

ASSET & Microsoft Visio Interoperability

Revision History
1.00

August 6, 2002

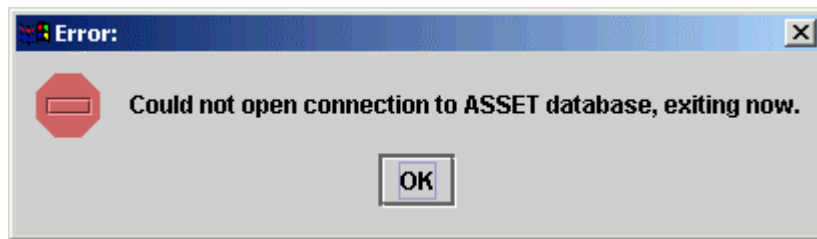
Initial Version

Introduction:

This document attempts to describe and resolve the interoperability issues between ASSET and Microsoft Visio 2000 Enterprise, and Visio 2002 professional. These issues mainly occur during the ASSET installation, when the ASSET installer attempts to change the default systems administrator or 'sa' user account password to connect to the Microsoft SQL Server Desktop Engine (MSDE) 1.0 subsystem.

Who should read this document?

Users of NIST ASSET should follow the instructions provided in this document if the following error or similar image appears`:



This error could occur when using either ASSET System or ASSET Manager, and during attempts to create a new assessment, import assessments, and/or generate reports.

Background:

Beginning with Visio 2000 Enterprise, Microsoft offered a feature that required the use of the MSDE or a complete Microsoft SQL Server. NIST ASSET also uses MSDE for its data storage and retrieval. On a default installation of MSDE 1.0, the 'sa' account has a blank password. The following quote is taken from a Microsoft.com webpage that describes the AutoDiscovery and Layout feature of Visio:

"...Visio Enterprise 2000 AD&L and the AD&L solution from Visio Enterprise Network Tools 2002 use MSDE to store network information discovered during the AutoDiscovery process. Visio Enterprise installs MSDE when AutoDiscovery and Layout is installed if neither MSDE nor SQL Server resides on your system."

Visio expects the 'sa' account password to not change. If the ASSET installer successfully changes this password, this feature of Visio will fail to operate. The following URL describes how to resolve this problem within Microsoft Visio to enable this feature again:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/visio/visio2002/maintain/vis_msde.asp

Laboratory testing has revealed that the password for the 'sa' account is not set to anything other than the default when Visio is installed prior to NIST ASSET. See the **Password Verification Tests** section for tests to perform on your system to verify the password for this 'sa' account.

MSDE Vulnerabilities:

There are several known vulnerabilities associated with the MSDE, and these are outside the scope of this discussion, but they are discussed in the ASSET User Manual. The following URLs describe the vulnerabilities surrounding the MSDE system:

- <http://www.sqlmag.com/Articles/Index.cfm?Action=News>
- <http://online.securityfocus.com/search?submit=yes&category=1&order=ASC&query=MSDE>

Problem Description:

The NIST ASSET installer adopts a very aggressive two-step approach to mitigating vulnerabilities introduced by the MSDE system through the Database Password Utility. After the MSDE system has been installed and the appropriate databases have been created the installer attempts to change the password of the 'sa' account to a value of **nis7@ss3t**. The installer then runs the ASSET Database Password Utility to change the password once again, adding a second layer of security to the password change process. The following image shows the interface of the NIST ASSET Database Password Utility.



Instructions on the use of the NIST ASSET Database Password utility can be found in the NIST ASSET User Manual.

Password Verification Tests

This section describes the tests that verify the password of the 'sa' account. Users should only perform these tests if they have received the error shown in the "**Who should read this**

