

# Procédure de désinstallation du connecteur AMP si le mot de passe est oublié

## Contenu

[Introduction](#)

[Connecteur connecté](#)

[Le connecteur est déconnecté](#)

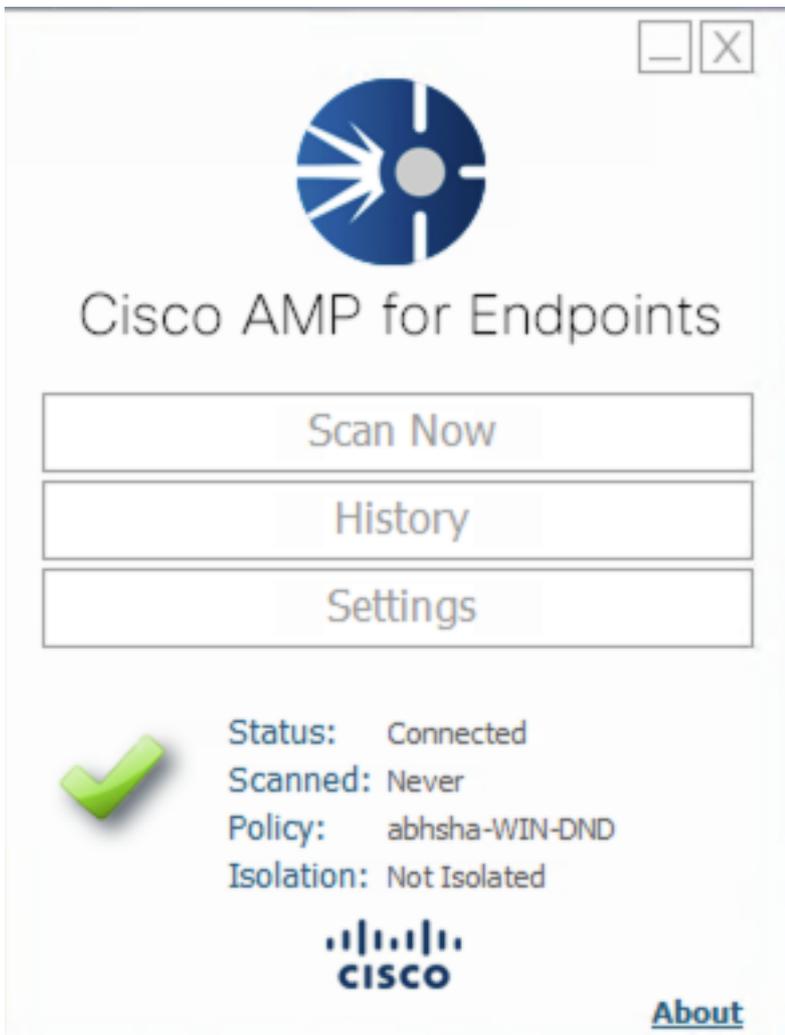
## Introduction

Ce document décrit la procédure de désinstallation du connecteur Advanced Malware Protection (AMP) de Cisco au cas où la désinstallation serait bloquée par la fonction de protection du connecteur qui nécessite un mot de passe pour être fourni et que ce mot de passe est oublié. Il y a 2 scénarios dans ce cas, et cela dépend de si le connecteur indique « Connecté » au cloud AMP. Il s'applique uniquement au système d'exploitation Windows, car Connector Protection est une fonctionnalité disponible uniquement sur le système d'exploitation Windows.

## Connecteur connecté

Étape 1. Cliquez sur l'icône de la barre d'état et ouvrez le connecteur Cisco AMP for Endpoints.

