

# 忘記密碼時解除安裝AMP聯結器的過程

## 目錄

[簡介](#)

[聯結器已連線](#)

[聯結器已斷開](#)

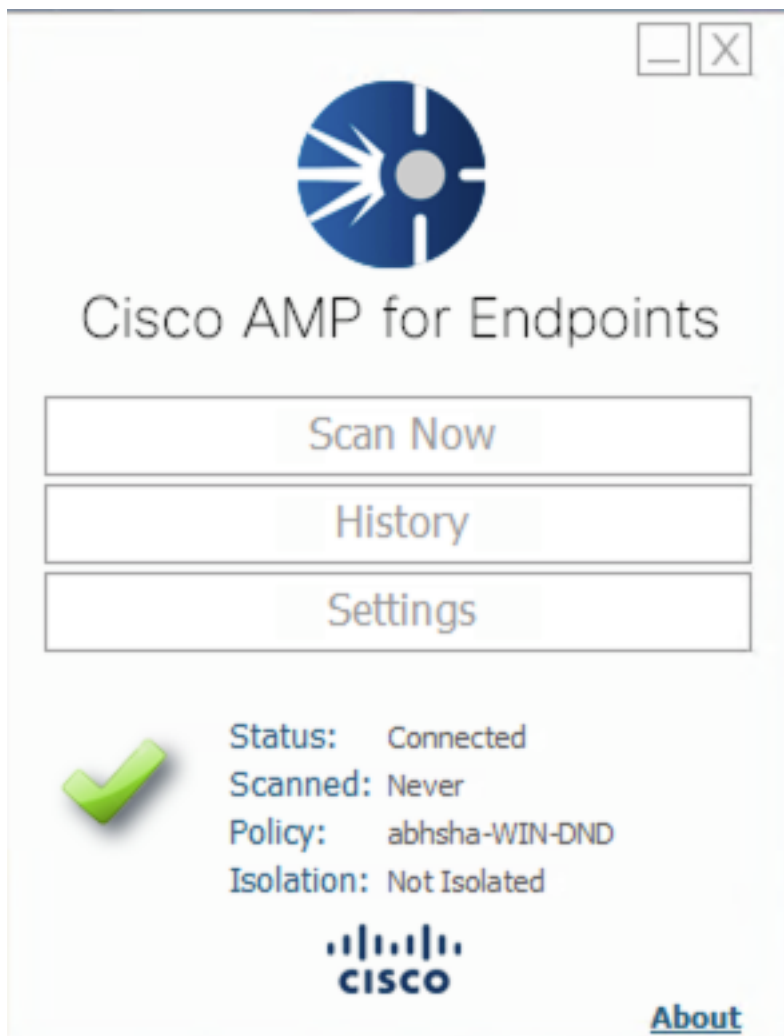
## 簡介

本檔案介紹在聯結器保護功能阻止解除安裝的情況下解除安裝Cisco Advanced Malware Protection(AMP)聯結器的步驟，該功能要求提供密碼，但忘記了密碼。此案例有兩種情況，具體取決於聯結器是否顯示「已連線」到AMP雲。它僅適用於Windows作業系統，因為聯結器保護是一項僅在Windows作業系統上可用的功能。

## 聯結器已連線

步驟1.按一下托盤圖示並開啟面向終端的思科AMP的終端聯結器。

步驟2.確保聯結器顯示為已連線。



步驟3.請注意，該策略已分配給該連結器。

步驟4.導航到面向終端的AMP控制檯並搜尋之前記錄的策略。

步驟5.展開原則並按一下Duplicate，如下圖所示。

The screenshot shows the configuration page for a policy named 'abhsha-WIN-DND'. The interface is divided into several sections: 'Modes and Engines', 'Exclusions', 'Proxy', and 'Groups'. The 'Exclusions' section lists 'AbhishekSha-TEST' and 'Microsoft Windows Default'. The 'Proxy' section is 'Not Configured'. The 'Groups' section lists 'abhsha-DND'. Below these sections is the 'Outbreak Control' section, which includes 'Custom Detections - Simple', 'Custom Detections - Advanced', 'Application Control', and 'Network'. At the bottom of the page, there are several buttons: 'View Changes', 'Download XML', 'Duplicate', 'Edit', and 'Delete'. The 'Duplicate' button is highlighted with a red circle.

