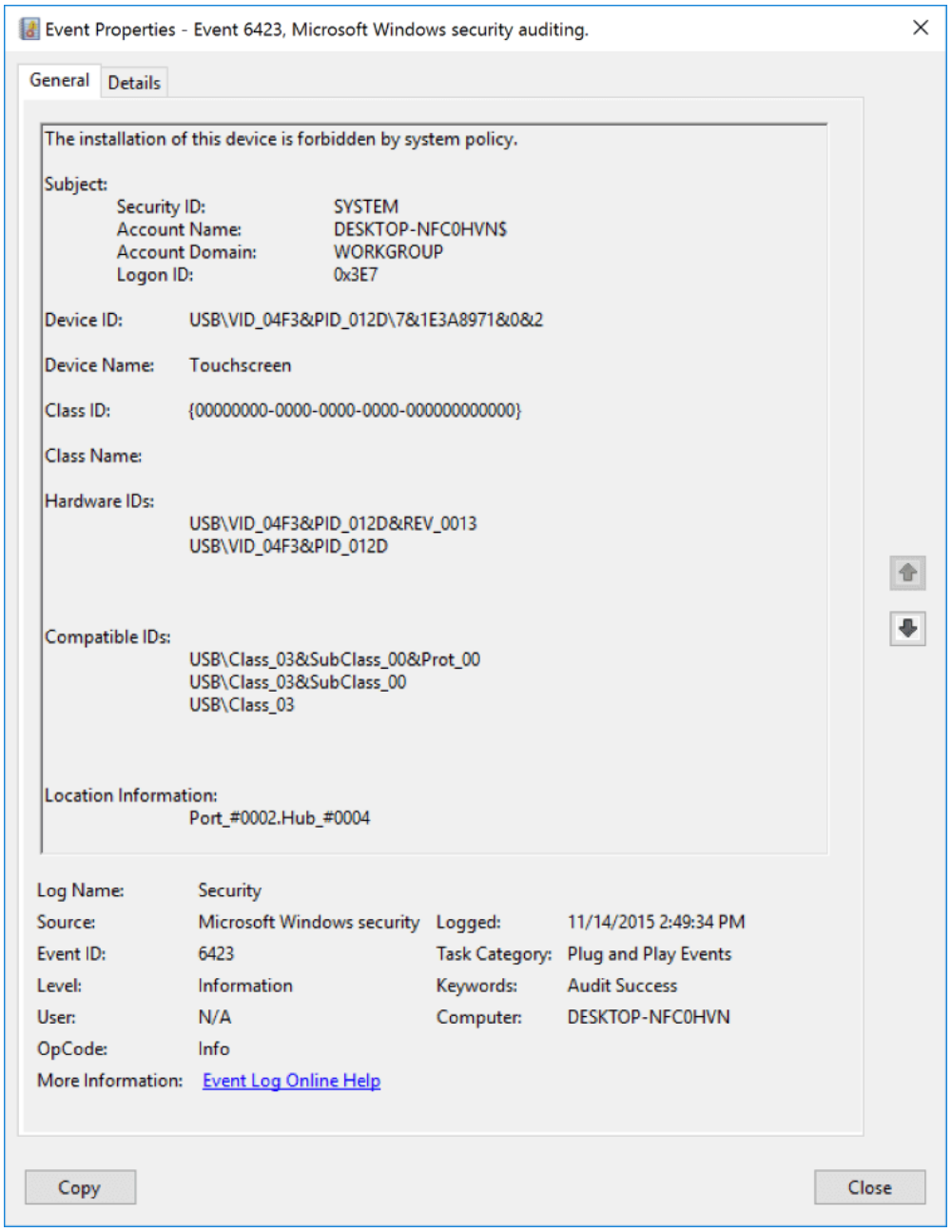
6423(S): The installation of this device is forbidden by system policy.

Article • 09/09/2021 • 1 contributor

Subcategory: Audit PNP Activity

Event Description:

This event generates every time installation of this device is forbidden by system policy.



Device installation restriction group policies are located here: **\Computer Configuration\Administrative Templates\System\Device Installation\Device Installation Restrictions**. If one of the policies restricts installation of a specific device, this event will be generated.

> **Note** For recommendations, see Security Monitoring Recommendations for this event.

