Procedura per disinstallare il connettore AMP in caso di dimenticanza della password

Sommario

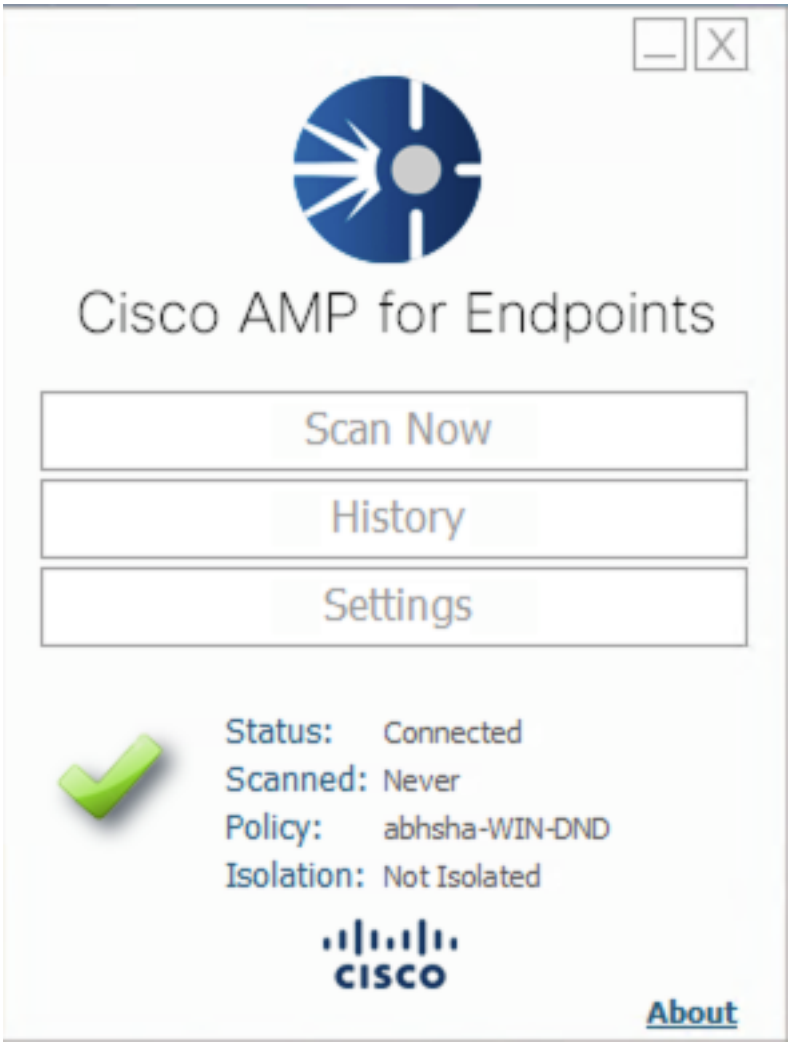
Introduzione

Questo documento descrive la procedura per disinstallare il connettore Cisco Advanced Malware Protection (AMP) nel caso in cui la disinstallazione sia bloccata dalla funzione di protezione del connettore che richiede l'immissione di una password, e tale password venga dimenticata. Esistono due scenari in questo caso e dipende dal fatto che il connettore visualizzi "Connesso" al cloud AMP. Si applica solo al sistema operativo Windows, poiché la protezione del connettore è una funzionalità disponibile solo nel sistema operativo Windows.

Connettore connesso

Passaggio 1. Fare clic sull'icona nell'area di notifica e aprire Cisco AMP for Endpoints Connector.

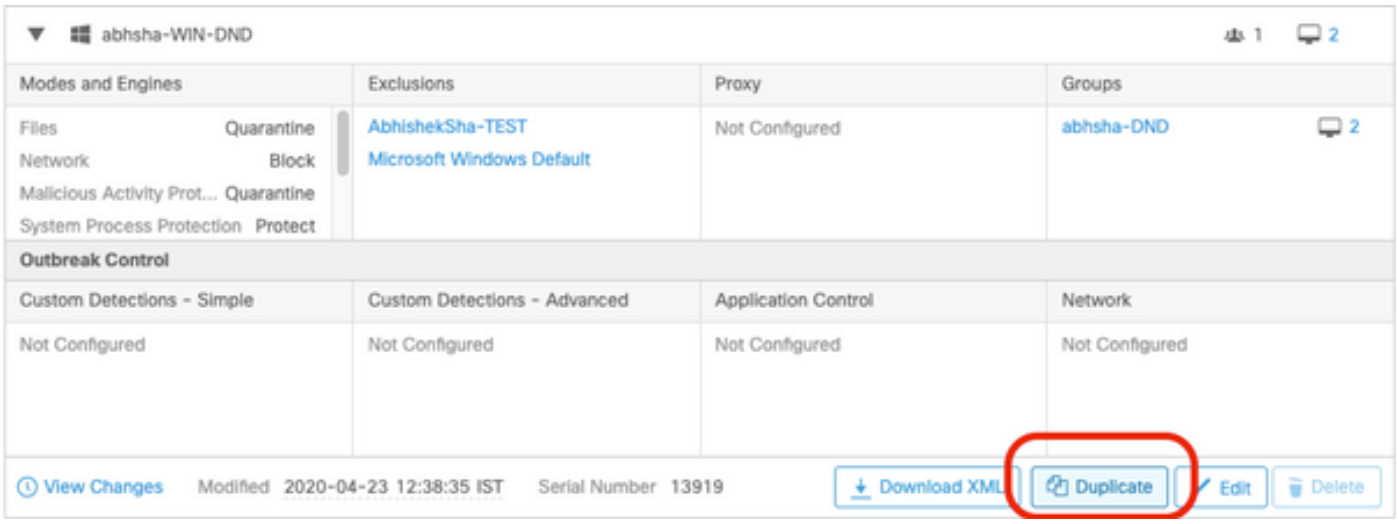
Passaggio 2. Verificare che il connettore sia indicato come connesso.



