

How to collect ProcMon logs to troubleshoot AMP issues at startup

Contents

[Introduction](#)

[Procedure:](#)

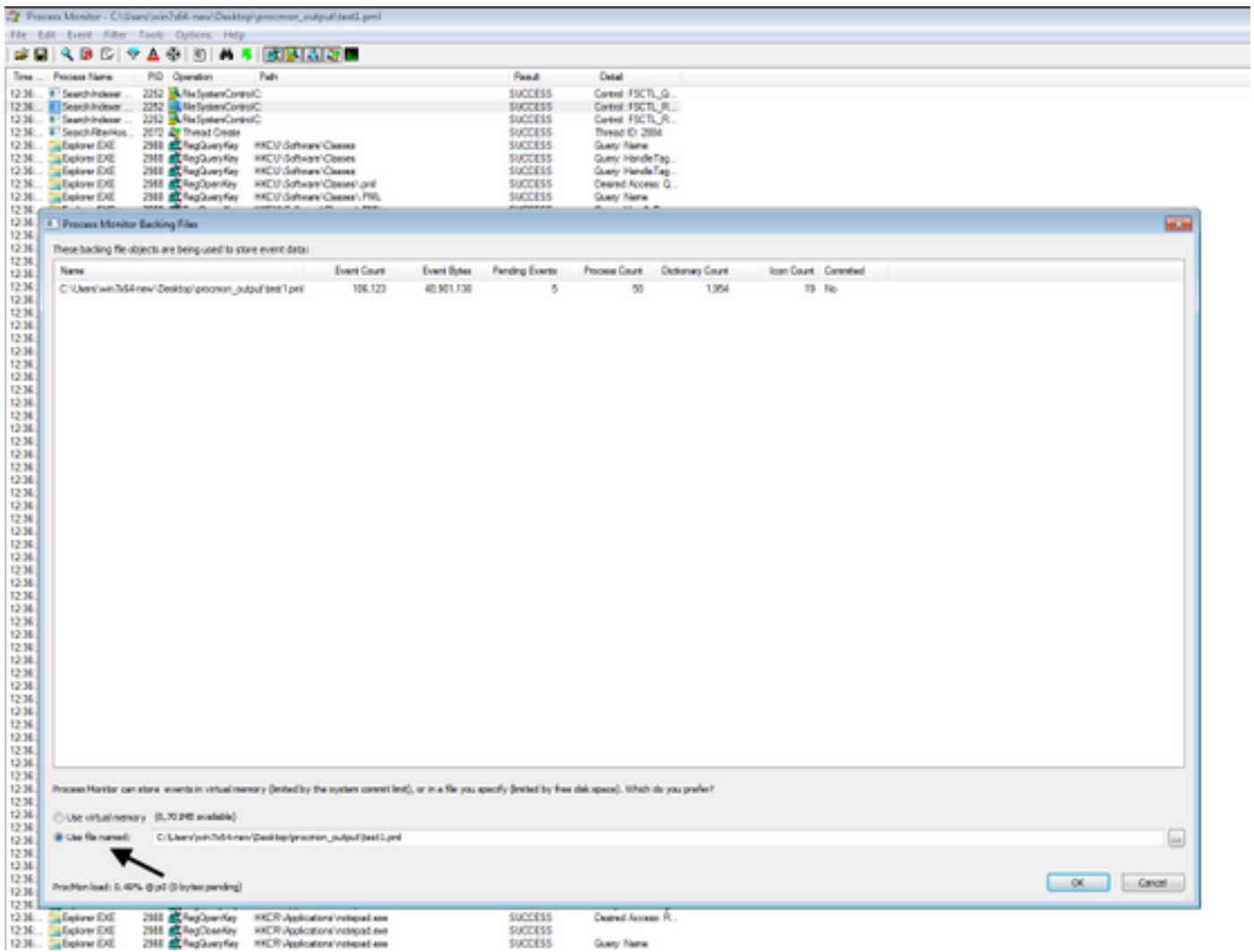
Introduction

As a System Administrator, you may want to obtain detailed logs using the Process Monitor (procmon.exe) to determine, if the FireAMP connector experiences hangs during the computer startup process. These logs will also be requested by Cisco TAC in order to troubleshoot such issues. Process Monitor is a free utility that can help us here. This can be downloaded freely from <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon>

