



# IAM

## AD SSO Troubleshooting Guide

**Version 12.0.18**



## Change Log

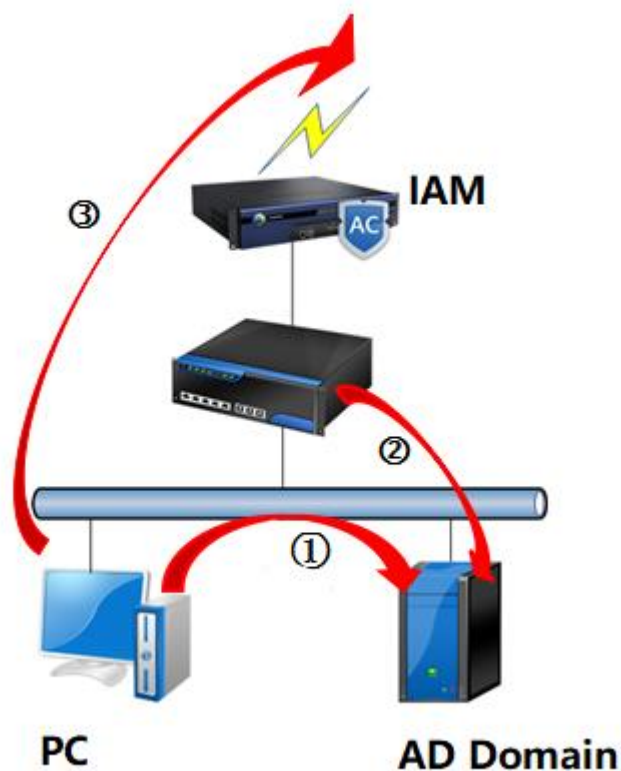
| Date        | Change Description                |
|-------------|-----------------------------------|
| Jul 2, 2019 | Version 12.0.18 document release. |
|             |                                   |

# CONTENT

|  |   |
|--|---|
| Chapter 1 Troubleshooting .....            | 1 |
| 1.1 Principle introduction.....            | 1 |
| 1.2 Check Configuration .....              | 1 |
| 1.2.1 Check configuration in IAM.....      | 1 |
| 1.2.2 Check AD Domain configuration .....  | 2 |
| 1.2.3 Check connectivity .....             | 3 |
| 1.3 Advanced Troubleshooting .....         | 4 |
| 1.3.1 Use wbemtest to troubleshooting..... | 4 |
| 1.3.2 Check Event ID .....                 | 7 |
| 1.3.3 Check AD Domain .....                | 7 |

