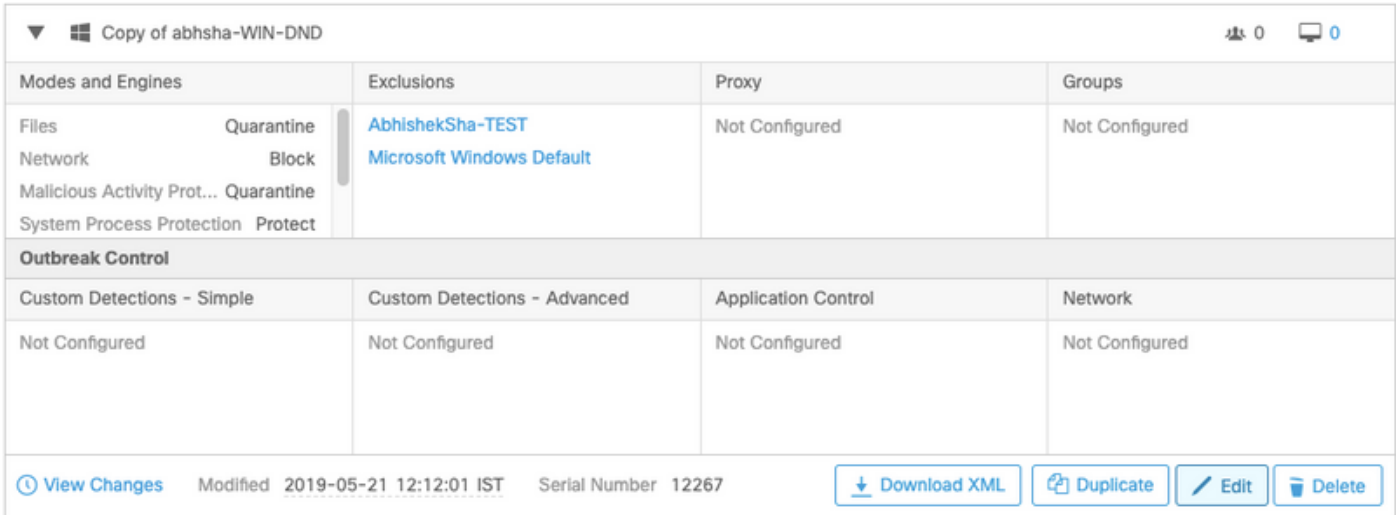
Schritt 3: Beachten Sie, dass die Richtlinie diesem Anschluss zugewiesen wurde.

Schritt 4: Navigieren Sie zu Ihrer AMP für Endgeräte-Konsole, und suchen Sie nach der zuvor erwähnten Richtlinie.

Schritt 5: Erweitern Sie die Richtlinie, und klicken Sie auf **Duplizieren** wie im Bild gezeigt.

