Files

7a806a1

Go to file

- Application-Addon-Event-P...
- Error Instrument.xml
- Intel-iaLPSS-GPIO.xml
- Intel-iaLPSS-I2C.xml
- Intel-iaLPSS2-GPIO2.xml
- Intel-iaLPSS2-I2C.xml
- LsaSrv.xml
- Microsoft Edge Etw.xml
- Microsoft-Antimalware-AM...
- Microsoft-Antimalware-Engi...
- Microsoft-Antimalware-Prot...
- Microsoft-Antimalware-RTP....
- Microsoft-Antimalware-Sca...
- Microsoft-Antimalware-Serv...
- Microsoft-Antimalware-Uac...
- Microsoft-AppV-Client-Stre...
- Microsoft-AppV-Client.xml
- Microsoft-AppV-ServiceLog....
- Microsoft-AppV-SharedPerf...
- Microsoft-Client-License-Fle...
- Microsoft-Client-Licensing-...
- Microsoft-Gaming-Services....

EVTX-ETW-Resources / ETWProvidersManifests / Windows11 / 22H2 / W11_22H2_Pro_20221220_22621.963 / WEPExplorer / LsaSrv.xml

AndrewRathbun add December 2022 ISOs af147a0 · 2 years ago History

Code Blame 1377 lines (1003 loc) · 44.7 KB Raw

```xml
<Providers>
    <Provider>
        <Name>LsaSrv</Name>
        <Metadata>
            <Guid>{199FE037-2B82-40A9-82AC-E1D46C792B99}</Guid>
            <ResourceFilePath>%windir%\System32\lsasrv.dll</ResourceFilePath>
            <ParameterFilePath></ParameterFilePath>
            <MessageFilePath>%windir%\System32\lsasrv.dll</MessageFilePath>
            <HelpLink></HelpLink>
            <PublisherMessage>Microsoft-Windows-LSA</PublisherMessage>
            <Channels>
                <Channel>
                    <Message>System</Message>
                    <Path>System</Path>
                    <Index>0</Index>
                    <Id>8</Id>
                    <Imported>true</Imported>
                </Channel>
                <Channel>
                    <Message></Message>
                    <Path>Microsoft-Windows-LSA/Performance</Path>
                    <Index>1</Index>
                    <Id>16</Id>
                    <Imported>false</Imported>
                </Channel>
                <Channel>
                    <Message>Operational</Message>
                    <Path>Microsoft-Windows-LSA/Operational</Path>
                    <Index>2</Index>
                    <Id>17</Id>
                    <Imported>false</Imported>
                </Channel>
                <Channel>
                    <Message>Diagnostic</Message>
                    <Path>Microsoft-Windows-LSA/Diagnostic</Path>
                    <Index>3</Index>
                    <Id>18</Id>
                    <Imported>false</Imported>
                </Channel>
            </Channels>
            <Levels>
                <Level>
                    <Message>Critical</Message>
                    <Name>win:Critical</Name>
                    <Value>1</Value>
                </Level>
                <Level>
                    <Message>Error</Message>
                    <Name>win:Error</Name>
                    <Value>2</Value>
                </Level>
                <Level>
                    <Message>Warning</Message>
                    <Name>win:Warning</Name>
```