Event XML:

```
- <Event xmlns="http://schemas.microsoft.com/win/2004/08/eve
- <System>
 <Provider Name="Microsoft-Windows-Security-Auditing" Guid='
 <EventID>6423</EventID>
 <Version>0</Version>
 <Level>0</Level>
 <Task>13316</Task>
 <Opcode>0</Opcode>
 <Keywords>0x8020000000000000</Keywords>
 <TimeCreated SystemTime="2015-11-14T22:49:34.647975900Z" />
 <EventRecordID>488</EventRecordID>
 <Correlation />
 <Execution ProcessID="828" ThreadID="1924" />
 <Channel>Security</Channel>
 <Computer>DESKTOP-NFC0HVN</Computer>
 <Security />
 </System>
- <EventData>
 <Data Name="SubjectUserSid">S-1-5-18</Data>
 <Data Name="SubjectUserName">DESKTOP-NFC0HVN$</Data>
 <Data Name="SubjectDomainName">WORKGROUP</Data>
 <Data Name="SubjectLogonId">0x3e7</Data>
 <Data Name="DeviceId">USB\\VID\_04F3&PID\_012D\\7&1E3A8971&
 <Data Name="DeviceDescription">Touchscreen</Data>
 <Data Name="ClassId">{00000000-0000-0000-0000-000000000000}
 <Data Name="ClassName" />
 <Data Name="HardwareIds">USB\\VID\_04F3&PID\_012D&REV\_0013
 <Data Name="CompatibleIds">USB\\Class\_03&SubClass\_00&Prot
 <Data Name="LocationInformation">Port\_\#0002.Hub\_\#0004</
 </EventData>
</Event>
```

Required Server Roles: None.

Minimum OS Version: Windows 10 [Version 1511].

Event Versions: 0.

Field Descriptions:

Subject:

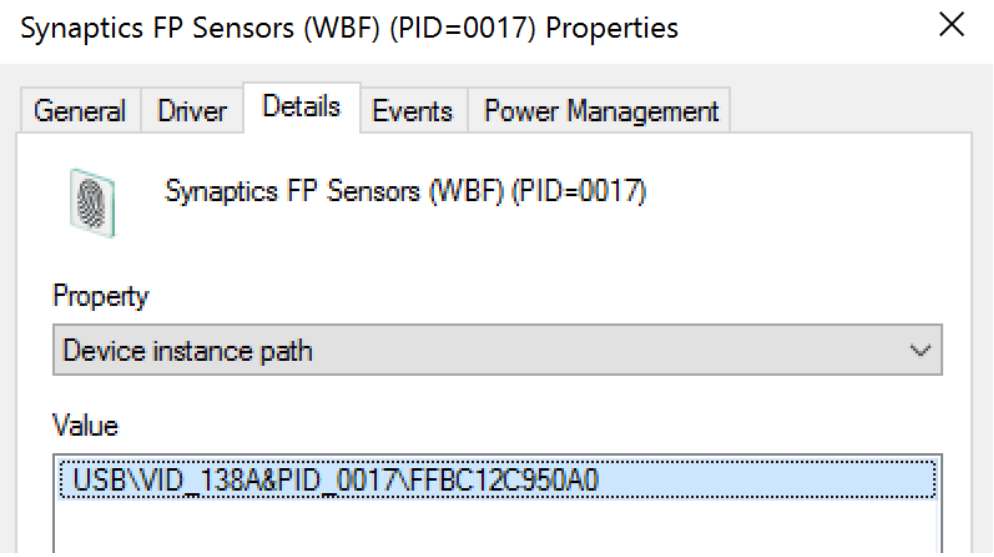
- **Security ID** [Type = SID]: SID of account that forbids the device installation. Event Viewer automatically tries to resolve SIDs and show the account name. If the SID cannot be resolved, you will see the source data in the event.

> **Note** A **security identifier (SID)** is a unique value of variable length used to identify a trustee (security principal). Each account has a unique SID that is issued by an authority, such as an Active Directory domain controller, and stored in a security database. Each time a user logs on, the system retrieves the SID for that user from the database and places it in the access token for that user. The system uses the SID in the access token to identify the user in all subsequent interactions with Windows security. When a SID has been used as the unique identifier for a user or group, it cannot ever be used again to identify another user or group. For more information about SIDs, see Security identifiers.