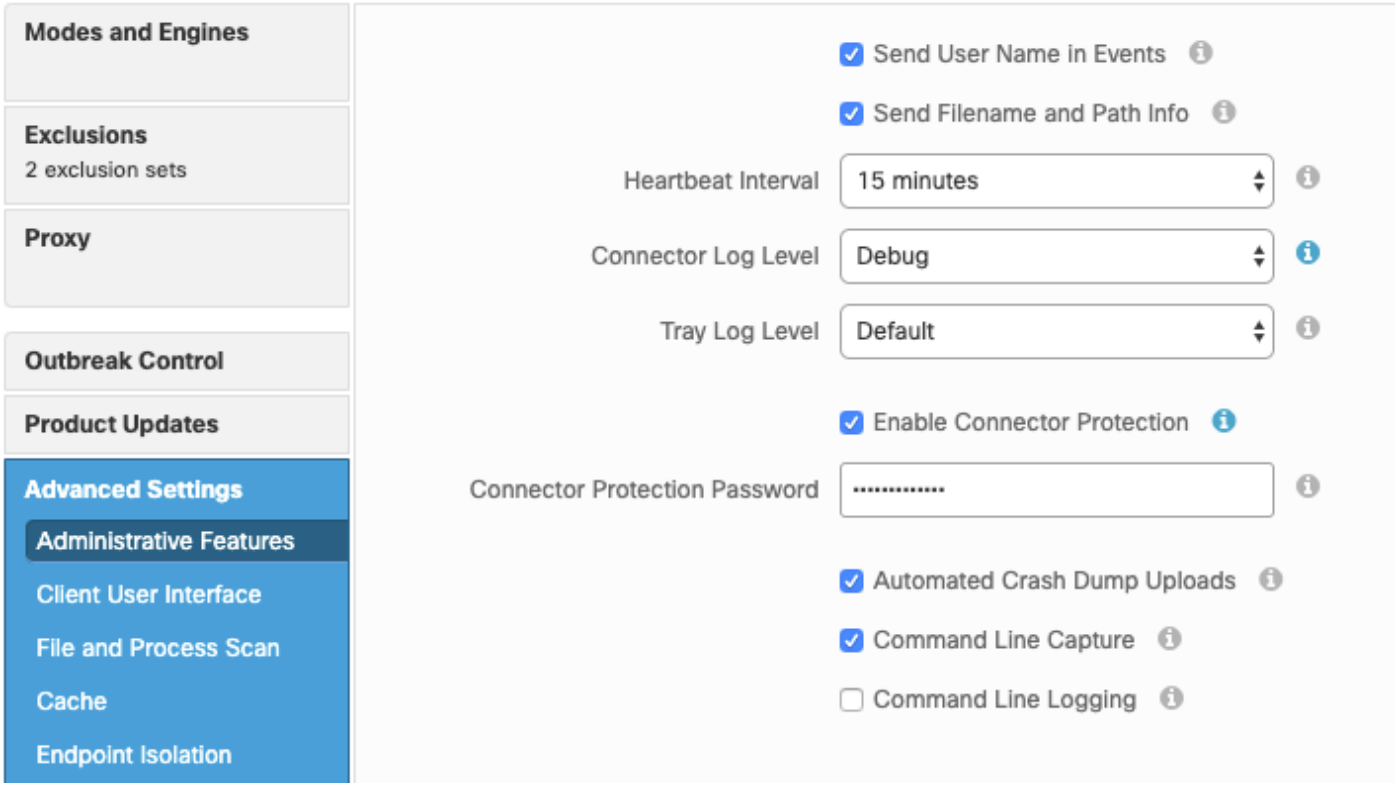


Schritt 6: Eine neue Richtlinie mit dem Namen "Kopie von.." wird erstellt. Klicken Sie auf **Bearbeiten**, um diese Richtlinie wie im Bild gezeigt zu bearbeiten.



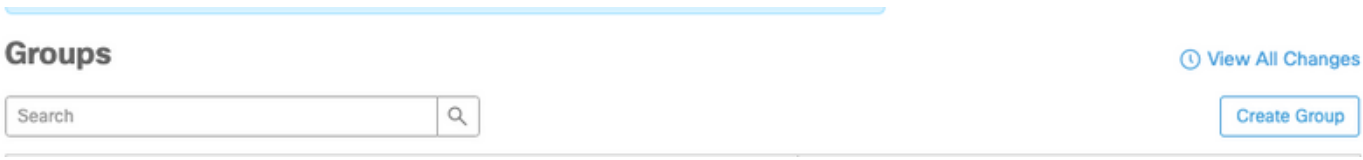
Schritt 7: Navigieren Sie auf der Seite **Richtlinie bearbeiten** zu **Erweiterte Einstellungen > Verwaltungsfunktionen.**

Schritt 8: Ersetzen Sie im Feld **Connector Password Protection** (**Connector-Kennwortschutz**) das Kennwort durch ein neues Kennwort, das wie im Bild gezeigt aufgerufen werden kann.