步驟6.名為「副本.....」的新策略 將被建立。按一下「Edit」以編輯此原則，如下圖所示。

The screenshot shows the configuration page for a policy named 'Copy of abhsha-WIN-DND'. The interface is divided into several sections: 'Modes and Engines', 'Exclusions', 'Proxy', and 'Groups'. The 'Exclusions' section lists 'AbhishekSha-TEST' and 'Microsoft Windows Default'. The 'Proxy' section is 'Not Configured'. The 'Groups' section is 'Not Configured'. Below these sections is the 'Outbreak Control' section, which includes 'Custom Detections - Simple', 'Custom Detections - Advanced', 'Application Control', and 'Network'. At the bottom of the page, there are several buttons: 'View Changes', 'Download XML', 'Duplicate', 'Edit', and 'Delete'. The 'Edit' button is highlighted with a red circle.

步驟7.在Edit Policy頁面中，導覽至Advanced Settings > Administrative Features.

步驟8.在Connector Password Protection欄位中，將密碼替換為可以重新呼叫的新密碼，如下圖所示。

**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 ⓘ

Send Filename and Path Info ⓘ

Heartbeat Interval: 15 minutes ⓘ

Connector Log Level: Debug ⓘ

Tray Log Level: Default ⓘ

Enable Connector Protection ⓘ

Connector Protection Password: .....

Automated Crash Dump Uploads ⓘ

Command Line Capture ⓘ

Command Line Logging ⓘ

步驟9.按一下**Save**按鈕以儲存此原則。

步驟10.定位至**管理>組**，然後建立新組。

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

Search

步驟11.輸入組名稱，然後選擇**Windows策略**作為先前編輯的策略。按一下「**Save**」按鈕，如下圖所示。

## < 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)"/>

步驟12.導覽至Management > Computers，然後搜尋嘗試解除安裝AMP聯結器的電腦。

步驟13.展開電腦，然後按一下**移動到組**。從出現的對話方塊中，選擇先前建立的「組」。

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](#)