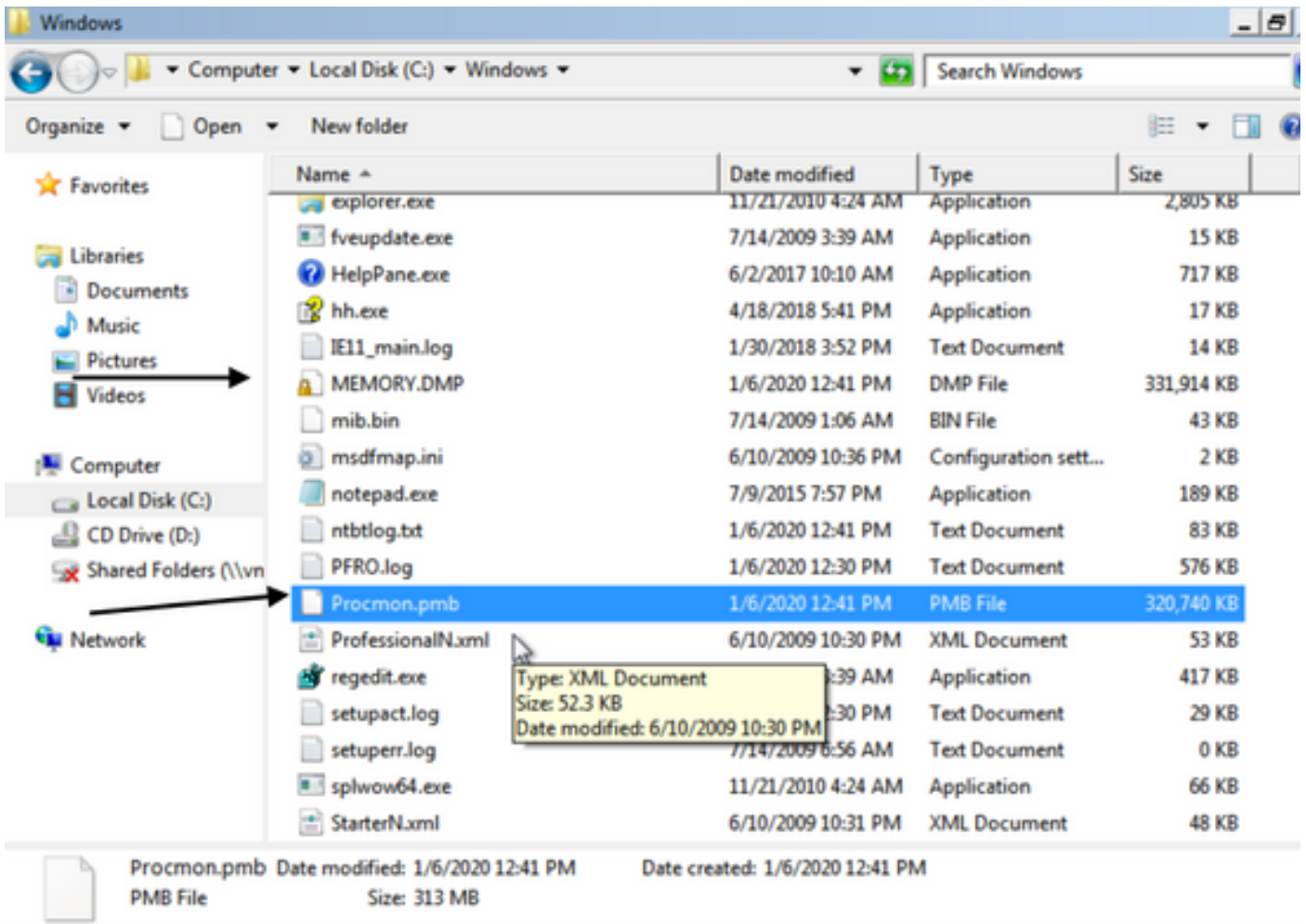
This document describes the steps on how to collect ProcMon logs and Memory dump if the problem occurs during a system boot process (which means that it's generating BSODs at boot). These logs are required to capture the system events taking place during boot.

Procedure:

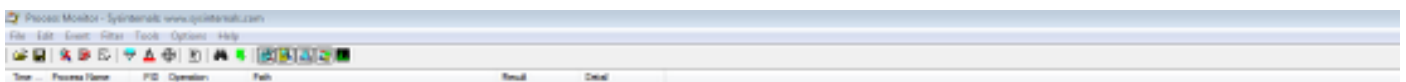
1. Set-up the test machines in such a way so that the issue can be reproduced easily.
2. Download and Run the ProcMon tool as administrator. Go to **File -> Process Monitor Backing Files** and select a **Path**.