Microsoft-Windows Networ...
Microsoft-Windows-AAD.xml
Microsoft-Windows-ACL-UI...
Microsoft-Windows-ADSI.xml
Microsoft-Windows-AIT.xml
Microsoft-Windows-ASN1.x...

```
                        <Value>3</Value>
                    </Level>
                    <Level>
                        <Message>Information</Message>
                        <Name>win:Informational</Name>
                        <Value>4</Value>
                    </Level>
                </Levels>
                <Tasks>
                    <Task>
                        <Message>Security Package Manager</Message>
                        <Name>CATEGORY_SPM</Name>
                        <Value>1</Value>
                    </Task>
                    <Task>
                        <Message>Locator</Message>
                        <Name>CATEGORY_LOCATOR</Name>
                        <Value>2</Value>
                    </Task>
                    <Task>
                        <Message>SPNEGO (Negotiator)</Message>
                        <Name>CATEGORY_NEGOTIATE</Name>
                        <Value>3</Value>
                    </Task>
                    <Task>
                        <Message>Logon Cache</Message>
                        <Name>CATEGORY_LOGON_CACHE</Name>
                        <Value>4</Value>
                    </Task>
                    <Task>
                        <Message>LSA Logon</Message>
                        <Name>CATEGORY_LSA_LOGON</Name>
                        <Value>5</Value>
                    </Task>
                    <Task>
                        <Message>LSA SID-Name Lookup</Message>
                        <Name>CATEGORY_LSA_LOOKUP</Name>
                        <Value>6</Value>
                    </Task>
                    <Task>
                        <Message>Max</Message>
                        <Name>CATEGORY_MAX_CATEGORY</Name>
                        <Value>7</Value>
                    </Task>
                </Tasks>
                <Opcodes>
                    <Opcode>
                        <Message>Start</Message>
                        <Name>win:Start</Name>
                        <Value>1</Value>
                        <Task>0</Task>
                    </Opcode>
                    <Opcode>
                        <Message>Stop</Message>
                        <Name>win:Stop</Name>
                        <Value>2</Value>
                        <Task>0</Task>
                    </Opcode>
                </Opcodes>
                <Keywords>
                    <Keyword>
                        <Message></Message>
                        <Name>WPDBusEnumStartTrigger</Name>
```

```
                <Level>Information</Level>
                <Message><![CDATA[
The Security System has received an authentication request directly for authentication
                <Template><![CDATA[
<template xmlns="http://schemas.microsoft.com/win/2004/08/events">
  <data name="Protocol" inType="win:UnicodeString" outType="xs:string"/>
</template>
]]></Template>
            </Event>
            <Event>
                <Id>40968</Id>
                <Version>0</Version>
                <Channel>System</Channel>
                <Level>Warning</Level>
                <Message><![CDATA[
The Security System has received an authentication request that could not be decoded. T
                <Template><![CDATA[
]]></Template>
            </Event>
            <Event>
                <Id>40969</Id>
                <Version>0</Version>
                <Channel>System</Channel>
                <Level>Information</Level>
                <Message><![CDATA[
The Security System has received an authentication attempt, and determined that the pro
                <Template><![CDATA[
<template xmlns="http://schemas.microsoft.com/win/2004/08/events">
  <data name="Protocol" inType="win:UnicodeString" outType="xs:string"/>
</template>
]]></Template>
            </Event>
            <Event>
                <Id>45056</Id>
                <Version>0</Version>
                <Channel>System</Channel>
                <Level>Warning</Level>
                <Message><![CDATA[
Logon cache was disabled. Intermittent authentication failures may result during period
                <Template><![CDATA[
]]></Template>
            </Event>
            <Event>
                <Id>45057</Id>
                <Version>0</Version>
                <Channel>System</Channel>
                <Level>Information</Level>
                <Message><![CDATA[
A failed logon attempt has caused a logon cache entry for user %1 to be deleted. The au
                <Template><![CDATA[
<template xmlns="http://schemas.microsoft.com/win/2004/08/events">
  <data name="Username" inType="win:UnicodeString" outType="xs:string"/>
  <data name="Package" inType="win:UnicodeString" outType="xs:string"/>
  <data name="Error" inType="win:UnicodeString" outType="xs:string"/>
</template>
]]></Template>
            </Event>
            <Event>
                <Id>45058</Id>
                <Version>0</Version>
                <Channel>System</Channel>
                <Level>Information</Level>
                <Message><![CDATA[
A logon cache entry for user %1 was the oldest entry and was removed. The timestamp of
                <Template><![CDATA[
<template xmlns="http://schemas.microsoft.com/win/2004/08/events">
  <data name="UserName" inType="win:UnicodeString" outType="xs:string"/>
  <data name="TimeStamp" inType="win:SYSTEMTIME" outType="xs:dateTime"/>
</template>
]]></Template>
            </Event>
        </EventMetadata>
    </Provider>
</Providers>
```