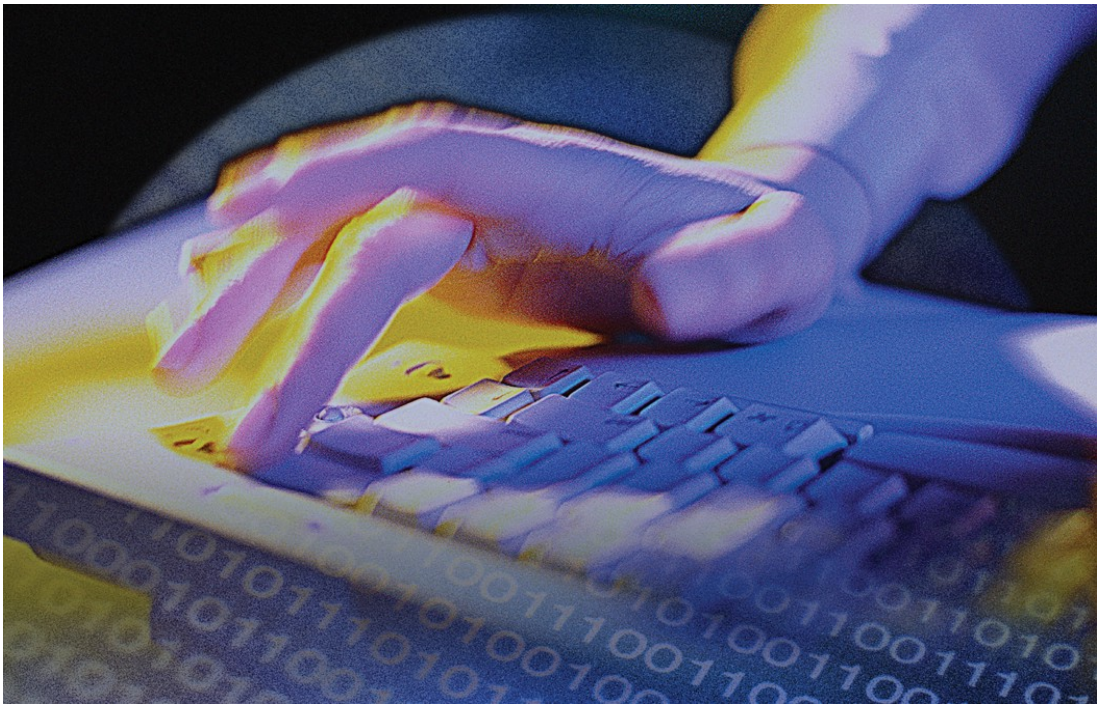
National Institute of
Standards and Technology
Technology Administration
U.S. Department of Commerce

NISTIR 6885 2004 ED

Automated Security Self-Evaluation Tool User Manual

Marianne Swanson, Marc Stevens,
Ivette Jimenez, Vlad Korolev



NISTIR 6885 2004 ED

Automated Security Self-Evaluation Tool User Manual

Marianne Swanson,
Marc Stevens, Ivette Jimenez,
Vlad Korolev

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

December 2004

U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary of Commerce for Technology

National Institute of Standards and Technology
Areden L. Bement, Jr., Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON: 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov — Phone: (202) 512-1800 — Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

Acknowledgements

The authors wish to express their thanks to staff at NIST and at other organizations who reviewed drafts of this document. In particular, Murugiah Souppaya and Michael Reilly, NIST, and Jonathan Smith, Booz Allen Hamilton, provided valuable insights that contributed substantially to the technical content of this document.

Table of Contents

Table of Figures

1 Introduction

Organizations must plan for security, ensure that the appropriate officials are assigned security responsibility, and authorize system processing prior to operations and periodically thereafter. These management responsibilities presume that responsible organization officials understand the risks and other factors that could negatively impact their mission goals. Moreover, these officials must understand the current status of security programs and controls in order to make informed judgments and investments that appropriately mitigate risks to an acceptable level.

An important element of measuring the status of information technology (IT) security within an organization is to perform routine self-assessments of an organization's IT systems. There are many methods and tools available to help agency officials determine the current status of their security programs relative to existing policy. Ideally many of these methods and tools would be implemented on an ongoing basis to systematically identify programmatic weaknesses and, where necessary, establish targets for continuing improvement. For a self-assessment to be effective, a risk assessment[1] should be conducted in conjunction with or prior to the self-assessment. A self-assessment does not eliminate the need for a risk assessment.

The Automated Security Self-Evaluation Tool (ASSET) automates the process of completing a system self-assessment. ASSET will assist organizations in completing the self-assessment questionnaire contained in NIST Special Publication (SP) 800-26, *Security Self-Assessment Guide for Information Technology Systems*.

1.1 Description of ASSET

ASSET may be used to gather data and generate reports related to the status of the self-assessment. The intent of this tool is to provide a centralized place for the collection of data used to assess a system. ASSET contains the specific control objectives and suggested techniques for measuring the security of a system or group of interconnected systems as described in NIST SP 800-26. The control objectives and techniques are taken from long-standing requirements found in statute, policy, and guidance on security. ASSET consists of two host-based applications: ASSET – System and ASSET – Manager. This document explains ASSET – System. Appendix B of this document explains the unique functions of ASSET – Manager.

- **ASSET – System** facilitates the gathering of individual system data. It provides a limited reporting capability and allows the user to determine the completeness of an individual system assessment in progress.

- **ASSET – Manager** aggregates individual system assessments created by ASSET – System. It assists managers in developing an organization-wide perspective on the state of IT system security.

The reporting features of ASSET are designed to provide users with a clear picture of the security status of their resources, as specified in NIST SP 800-26. The reports available from ASSET can be generated and interpreted by the users who use the application. See Section 4.8 for additional information on the ASSET – System reporting features.

[1] See NIST Special Publication 800-30, Risk Management Guide for Information Technology Systems, January 2002, for more information on conducting a risk assessment.

ASSET stores data collected for the system self-assessment. The tool generates a system summary report, which provides a snapshot of assessment results. Unformatted reports can be exported to any popular spreadsheet or charting program. Formatted reports are available for export to Microsoft Excel. The results of the questionnaire can be used as input to a report evaluating an organization-wide IT security program. By sampling completed questionnaires, an agency can determine how well their policies and procedures are being followed and where resources should be expended.

A Federal Information Security Management Act (FISMA) reporting template has been developed to facilitate the extraction of data from ASSET – Manager to use in FISMA-required reports to OMB. Appendix C of this document explains the use of the FISMA reporting template.

1.2 Scope of Manual

This manual is intended to help users of ASSET – System understand each function of the tool and how the tool can be used to complete self-assessments. The term ASSET will be used for the remainder of the document to refer to ASSET – System. The target audience of this manual is the reporter/assessor[2]. This manual will use the term "you" to refer to this target audience. All other roles and responsibilities will be explicitly identified when referenced in the manual.

Tool functionality is the focus of this manual, not the substantive issues associated with NIST SP 800-26[3]. This manual does not attempt to address all navigation paths that could be used to answer sections of the self-assessment. As with most systems, there are multiple ways to address the information requested by ASSET. Because ASSET is a data collection and reporting tool, it does not provide users with techniques to analyze the data collected.

Section 1 of this manual provides a general introduction to the concept of IT security self-assessments and some considerations for the use of ASSET. Section 2 describes general roles and responsibilities for those who are involved in a typical IT security self-assessment. Section 3 describes the process to install ASSET. Section 4 provides detailed operating instructions for ASSET – System. Appendix A provides a glossary of commonly used terms in this manual and within ASSET. Appendix B provides detailed operating instructions for ASSET – Manager. This appendix also provides some strategies and considerations for employing ASSET in an operational environment. Appendix C of this document explains the use of the FISMA reporting template. Appendix D provides the critical business rules that were used in developing this application.

1.3 Considerations

The control objectives and techniques presented in ASSET and NIST SP 800-26 can be applied to organizations in private and public sectors. To perform the examination and testing required to complete the questionnaire, the assessor must be familiar with and able to apply a core knowledge set of IT security basics needed to protect information and systems. In some cases, especially in the area of examining and testing technical controls, assessors with specialized technical expertise will be needed to ensure that the questionnaire's answers are reliable.

[2] Roles are explained in Section 2.

