

# Re: SceCli Error 1202 filling up the Event Log!

---

*Source:*

[http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.advanced\\_server/2005-04/msg00009.html](http://www.tech-archive.net/Archive/Win2000/microsoft.public.win2000.advanced_server/2005-04/msg00009.html)

---

- *From:* "Cameron Dorrough" <[cdorrough@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:cdorrough@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)>
  - *Date:* Fri, 1 Apr 2005 09:12:35 +1000
- 

Hi. A quick question: Are you doing this in Safe Mode??

My system has been fine ever since. Good luck :-)

Cameron:-)

"LThibx" <[lthibx@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:lthibx@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote in message  
[news:FE3AF5D9-50BC-41EF-BEC1-7874AADD91A3@xxxxxxxxxxxxxxxxxxxx](mailto:news:FE3AF5D9-50BC-41EF-BEC1-7874AADD91A3@xxxxxxxxxxxxxxxxxxxx)

- > Please excuse my first post. My first message was inadvertantly posted
- > before it was complete.
- >
- > Glenn,
- >
- > I have the same exact problem that Cameron Dorrough had reported. I am
- > attempting to bring a new Win2003 DC online which will eventually replace
- my
- > Win2000 DC (2 separate machines). I receive the same error on my Win2003
- > box. My Win2000 DC applies GP fine. I have attempted your solution, but
- > after restarting the Win2003 server, the secdit.sdb database does not get
- > rebuilt, thought the log and chk files do.
- >
- > I now receive different events the in Applicaiton log, due the non
- existence
- > of the secdit.sdb. I have found KB article 278316 which describes how to
- > recreate it, but when I attempt to import any .inf template. I receive
- > messages under two scenarios:
- > Using secdit.sdb as the database name to create, I receive 'Access is
- > denied.
- > Import Failed. Make sure that you have rith right permissions to this
- > object'.
- >
- > Using some other db name, such as test.sdb, I receive 'An extended
- error
- > has
- > occured. Import Failed'
- >
- > I receive the messages above regardless of the .inf I choose. I am logged
- > in as Administrator.

Re: SceCli Error 1202 filling up the Event Log!

> Can you provide any insight?

>

>

>

> "LThibx" wrote:

>

>> Glenn,

>>

>> I have the same exact problem that Cameron Dorrough had reported. I am  
>> attempting to bring a new Win2003 DC online which will eventually  
replace my

>> Win2000 DC (2 separate machines). I receive the same error on my  
Win2003

>> box. My Win2000 DC applies GP fine. I have attempted your solution,  
but

>> after restarting the Win2003 server, the secdit.sdb database does not  
get

>> rebuilt, though the log and chk files do. I know receive different  
events

>> the in Applicaiton log, due the non existence of the secdit.sdb. I have

>> found KB article 278316 which describes how to recreate it, but when I

>> attempt to import any .inf template. I receive messages under two  
scenarios:

>>

>>

>>

>> I have been unsuccessful in recreating the secdit.sdb. I found KB

>> articleCan you provide any insight?

>>

>> "Glenn L" wrote:

>>

>>> I have never seen "Error deleting SCP" and don't really know  
specifically

>>> what SCP stands for.

>>> I don't know of any increased logging short of attaching a debugger to

>>> winlogon.exe to find out what scecli.dll is doing when it applies.

>>> However, I suspect this can be fixed by simply blowing away the local

>>> security database and have it recreated.

>>>

>>> The procedure is straight forward, however you need to prepare for it  
and

>>> plan for a short outage in service.

>>> This is just a member server right?

>>> the database (local group policy) contains out of the box security  
settings.

>>> If you have made any modifications to the local group policy under  
"computer

>>> configuration\windows settings\security settings, you should inventory  
those

>>> settings.

>>> Once the settings are inventoried, do the following:

Re: SceCli Error 1202 filling up the Event Log!

Re: SceCli Error 1202 filling up the Event Log!

>>>  
>>> browse to c:\windows\security\database & rename secedit.sdb  
>>> browse to c:\windows\security & rename edb.chk, edb.log, res1.log, &  
>>> res2.log  
>>> reboot the server. A new blank database, chkpoint, and logs will be  
>>> created.  
>>> All default out of the box security and local group policy settings  
are gone  
>>> at this point.  
>>> You need to reapply them to the server.  
>>> follow the procedure in <http://support.microsoft.com/?kbid=313222>  
>>> This works on W2K and W2K3 server as well.  
>>> Then reapply local security settings you inventoried previously.  
>>> At this point you should be able to execute a gpupdate /force and get  
a  
>>> \*happy\* scecli 1704 event.  
>>>  
>>> Cheers!  
>>>  
>>> ---  
>>> Glenn L  
>>> CCNA, MCSE 2000/2003 + Security  
>>>  
>>> "Cameron Dorrough" <cdorrough@xxxxxxxxxxxxxxxxxxxxxxxx> wrote in message  
>>> [news:d00jf6\\$3f1\\$1@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:d00jf6$3f1$1@xxxxxxxxxxxxxxxxxxxxxxxx)  
>>>> Thanks Glenn, I'd already set the ExtensionDebugLevel to 0x2.. is  
there  
>>>> anything else I can do?  
>>>>  
>>>> The App Log is filling up every couple of days with the SceCli error  
and  
>>>> nothing else! If there were any other errors, this might have been  
fixed  
>>>> by  
>>>> now. I'll include the entire Winlogon.log file below. None of it  
means  
>>>> anything to me (or to Microsoft apparently):  
>>>>  
>>>> \*\*\*\*\*  
>>>> Error 0 to send control flag 1 over to server.  
>>>> GPLinkDomain GPO\_INFO\_FLAG\_BACKGROUND )  
>>>> GPLinkOrganizationUnit GPO\_INFO\_FLAG\_BACKGROUND )  
>>>>  
>>>> [Mapping] gpt00000.dom = Default Domain Policy  
>>>> -----  
>>>> 03/01/2005 13:09:58  
>>>> Administrative privileged user logged on.  
>>>> Invoke Registry Value Delay Filter.  
>>>> Analyze machine\software\microsoft\windows  
>>>> nt\currentversion\setup\recoveryconsole\securitylevel.  
>>>> Analyze machine\software\microsoft\windows