# Chapter 1 Troubleshooting

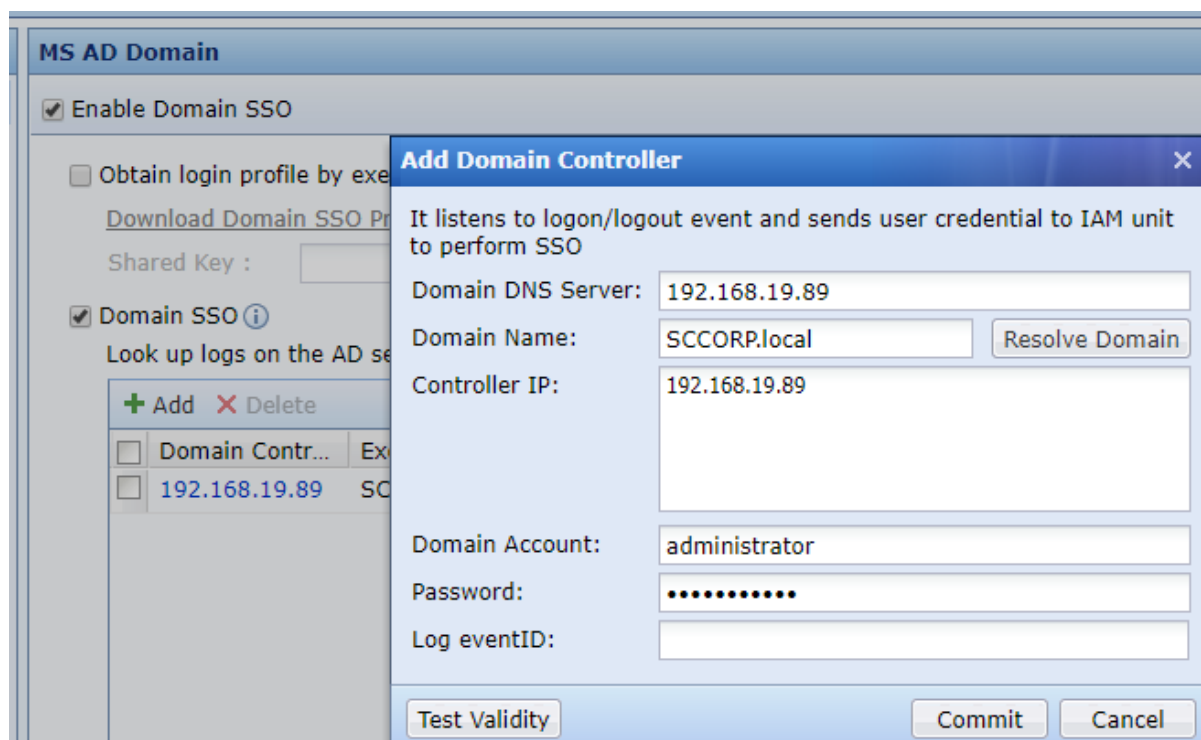
## 1.1 Principle introduction



1. PC join AD Doamin.
2. IAM read logon log and account logon log from AD Domain, if IAM get valid information, then the user will be authenticated automatically and PC able to access internet.

