

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

Sommario

[Introduzione](#)

[Connettore connesso](#)

[Connettore disconnesso](#)

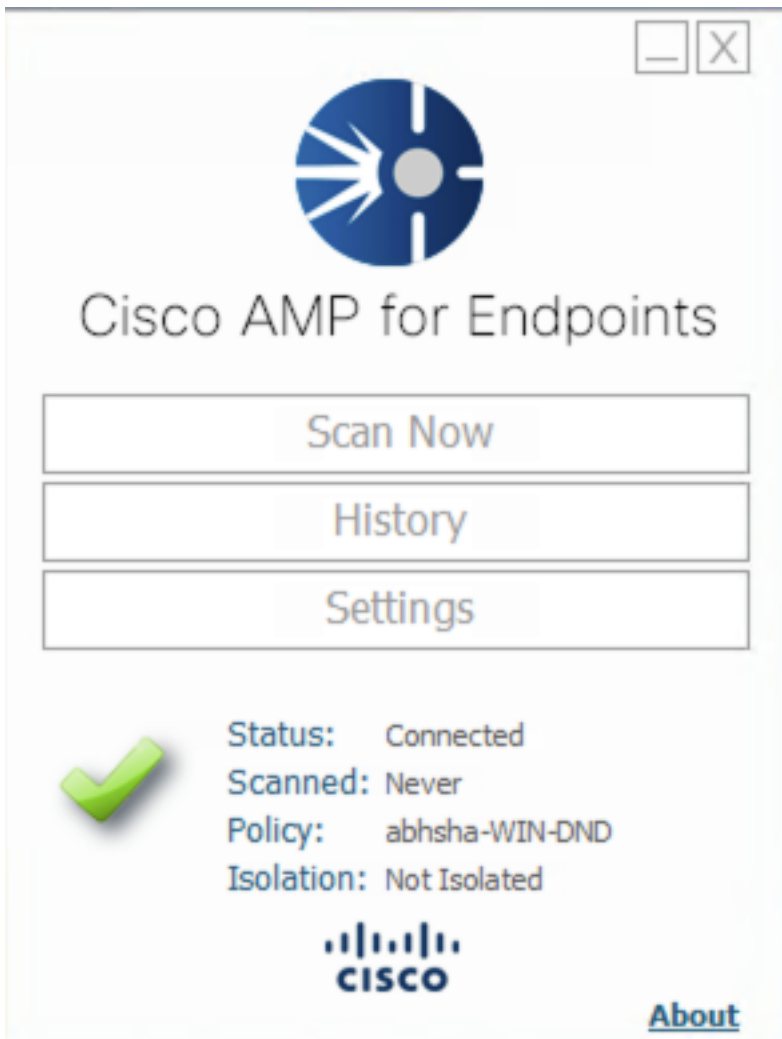
Introduzione

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.

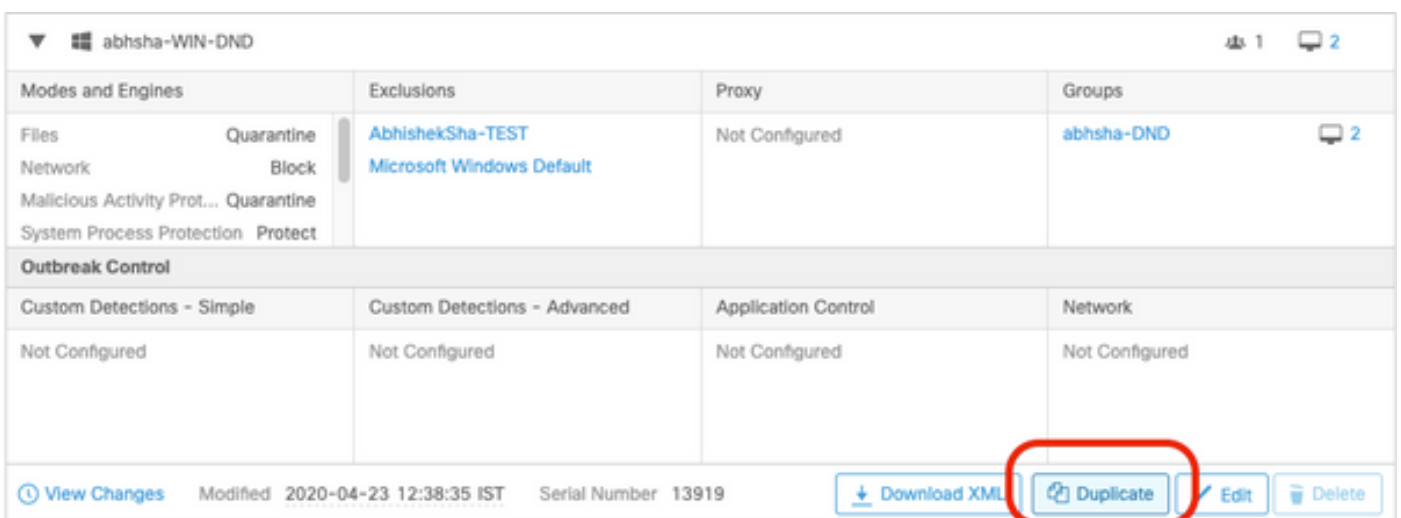
Passaggio 2. Verificare che il connettore sia indicato come connesso.



