



{F312195E-3D9D-447A-A3F5-08DFFA24735E}

Eine Gruppenrichtlinie lässt sich nicht verarbeiten und im Ereignisprotokoll unter SYSTEM finden wir eine **Warnung** mit der Ereignis-ID 1085.

„Fehler beim Anwenden der Einstellungen. Die Einstellungen besitzen möglicherweise eine eigene Protokolldatei.“

Dieser Fehler kommt in der Regel dann zustande, wenn versucht wird etwas zu starten was es nicht gibt, oder mit einem falschen Wert konfiguriert ist; der nicht interpretiert werden kann.

Event Viewer - System - Anzahl von Ereignissen: 4

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkategorie
Informationen	24.12.2021 12:12:11	Eventlog	104	Protokoll gelöscht
Warnung	24.12.2021 12:12:17	GroupPolicy (Microsoft-Windows-GroupPolicy)	1085	Keine
Informationen	24.12.2021 12:12:17	GroupPolicy (Microsoft-Windows-GroupPolicy)	1500	Keine
Informationen	24.12.2021 12:12:17	GroupPolicy (Microsoft-Windows-GroupPolicy)	1501	Keine

Ereignis 1085, GroupPolicy (Microsoft-Windows-GroupPolicy)

Allgemein Details

Fehler beim Anwenden der '{F312195E-3D9D-447A-A3F5-08DFFA24735E}'-Einstellungen. Die '{F312195E-3D9D-447A-A3F5-08DFFA24735E}'-Einstellungen besitzen möglicherweise eine eigene Protokolldatei. Klicken Sie auf den Link 'Weitere Informationen'.

Protokollname: System
Quelle: GroupPolicy (Microsoft-Win
Protokolliert: 24.12.2021 12:12:17
Ereignis-ID: 1085
Aufgabenkategorie: Keine
Ebene: Warnung
Schlüsselwörter:
Benutzer: SYSTEM
Computer: DC10.bsprod.local
Vorgangscod: (1)
Weitere Informationen: [Onlinehilfe](#)

Parallel unter den Anwendungs- und Dienstprotokollen sehen wir einen **Fehler** bezogen auf die obere Warnung mit der Ereignis-ID 7016.

Event Viewer - Betriebsbereit - Anzahl von Ereignissen: 6.889

Ebene	Datum und Uhrzeit	Quelle	Ereignis-ID	Aufgabenkate...
Informationen	24.12.2021 13:30:25	GroupPolicy (Microsoft-Windows-GroupPolicy)	5016	Keine
Informationen	24.12.2021 13:30:25	GroupPolicy (Microsoft-Windows-GroupPolicy)	4016	Keine
Fehler	24.12.2021 13:30:25	GroupPolicy (Microsoft-Windows-GroupPolicy)	7016	Keine
Informationen	24.12.2021 13:30:25	GroupPolicy (Microsoft-Windows-GroupPolicy)	4016	Keine
Informationen	24.12.2021 13:30:25	GroupPolicy (Microsoft-Windows-GroupPolicy)	5016	Keine
Informationen	24.12.2021 13:30:25	GroupPolicy (Microsoft-Windows-GroupPolicy)	4016	Keine

Ereignis 7016, GroupPolicy (Microsoft-Windows-GroupPolicy)

Allgemein Details

Die Verarbeitung der '{F312195E-3D9D-447A-A3F5-08DFFA24735E}'-Erweiterung wurde in 15 Millisekunden abgeschlossen.

Protokollname: Microsoft-Windows-GroupPolicy/Betriebsbereit
Quelle: GroupPolicy (Microsoft-Win
Protokolliert: 24.12.2021 13:30:25
Ereignis-ID: 7016
Aufgabenkategorie: Keine
Ebene: Fehler
Schlüsselwörter:
Benutzer: SYSTEM
Computer: DC10.bsprod.local
Vorgangscod: (2)
Weitere Informationen: [Onlinehilfe](#)



{F312195E-3D9D-447A-A3F5-08DFFA24735E}

Ein manuell ausgeführtes GPUPDATE zeigt den Fehler ebenfalls noch einmal an.