[3] For additional information on substantive questions, please see NIST Special Publication 800-26 and the IT Security Assessment Framework, November 2000, issued by the Federal Chief Information Officer Council (Appendix C of NIST Special Publication 800-26).

1.3.1 Security

ASSET depends on host-based security resident within the desktop or laptop where ASSET is installed. There is no password protection provided for accessing the application or data therein. The login screen is strictly for identification, not authentication. It is assumed that any system where ASSET resides will have the appropriate security controls to ensure the protection of the collected information.

NOTE: Security is neither included in ASSET nor provided for data transmitted between ASSET – System and ASSET – Manager.

ASSET uses the Microsoft Data Engine (MSDE)[4] as its database engine and the Java Runtime Environment (JRE). Therefore, ASSET has all the vulnerabilities that are associated with MSDE and JRE.

Mitigating the associated vulnerabilities of MSDE can generally be accomplished in two ways: organization-wide perimeter security and vendor provided patches for MSDE. Additionally, the installation procedures contained in Section 5 can mitigate two of the most significant vulnerabilities of MSDE. Users of ASSET may view a current list of MSDE and JRE vulnerabilities and the method to mitigate the vulnerability at the following website:

http://icat.nist.gov

1.3.2 Importance of uninstalling ASSET after assessment is complete

Managers should consider uninstalling ASSET from systems after the self-assessment for the organization is complete. There are two reasons why ASSET should be uninstalled after the completion of the self-assessment:

- Access to uncontrolled and unprotected sensitive assessment data within an organization by personnel without a 'need to know' is avoided; and
- Ensuring that MSDE and JRE have the latest patches and service packs installed when ASSET is deployed in large numbers can become difficult. Without the latest patches installed, a system could be exposed to new and currently unidentified vulnerabilities associated with MSDE and JRE.

[4] More information related to the role of MSDE in ASSET is provided in Section 3.2.

2 Roles and Responsibilities

The roles described below are based on the process associated with conducting a typical self-assessment. Responsibilities are mapped to roles, not necessarily to specific people. It is possible that a person can have multiple roles.

2.1 Manager

The manager is the person who will be ultimately responsible for the assessment. Frequently, the person serving in the manager role is a program official with responsibility for IT security or the Chief Information Officer (CIO).

2.2 Reporter

The reporter needs to understand how to deploy, install, and execute ASSET. The reporter will be involved primarily with the use of ASSET – Manager. Other requirements of the reporter include:

- Importing system data from multiple assessors into ASSET – Manager
- Ensuring that all questions are answered for all systems
- Developing final reports organization-wide of the self-assessment results.

2.3 Assessor

The assessor is the person responsible for submitting one or more assessments to the reporter. They are the first point of contact in the event that there are any questions related to responses on the assessment. This person will ensure that all questions within the questionnaire are answered. Within ASSET, the terms assessor, primary assessor, and secondary assessor are used. On occasion, secondary assessors may be subject matter experts (SMEs).[5]

The assessor is responsible for the following:

- Ensuring that all questions are answered for each system under an assessor's review
- Interacting with the SME to gather and clarify system information
- Entering individual system data into ASSET.

2.4 Subject Matter Expert

The SME is an individual who is knowledgeable on specific topic areas (i.e., physical security, networks). The SME helps the assessor gather data related to the assessment. A SME is someone who may have specific input to a number of questions but is not responsible for the overall completion of the assessment. When used, SMEs should be identified for each question where they respond. Generally, a SME will be identified as a secondary assessor within ASSET. Although a person can be an assessor and an SME, generally this title is reserved for people who have specific knowledge and can provide clarification about a response to a specific question.

Key traits of a SME include:

[5] The role of subject matter experts is discussed in Section 2.4.

- Knowledgeable about the system and/or topic being assessed
- Provides specific responses to assessment questions
- Interacts with the assessor on an as-needed basis.

3 Installation

3.1 Requirements for Installation

Microsoft Windows® is the required operating system for ASSET. Much of the organization and logic of the ASSET installation process is similar to that required for other MS Windows application installations. ASSET installation files are available on NIST ASSET website:

http://csrc.nist.gov/asset/

NOTE: Internet connectivity is NOT a requirement for use of ASSET.

3.1.1 Hardware

The following are minimum hardware requirements to run ASSET:

- Pentium III – 1.0 GHz processor (or equivalent x86 compatible architecture)
- 256 MB RAM
- 120 MB of free disk space

NOTE: Each completed assessment in ASSET requires an additional 3 megabytes of hard disk space.

3.1.2 Software

The following minimum software is required for ASSET:

- ASSET was designed to operate with Windows 2000 Professional
- JRE version 1.2 or greater installed
- MSDE version 1.0 installed

NOTE: The ASSET installation process will install all required software, including JRE and MSDE.

3.2 Installation Process

3.2.1 Considerations for Installing ASSET v2

There are two ways you can install ASSET v2: full or incremental upgrade. The full install provides a complete installation of ASSET v2 for those users that do not have ASSET on their computers. You may also upgrade from ASSET v1 to ASSET v2 by using the upgrade installer. Both installers are available on the NIST website. Users that upgrade will not receive a v2 user manual (available on the NIST ASSET website) or the Database Manager utility, but all other functionality is the same as a full install.

The ASSET v2 full installer requires that either Microsoft Access 9.0 or Office Server Extensions or later (both are available as part of Microsoft Office 2000) be installed on your computer or that MSDE 1.0 be already installed. If you cannot install Microsoft Access or Office Server Extensions, you should first install ASSET v1.04, located at the NIST ASSET website and then use the upgrade installer (located at the NIST ASSET website) to move to v2.

Additionally, ASSET v2 has not been tested with MSDE 2000. Since only one version of MSDE can be installed on any one computer, users that wish to install ASSET v2 must first ensure that MSDE 2000 is not installed. If MSDE 2000 is installed, it must be removed before proceeding with the full install.

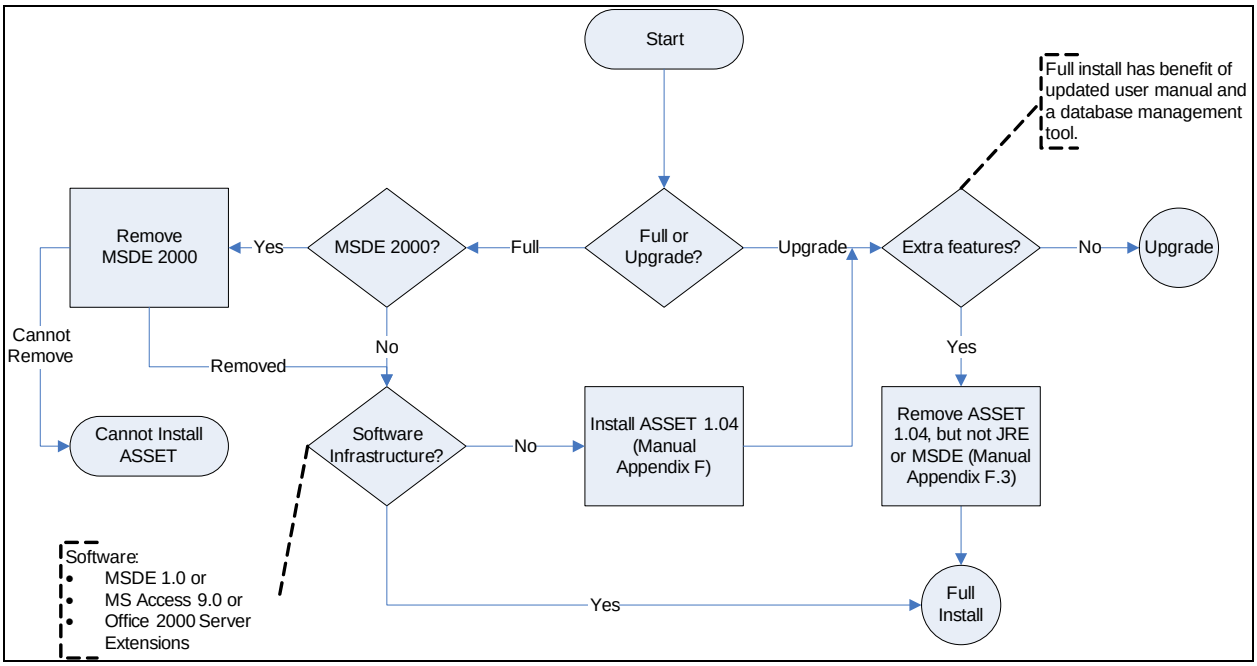


Figure 3.1 – Overview of Installation Process

A flowchart is provided above to assist you in understanding the decision process for using either the full or upgrade install paths. Appendix G has more detailed flowcharts for the full and upgrade install processes.