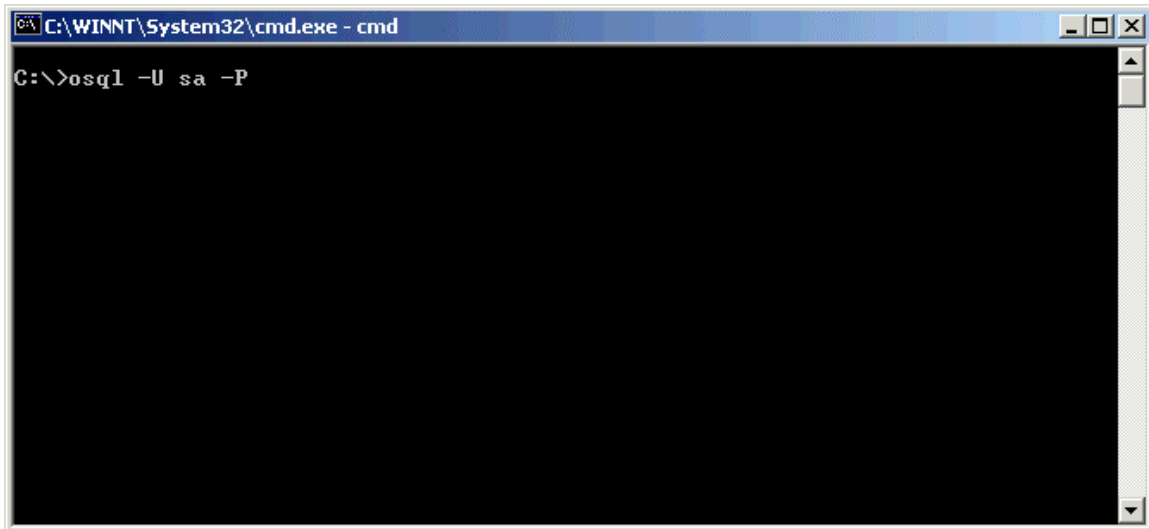
document?" section. The verification of the password for the 'sa' account is a three-step process.

1. Verify that the password for the 'sa' account is not blank.

To perform this test open a command prompt window and enter the following syntax exactly as shown here:

```
C:\>osql -U sa -P
```

as shown in the following figure:



This syntax attempts to login to the MSDE system using the 'sa' account with no password. Users will receive only one of the two following responses:

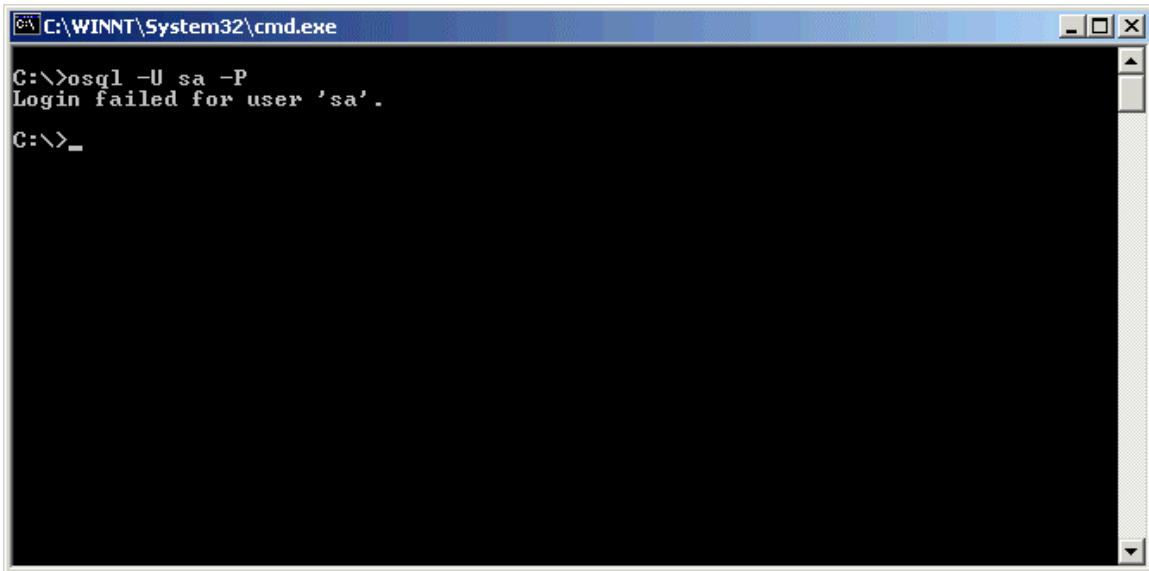
- Failed login: A failed login is indicated by the following message displayed in the command window:

```
C:\>osql -U sa -P
```

```
Login failed for user 'sa'
```

```
C:\>
```

This is shown in the following figure:

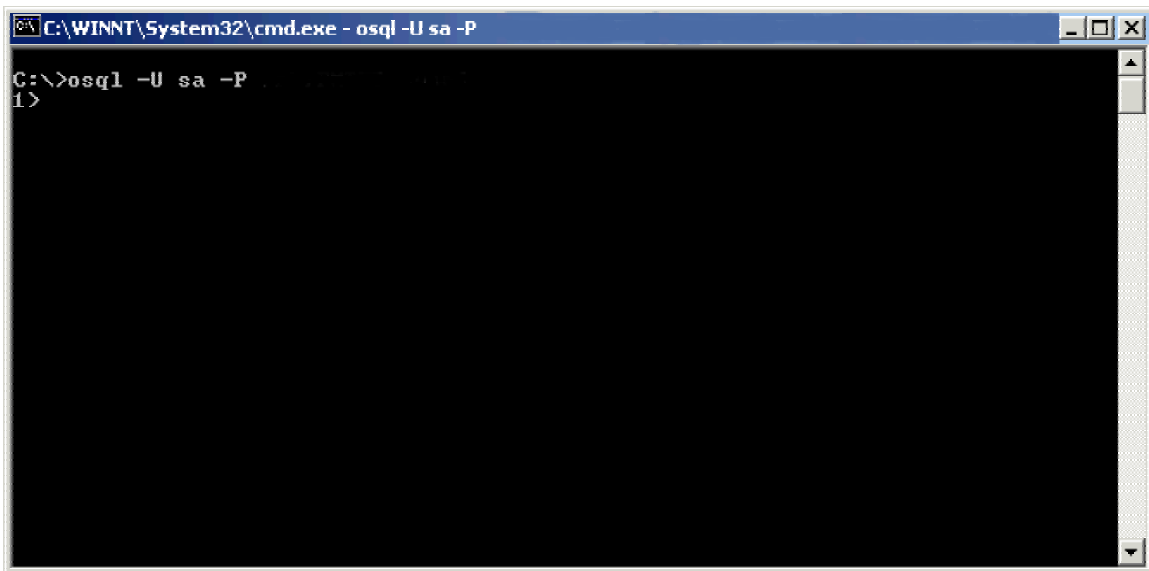


```
C:\WINNT\System32\cmd.exe
C:\>osql -U sa -P
Login failed for user 'sa'.
C:\>_
```

- Successful login: A successful login is shown in the following message:

```
C:\>osql -U sa -P
1>
```

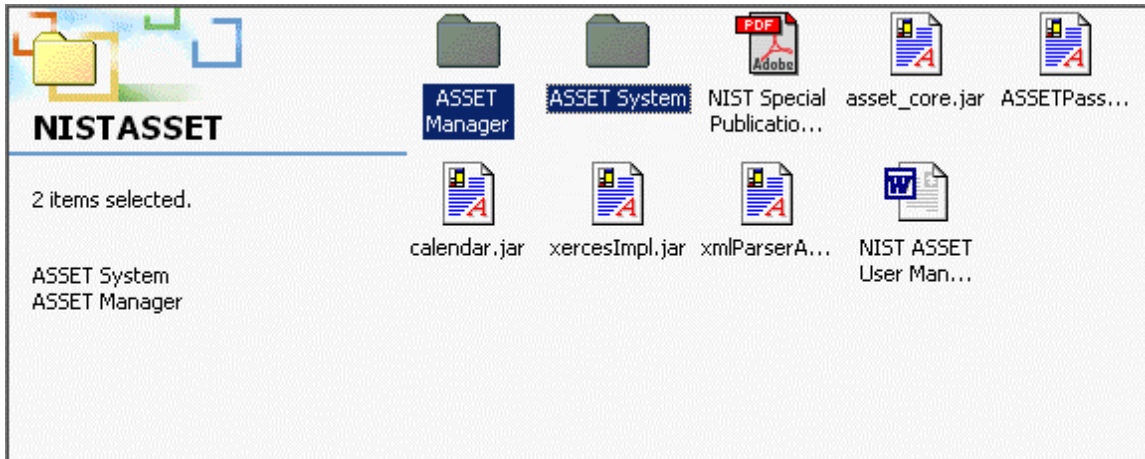
This message indicates that the password for the 'sa' account was indeed blank. The 1> is the command prompt for MSDE. This result is shown in the following figure:



```
C:\WINNT\System32\cmd.exe - osql -U sa -P
C:\>osql -U sa -P
1>
```

2. If the password for the 'sa' account was not blank then proceed to step 3, otherwise verify that the password stored for ASSET System and ASSET Manager is blank as well.