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.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced	Application Control	Network
Not Configured		Not Configured	Not Configured	Not Configured

[View Changes](#) Modified 2019-05-21 12:12:01 IST Serial Number 12267
 [Download XML](#) [Duplicate](#) [Edit](#) [Delete](#)

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.

Modes and Engines

Exclusions
2 exclusion sets

Proxy

Outbreak Control

Product Updates

Advanced Settings

- Administrative Features
- Client User Interface
- File and Process Scan
- Cache
- Endpoint Isolation

Send User Name in Events i

Send Filename and Path Info i

Heartbeat Interval: i

Connector Log Level: i

Tray Log Level: i

Enable Connector Protection i

Connector Protection Password: i

Automated Crash Dump Uploads i

Command Line Capture i

Command Line Logging i

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

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

Groups [View All Changes](#)

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.

< New Group

Name	<input type="text" value="TZ-TEST-GROUP"/>
Description	<input type="text"/>
Parent Group	<input type="text"/>
Windows Policy	<input type="text" value="Copy of abhsha-WIN-DND - #1"/>
Android Policy	<input type="text" value="Default Policy (Vanilla Android)"/>
Mac Policy	<input type="text" value="Default Policy (Vanilla OSX)"/>
Linux Policy	<input type="text" value="Default Policy (Vanilla Linux)"/>
Network Policy	<input type="text" value="Default Policy (network_policy)"/>
iOS Policy	<input type="text" value="Default Policy (Audit)"/>

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.

DESKTOP-RESMRDG in group abhsha-DND		Definitions Outdated	
Hostname	DESKTOP-RESMRDG	Group	abhsha-DND
Operating System	Windows 10 Pro	Policy	abhsha-WIN-DND
Connector Version	7.2.7.11687	Internal IP	10.197.225.213
Install Date	2020-04-23 12:35:56 IST	External IP	72.163.220.18
Connector GUID	48838c52-f04f-454a-8c3a-5e55f7366775	Last Seen	2020-04-23 12:49:01 IST
Definition Version	TETRA 64 bit (None)	Definitions Last Updated	None
Update Server	tetra-defs.amp.cisco.com		
Processor ID	0fabfbff000006f2		
Events Device Trajectory Diagnostics View Changes			
<input type="button" value="Scan..."/> <input type="button" value="Diagnose..."/> <input type="button" value="Move to Group..."/> <input type="button" value="Delete"/>			

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.