This section of the user manual provides a detailed description of the process for a new installation of ASSET. Users should refer to Appendix G and the NIST ASSET website for instructions on upgrading from v1 to v2.

Three major components are installed on your computer during the installation process:

- MSDE
- JRE
- ASSET program files

NOTE: Microsoft allows only one installation of MSDE on a single computer. If MSDE 2000 or later is installed on your computer, it must first be removed prior to installation.

The ASSET application and its program files are installed in the **Program Files** folder. If your computer has restricted access to this folder, your systems administrator will need to grant you permission to access the **NISTASSET** folder within the **Program Files** folder.

Additionally, the MSDE administrator password must be set and the ASSET database must be initialized. Section 3.2.2 provides guidance on completing these actions.

NOTE: Setting the MSDE administrator password is critical to eliminating one of the identified MSDE vulnerabilities.

One vulnerability with MSDE exists because MSDE is designed to allow your computer to function as a database server. The final action that you should perform in the installation process, which is not done automatically during the installation process, is to turn off this MSDE network functionality. (See Section 3.2.5 for instructions on how to turn off MSDE network functionality.)

NOTE: Turning off MSDE network functionality is not required by ASSET but it eliminates a number of MSDE vulnerabilities. If your computer requires MSDE network functionality, you should not perform this last installation process. If you are unsure if you need this functionality, consult your network administrator. MSDE vulnerabilities can be mitigated in other ways should you need to have MSDE network functionality. Examples include additional host-based or network-based security.

3.2.2 Installing ASSET and its Required Components

To install ASSET, double click the **InstallASSETv2.exe** file that you downloaded onto your computer from the NIST ASSET website. Click on the **Next** button to proceed with the installation.

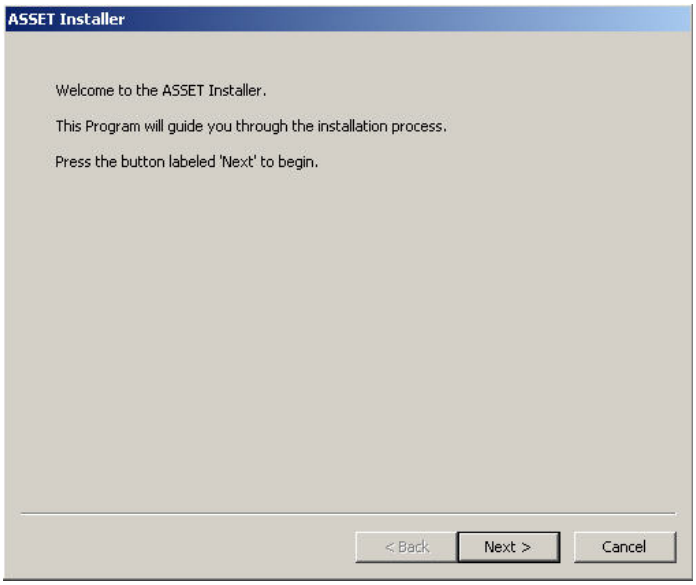


Figure 3.2 – ASSET Installation Start Screen

The licensing provisions of ASSET will be displayed. If you agree, **select** the check box. You must agree to the licensing provisions of ASSET if you wish to proceed with installation.

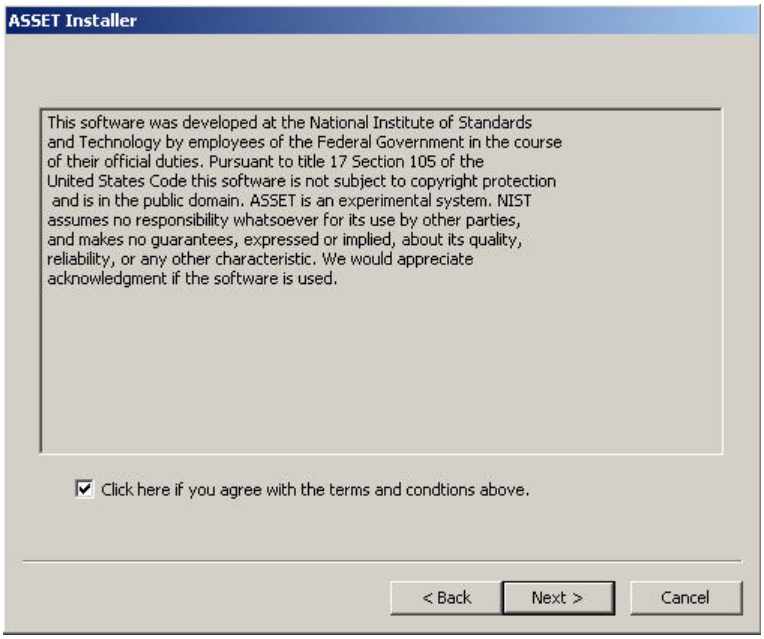


Figure 3.3 – License Agreement

Two options are available for installation: install ASSET – System only or install both ASSET – System and ASSET – Manager. In either option, all necessary components (MSDE and JRE) will be installed.

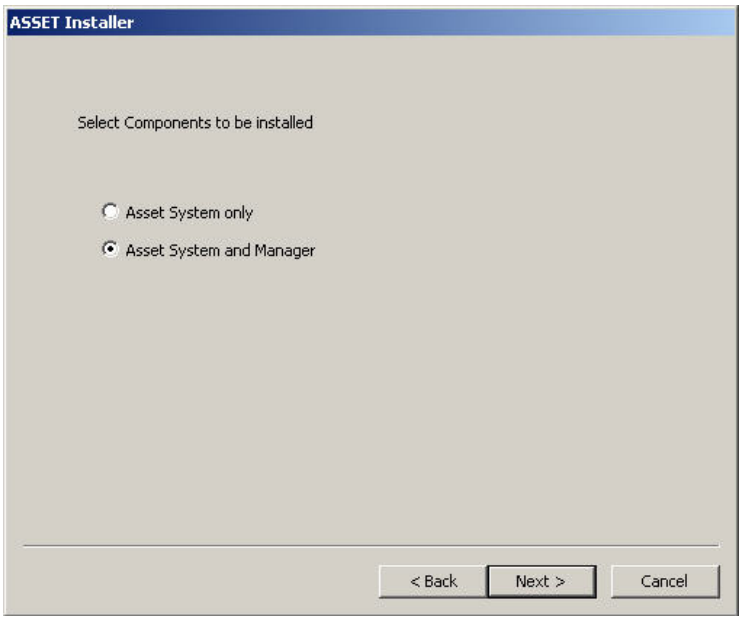


Figure 3.4 – Installation Types

NOTE: If you install only ASSET – System and later want to add ASSET – Manager, you will need to backup / export your data, uninstall ASSET – System and then install both ASSET – System and Manager. You will need to import your data after the install.

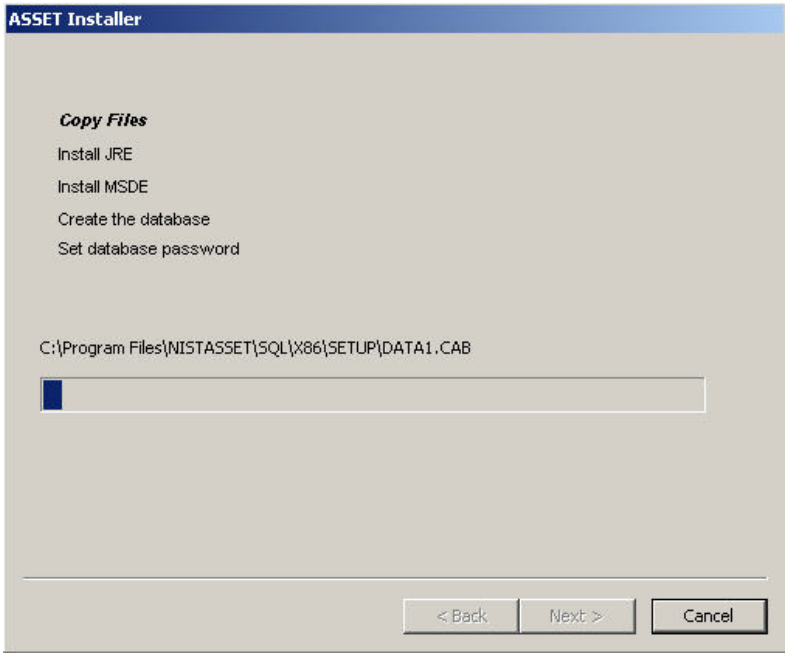


Figure 3.5 – Setup Status

The ***bold italic*** text on the status screen above indicates the step that the installer has reached in the installation process. If JRE or MSDE is detected on your computer, the ASSET installer will skip these steps.