## 1.2 Check Configuration

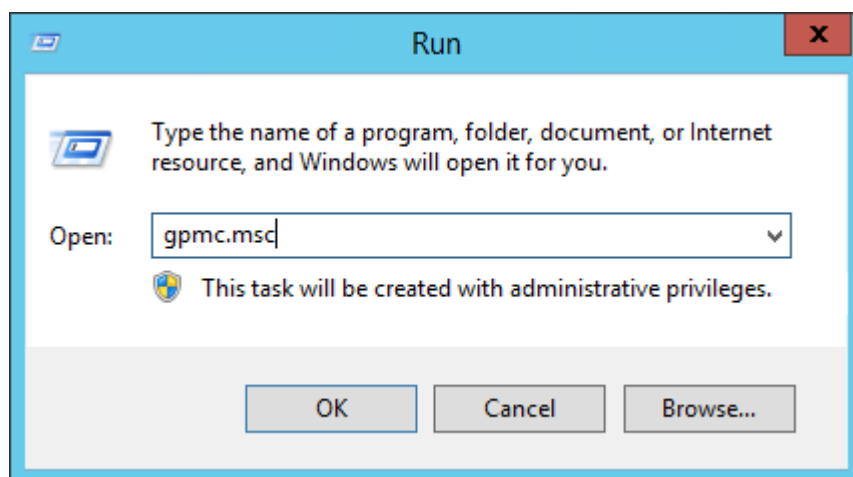
### 1.2.1 Check configuration in IAM

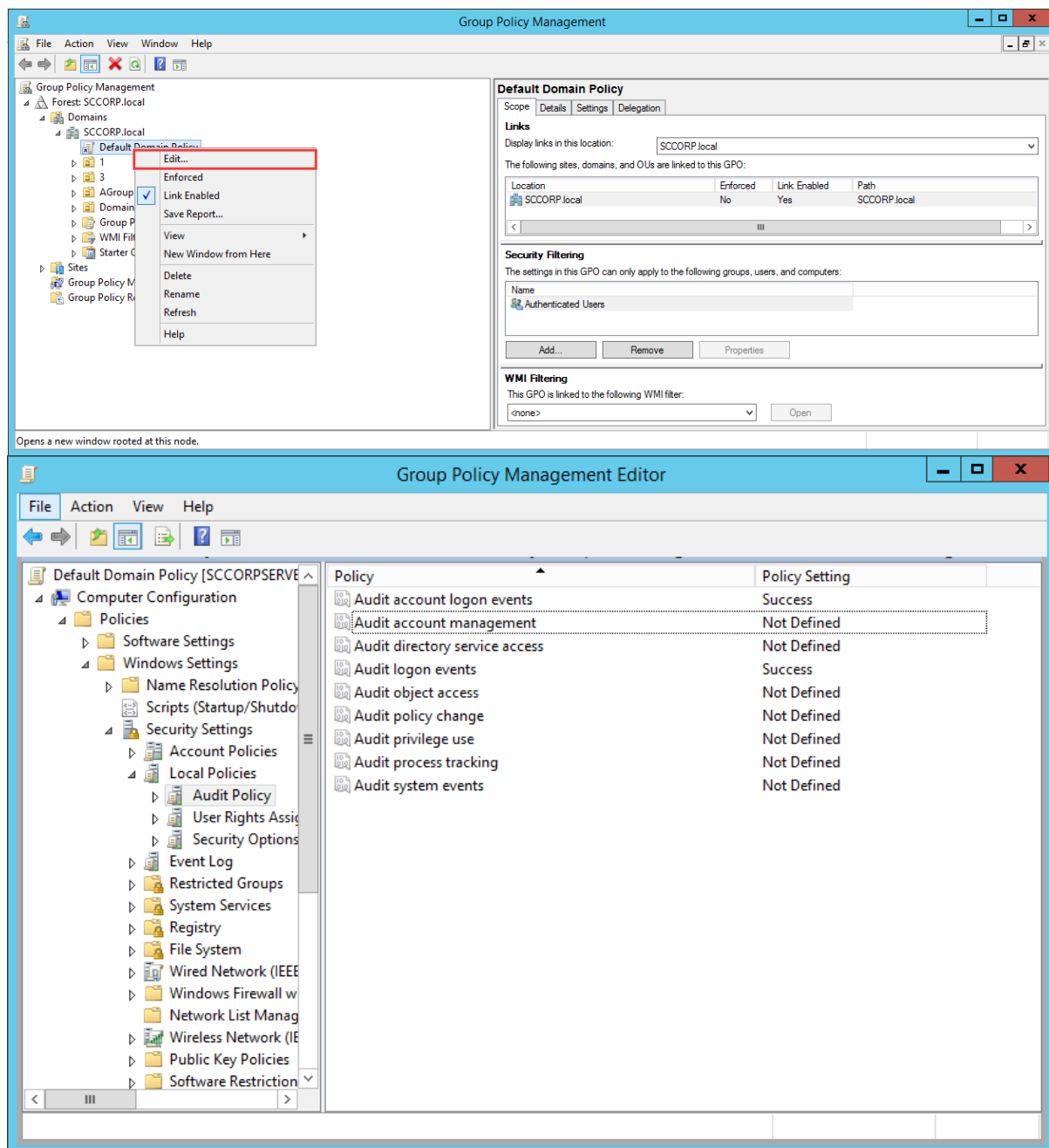


- Check whether Domain Name is fill in completely.
- Check whether the password Password is fill in correctly.
- It's recommended to use administrator user account to test.

### 1.2.2 Check AD Domain configuration

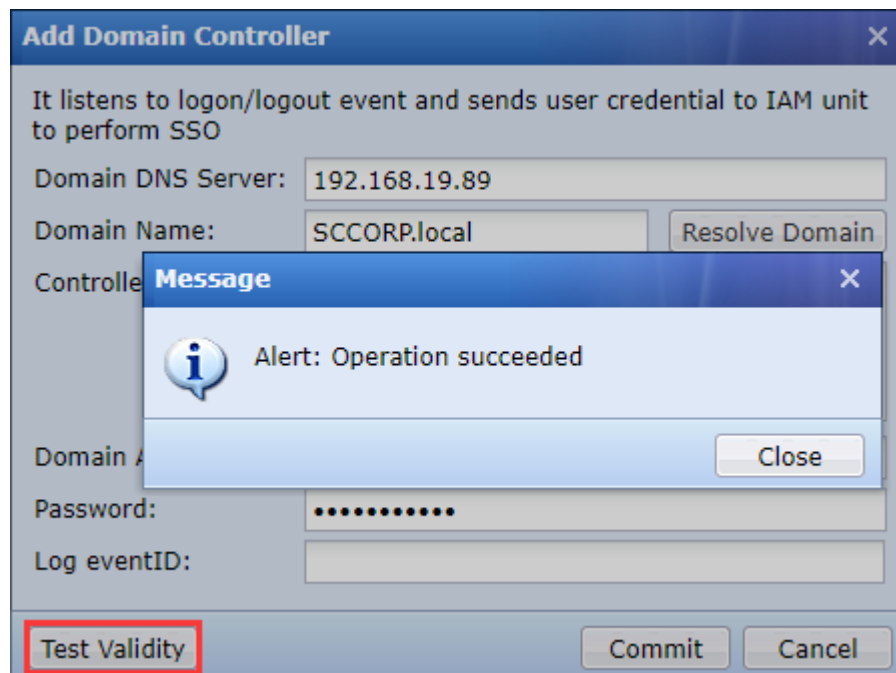
- The most important configuration is that you must Open Audit Log Settings, you can following method: Input **gpmc.msc** in **cmd** or **Run**, edit the **Default Domain Policy**, check **Computer Configuration**, check **Policies**, check **Windows Settings**, check **Security Settings**, check **Local Policy**, Check **Audit Policy**, set **Audit account logon events** success, set **Audit logon events** success.