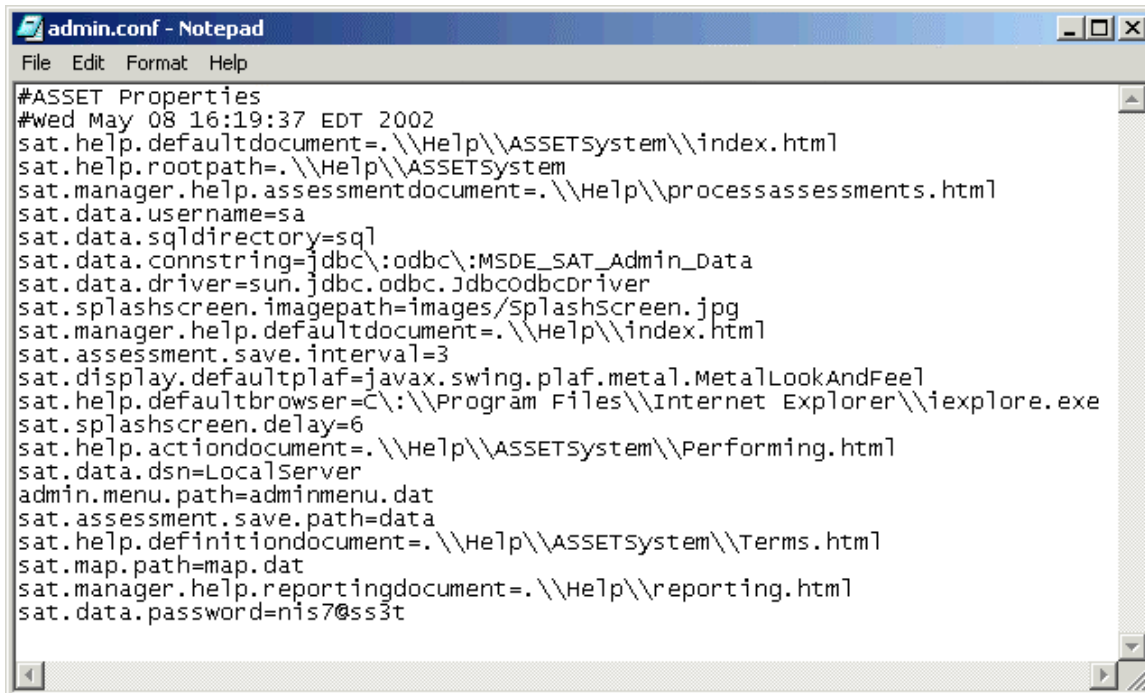
Open the configuration files **sat.conf**, and **admin.conf**. These files are located in the **C:\Program Files\NISTASSET\ASSET System** and **ASSET Manager** folders as shown in the following figure:



These property files contain a line that starts with the following text:

sat.data.password=

When the 'sa' account password is blank the property file **admin.conf** may look similar to the following figure:



The values in **admin.conf** and the file **sat.conf** will contain the same value. To fix this problem the **sat.data.password** line must be edited in both files, and if present the value 'nis7@ss3t', or any other value must be removed such that the line **sat.data.password** reads as follows:

sat.data.password=

3. Verify that the password for the 'sa' account is not **nis7@ss3t**

This value is what the ASSET database password utility attempts to change the 'sa' account password to prior to allowing users to choose their own password. If steps 1 and 2 have been completed, and the password for the 'sa' account is not blank, then step 1 should be repeated and the password used to test the MSDE system should be the value **nis7@ss3t**

4. If the password for the 'sa' account is verified not to be **nis7@ss3t**, proceed to step 5 otherwise step 2 should be repeated and instead of setting the property **sat.data.password** to a blank value, it should be set to **nis7@ss3t**

5. Verify that the password for the 'sa' account is the value set in the ASSET property files.

If the password for the 'sa' account is in fact verified not to be **nis7@ss3t**, and not blank, then the next step is to verify that the password for the 'sa' account is the value that is stored in the ASSET property files **admin.conf** and **sat.conf** (similar to step 2). In this case users should check to see that the password for the 'sa' account is the value of the property **sat.data.password** again similar to step 2.

Summary

If users are unable to log into the MSDE system with any of the tests described above then the password for the MSDE system is set to a value that must be determined before installing ASSET. Since MSDE stores these passwords in encrypted format it is essentially impossible to give advice to users that do not know their MSDE 'sa' account passwords. The only advice that can be given in this case is to uninstall MSDE and reinstall using the ASSET installer.