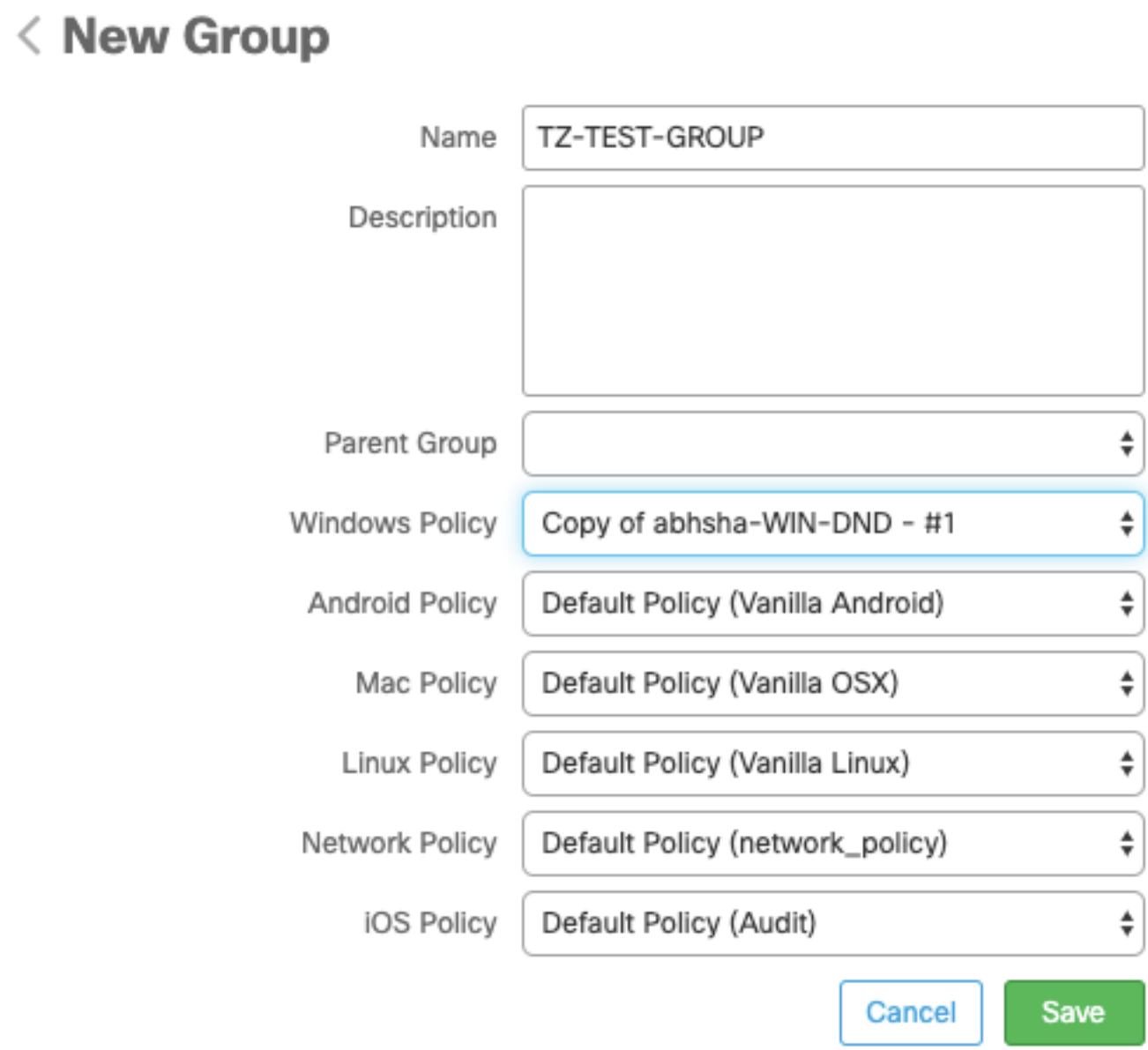


Schritt 9: Klicken Sie auf die Schaltfläche **Speichern**, um diese Richtlinie zu speichern.

Schritt 10: Navigieren Sie zu **Verwaltung > Gruppen**, und erstellen Sie eine neue Gruppe.