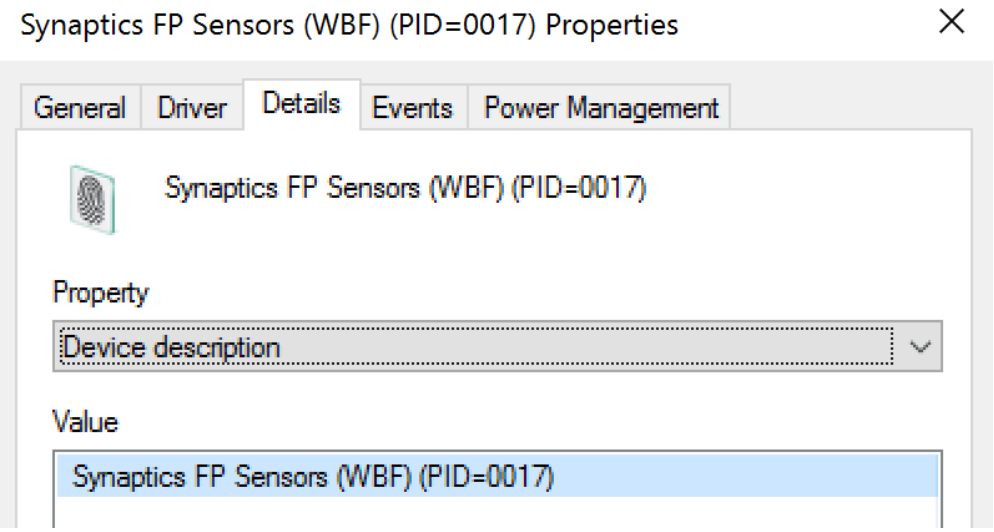
- **Account Name** [Type = UnicodeString]: the name of the account that forbids the device installation.
- **Account Domain** [Type = UnicodeString]: subject's domain or computer name. Formats vary, and include the following:
  - Domain NETBIOS name example: CONTOSO
  - Lowercase full domain name: contoso.local
  - Uppercase full domain name: CONTOSO.LOCAL
  - For some well-known security principals, such as LOCAL SERVICE or ANONYMOUS LOGON, the value of this field is "NT AUTHORITY".
  - For local user accounts, this field will contain the name of the computer or device that this account belongs to, for example: "Win81".

- **Logon ID** [Type = HexInt64]**:** hexadecimal value that can help you correlate this event with recent events that might contain the same Logon ID, for example, "4624: An account was successfully logged on."

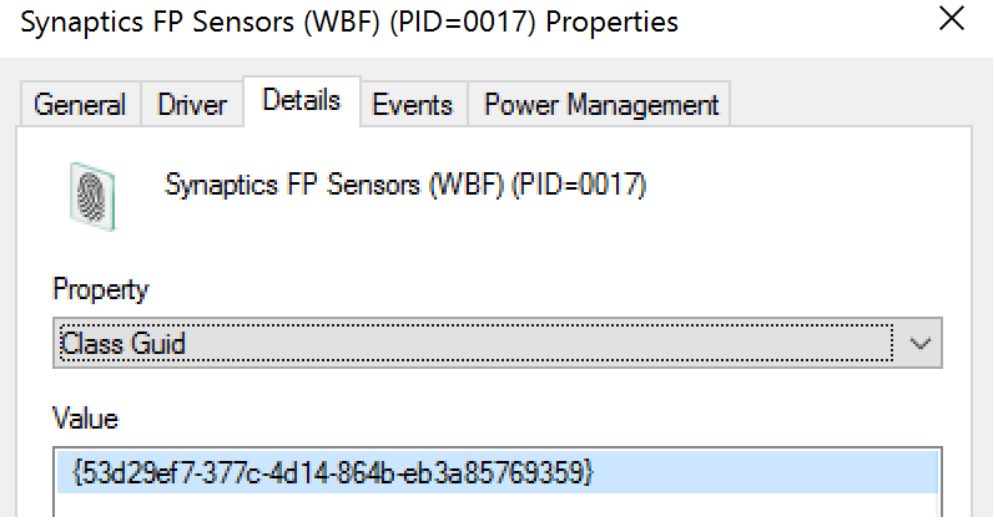
Device ID [Type = UnicodeString]: "**Device instance path**" attribute of device. To see device properties, start Device Manager, open specific device properties, and click "Details":