Re: SceCli Error 1202 filling up the Event Log!

```
>>>> nt\currentversion\setup\recoveryconsole\setcommand.
>>>> Analyze machine\software\microsoft\windows
>>>> nt\currentversion\winlogon\allocatecdroms.
>>>> Analyze machine\software\microsoft\windows
>>>> nt\currentversion\winlogon\allocatedasd.
>>>> Analyze machine\software\microsoft\windows
>>>> nt\currentversion\winlogon\allocatefloppies.
>>>> Analyze machine\software\microsoft\windows
>>>> nt\currentversion\winlogon\cachedlogonscount.
>>>> Analyze machine\software\microsoft\windows
>>>> nt\currentversion\winlogon\passwordexpirywarning.
>>>> Analyze machine\software\microsoft\windows
>>>> nt\currentversion\winlogon\scremoveoption.
>>>> Analyze
>>>>
machine\software\microsoft\windows\currentversion\policies\system\disablecad
>>>> .
>>>> Analyze
>>>>
machine\software\microsoft\windows\currentversion\policies\system\dontdispla
>>>> ylastusername.
>>>> Analyze
>>>>
machine\software\microsoft\windows\currentversion\policies\system\legalnotic
>>>> ecaption.
>>>> Analyze
>>>>
machine\software\microsoft\windows\currentversion\policies\system\legalnotic
>>>> etext.
>>>> Analyze
>>>>
machine\software\microsoft\windows\currentversion\policies\system\shutdownwi
>>>> thoutlogon.
>>>> Analyze
machine\system\currentcontrolset\control\lsa\auditbaseobjects.
>>>> Analyze
machine\system\currentcontrolset\control\lsa\crashonauditfail.
>>>> Analyze
>>>> machine\system\currentcontrolset\control\lsa\fullprivilegeauditing.
>>>> Analyze
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel.
>>>> Analyze
machine\system\currentcontrolset\control\lsa\restrictanonymous.
>>>> Analyze
machine\system\currentcontrolset\control\print\providers\lanman
>>>> print services\servers\addprinterdrivers.
>>>> Analyze machine\system\currentcontrolset\control\session
manager\memory
>>>> management\clearpagefileatshutdown.
>>>> Analyze machine\system\currentcontrolset\control\session
>>>> manager\protectionmode.
```

Re: SceCli Error 1202 filling up the Event Log!

```
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\lanmanserver\parameters\autodiscon
>>>> nect.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforc
>>>> edlogoff.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecu
>>>> ritysignature.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresec
>>>> uritysignature.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enabl
>>>> eplaintextpassword.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enabl
>>>> esecuritysignature.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requi
>>>> resecuritysignature.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswor
>>>> dchange.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\netlogon\parameters\requiresignors
>>>> eal.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongk
>>>> ey.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechan
>>>> nel.
>>>> Analyze
>>>>
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechan
>>>> nel.
>>>> Analyze MACHINE\System\CurrentControlSet\Control\Lsa\SubmitControl.
>>>> Analyze MACHINE\Software\Microsoft\Non-Driver Signing\Policy.
>>>> Analyze MACHINE\Software\Microsoft\Driver Signing\Policy.
```

Re: SceCli Error 1202 filling up the Event Log!