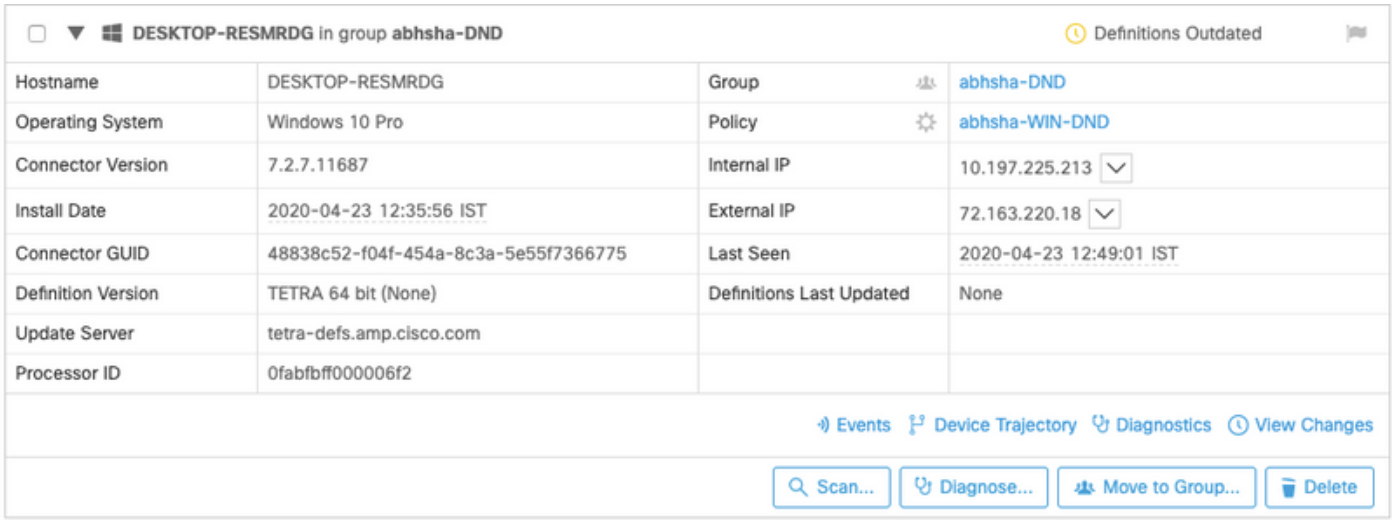


Schritt 11: Geben Sie einen Gruppennamen ein, und wählen Sie die **Windows-Richtlinie** als zuvor bearbeitete Richtlinie aus. Klicken Sie auf die Schaltfläche **Speichern**, wie im Bild gezeigt.



Schritt 12: Navigieren Sie zu **Verwaltung > Computer**, und suchen Sie nach dem Computer, auf dem Sie versuchen, den AMP-Anschluss zu deinstallieren.

Schritt 13: Erweitern Sie den Computer, und klicken Sie auf **Zu Gruppe verschieben**. Wählen Sie im angezeigten Dialogfeld die zuvor erstellte Gruppe aus.



Schritt 14: Warten Sie, bis die Richtlinie auf dem Endpunkt aktualisiert wird. Dieser Vorgang dauert in der Regel zwischen 30 und 1 Stunde und hängt vom konfigurierten Intervall ab.

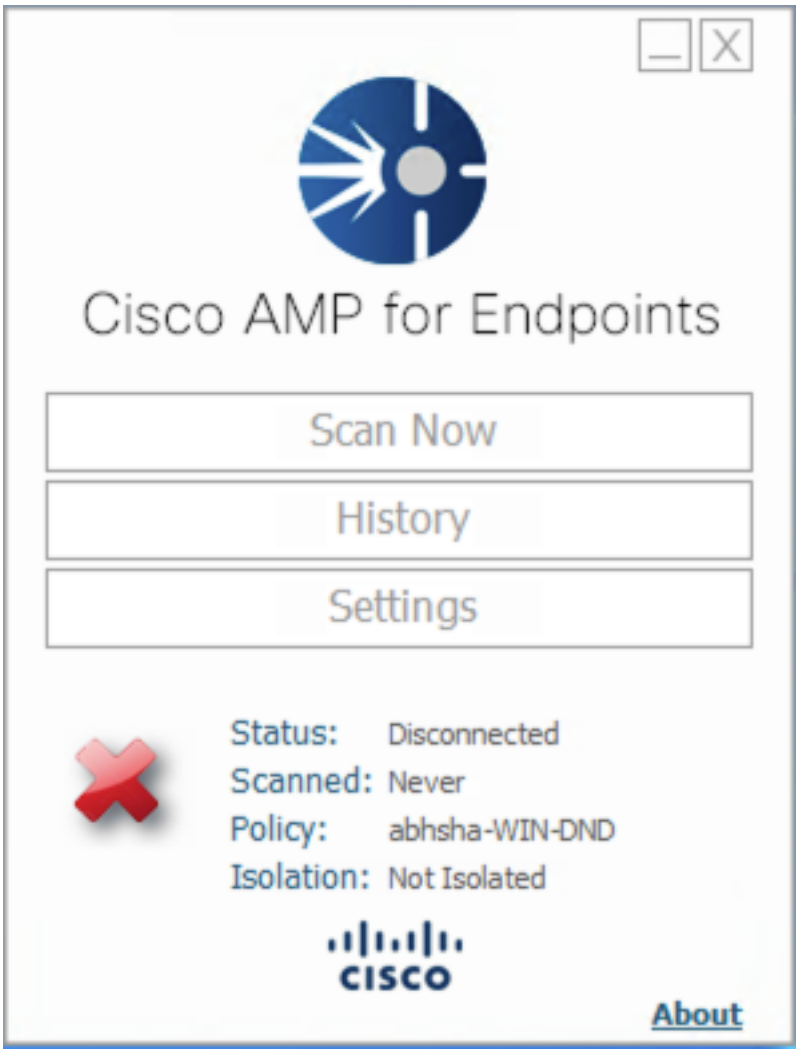
Schritt 15: Nachdem die Richtlinie auf dem Endgerät aktualisiert wurde, können Sie den Connector mithilfe des neu konfigurierten Kennworts deinstallieren.