An error may be displayed in the installation process that states the 'Service has not been started.' You should press OK to proceed with the installation.

The installer will then walk you through the installation of JRE.

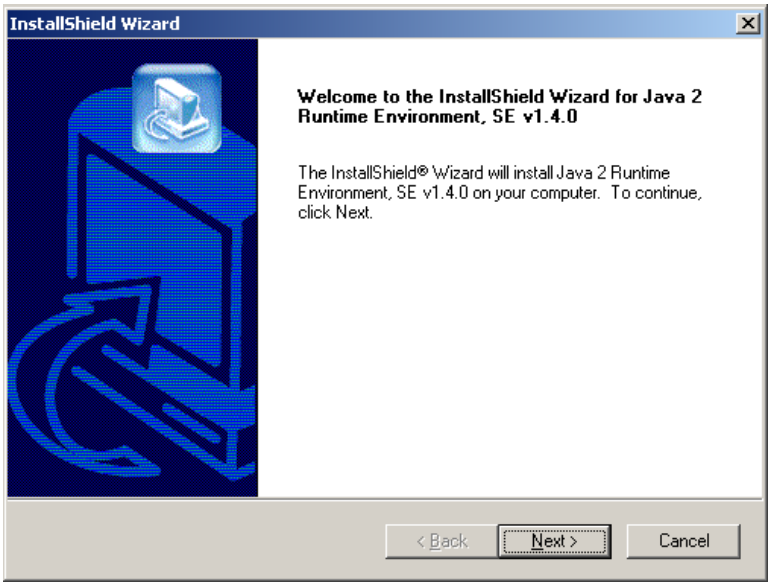


Figure 3.6 – JRE Installation

You will then be prompted to accept the JRE license agreement. You must accept this agreement to proceed with installation.

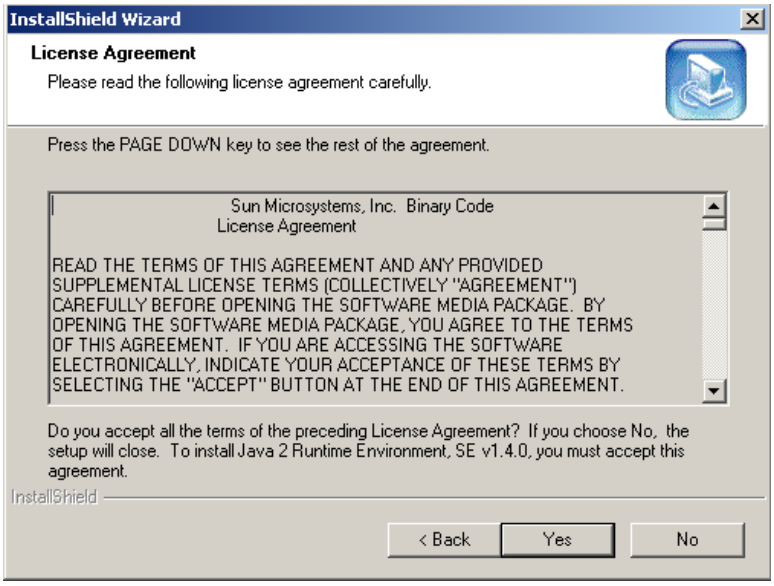


Figure 3.7 – JRE Installation License Agreement

You will be prompted to select the location in which you wish to install the JRE files.

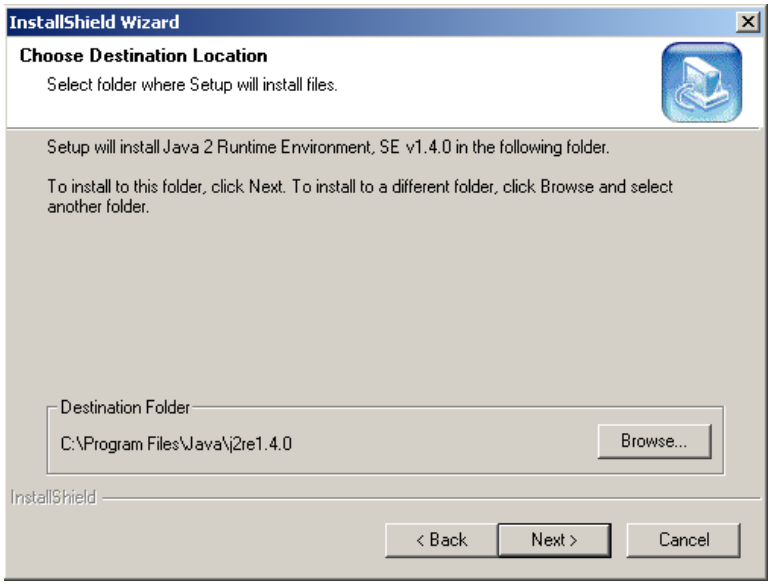


Figure 3.8 – JRE Destination Location

At this point in the installation process, you will be asked to select the browsers you wish to use JRE (ASSET).

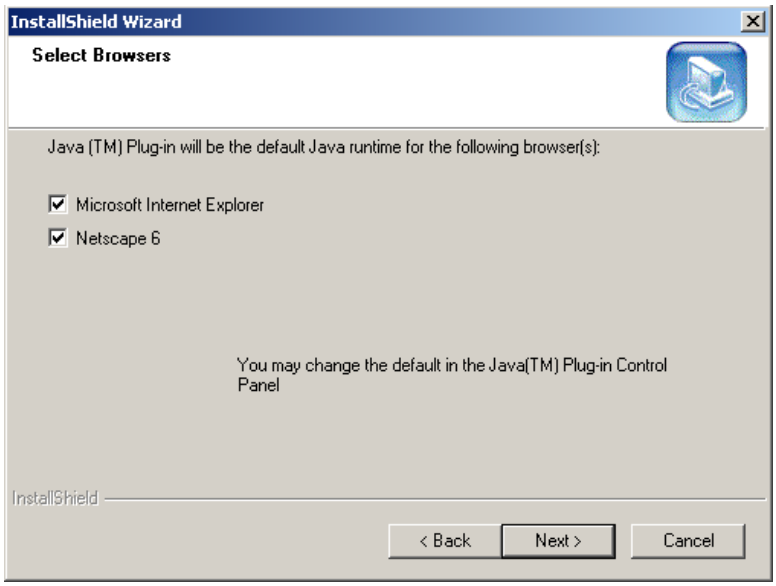


Figure 3.9 – JRE Browsers

The installer will then walk you through the installation of MSDE. If MSDE is already installed, the installer will proceed forward and not reinstall MSDE.

You should select **Local Install** and then **Next**.

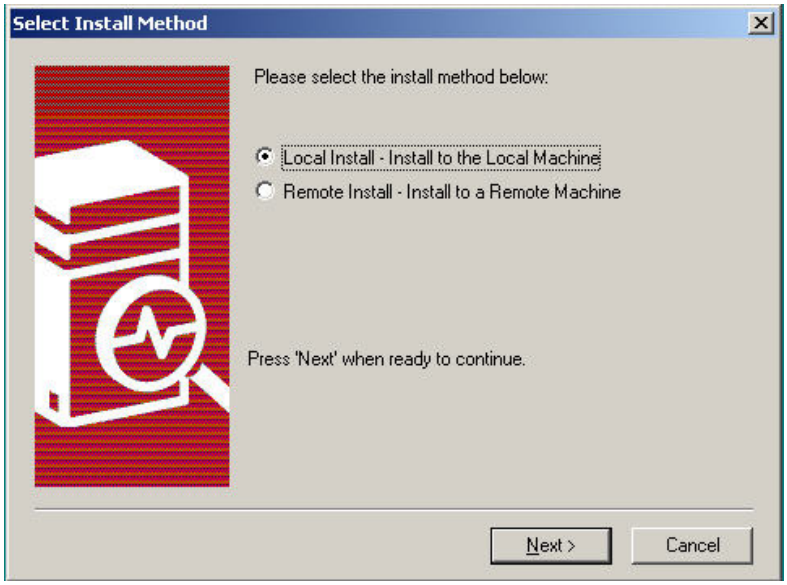


Figure 3.10 – MSDE Select Install Method

Select **Next** at the MSDE Installation Welcome Screen.