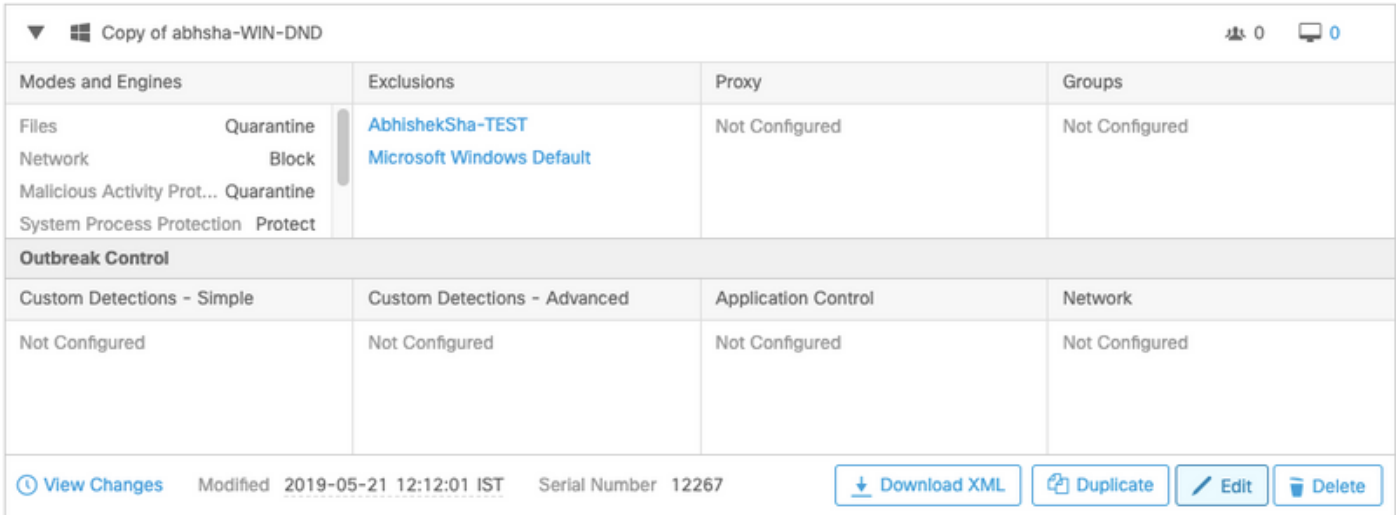
Passaggio 3. Il criterio è stato assegnato al connettore.

Passaggio 4. Passare alla console AMP for Endpoints e cercare il criterio annotato in precedenza.

Passaggio 5. Espandere il criterio e fare clic su **Duplica**, come mostrato nell'immagine.