>>>> Parsing template C:\WINNT\security\templates\policies\gpt00000.dom.  
>>>> Error 1208: An extended error has occurred.  
>>>> Error deleting SCP.  
>>>> ----Configuration engine is initialized with error.----  
>>>>  
>>>> ----Un-initialize configuration engine...  
>>>>  
>>>> I am rather frustrated but I do appreciate your help.  
>>>>  
>>>> BTW, 'gpupdate' doesn't seem to work, but 'secdit' does and that's  
how I  
>>>> generated the above..  
>>>>  
>>>> Thanks again,  
>>>> Cameron:-)  
>>>>  
>>>> "Glenn L" <the.only(delete)@gmail dot com> wrote in message  
>>>> [news:edpIuIfHFHA.2924@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:edpIuIfHFHA.2924@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)  
>>>>> I suggest you turn up winlogon logging to possibly get more detail  
on  
>>>>> this.  
>>>>>  
>>>>>  
>>>>> Registry Location –  
>>>>>  
HKLM\Software\Microsoft\WindowsNT\CurrentVersion\WinLogon\GPEExtensions\  
>>>>> {827D319E-6EAC-11D2-A4EA-00C04F79F83A  
>>>>>  
>>>>> Registry Setting – Add the REG\_DWORD value  
"ExtensionDebugLevel"  
>>>>> and set it to 0x2  
>>>>>  
>>>>> Then execute a gpupdate /force  
>>>>> verify you get the 1202 event  
>>>>>  
>>>>> Then review and post the winlogon.log to this thread.  
>>>>>  
>>>>>  
>>>>> --  
>>>>> Glenn L  
>>>>> CCNA, MCSE 2000/2003 + Security  
>>>>>  
>>>>> "Cameron Dorrrough" <cdorrrough@xxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in  
message  
>>>>>> [news:cvgden\\$m3c\\$1@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:cvgden$m3c$1@xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx)  
>>>>>> Okay, maybe I should have been a bit more specific..  
>>>>>>  
>>>>>> The bottom part of my Winlogon.log shows:  
>>>>>>  
>>>>>> Parsing template  
C:\WINNT\security\templates\policies\gpt00000.dom.

Re: SceCli Error 1202 filling up the Event Log!

>>>>> Error 1208: An extended error has occurred.  
>>>>> Error deleting SCP.  
>>>>> -----Configuration engine is initialized with error.-----  
>>>>>  
>>>>> Does anyone know how I can fix this?  
>>>>>  
>>>>> Thanks,  
>>>>> Cameron:-)  
>>>>>  
>>>>> "Jerold Schulman" <Jerry@xxxxxxxxxxx> wrote in message  
>>>>> <[news:qadm1151b06ipqm8njkntrtumo6pdsbk@xxxxxxxxxxx](mailto:news:qadm1151b06ipqm8njkntrtumo6pdsbk@xxxxxxxxxxx)  
>>>>>>  
>>>>>> The following articles were returned from the KB with a boolean  
search  
>>>>>> (scecli and 1202 and (1208 or 0x4b8)):  
>>>>>>> <http://support.microsoft.com?kbid=260715> "Event ID 1000 and 1202  
After  
>>>>>>> Configuring Policies "  
>>>>>>> <http://support.microsoft.com?kbid=278316> "ESENT event IDs 1000  
1202  
>>>>>>> 412  
>>>>>>> and 454 are logged repeatedly in the Application log "  
>>>>>>> <http://support.microsoft.com?kbid=285903> "At Startup Error 1332  
Occurs  
>>>>>>> Message Reports Lack of Mapping Between Account Names and  
Security IDs  
>>>>>>> Inability to Find Power Users "  
>>>>>>> <http://support.microsoft.com?kbid=296854> "Restricted Groups Are  
>>>>>>> Limited  
>>>>>>> to  
>>>>>>> Local Domain Members Only "  
>>>>>>> <http://support.microsoft.com?kbid=324383> "Troubleshooting SCECLI  
1202  
>>>>>>> Events "  
>>>>>>> <http://support.microsoft.com?kbid=827012> "#34Windows Cannot Read  
>>>>>>> Template  
>>>>>>> Information#34 Error Message When You Try to View a Windows  
XP-based  
>>>>>>> Template in a Windows 2000 Domain "  
>>>>>>> <http://support.microsoft.com?kbid=835901> "A Restricted Groups  
policy  
>>>>>>> setting may not remove security identifiers in Windows 2000  
Server "  
>>>>>>>  
>>>>>>>  
>>>>>>>  
>>>>>>>> On Tue, 22 Feb 2005 15:12:30 +1100, "Cameron Dorrrough"  
>>>>>>>> <[cdorrrough@xxxxxxxxxxxxxxxxxxxxxxxxxxxx](mailto:cdorrrough@xxxxxxxxxxxxxxxxxxxxxxxxxxxx)> wrote:  
>>>>>>>>  
>>>>>>>>> Since yesterday we are getting the following error on our main  
file



Re: SceCli Error 1202 filling up the Event Log!

>>>>  
>>>  
>>>  
>>>

.

---

• **Follow-Ups:**

- ◆ **Re: SceCli Error 1202 filling up the Event Log!**  
◇ From: LThibx

• **References:**

- ◆ **Re: SceCli Error 1202 filling up the Event Log!**  
◇ From: LThibx
- ◆ **Re: SceCli Error 1202 filling up the Event Log!**  
◇ From: LThibx

- Prev by Date: **Re: SceCli Error 1202 filling up the Event Log!**
- Next by Date: **Re: problem when we start a service**
- Previous by thread: **Re: SceCli Error 1202 filling up the Event Log!**
- Next by thread: **Re: SceCli Error 1202 filling up the Event Log!**
- Index(es):
  - ◆ **Date**
  - ◆ **Thread**