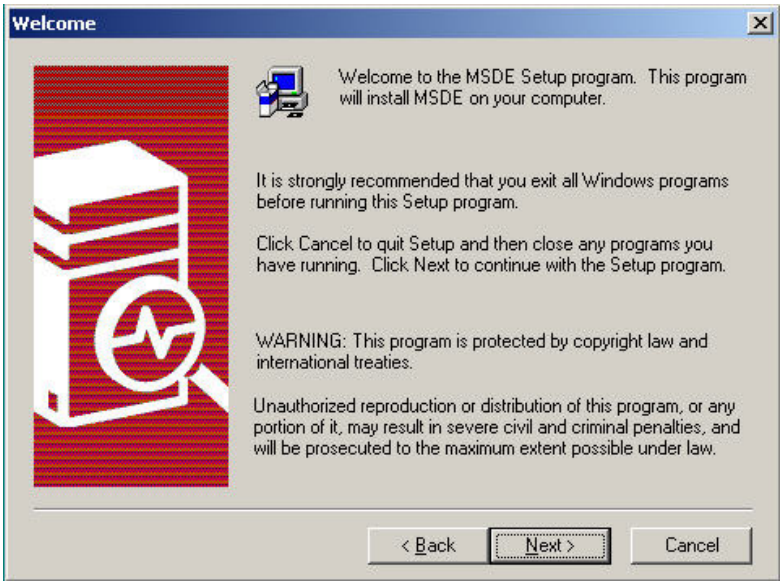


Figure 3.11 – MSDE Installation Welcome Screen

The installer should insert the computer's name and company name into the user information screen. You can change this information at your discretion.

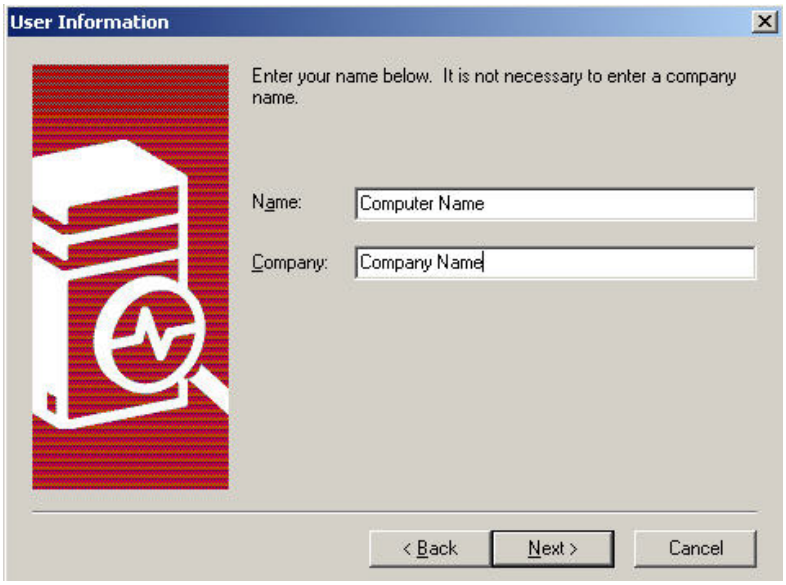


Figure 3.12 – MSDE Installation User Information

Select **Next** at the Setup Type screen.

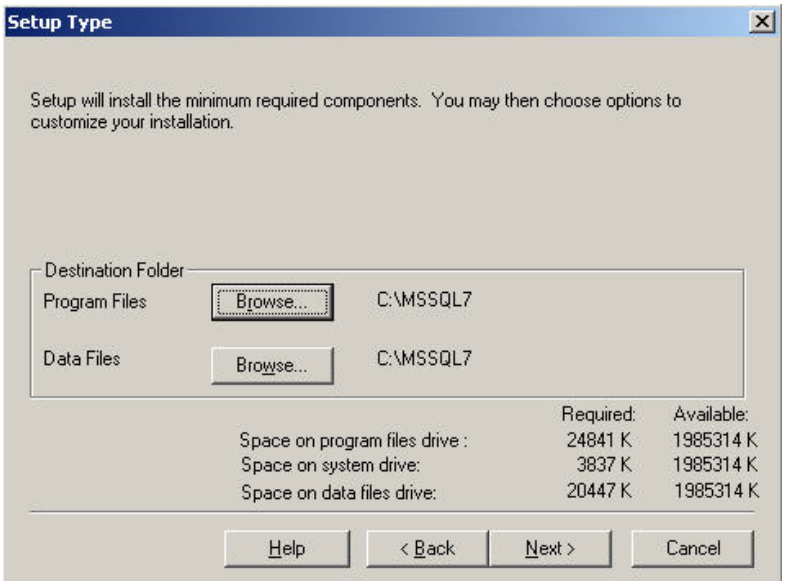


Figure 3.13 – MSDE Setup Type Screen

The character set should be set to the default setting. Then, press **Next**.

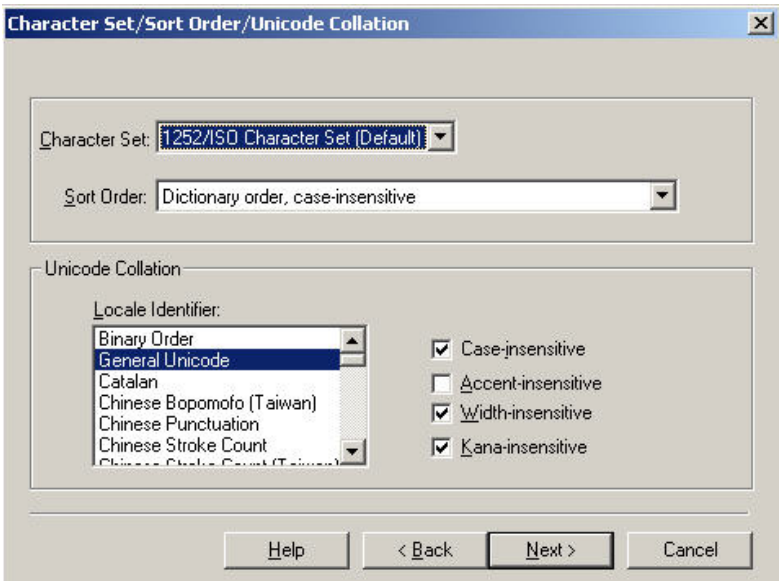


Figure 3.14 – MSDE Character Set Screen

Press **Next** at the Network Libraries screen.

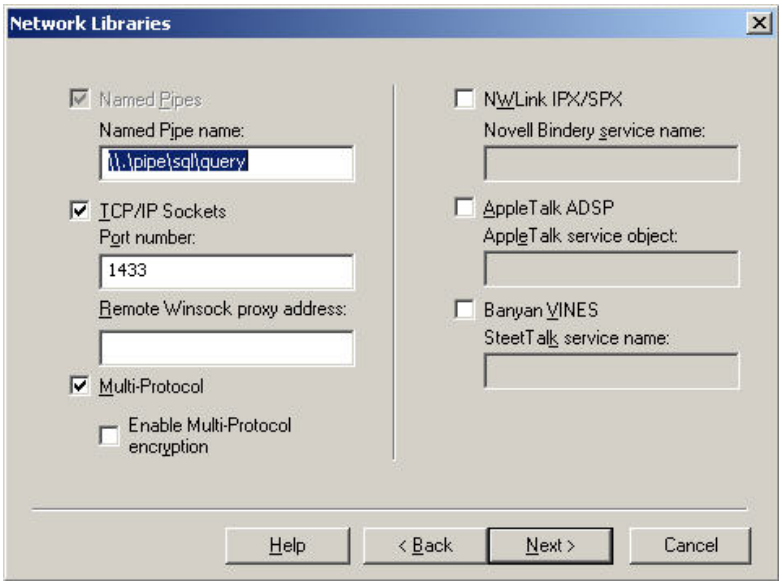


Figure 3.15 – MSDE Network Libraries Screen

Change the Service Settings to **Use the Local System account** and press **Next**.