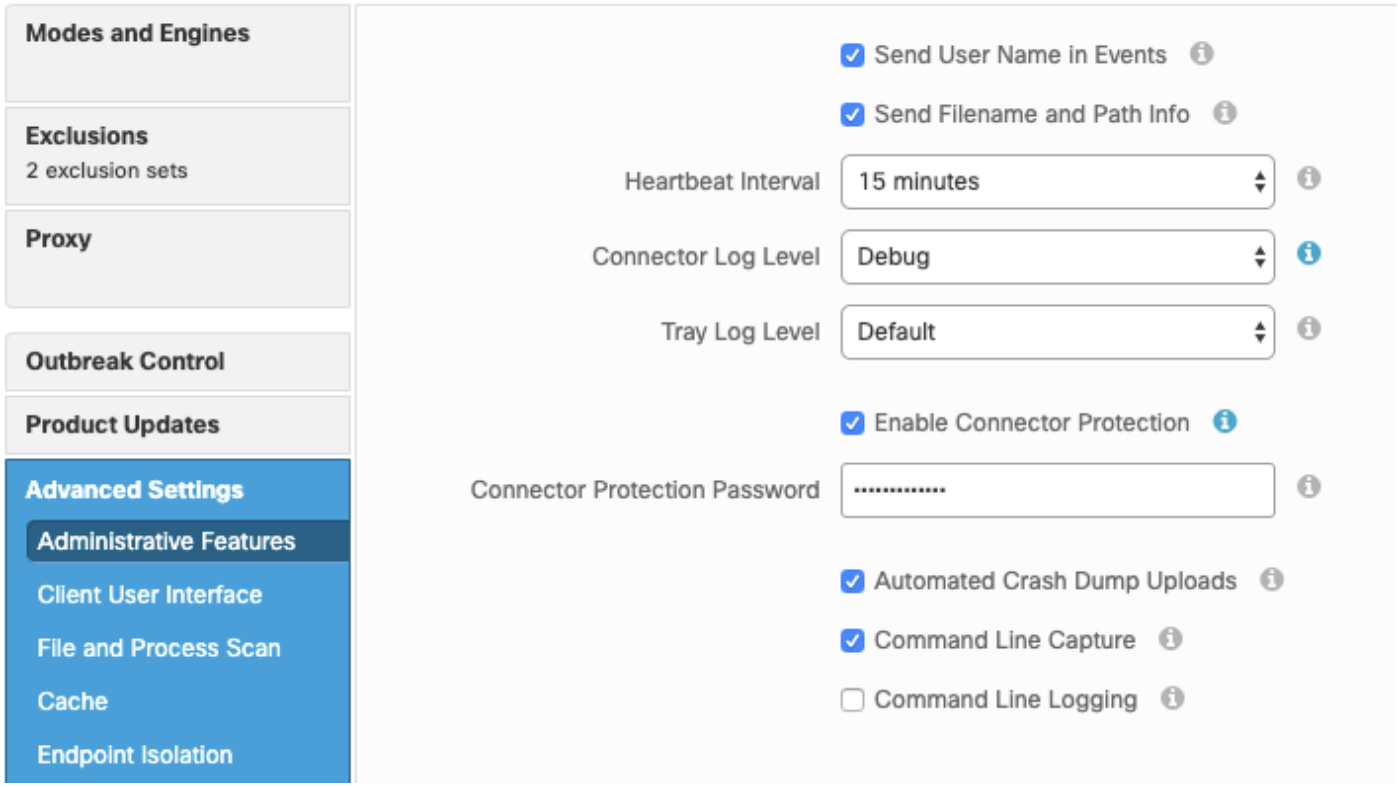


Passaggio 6. Una nuova regola denominata "Copia di..." verrà creato. Per modificare questo criterio, fare clic su **Edit** (Modifica), come mostrato nell'immagine.



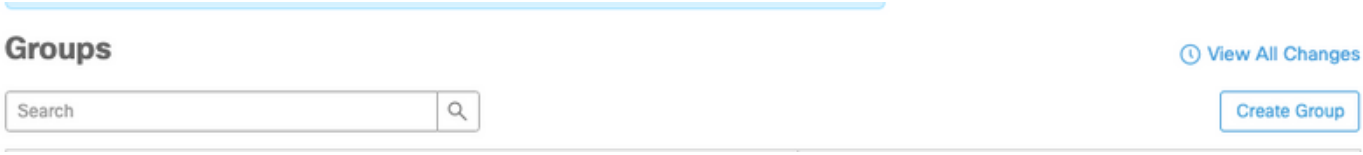
Passaggio 7. Nella pagina **Modifica criterio**, passare a **Impostazioni avanzate > Funzioni amministrative.**

Passaggio 8. Nel campo **Connector Password Protection** (Protezione password connettore), sostituire la password con una nuova password che possa essere richiamata, come mostrato nell'immagine.