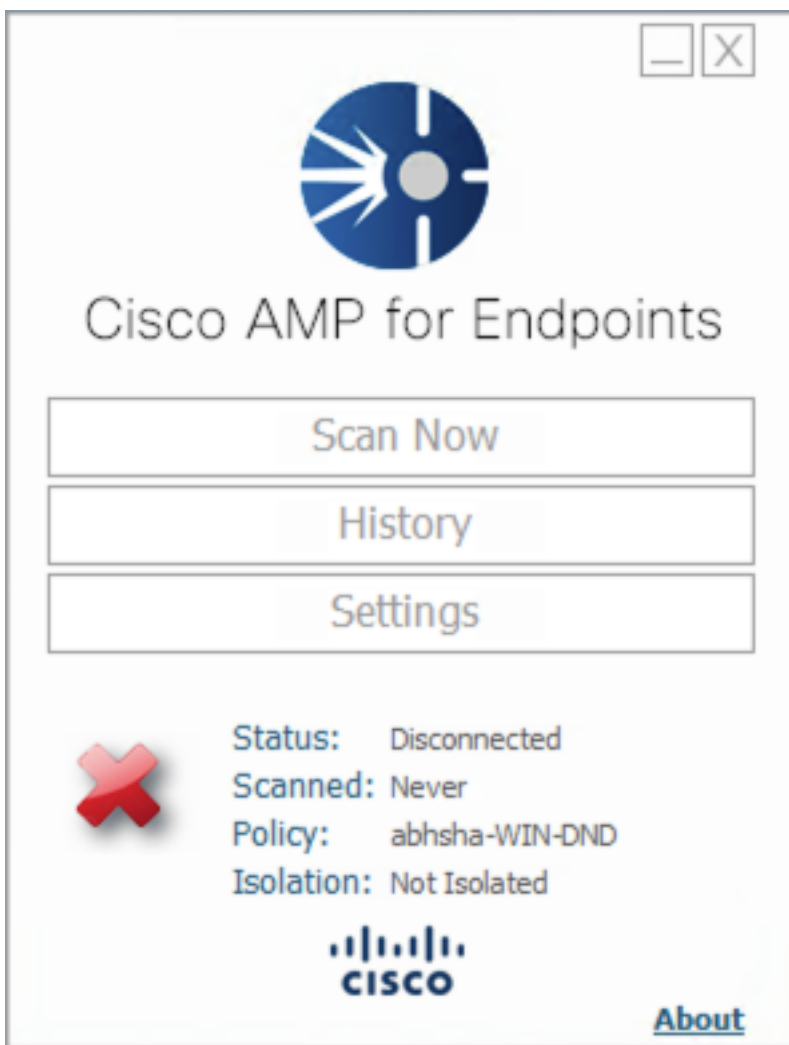
Passaggio 15. Dopo aver aggiornato il criterio sull'endpoint, sarà possibile disinstallare il connettore utilizzando la nuova password configurata.

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.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	abhsha-DND 2
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced		Network
Not Configured		Not Configured		Not Configured

[View Changes](#) Modified 2020-04-23 12:38:35 IST Serial Number 13919
 [Download XML](#)

[Duplicate](#)
[Edit](#)
[Delete](#)

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

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Malicious Activity Prot...	Quarantine			
System Process Protection	Protect			
Outbreak Control				
Custom Detections - Simple		Custom Detections - Advanced		Network
Not Configured		Not Configured		Not Configured

[View Changes](#) Modified 2019-05-21 12:12:01 IST Serial Number 12267
 [Download XML](#)
[Duplicate](#)
[Edit](#)
[Delete](#)

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.

The screenshot shows the configuration page for 'Advanced Settings' under 'Administrative Features'. The left sidebar lists various settings categories: Modes and Engines, Exclusions (2 exclusion sets), Proxy, Outbreak Control, Product Updates, and Advanced Settings (selected). Under 'Advanced Settings', 'Administrative Features' is selected, with sub-options: Client User Interface, File and Process Scan, Cache, and Endpoint Isolation.

The main configuration area includes the following settings:

- Send User Name in Events *i*
- Send Filename and Path Info *i*
- Heartbeat Interval: 15 minutes *i*
- Connector Log Level: Debug *i*
- Tray Log Level: Default *i*
- Enable Connector Protection *i*
- Connector Protection Password: *i*
- Automated Crash Dump Uploads *i*
- Command Line Capture *i*
- Command Line Logging *i*

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.

The screenshot shows a table of criteria for the endpoint 'abhsa-WIN-DND'. The table has four columns: Modes and Engines, Exclusions, Proxy, and Groups. The 'Exclusions' column is expanded to show 'AbhishekSha-TEST' and 'Microsoft Windows Default'. The 'Groups' column shows 'abhsa-DND' with a notification icon and the number '2'.