### 1.2.3 Check connectivity

- You can click Test Validity to test connectivity.

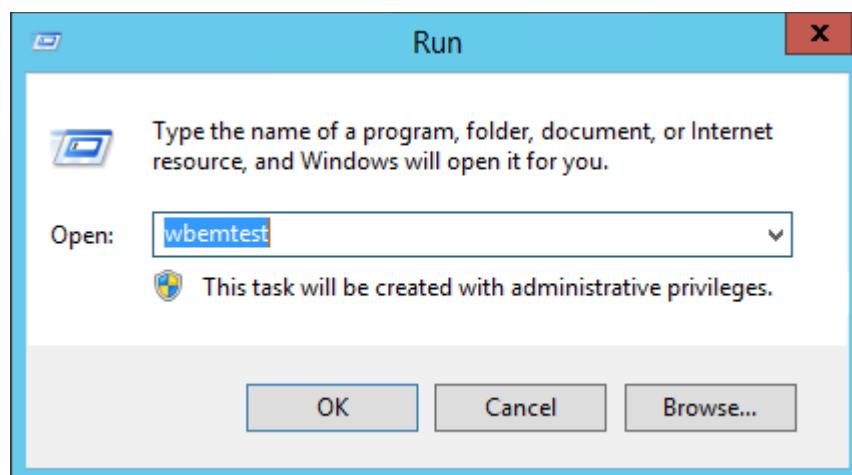


## 1.3 Advanced Troubleshooting

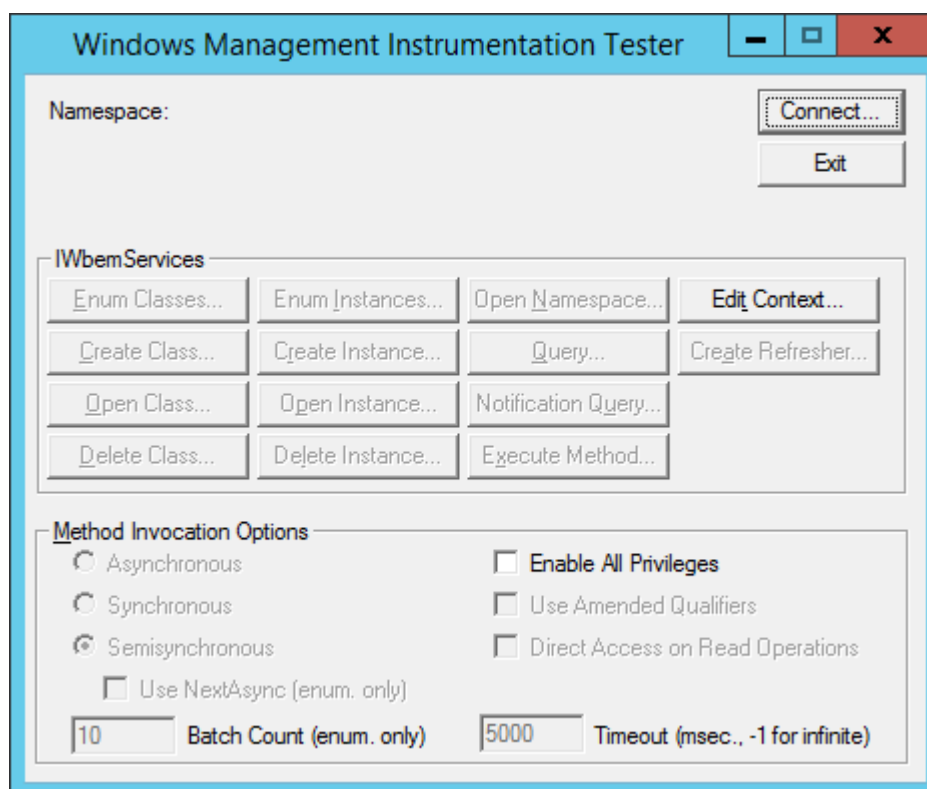
### 1.3.1 Use wbemtest to troubleshooting