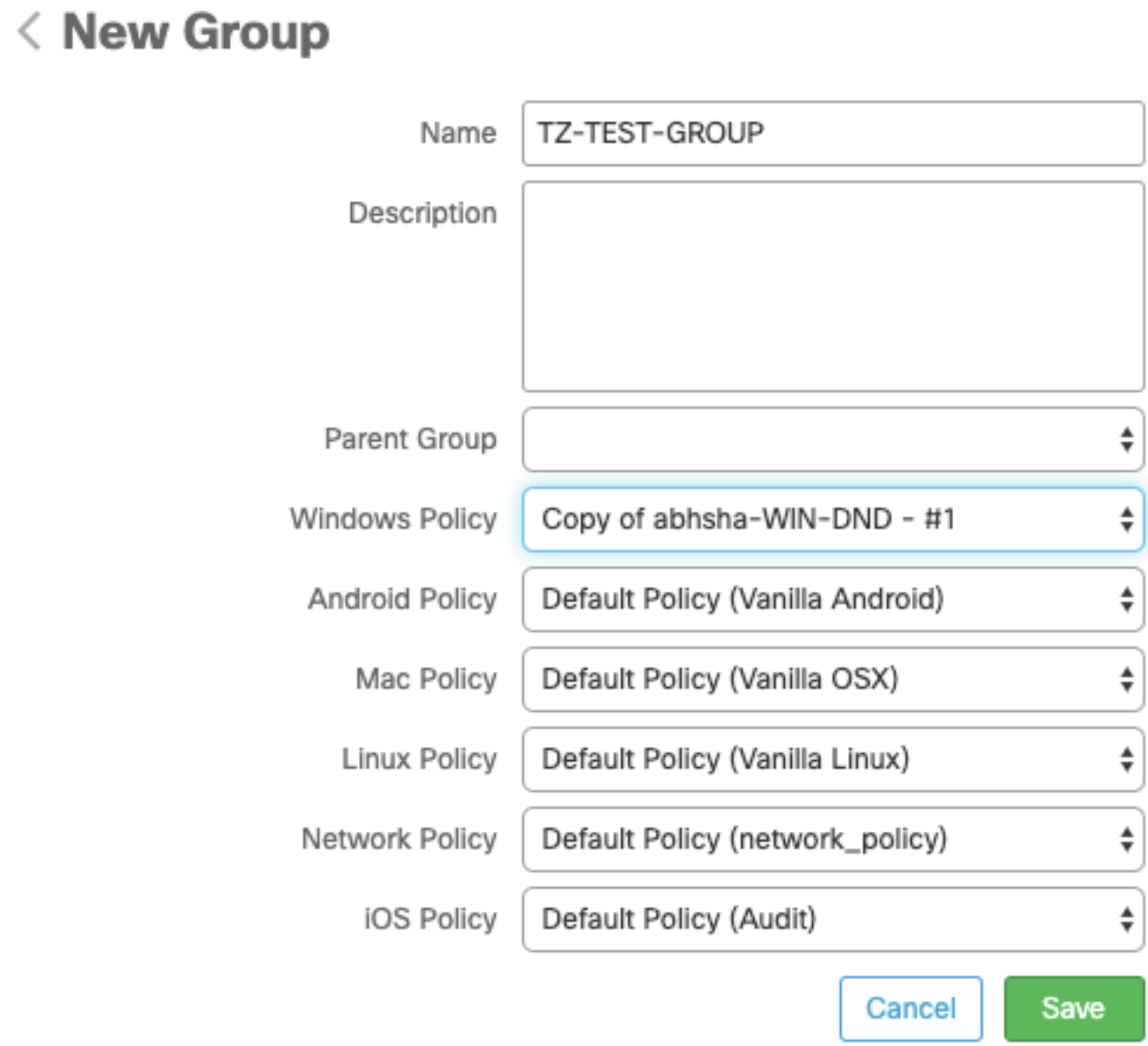


Passaggio 9. Per salvare il criterio, fare clic sul pulsante **Salva**.

Passaggio 10. Passare a **Gestione > Gruppi** e creare un nuovo gruppo.

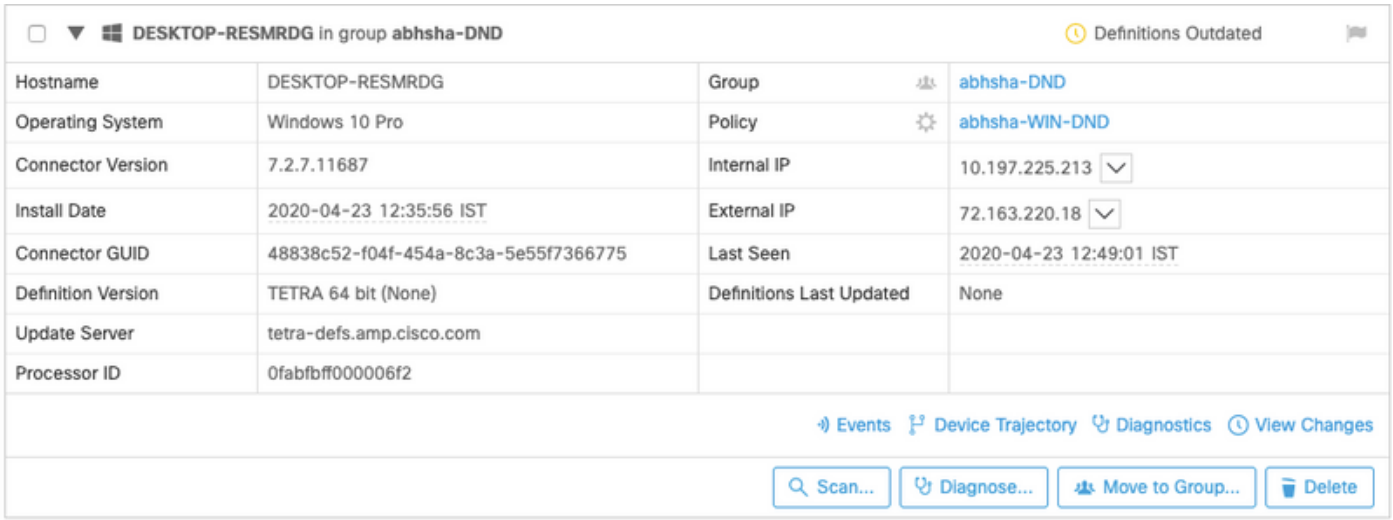


Passaggio 11. Immettere un nome di gruppo e selezionare il **criterio Windows** come criterio modificato in precedenza. Fare clic sul pulsante **Save** (Salva) come mostrato nell'immagine.



Passaggio 12. Passare a **Gestione > Computer** e cercare il computer in cui si tenta di disinstallare il connettore AMP.