步驟14.等待終端上更新策略。此過程通常需要30分鐘到1小時，具體取決於配置的時間間隔。

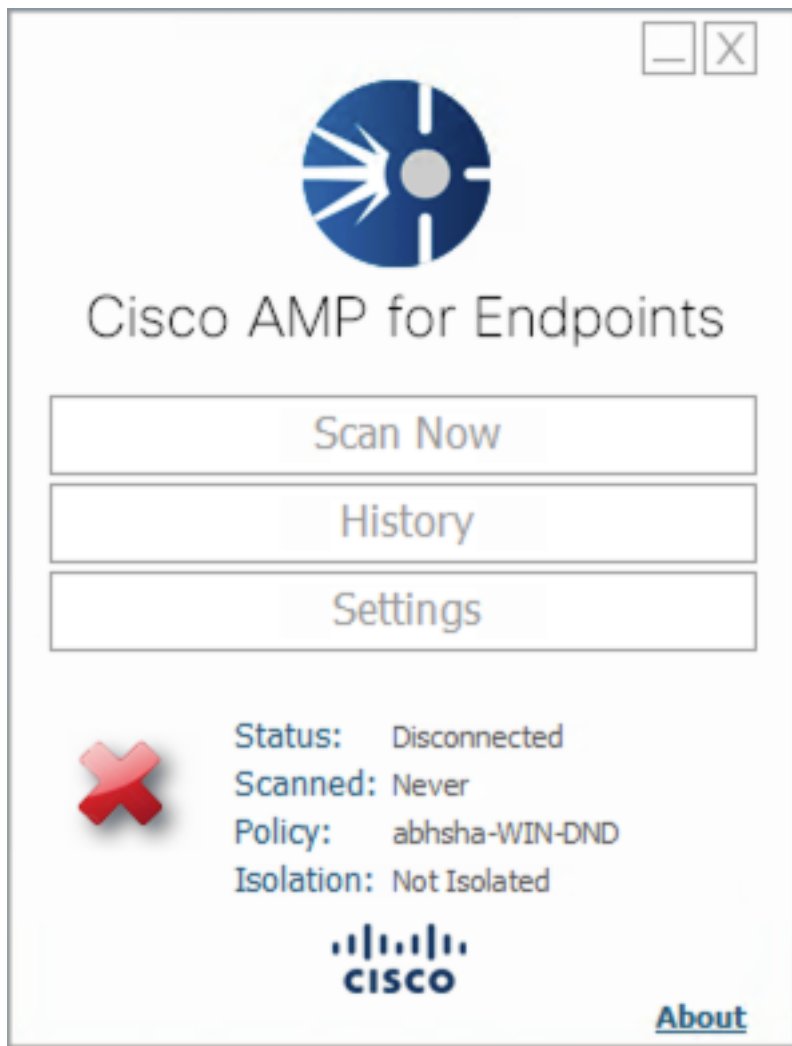
步驟15.在端點上更新策略後，您就可以使用新配置的密碼解除安裝聯結器。

## 聯結器已斷開

如果聯結器與AMP雲端斷開連線，則能夠在安全模式下啟動電腦非常重要。

步驟1.按一下托盤圖示並開啟面向終端的思科AMP的終端聯結器。

步驟2.確保聯結器顯示為已斷開連線。



步驟3.注意已分配給該聯結器的策略。

步驟4.導航到面向終端的AMP控制檯並搜尋之前記錄的策略。

步驟5.展開原則並按一下**Duplicate**，如下圖所示。

Modes and Engines		Exclusions	Proxy	Groups
Files	Quarantine	AbhishekSha-TEST	Not Configured	abhsa-DND <span>2</span>
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](#)

步驟6.名為「副本.....」的新策略 將被建立。按一下**Edit**以編輯此策略。

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](#)

步驟7.在Edit Policy頁面，導航到**Advanced Settings > Administrative Features**。

步驟8.在**Connector Password Protection**欄位中，將密碼替換為可以重新呼叫的新密碼。

<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	

步驟9.按一下**Save**按鈕以儲存此原則。

步驟10.定位至**管理>策略**，然後搜尋新複製的策略。

步驟11.展開策略並按一下**下載XML**。名為policy.xml的檔案將儲存到您的電腦。

abhsa-WIN-DND <span>1</span> <span>2</span>			
<b>Modes and Engines</b>	<b>Exclusions</b>	<b>Proxy</b>	<b>Groups</b>
Files: Quarantine Network: Block Malicious Activity Prot...: Quarantine System Process Protection: Protect	AbhishekSha-TEST Microsoft Windows Default	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
View Changes Modified 2020-04-23 12:38:35 IST Serial Number 13919		Download XML	Duplicate Edit Delete

步驟12.將此policy.xml複製到受影響的終結點。

步驟13.在**Safe**模式下重新啟動受影響的終端。

步驟14.受影響的終端進入**安全模式**後，導航至C:\Program Files\Cisco\AMP。

步驟15.在此資料夾中，搜尋名為policy.xml的檔案，並將其重新命名為policy\_old.xml。

The screenshot shows a Windows File Explorer window with the following table of contents:

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

步驟16.現在，將先前複製的policy.xml貼上到此資料夾。

步驟17.複製檔案後，可以正常執行解除安裝操作，並且必須在密碼提示符下輸入新配置的密碼。

步驟18.這是可選步驟。由於連結器在電腦斷開連線時已被解除安裝，電腦條目將保留在控制檯上。因此，您可以導航到**管理>電腦**並展開受影響的終結點。按一下**Delete**以刪除端點。