Verbindung getrennt

Wenn der Connector von der AMP-Cloud getrennt wird, ist es wichtig, den Computer im abgesicherten Modus starten zu können.

Schritt 1: Klicken Sie auf das Taskleistensymbol, und öffnen Sie den Cisco AMP für Endpoints-Connector.

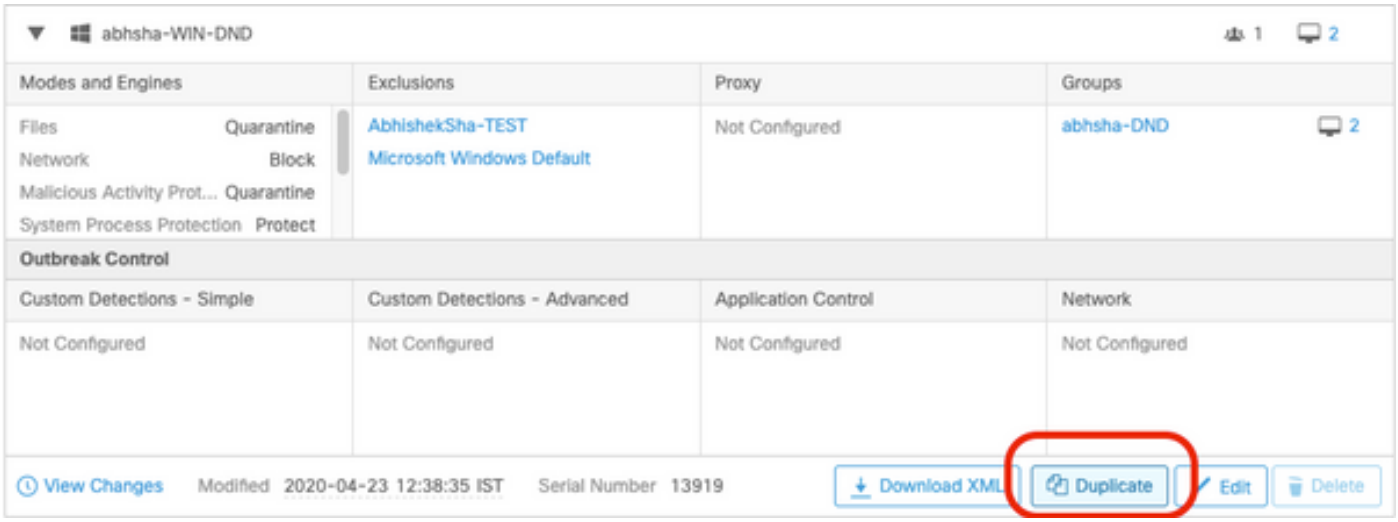
Schritt 2: Stellen Sie sicher, dass der Anschluss als getrennt angezeigt wird.



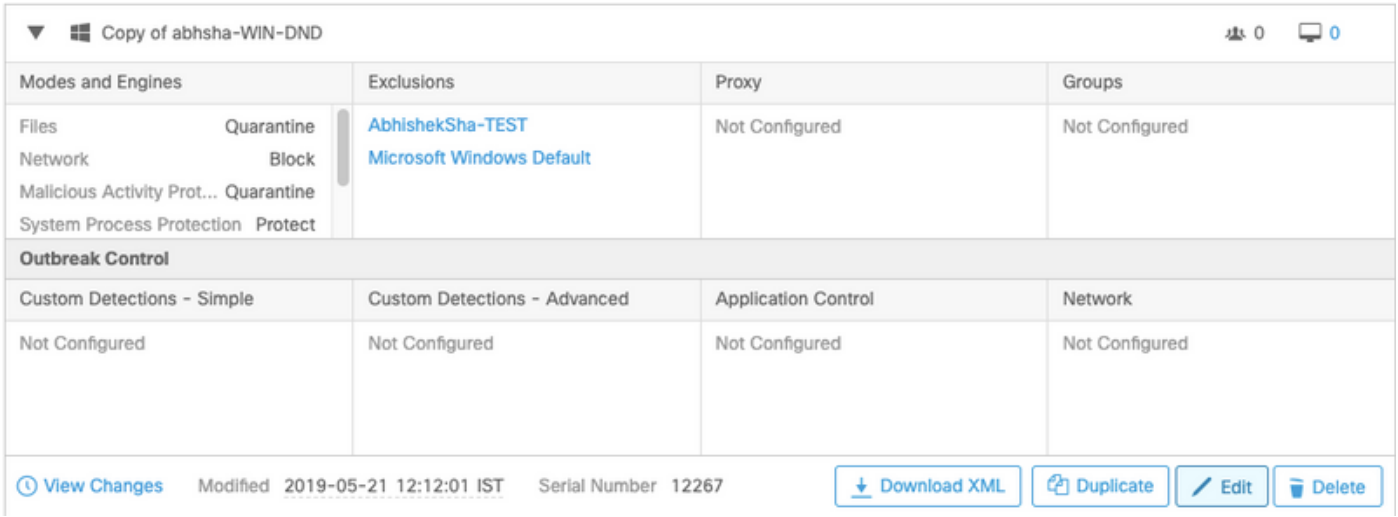
Schritt 3: Beachten Sie die Richtlinie, die diesem Anschluss zugewiesen wurde.