Passaggio 13. Espandere il computer e fare clic su **Sposta nel gruppo**. Nella finestra di dialogo visualizzata, selezionare il gruppo creato in precedenza.



Passaggio 14. Attendere che il criterio venga aggiornato sull'endpoint. In genere sono necessari da 30 minuti a 1 ora e dipende dall'intervallo configurato.

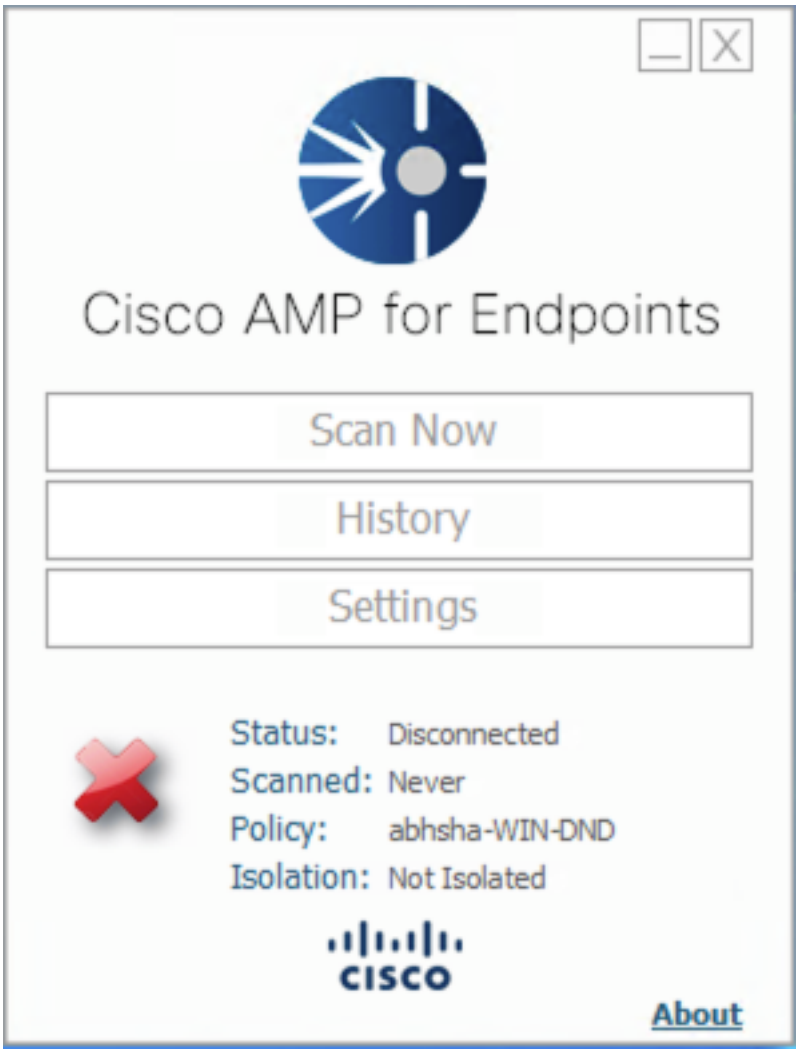
Passaggio 15. Dopo aver aggiornato il criterio sull'endpoint, sarà possibile disinstallare il connettore utilizzando la nuova password configurata.

Connettore disconnesso

Se il connettore è disconnesso dal cloud AMP, è importante poter avviare il computer in modalità provvisoria.

Passaggio 1. Fare clic sull'icona nell'area di notifica e aprire Cisco AMP for Endpoints Connector.

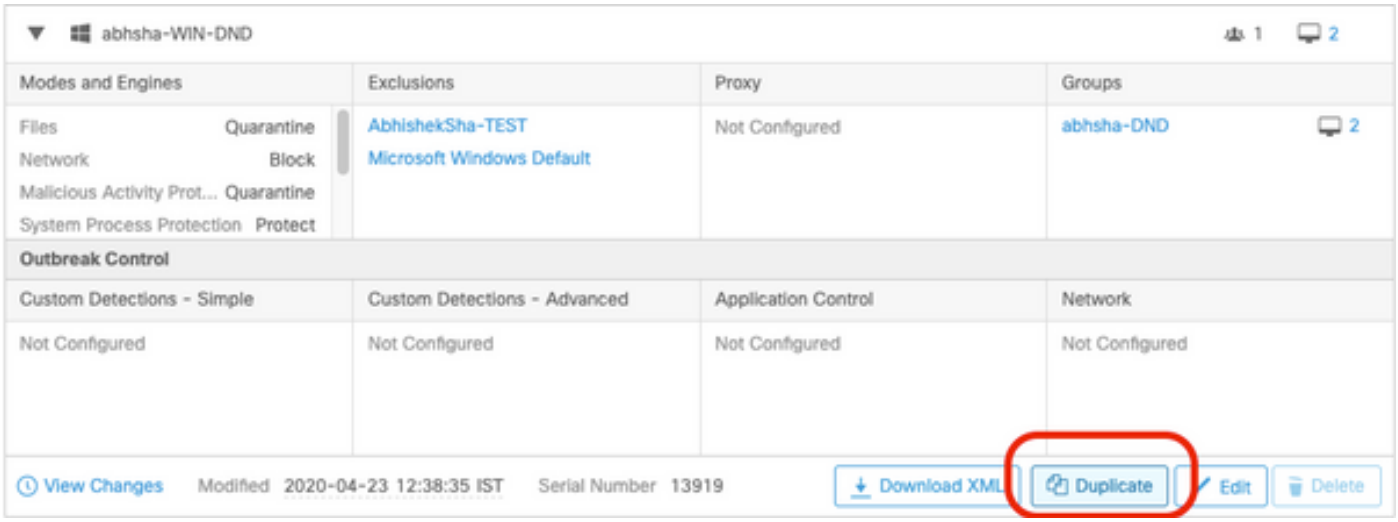
Passaggio 2. Verificare che il connettore sia indicato come disconnesso.