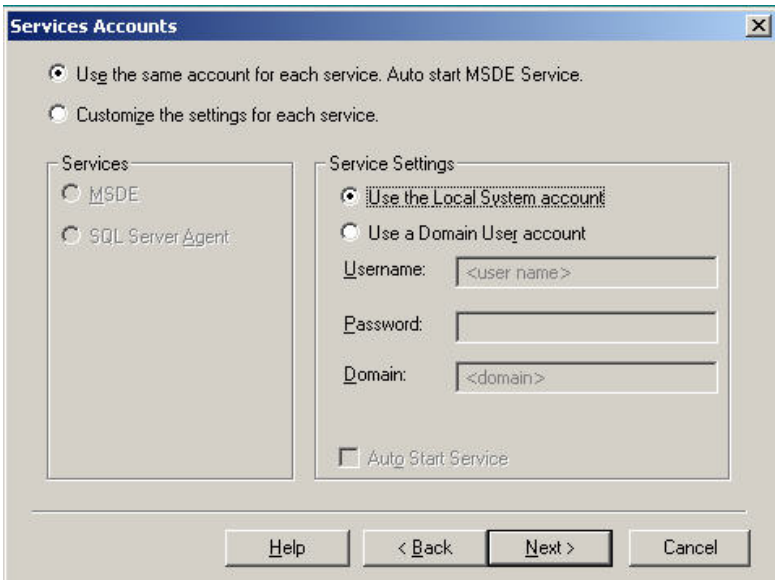


Figure 3.16 – MSDE Services Accounts Screen

Select **Next** to begin the installation process.

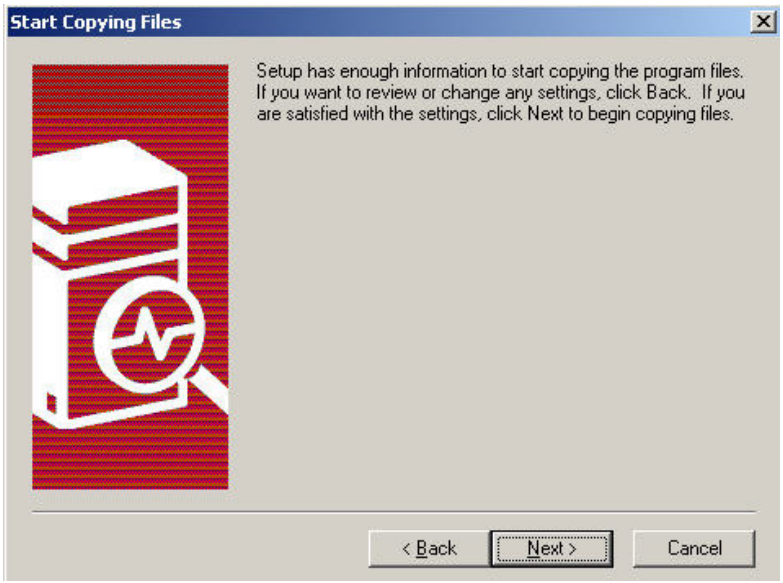


Figure 3.17 – MSDE Start Copying Files Screen

A progress bar will be displayed in the lower right corner of the screen.

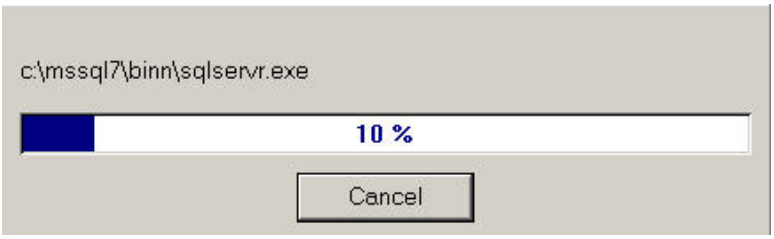


Figure 3.18 – MSDE Installation Progress Bar

Click **Finish** to complete the installation of MSDE.

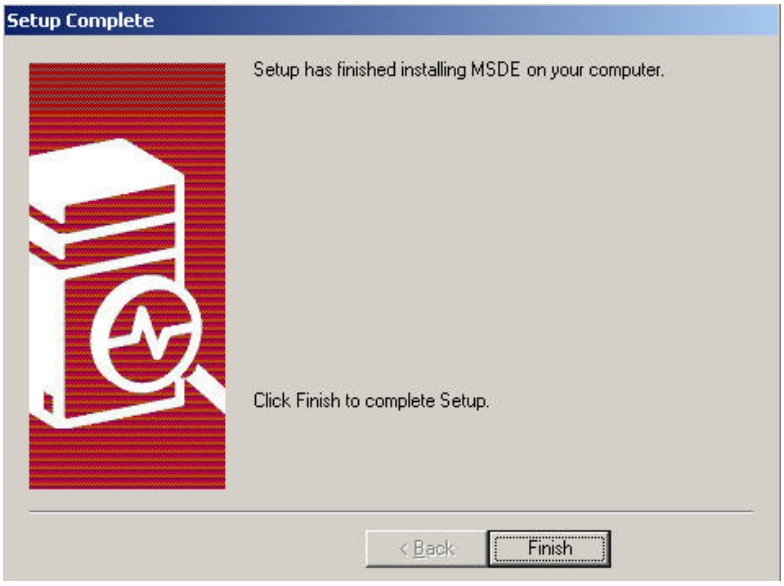


Figure 3.19 – MSDE Installation Finished Screen

The ASSET installer will display a screen indicating that the installation of MSDE is complete. Click **OK**.

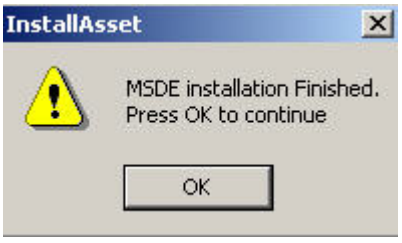


Figure 3.20 – MSDE Installation Complete Window

At this point in the installation process, the installer will create the necessary databases for ASSET – System and/or ASSET – Manager. Finally, the installer sets the ASSET database administrator password to a random value, thus eliminating one other MSDE vulnerability.

3.2.3 ASSET Installation Completion

The ASSET installation process is now complete. Click **Finish** to complete the installation.

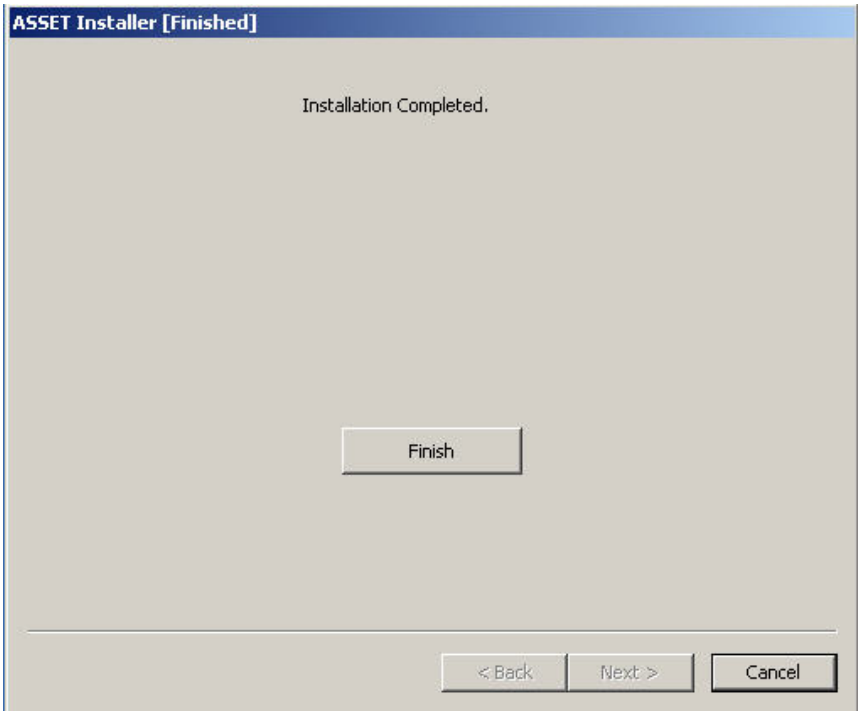


Figure 3.21 – ASSET Installation Complete

Once the ASSET installation process is complete, you may locate the ASSET program files in the NISTASSET folder within your Program Files folder (e.g., C:\Program Files\NISTASSET).