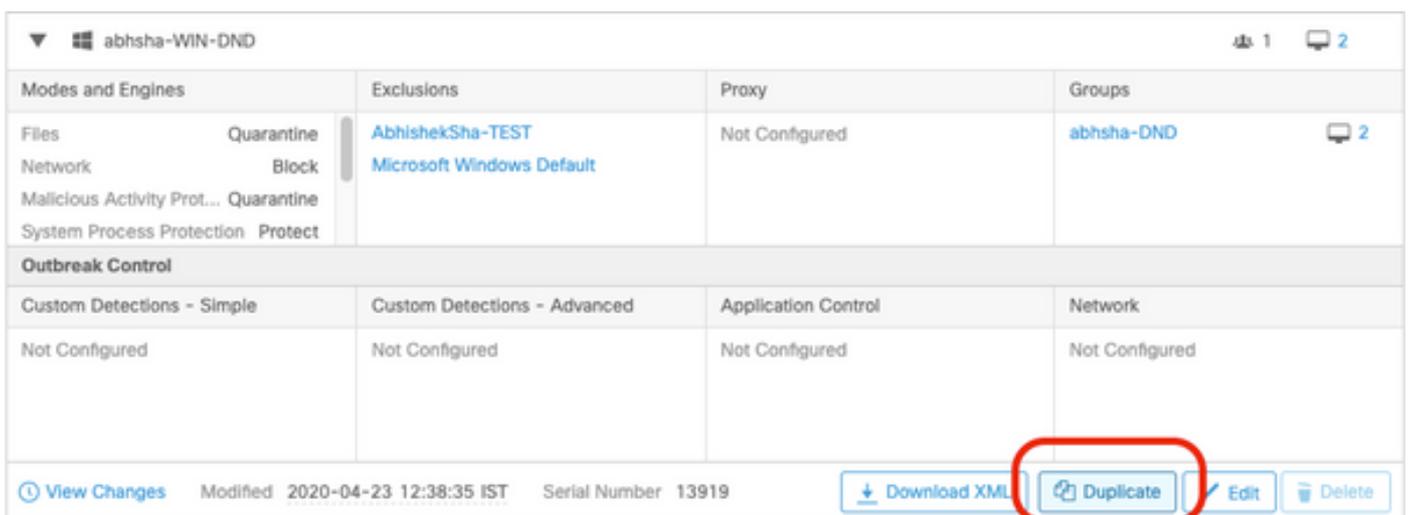
Étape 2. Assurez-vous que le connecteur est indiqué comme étant connecté.



Étape 3. Notez que la stratégie a été affectée à ce connecteur.

Étape 4. Accédez à la console AMP for Endpoints et recherchez la stratégie précédemment notée.

Étape 5. Développez la stratégie et cliquez sur **Dupliquer** comme indiqué dans l'image.



Étape 6. Une nouvelle stratégie appelée « Copie de... » sera créé. Cliquez sur **Modifier** afin de modifier cette stratégie comme indiqué dans l'image.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	Not Configured
Network	Block	Microsoft Windows Default		
Mallicious 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](#)

Étape 7. À la page **Modifier la stratégie**, accédez à **Paramètres avancés > Fonctions administratives**.

Étape 8. Dans le champ **Protection par mot de passe du connecteur**, remplacez le mot de passe par un nouveau mot de passe qui peut être rappelé comme indiqué dans l'image.

**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

Étape 9. Cliquez sur le bouton **Enregistrer** afin d'enregistrer cette stratégie.

Étape 10. Accédez à **Management > Groups** et créez un nouveau groupe.

**Groups** [View All Changes](#)

Étape 11. Entrez un nom de groupe et sélectionnez la **stratégie Windows** comme stratégie précédemment modifiée. Cliquez sur le bouton **Enregistrer** comme indiqué dans l'image.

## < 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)"/>

Étape 12. Accédez à **Management > Computers** et recherchez l'ordinateur sur lequel vous essayez de désinstaller le connecteur AMP.

Étape 13. Développez l'ordinateur et cliquez sur **Déplacer vers le groupe**. Dans la boîte de dialogue qui s'affiche, sélectionnez le groupe précédemment créé.

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](#)

Étape 14. Attendez que la stratégie soit mise à jour sur le point de terminaison. Cela prend généralement entre 30 minutes et 1 heure et dépend de l'intervalle configuré.