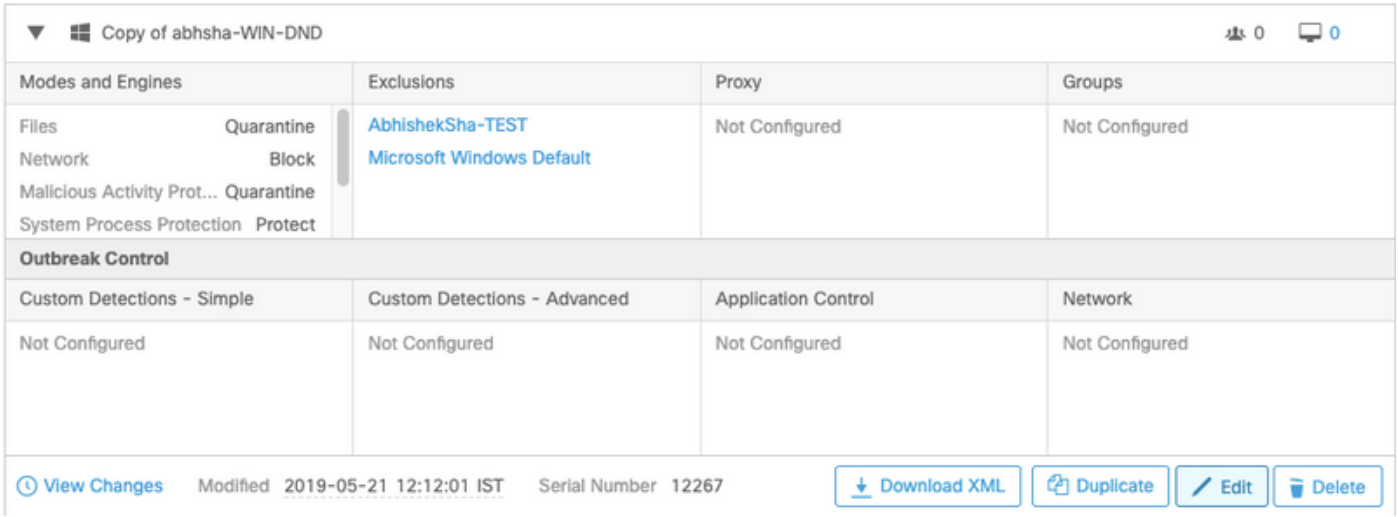
Passaggio 3. Annotare il criterio assegnato al connettore.

Passaggio 4. Passare alla console AMP for Endpoints e cercare il criterio annotato in precedenza.

Passaggio 5. Espandere il criterio e fare clic su **Duplica**, come mostrato nell'immagine.