Shortcuts for ASSET, the user manual, and NIST SP 800-26 are placed on the Start menu. Shortcuts for ASSET are placed on the **Start Menu > Programs > NIST ASSET** menu.

Figure 3.22 – ASSET Shortcuts

NOTE: Although restarting your computer is not necessary after ASSET is installed, it is a good practice to restart once installation is complete.

*NOTE: It is highly recommended that you now install the latest service pack for MSDE, which is in the **Service Packs** folder. See section 3.2.6 for additional information.*

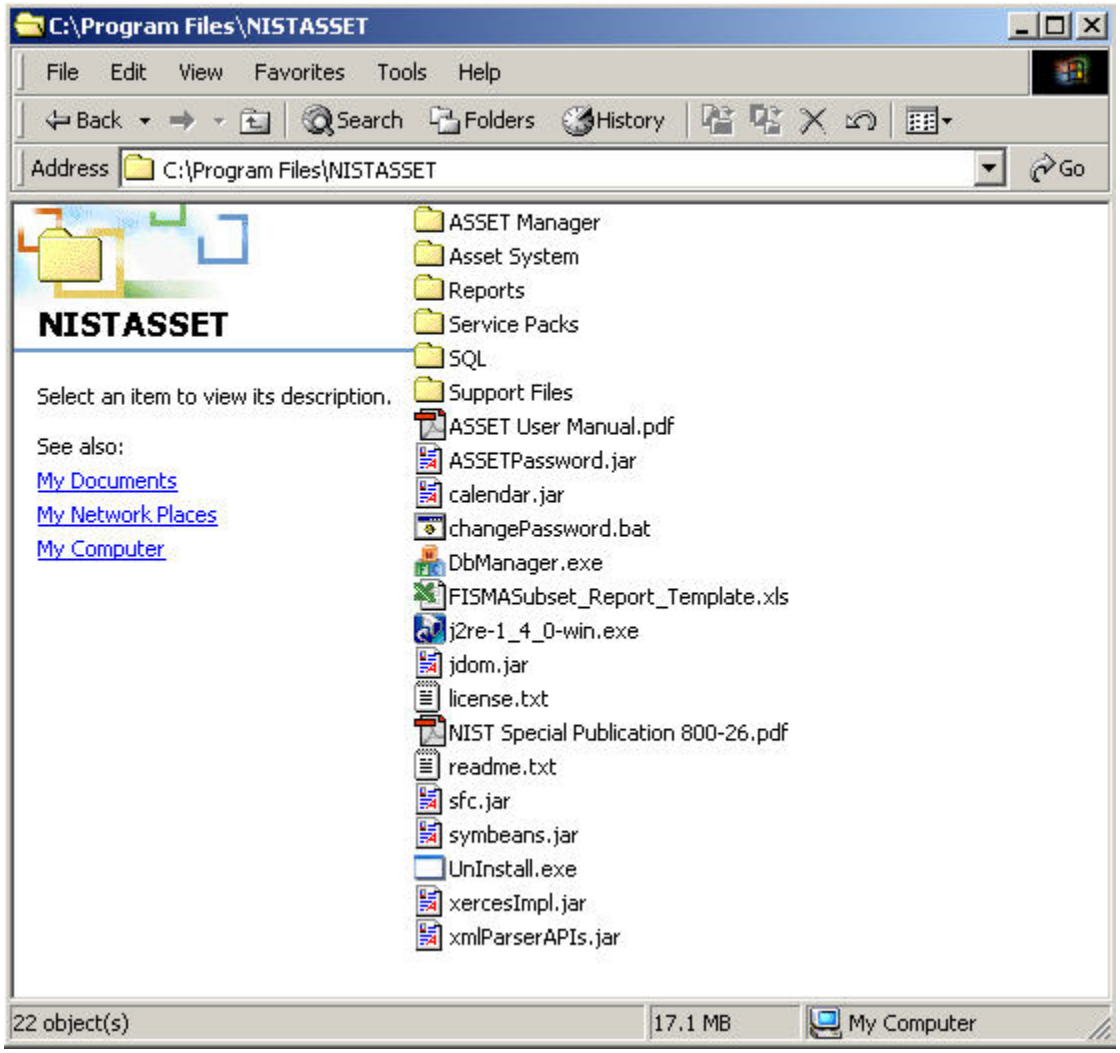


Figure 3.23 – ASSET Folder Structure

3.2.4 Setting ASSET Administrator Database Password

This section describes the operation of the ASSET Database Password Utility (ADPU). This utility is designed to change the default password of the MSDE database system that powers the NIST ASSET application. The default installation of MSDE creates an account with a username of “sa” and no

password. Several vulnerabilities have been known to exploit this blank password to gain access to a system with MSDE installed.

The operation of the ADPU depends on user interaction. The Installer will automatically set a random password during the installation process, however, your organization's password policy may require you to periodically change this password. You may access the ADPU at C:\Program Files\NISTASSET\ASSETPassword.jar or from the **Start Menu** to change the password.

If you decide to choose your own password, you will need to confirm the password before you can change it with the MSDE system.

NOTE: It is not necessary to remember this password as it will only be used once and you will not be required to enter it again.

The ADPU user interface is displayed in the following figure:

Figure 3.24 – ADPU User Interface

Manual selection of password. You have the option to choose a password. If you wish to choose a password, enter it into the text box in the ADPU user interface. There is no limit on the password that you choose. The only requirement is that the maximum length of the password must be less than 128 characters.[6]

Figure 3.25 – ADPU Password Textbox

Once you have entered a password once, you must press the Change Password button in order to initiate the password change. In order to confirm the password you entered, you will be required to enter the password again. The following figure shows the ADPU program requiring you to re-enter the password.

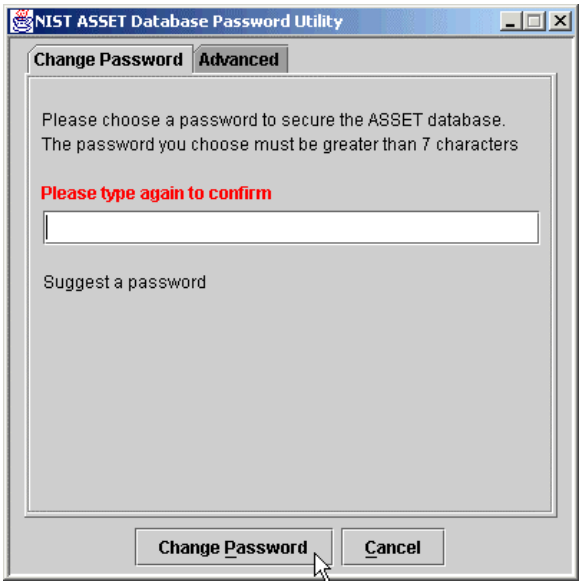


Figure 3.26 – ADPU Password Confirmation

[6] Asterisks are indicated as a security feature to mask the password.

Automatic selection of password. The ADPU program can suggest a random password. To have ADPU suggest a password, click on the **Suggest a Password** link. The following figure shows how to prompt the ADPU program to suggest a password for you.

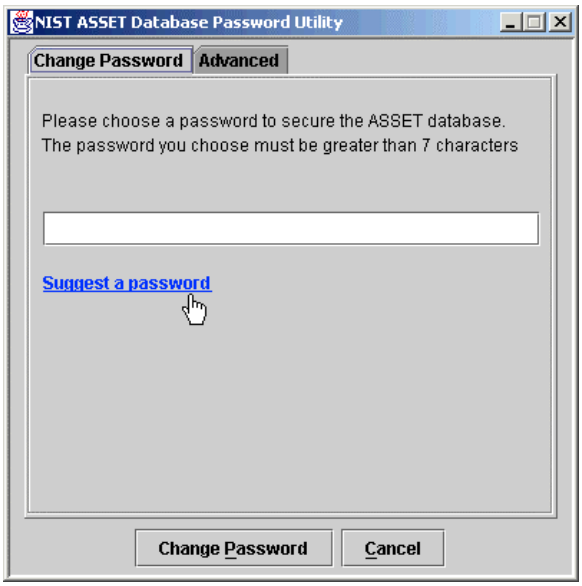


Figure 3.27 – APDU Automatic Password Selection

*NOTE: Once you choose a password or have one suggested for you by the APDU program, you need to submit the changed password by clicking on the **Change Password** button.*

Depending upon which ASSET applications you have installed, you may see either one or both of the following figures.