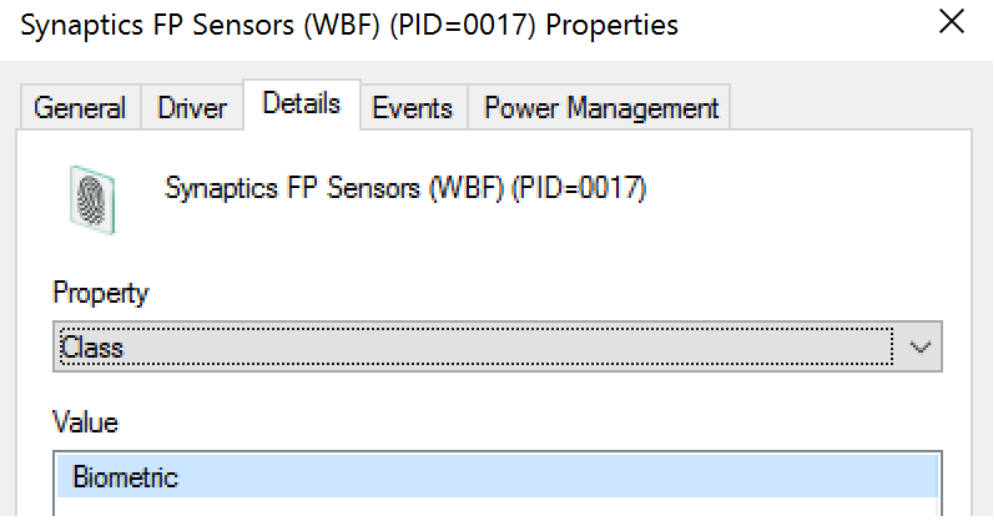
Device Name [Type = UnicodeString]: "**Device description**" attribute of device. To see device properties, start Device Manager, open specific device properties, and click "Details":



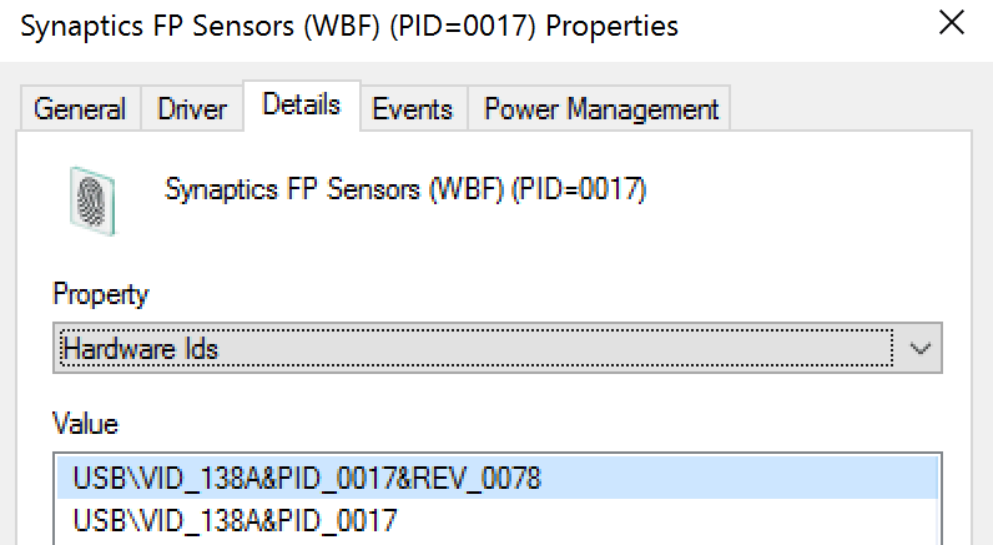
Class ID [Type = UnicodeString]: "**Class Guid**" attribute of device. To see device properties, start Device Manager, open specific device properties, and click "Details":