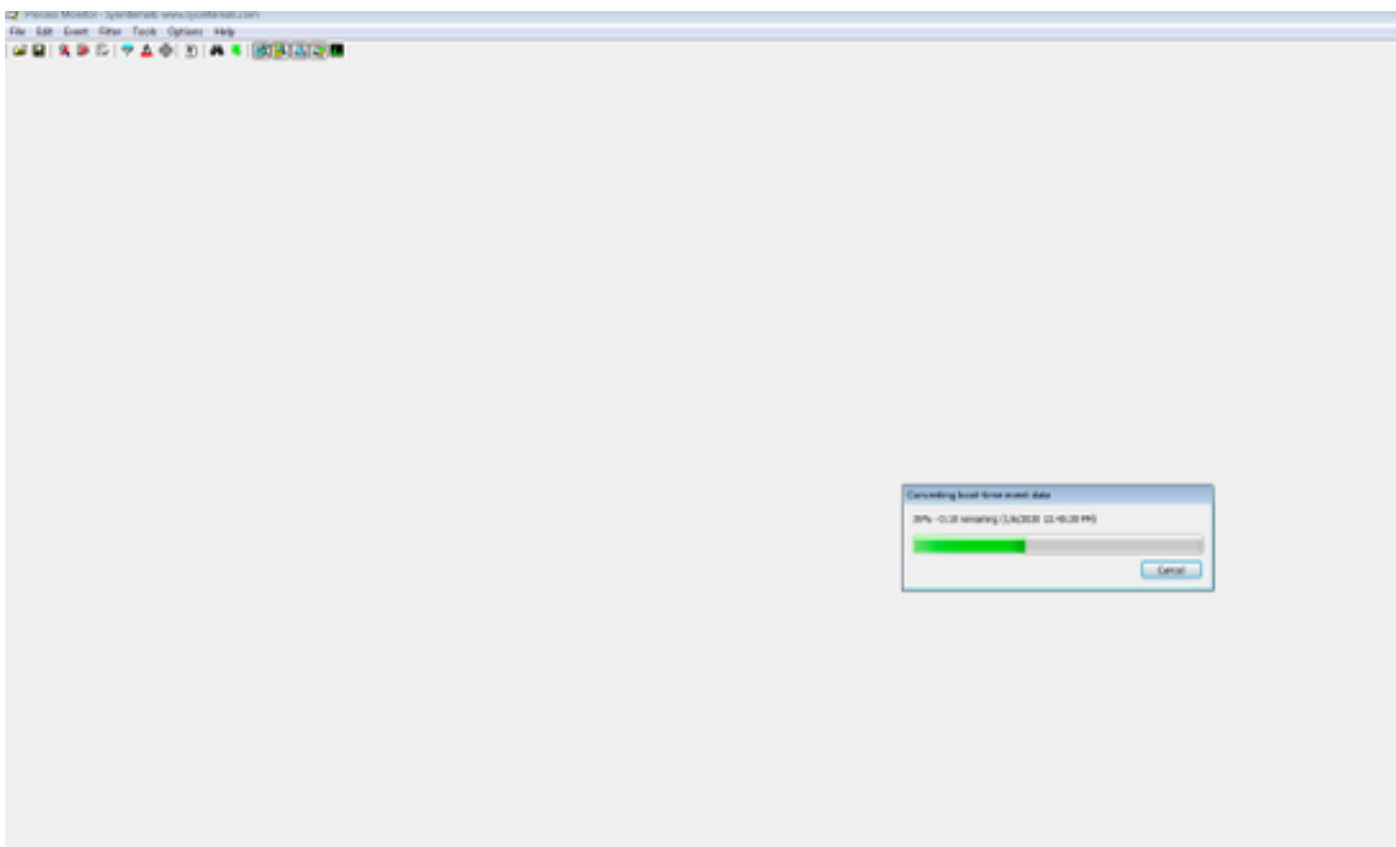


3. In Procmon Tool, go to **Options -> Enable Boot Logging**.



7. Optionally, if you are able to boot it into "normal mode" if the PMB files are generated in the C:\Windows folder, then if you launch ProcMon again, you will see the following logs. From this, you can re-save the events by clicking on the Save button.





Time	Process Name	PID	Operation	Path	Result	Detail
12:41...	smss.exe	292	Process Start		SUCCESS	Parent PID: 4, Com...
12:41...	smss.exe	292	Thread Create		SUCCESS	Thread ID: 296
12:41...	smss.exe	292	Load Image	C:\Windows\System32\smss.exe	SUCCESS	Image Base: 0x479...
12:41...	smss.exe	292	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x779...
12:41...	smss.exe	292	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\ima...	NAME NOT FOUND	Desired Access: Q...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	REPARSE	Desired Access: R...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	SUCCESS	Desired Access: R...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 1,024
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 1,024
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 74,752, Len...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 1,024, Leng...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 107,008, Le...
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 104,448, Le...
12:41...	smss.exe	292	Thread Create		SUCCESS	Thread ID: 300
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset: 104,448
12:41...	smss.exe	292	ReadFile	C:\Windows\System32\smss.exe	SUCCESS	Offset Length: 2,560
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MinNT	REPARSE	Desired I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\MinNT	NAME NOT FOUND	Desired I/O Flags: Normal
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	REPARSE	Desired Access: Al...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager...	SUCCESS	Desired Access: Al...
12:41...	smss.exe	292	RegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	
12:41...	smss.exe	292	RegSetValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_SZ, Le...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: R...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: R...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_DWO...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_DWO...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NAME NOT FOUND	Length: 4,094
12:41...	smss.exe	292	RegQueryValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Type: REG_MULT...
12:41...	smss.exe	292	RegDeleteValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 0, Name: A...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 1, Name: M...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 2, Name: N...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 3, Name: Pl...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 4, Name: P...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Index: 5, Name: U...
12:41...	smss.exe	292	RegEnumValue	HKLM\System\CurrentControlSet\Control\SESSION MANA...	NO MORE ENTRI...	Index: 6, Length: 4...
12:41...	smss.exe	292	RegCloseKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	
12:41...	smss.exe	292	RegOpenKey	HKLM\System\CurrentControlSet\Control\SESSION MANA...	SUCCESS	Desired Access: M...