wbemtest is a built-in tool that was included in Windows Operating System. it's use to query system information.

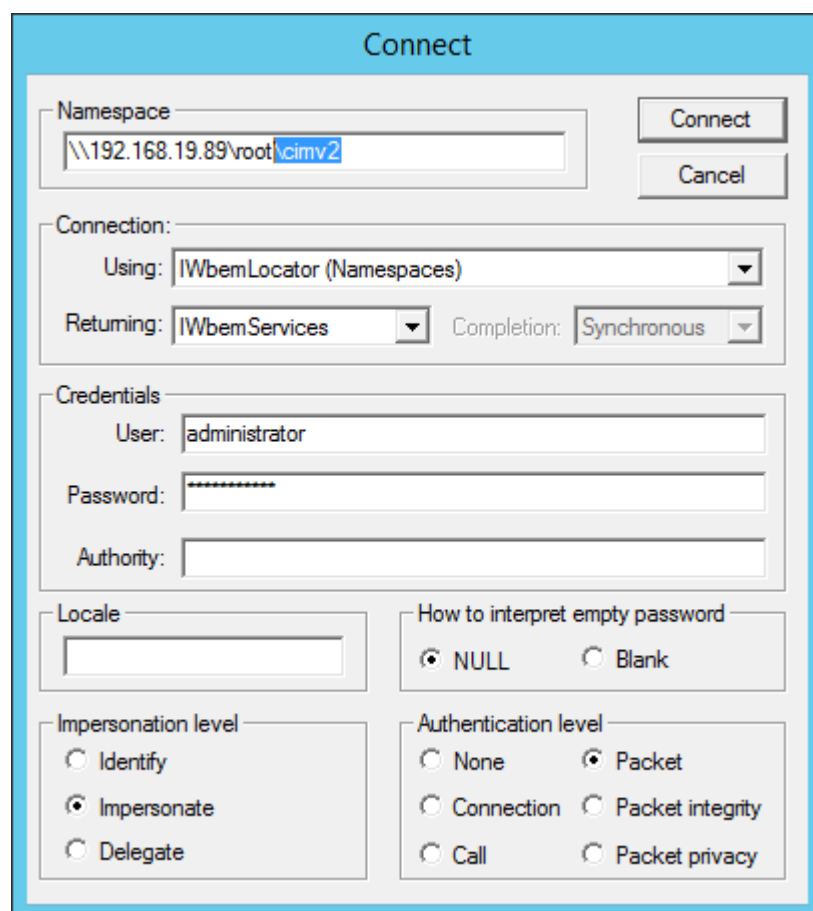
Input **wbemtest** in **cmd** or **Run**.



Click **Connect**.



- Fill in **User** and **password** of AD domain, write **Namespcae** as following format:  
**\\IP of AD Domain\root\cimv2**