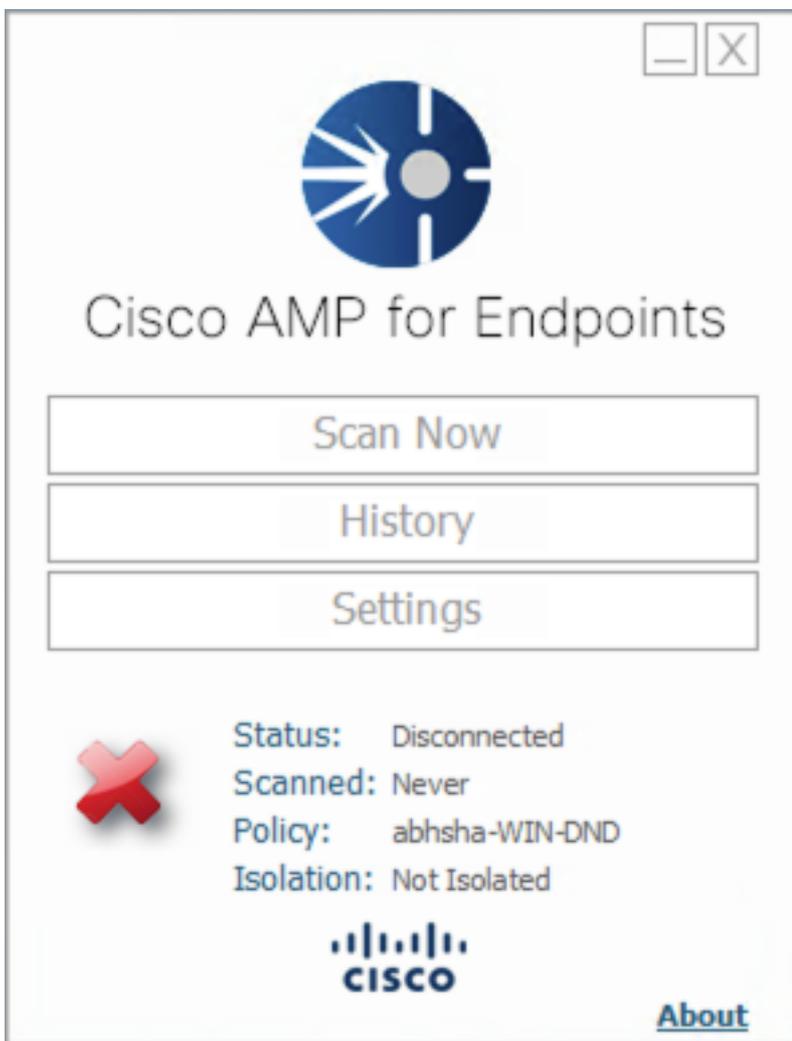
Étape 15. Une fois la stratégie mise à jour sur le point d'extrémité, vous pourrez désinstaller le connecteur à l'aide du mot de passe que vous venez de configurer.

## Le connecteur est déconnecté

Si le connecteur est déconnecté du cloud AMP, il est important de pouvoir démarrer l'ordinateur en mode sans échec.

Étape 1. Cliquez sur l'icône de la barre d'état et ouvrez le connecteur Cisco AMP for Endpoints.

Étape 2. Vérifiez que le connecteur est déconnecté.



Étape 3. Notez la stratégie affectée à ce connecteur.

Étape 4. Accédez à la console AMP for Endpoints et recherchez la stratégie précédemment notée.

Étape 5. Développez la stratégie et cliquez sur **Dupliquer** comme indiqué dans l'image.

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	abhsa-DND
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 2020-04-23 12:38:35 IST Serial Number 13919
 [Download XML](#)

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

Étape 6. Une nouvelle stratégie appelée « Copie de... » sera créé. Cliquez sur **Modifier** pour modifier cette stratégie.

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](#)

Étape 7. À la page Modifier la stratégie, accédez à **Paramètres avancés > Fonctions administratives**.

Étape 8. Dans le champ **Connector Password Protection**, remplacez le mot de passe par un nouveau mot de passe qui peut être rappelé.