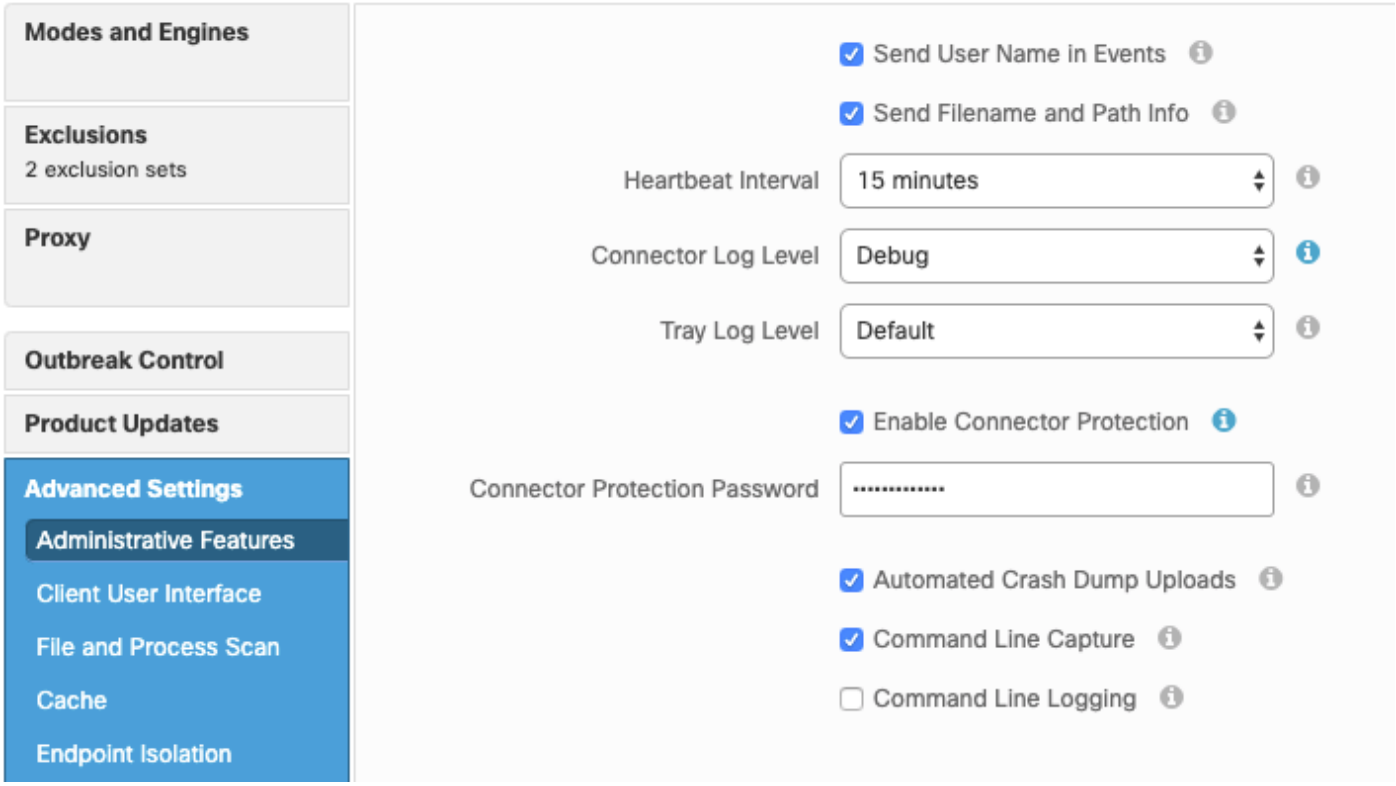


Passaggio 6. Una nuova regola denominata "Copia di..." verrà creato. Fare clic su **Modifica** per modificare il criterio.



Passaggio 7. Nella pagina Modifica criterio, passare a **Impostazioni avanzate > Funzioni amministrative**.

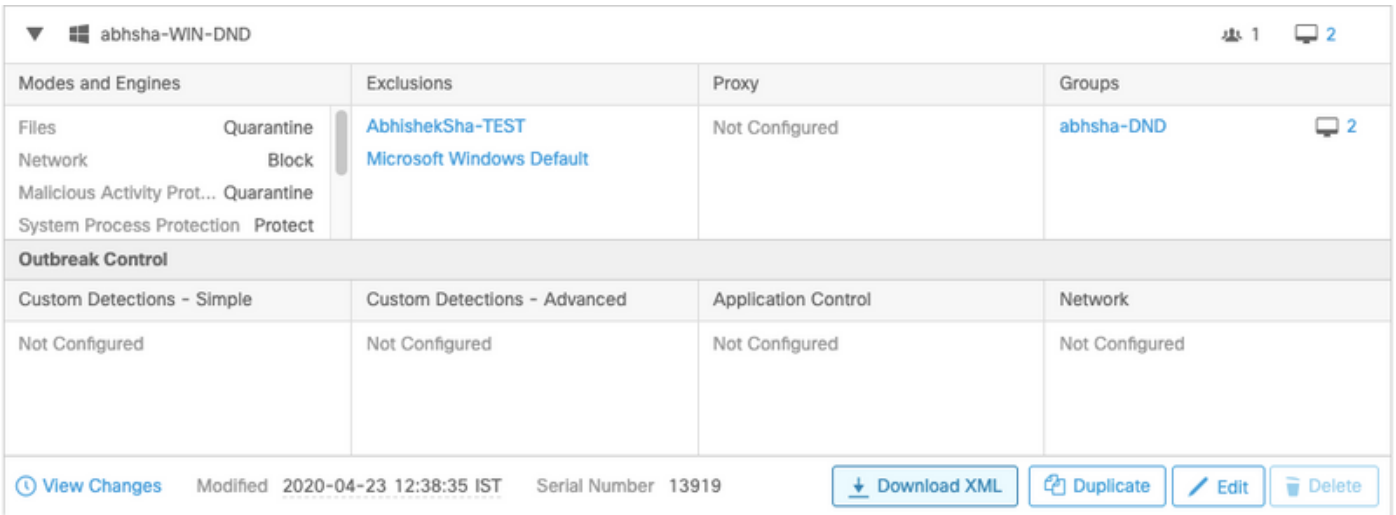
Passaggio 8. Nel campo **Connector Password Protection** (Protezione password connettore), sostituire la password con una nuova che possa essere richiamata.



Passaggio 9. Per salvare il criterio, fare clic sul pulsante **Salva**.

Passaggio 10. Passare a **Gestione > Criteri** e cercare il criterio appena duplicato.