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>gpupdate
Die Richtlinie wird aktualisiert...

Die Aktualisierung der Computerrichtlinie wurde erfolgreich abgeschlossen.

Bei der Verarbeitung der Computerrichtlinie sind folgende Warnungen aufgetreten:
Fehler beim Anwenden der "{F312195E-3D9D-447A-A3F5-08DFFA24735E}"-Einstellungen. Die "{F312195E-3D9D-447A-A3F5-08DFFA24735E}"-Einstellungen besitzen möglicherweise eine eigene Protokolldatei. Klicken Sie auf den Link "Weitere Informationen".
Die Aktualisierung der Benutzerrichtlinie wurde erfolgreich abgeschlossen.

Detaillierte Informationen hierzu finden Sie im Ereignisprotokoll bzw. führen Sie "GPRESULT /H GPREport.html" aus, um auf Informationen zu den Gruppenrichtlinienergebnissen zuzugreifen.

C:\Windows\system32>
```

Mithilfe eines Reg-Editors suche ich aus dem Fehlerprotokoll nach der GUID {F312195E-3D9D-447A-A3F5-08DFFA24735E}. Die GUID verweist auf die CSE VirtualizationBasedSecurity GPO (DeviceGuard / CredentialGuard)

The screenshot shows the Windows Registry Editor (RegEditor) with the path `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}` selected. The right pane displays the following values:

Name /	Typ	Daten
(Standard)	REG_SZ	(Wert nicht gesetzt)
DisplayName	REG_EXPAND_SZ	@dggpext.dll,-600
DllName	REG_EXPAND_SZ	dggpext.dll
EnableAsynchronousProcessing	REG_DWORD	0x00000000 (0)
NoUserPolicy	REG_DWORD	0x00000001 (1)
ProcessGroupPolicy	REG_SZ	ProcessVirtualizationBasedSecurityGroupPolicy

Below the main pane, a search results window titled "Suchergebnis" shows 23 entries found. The first entry is highlighted:

Schlüssel /	Wert	Typ	Daten
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		KEY	
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		KEY	
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions\{F312195E-3D9D-447A-A3F5-08DFFA24735E}		Extensions	REG_SZ {{{2A8FDC61-2347-4C87-92F6-B05EB91A201A}\{D02B1F72-3407-48AE-BA88-800000000000}



{F312195E-3D9D-447A-A3F5-08DFFA24735E}

Schauen wir uns, die auf die Domain Controller verlinkten GPOs mal etwas genauer an. Jetzt wird klar, dass es sich um die Richtlinie zur Aktivierung von [VBS \(Virtualization Based Security\)](#) / [Device Guard](#) handelt.

Es scheint, dass die Abhängigkeiten zuvor gar nicht evaluiert bzw. eingerichtet/konfiguriert wurden und deswegen der Fehler ausgegeben wird. Entweder entfernt man die fälschlicherweise verlinkte Richtlinie oder aktiviert/installiert die Abhängigkeiten damit VBS eingesetzt werden kann.

Ich entferne die Richtlinie, weil meine virtuelle Maschine die benötigten Abhängigkeiten nicht besitzt. Die [Virtualisierungs-basierten Sicherheitsfunktionen](#) nutzen eine Reihe von Sicherheitselementen wie [UEFI](#), [Secure Boot](#) und [Trusted Platform Module \(TPM\) 2,0](#).

Bereich	Detaile	Einstellungen	Delegierung
BSPROD\Domänen-Admins		Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
BSPROD\Organisations-Admins		Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein
NT-AUTORITÄT\Authentifizierte Benutzer		Lesen (durch Sicherheitsfilterung)	Nein
NT-AUTORITÄT\DOMÄNENCONTROLLER DER ORGANISATION		Lesen	Nein
NT-AUTORITÄT\SYSTEM		Einstellungen bearbeiten, löschen, Sicherheit ändern	Nein

Computerkonfiguration (Aktiviert) Ausblenden

Richtlinien Ausblenden

Administrative Vorlagen Ausblenden

Richtliniendefinitionen (ADMX-Dateien) wurden aus dem zentralen Speicher abgerufen.

System/Device Guard Ausblenden

Richtlinie	Einstellung	Kommentar
Virtualisierungsbasierte Sicherheit aktivieren	Aktiviert	
Plattform-Sicherheitsstufe auswählen:		Sicherer Start
Virtualisierungsbasierter Schutz der Codeintegrität:		Mit UEFI-Spare aktiviert
UEFI-Speicherattributabelle erforderlich		Deaktiviert
Credential Guard-Konfiguration:		Deaktiviert
Sichere Startkonfiguration:		Aktiviert

Benutzerkonfiguration (Deaktiviert) Ausblenden

Keine Einstellungen definiert