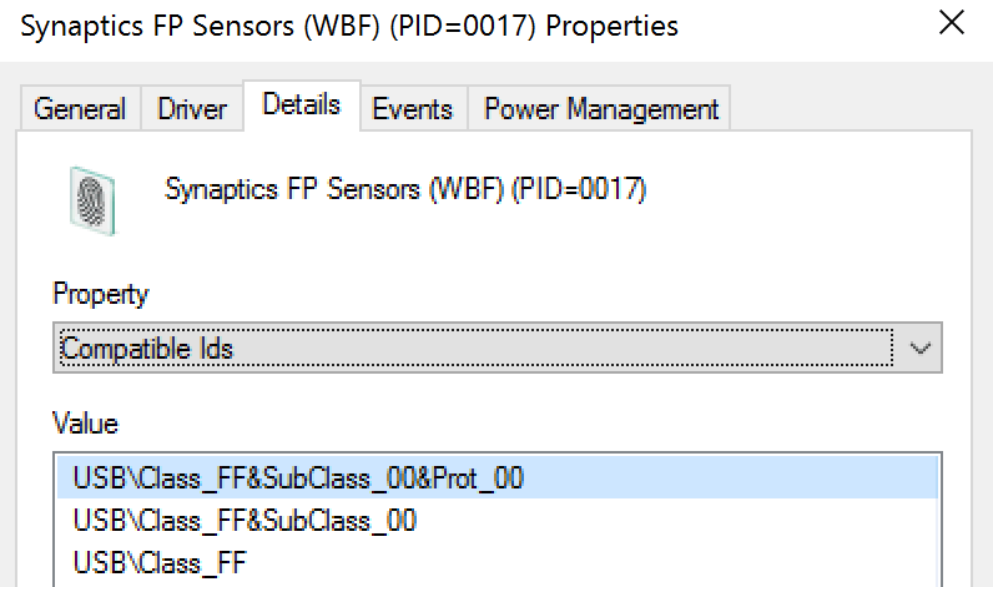
Class Name [Type = UnicodeString]: "**Class**" attribute of device. To see device properties, start Device Manager, open specific device properties, and click "Details":



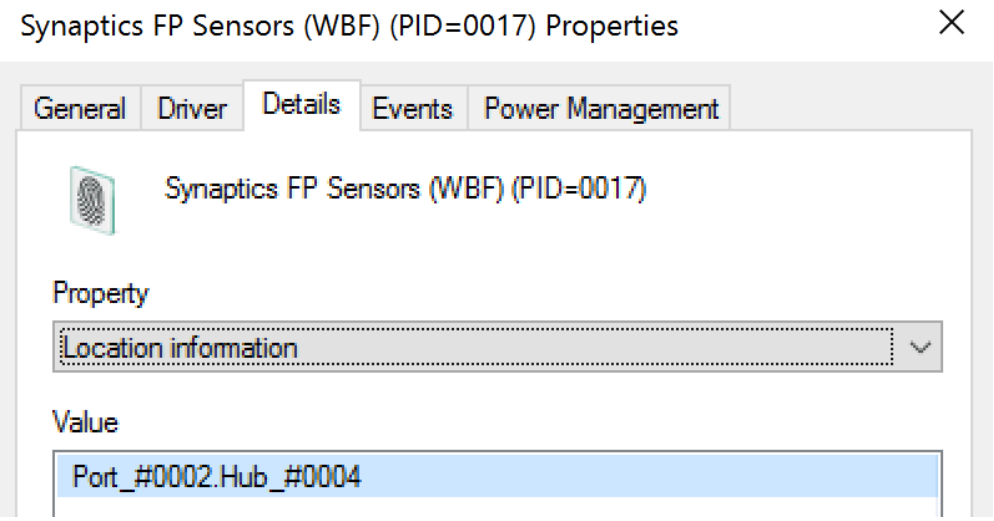
Hardware IDs [Type = UnicodeString]: "**Hardware Ids**" attribute of device. To see device properties, start Device Manager, open specific device properties, and click "Details":



Compatible IDs [Type = UnicodeString]: "**Compatible Ids**" attribute of device. To see device properties, start Device Manager, open specific device properties, and click "Details":



Location Information [Type = UnicodeString]: "**Location information**" attribute of device. To see device properties, start Device Manager, open specific device properties, and click "Details":



Security Monitoring Recommendations

For 6423(S): The installation of this device is forbidden by system policy.

> **Important** For this event, also see Appendix A: Security monitoring recommendations for many audit events.

- If you want to track device installation policy violations then you need to track every event of this type.
- Because this event is typically triggered by the SYSTEM account, we recommend that you report it whenever **"Subject\Security ID"** is not SYSTEM.
- You can use this event to track the policy violations and related information shown in the following table by using the listed fields:

Expand table

Policy violation and related information to monitor	Field to use

Device installation policy violations, **Device Instance Path**	"**Device ID**"
Device installation policy violations, **Device Description**	"**Device Name**"
Device installation policy violations, **Class GUID**	"**Class ID**"
Device installation policy violations, **Hardware IDs**	"**Hardware IDs**"
Device installation policy violations, **Compatible IDs**	"**Compatible IDs**"
Device installation policy violations, **Location information**	"**Location Information**"