Schritt 4: Navigieren Sie zu Ihrer AMP für Endgeräte-Konsole, und suchen Sie nach der zuvor erwähnten Richtlinie.

Schritt 5: Erweitern Sie die Richtlinie, und klicken Sie auf **Duplizieren** wie im Bild gezeigt.

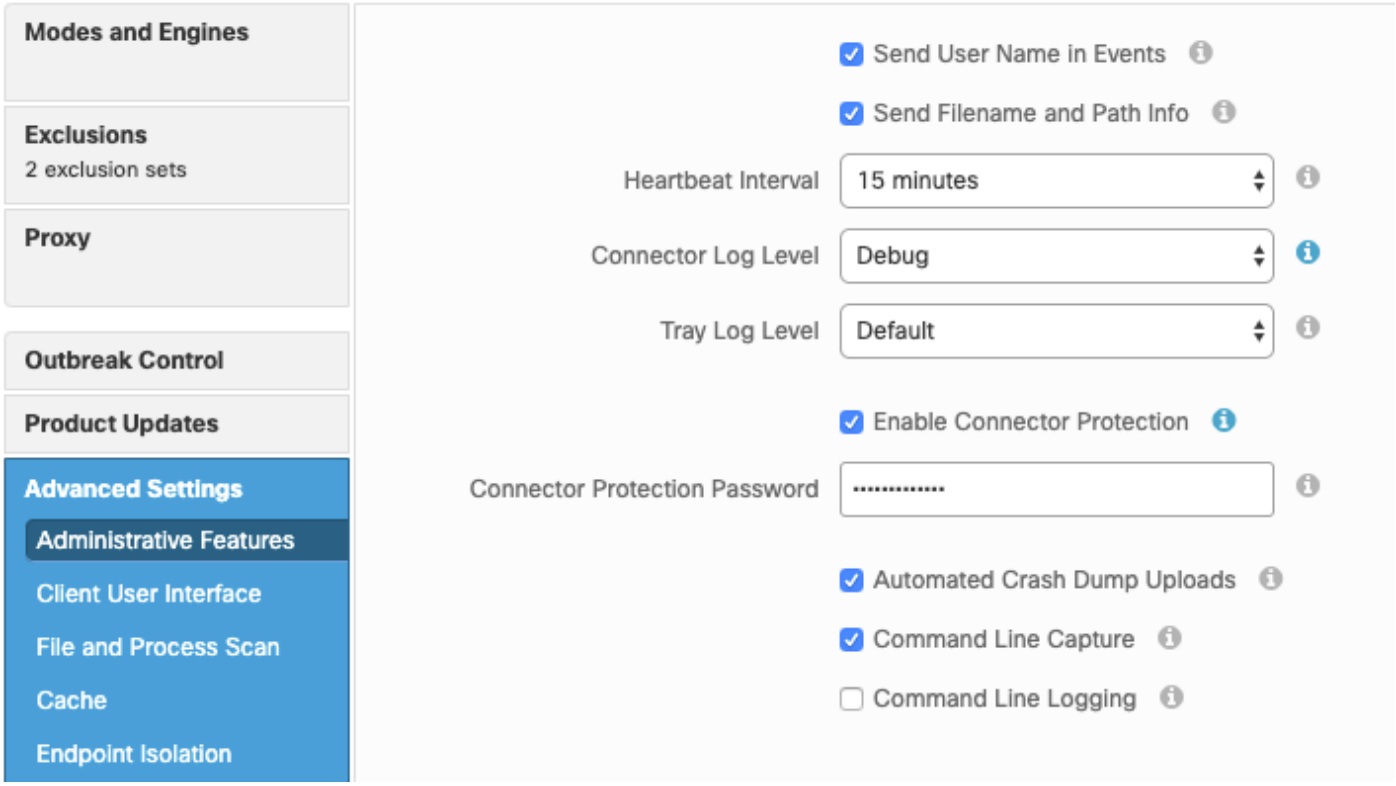


Schritt 6: Eine neue Richtlinie mit dem Namen "Kopie von.." wird erstellt. Klicken Sie auf **Bearbeiten**, um diese Richtlinie zu bearbeiten.