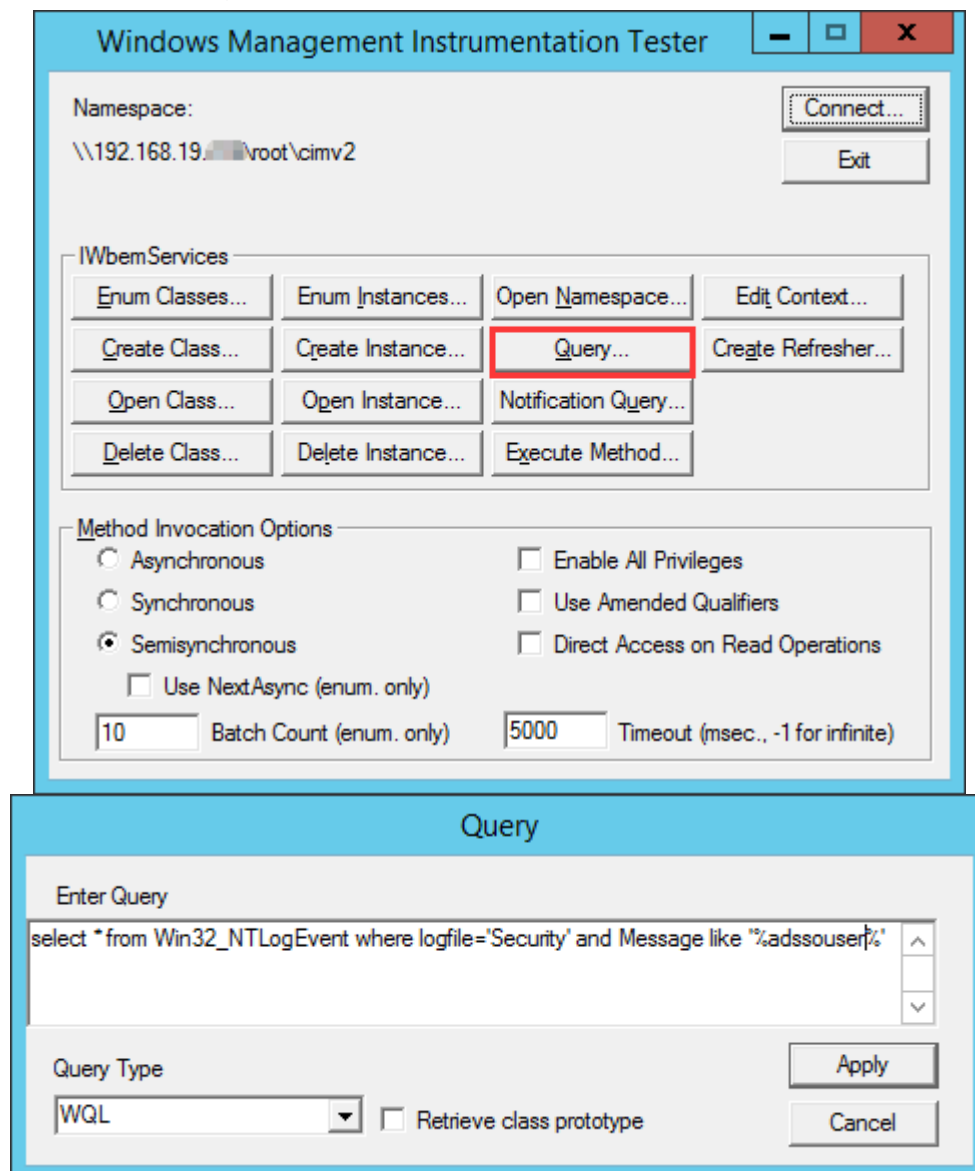




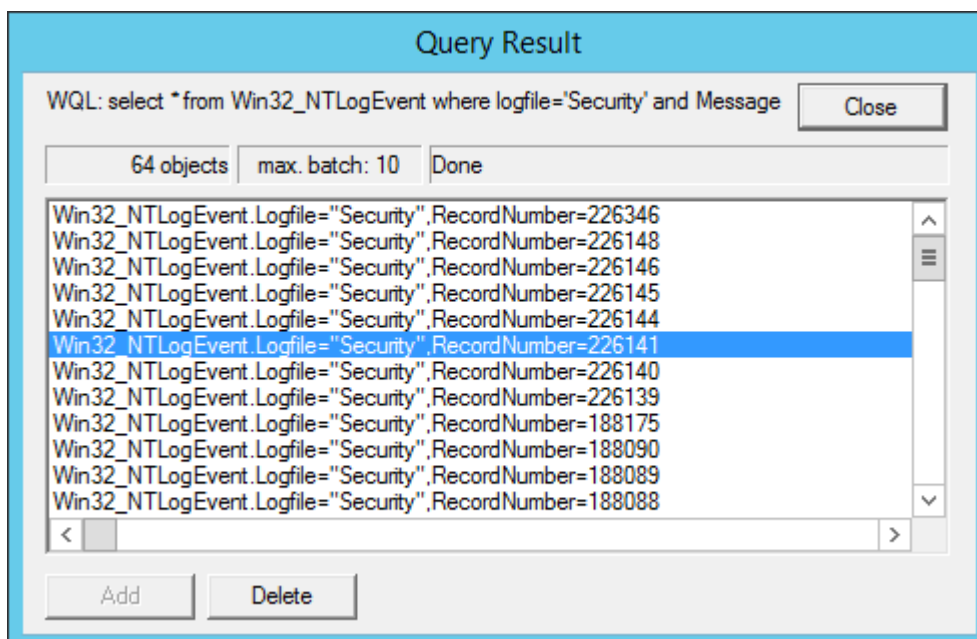
- Click Query and fill in query segment as following:

**select \* from Win32\_NTLogEvent where logfile='Security' and Message like '%xxx%'**

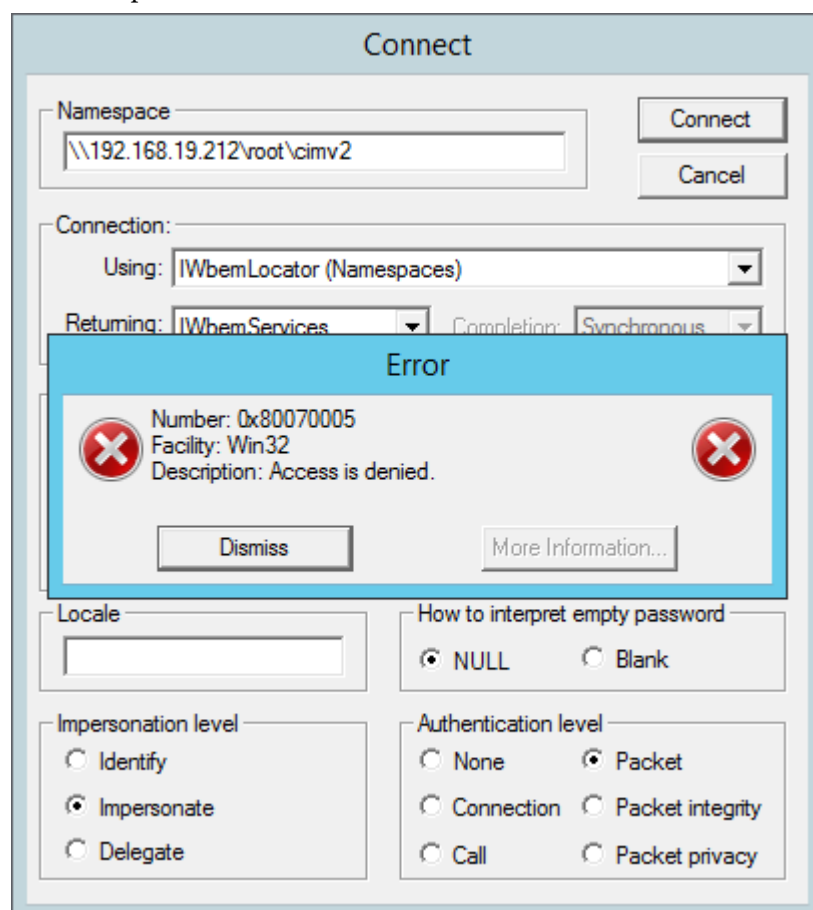
**xxx** is account you use to login



- If you see information such as following log, that means log was created in AD Domain.



- If you see following error, it might because of user account that you used doesn't have permission to access AD Domain, please use administrator account to test.