<b>Modes and Engines</b>	<input checked="" type="checkbox"/> Send User Name in Events <span>i</span>
<b>Exclusions</b> 2 exclusion sets	<input checked="" type="checkbox"/> Send Filename and Path Info <span>i</span>
<b>Proxy</b>	Heartbeat Interval: 15 minutes <span>i</span>
<b>Outbreak Control</b>	Connector Log Level: Debug <span>i</span>
<b>Product Updates</b>	Tray Log Level: Default <span>i</span>
<b>Advanced Settings</b>	<input checked="" type="checkbox"/> Enable Connector Protection <span>i</span>
<b>Administrative Features</b>	Connector Protection Password: .....
Client User Interface	<input checked="" type="checkbox"/> Automated Crash Dump Uploads <span>i</span>
File and Process Scan	<input checked="" type="checkbox"/> Command Line Capture <span>i</span>
Cache	<input type="checkbox"/> Command Line Logging <span>i</span>
Endpoint Isolation	

Étape 9. Cliquez sur le bouton **Enregistrer** afin d'enregistrer cette stratégie.

Étape 10. Accédez à **Management > Politiques** et recherchez la stratégie qui a été dupliquée.

Étape 11. Développez la stratégie et cliquez sur **Télécharger le fichier XML**. Un fichier nommé **policy.xml** sera enregistré sur votre ordinateur.

abhsa-WIN-DND <span>1</span> <span>2</span>			
Modes and Engines	Exclusions	Proxy	Groups
Files Network Malicious Activity Prot... System Process Protection	Quarantine Block Quarantine Protect	Not Configured	abhsa-DND <span>2</span>
<b>Outbreak Control</b>			
Custom Detections - Simple	Custom Detections - Advanced	Application Control	Network
Not Configured	Not Configured	Not Configured	Not Configured
<a href="#">View Changes</a> Modified 2020-04-23 12:38:35 IST Serial Number 13919		<a href="#">Download XML</a>	<a href="#">Duplicate</a> <a href="#">Edit</a> <a href="#">Delete</a>

Étape 12. Copiez ce **policy.xml** sur le point de terminaison affecté.

Étape 13. Redémarrez le point de terminaison affecté en **mode sans échec**.

Étape 14. Une fois le point de terminaison affecté en **mode sans échec**, accédez à **C:\Program Files\Cisco\AMP**.

Étape 15. Dans ce dossier, recherchez un fichier nommé **policy.xml** et renommez-le **policy\_old.xml**.

Name	Date modified	Type	Size
update	4/23/2020 11:59 AM	File folder	
URLScanner	4/23/2020 11:59 AM	File folder	
2020-04-23 11-59-18	4/23/2020 11:59 AM	Windows Perform...	0 KB
cache	4/23/2020 12:33 PM	Data Base File	252 KB
cache.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
cache.db-wal	4/23/2020 12:33 PM	DB-WAL File	4,036 KB
filetypes	4/23/2020 11:59 AM	XML Document	3 KB
history	4/23/2020 12:34 PM	Data Base File	68 KB
historyex	4/23/2020 11:59 AM	Data Base File	4 KB
historyex.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
historyex.db-wal	4/23/2020 12:27 PM	DB-WAL File	137 KB
jobs	4/23/2020 11:59 AM	Data Base File	4 KB
jobs.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
jobs.db-wal	4/23/2020 11:59 AM	DB-WAL File	13 KB
local.old	4/23/2020 12:32 PM	OLD File	4 KB
local	4/23/2020 12:32 PM	XML Document	4 KB
nfm_cache	4/23/2020 11:59 AM	Data Base File	4 KB
nfm_cache.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
nfm_cache.db-wal	4/23/2020 12:33 PM	DB-WAL File	61 KB
nfm_url_file_map	4/23/2020 11:59 AM	Data Base File	4 KB
nfm_url_file_map.db-shm	4/23/2020 11:59 AM	DB-SHM File	32 KB
nfm_url_file_map.db-wal	4/23/2020 12:08 PM	DB-WAL File	45 KB
policy	4/23/2020 12:30 PM	XML Document	20 KB

Étape 16. Maintenant, collez le fichier **policy.xml** précédemment copié dans ce dossier.

Étape 17. Une fois le fichier copié, la désinstallation peut être effectuée normalement et à l'invite du mot de passe, le mot de passe nouvellement configuré doit être entré.

Étape 18. Il s'agit d'une étape facultative. Comme le connecteur a été désinstallé lors de la déconnexion de la machine, l'entrée de l'ordinateur reste sur la console. Par conséquent, vous pouvez accéder à **Management > Computers** et développer le point de terminaison affecté. Cliquez sur **Supprimer** afin de supprimer le point de terminaison.