```
Administrator: Eingabeaufforderung
Microsoft Windows [Version 10.0.17763.2366]
(c) 2018 Microsoft Corporation. Alle Rechte vorbehalten.

C:\Windows\system32>gpupdate
Die Richtlinie wird aktualisiert...

Die Aktualisierung der Computerrichtlinie wurde erfolgreich abgeschlossen.
Die Aktualisierung der Benutzerrichtlinie wurde erfolgreich abgeschlossen.

C:\Windows\system32>
```

[Virtualisierungsbasierte Sicherheit \(VBS\)](#)

[Grundlegende Schutzmaßnahmen und zusätzliche Qualifikationen für den virtualisierungsbasierten Schutz der Codeintegrität](#)

[Windows Defender Credential Guard: Anforderungen](#)



{F312195E-3D9D-447A-A3F5-08DFFA24735E}

Die CSE-GUIDS lassen sich mithilfe der Powershell aus der Registrierung auslesen:

Get-ChildItem "HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\GPExtensions" | Out-GridView

Name	Property
{E5094040-C46C-4115-B030-04FB2E545B00}	(default) : Group Policy Regional Options DisplayName : @gpprefcl.dll,-20 DllName : C:\Windows\System32\gpprefcl.dll EnableAsynchronousProcessing : 1 EventSources : (Group Policy Regional Options,Application) GenerateGroupPolicy : GenerateGroupPolicyRegionOptions PerUserLocalSettings : 1 ProcessGroupPolicy : ProcessGroupPolicyRegionOptions ProcessGroupPolicyEx : ProcessGroupPolicyExRegionOptions
{E62688F0-25FD-4c90-8FF5-F50889D2E31F}	(default) : Group Policy Power Options DisplayName : @gpprefcl.dll,-21 DllName : C:\Windows\System32\gpprefcl.dll EnableAsynchronousProcessing : 1 EventSources : (Group Policy Power Options,Application) GenerateGroupPolicy : GenerateGroupPolicyPowerOptions PerUserLocalSettings : 1 ProcessGroupPolicy : ProcessGroupPolicyPowerOptions ProcessGroupPolicyEx : ProcessGroupPolicyExPowerOptions
{F312195E-3D9D-447A-A3F5-08DFFA24735E}	DisplayName : @dggpext.dll,-600 DllName : dggpext.dll EnableAsynchronousProcessing : 0 NoUserPolicy : 1 ProcessGroupPolicy : ProcessVirtualizationBasedSecurityGroupPolicy
{f3ccc681-b74c-4060-9f26-cd84525dca2a}	(default) : Audit Policy Configuration DisplayName : @auditse.dll,-3000 DllName : auditse.dll EnableAsynchronousProcessing : 1 ForceRefreshFG : 0 GenerateGroupPolicy : GenerateGroupPolicy MaxNoGPOListChangesInterval : 960 NoUserPolicy : 1 ProcessGroupPolicyEx : ProcessGroupPolicyEx
{F9C77450-3A41-477E-9310-9ACD617BD9E3}	(default) : Group Policy Applications DisplayName : @gpprefcl.dll,-15 DllName : C:\Windows\System32\gpprefcl.dll EnableAsynchronousProcessing : 1 EventSources : (Group Policy Applications,Application) GenerateGroupPolicy : GenerateGroupPolicyApplications NoMachinePolicy : 1 PerUserLocalSettings : 1