Passaggio 11. Espandere il criterio e fare clic su **Scarica XML.** Un file denominato **policy.xml** verrà salvato nel computer.

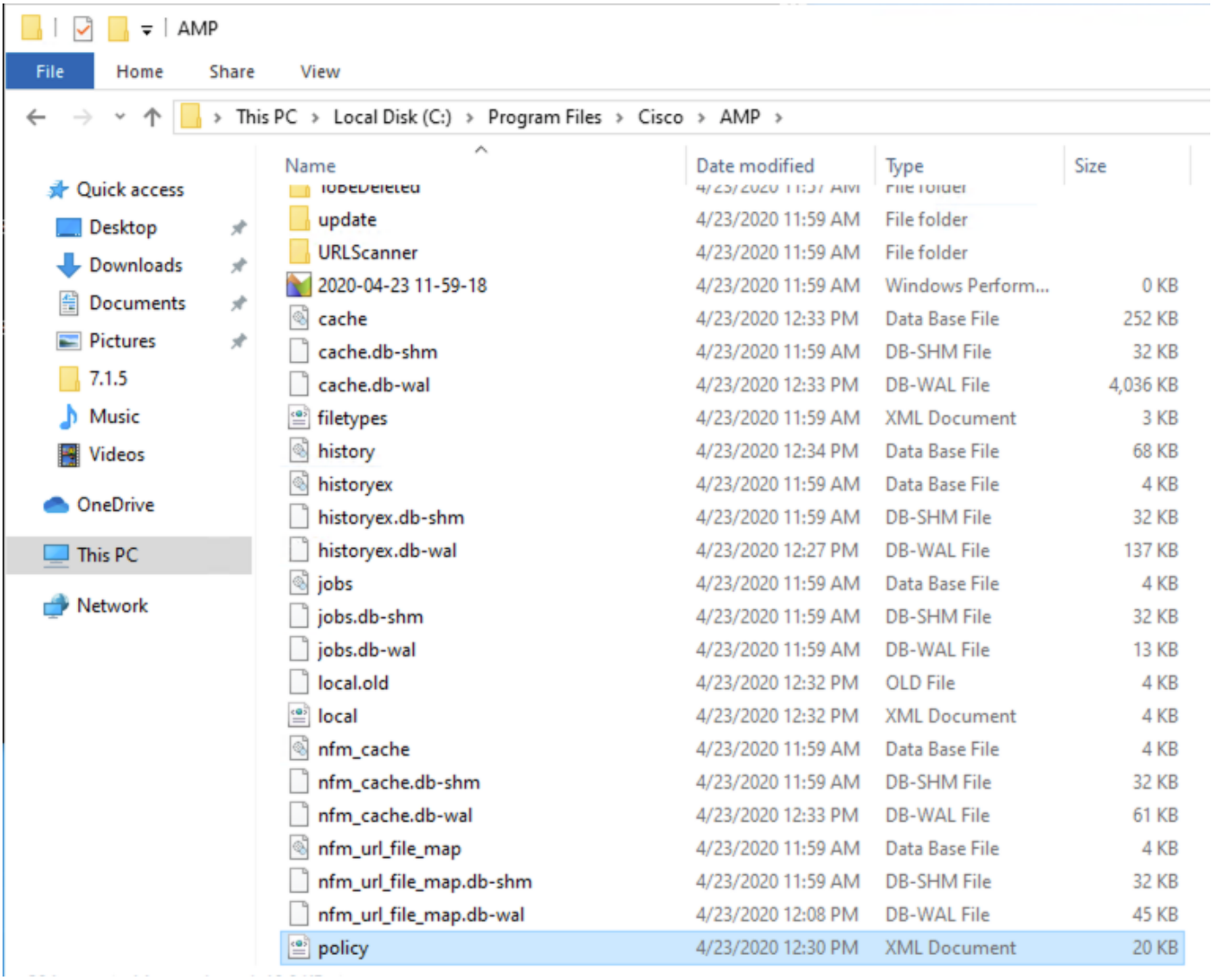


Passaggio 12. Copiare il file **policy.xml** nell'endpoint interessato.

Passaggio 13. Riavviare l'endpoint interessato in **modalità provvisoria**.

Passaggio 14. Quando l'endpoint interessato è in **modalità provvisoria**, passare a **C:\Program Files\Cisco\AMP**.

Passaggio 15. In questa cartella, cercare un file denominato **policy.xml** e rinominarlo in **policy_old.xml**.



Passaggio 16. Incollare il file **policy.xml** copiato in precedenza in questa cartella.

Passaggio 17. Dopo aver copiato il file, è possibile eseguire la disinstallazione normalmente e, quando viene richiesta la password, è necessario immettere la nuova password configurata.

Passaggio 18. Questo passaggio è facoltativo. Poiché il connettore è stato disinstallato quando il computer è stato disconnesso, la voce relativa al computer rimarrà sulla console. È quindi possibile passare a **Gestione > Computer** ed espandere l'endpoint interessato. Per eliminare l'endpoint, fare clic su **Delete**.