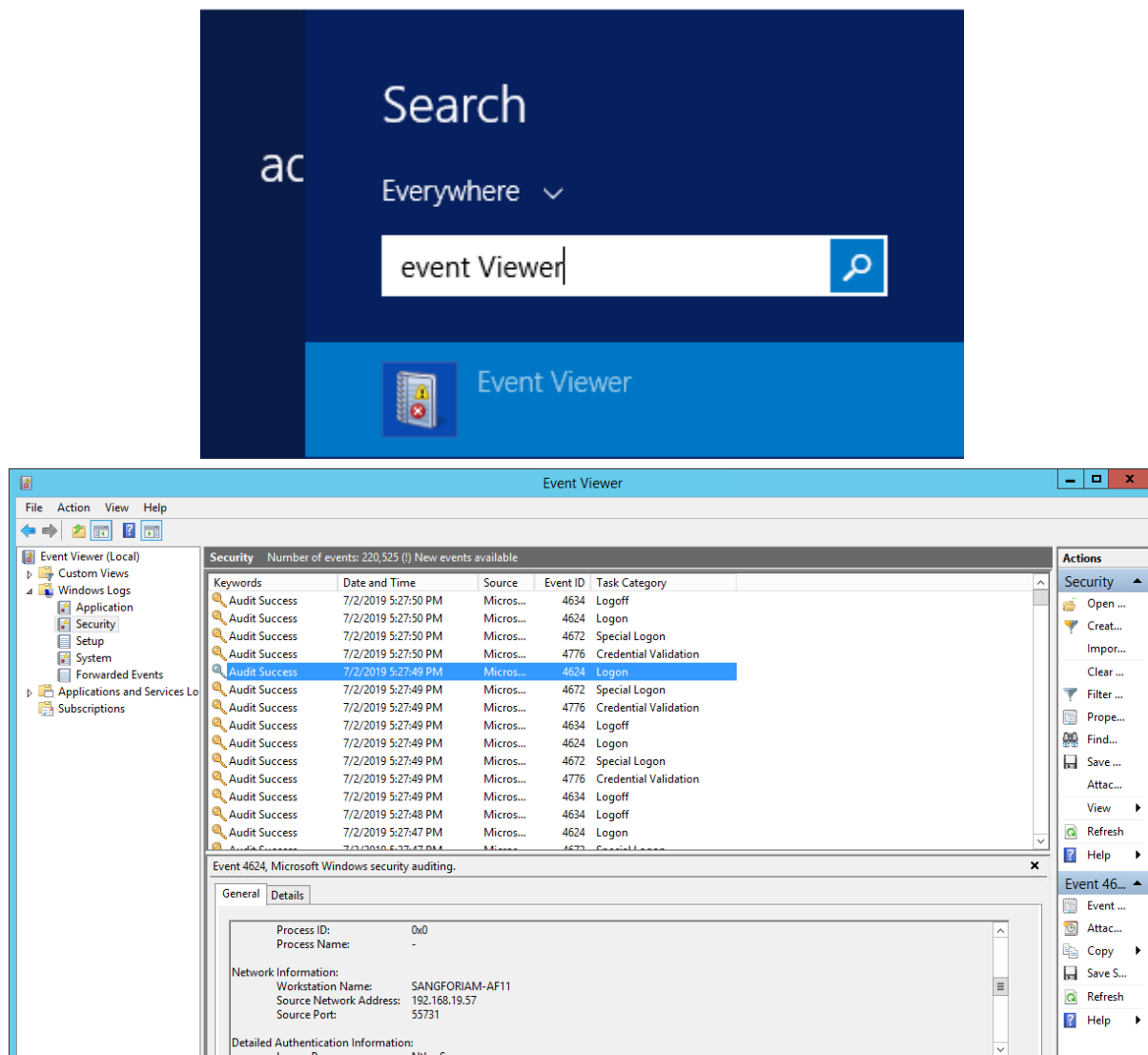
### 1.3.2 Check Event ID

The default Event ID of login log is 4624 or 672 or 540, but it may be changed by IT administrator, so, if it was changed, please fill in **Log EventID**.

### 1.3.3 Check AD Domain

Please check whether AD Domain generate Login log, insert **Event Viewer** in Run or Startup menu,

click **Windows Logs**, click **Security**, search whether the logs include in Logon log.





**SANGFOR**

Copyright © SANGFOR Technologies Inc. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of SANGFOR Technologies Inc.

SANGFOR is the trademark of SANGFOR Technologies Inc. All other trademarks and trade names mentioned in this document are the property of their respective holders.

Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. The information in this document is subject to change without notice. To obtain the latest version, contact the international service center of SANGFOR Technologies Inc