Schritt 7: Navigieren Sie auf der Seite Richtlinie bearbeiten zu **Erweiterte Einstellungen > Verwaltungsfunktionen**.

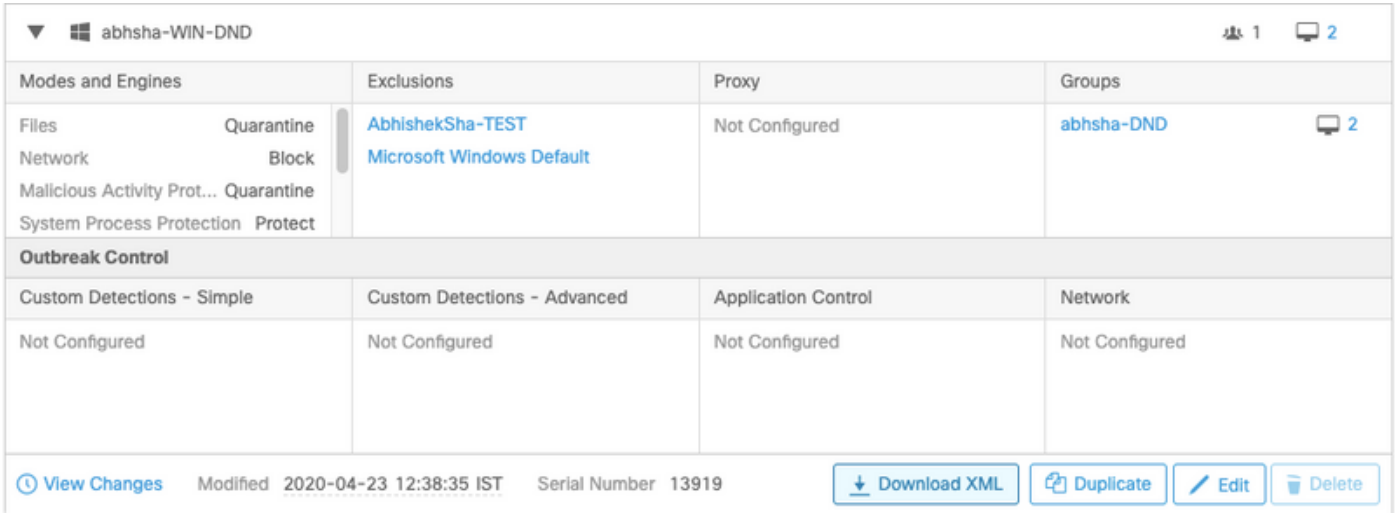
Schritt 8: Ersetzen Sie im Feld **Connector Password Protection** (**Connector-Kennwortschutz**) das Kennwort durch ein neues Kennwort, das Sie zurückrufen können.



Schritt 9: Klicken Sie auf die Schaltfläche **Speichern**, um diese Richtlinie zu speichern.

Schritt 10: Navigieren Sie zu **Management > Policies (Verwaltung > Richtlinien)**, und suchen Sie nach der Richtlinie, die neu dupliziert wurde.

Schritt 11: Erweitern Sie die Richtlinie, und klicken Sie auf **XML herunterladen.** Eine Datei mit dem Namen **policy.xml** wird auf Ihrem Computer gespeichert.