Modes and Engines	Exclusions	Proxy	Groups
Files Network Malicious Activity Prot... System Process Protection	Quarantine Block Quarantine Protect	Not Configured	abhsa-DND <i>i</i> 2
Outbreak Control			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured

At the bottom of the table, there is a status bar with the following information:

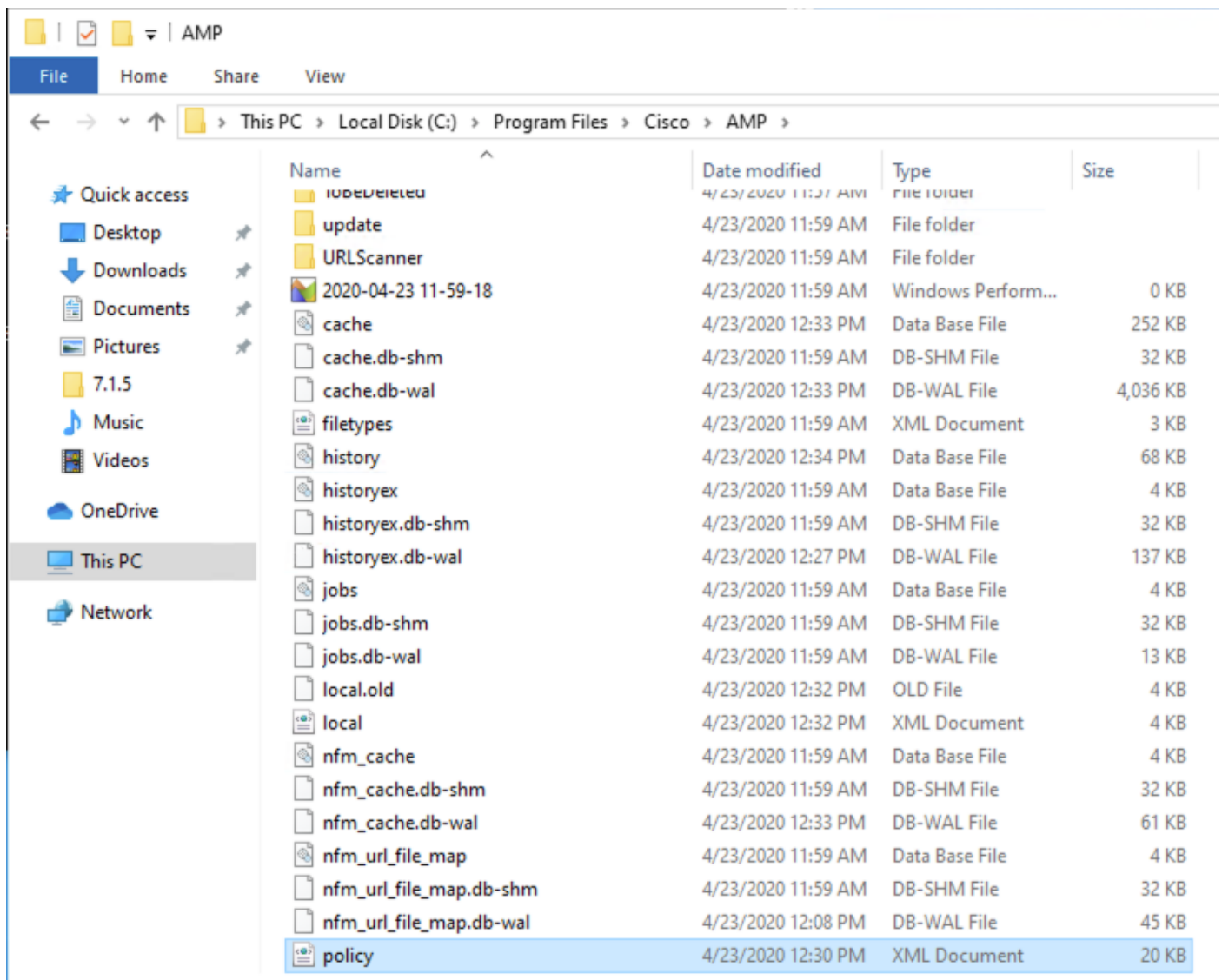
- [View Changes](#)
- Modified 2020-04-23 12:38:35 IST
- Serial Number 13919
- [Download XML](#)
- [Duplicate](#)
- [Edit](#)
- [Delete](#)

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**.