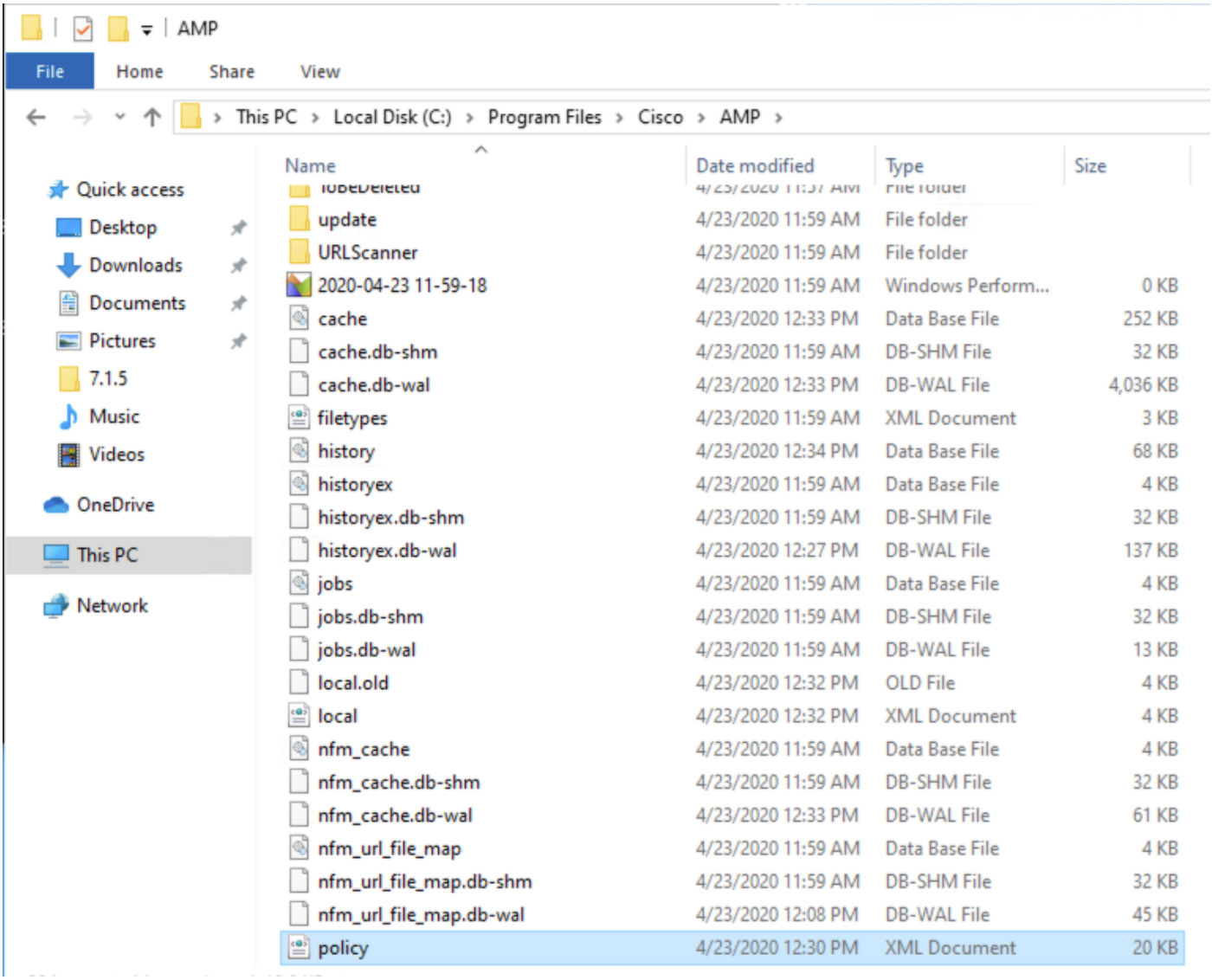


Schritt 12: Kopieren Sie diese **policy.xml** auf den betroffenen Endpunkt.

Schritt 13: Starten Sie den betroffenen Endpunkt im **abgesicherten Modus neu**.

Schritt 14: Sobald sich der betroffene Endpunkt im **abgesicherten Modus** befindet, navigieren Sie zu **C:\Program Files\Cisco\AMP**.

Schritt 15: Suchen Sie in diesem Ordner nach einer Datei mit dem Namen **policy.xml,** und benennen Sie diese in **policy_old.xml um**.



Schritt 16: Fügen Sie nun die zuvor kopierte **policy.xml** in diesen Ordner ein.

Schritt 17: Nachdem die Datei kopiert wurde, kann die Deinstallation normal ausgeführt werden. Bei der Kennworteingabeaufforderung muss das neu konfigurierte Kennwort eingegeben werden.

Schritt 18: Dies ist ein optionaler Schritt. Da der Anschluss beim Trennen der Verbindung deinstalliert wurde, bleibt der Computereintrag auf der Konsole. Daher können Sie zu **Management > Computers** navigieren und den betroffenen Endpunkt erweitern. Klicken Sie auf **Löschen**, um den Endpunkt zu löschen.