Figure 3.28 –ASSET System Password Changed Dialog Box

Figure 3.29 –ASSET Manager Password Changed Dialog Box

Click on **OK** to close the dialog boxes. Once you have followed these steps, the password of the ASSET application has been changed.

NOTE: Do not modify any of the settings on the Advanced property page without consulting your network administrator.

3.2.5 Database Manager (Deleting and Creating the ASSET Database)

The ASSET program folder contains an application that will assist you in managing the ASSET database. The Database Manager utility, also accessible via the **Start Menu**, allows the user to delete and recreate either or both ASSET System and Manager databases. This is useful if you have created a number of test assessments while learning ASSET and now want to clear out the database to begin the actual assessments. The interface for the Database Manager is shown in the following figure. If you try to delete a database after it has already been deleted or try to create a database that already exists, an error will be displayed.

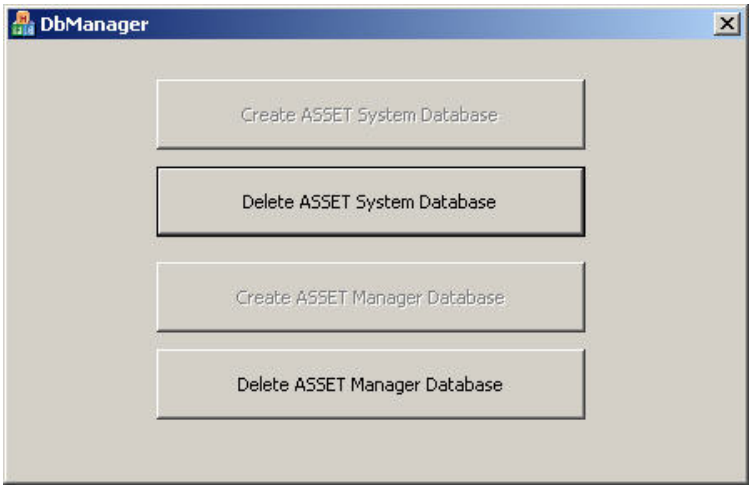


Figure 3.30 –ASSET Manager Password Changed Dialog Box

3.2.6 MSDE Service Pack Updates

The ASSET installation folder contains an application that will update MSDE from the baseline version 1.0 to version 1.0 with service pack 3 installed. This application is located in the **Service Packs** folder of the installation folder. To install MSDE service pack 3, double click on the one file in this folder and follow the prompts provided by the application.

NOTE: It is recommended that you stay current with patches and service packs of MSDE.

3.2.7 Disabling MSDE Network Communications

This section provides detailed steps to disable the network communications within their installation of MSDE. MSDE is the underlying database management system for ASSET. MSDE 1.0 contains several network-based vulnerabilities. Consult the following URL for specific vulnerability information on MSDE:

http://www.microsoft.com/technet/security/current.asp?productid=31&servicepackid=0&submit1=go

When initially installed, MSDE opens TCP port 1433 on the host machine. Other machines on a local area network (LAN) can connect to port 1433 (using TCP or NetBIOS protocols) for communications with services such as ODBC or an Active Server Page application. In addition to password vulnerabilities, there are some inherent design flaws in MSDE, which render any machine that has an unpatched version of MSDE installed, vulnerable to remote command execution. The steps provided in this section will close this network port permanently until the user decides to open it. Guidance on re-enabling network communication within MSDE is not provided in this document.

***WARNING**: If your organization uses MSDE for any business system, website, or other type of application within your enterprise, you could run the risk of disabling this system if the steps in this section are followed. DO NOT attempt any of the steps discussed in this section without first consulting your network administrator!*

NOTE: Disabling port 1433 does not disable normal TCP/IP or network connectivity.

NOTE: These steps are meant to occur once the ASSET application has completed its installation. If you receive any type of error from installing the ASSET, do not attempt to modify the MSDE settings; consult your network administrator instead.

Instructions for Disabling MSDE Network Communications:

1. Ensure that MSDE is running.

   You must ensure that the MSDE service has started on your machine before you attempt to edit the network settings. If the service has not started, you must start it so that the changes you make to the MSDE settings will persist.

   a. Check system tray for MSDE service icon. The following figure shows an example of the taskbar on a Windows 2000 professional machine.

Figure 3.31 – Task bar showing MSDE service is running

b. Look for the icon that represents a computer tower with a white circle imposed over top of it (The black arrow in the picture points to the correct icon). This icon represents the service status of MSDE.

c. If the icon shows a green triangle, the MSDE service is running normally. The following image shows an example of a system that does not have MSDE running.

Figure 3.32 – Task bar showing MSDE service stopped

d. If your task bar looks like this second figure instead of the first, you need to start the MSDE service.

i. To start the MSDE service, double click on the icon on your system tray that is shown in the previous two figures. It will open a window that looks similar to the following figure:

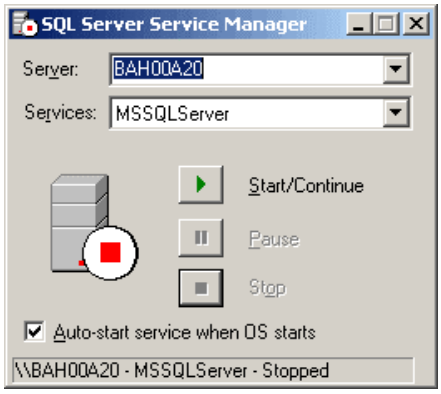


Figure 3.33 – MSDE Service Manager

ii. Click on the Start/Continue button to start the MSDE service. (NOTE: Although the window does say SQL Server Service Manager, for the purposes of these instructions MSDE and SQL Server can be considered as synonymous).

iii. Once the red square turns to a green triangle in the Service Manager window, the service has been started. The following figure illustrates the service as started:

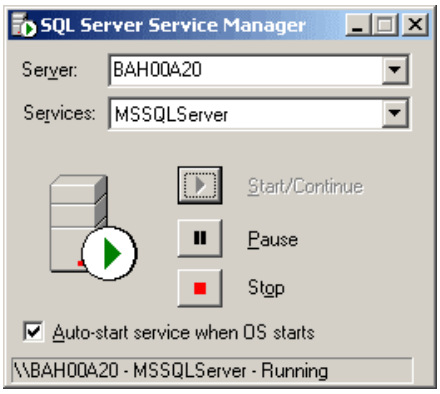


Figure 3.34 – MSDE Service Manager Shows MSDE Service as Running

2. Open **My Computer** window

   You must now locate and open the MSDE network communication configuration utility in the MSDE program folder. Although you can use the Windows explorer utility to do this, these instructions use the **My Computer** window found on the Windows desktop.

   Open the **My Computer** window by double clicking on the **My Computer** icon on your desktop. This is the drive where MSDE was installed.

3. Open Drive where MSDE was installed

   During installation, the MSDE install package will attempt to install MSDE on the same drive where you put your Windows or WINNT directory. This is the drive that you need to open in order to locate the MSDE folder.

   Once you have opened the drive where MSDE was installed, open the MSDE program folder. Unless you have already installed the MSDE application prior to installing ASSET, the name of the program folder will be MSSQL7. This is where the MSDE application was installed.

4. Open MSDE folder.

   Once you locate the MSDE folder MSSQL7, open it to search for a utility that is located in one of the subfolders.

   With the MSSQL7 folder highlighted from the previous step, double click on the MSSQL7 folder to open it.

5. Open the MSSQL7 Binn subfolder.

   The Binn folder (located within the MSSQL7 folder) contains the network configuration utility svrnetcn.exe, which allows you to configure the network communications of MSDE.

   To open the Binn subfolder, highlight the Binn folder in the MSSQL7 folder window and double click on it.

6. Locate and run network configuration utility.

   The svrnetcn.exe utility must be running to edit the MSDE network configuration.

   a. Double click on the svrnetcn.exe icon (located within the MSSQL7\Binn folder) to run the MSDE network configuration utility. The following figure shows the user interface of the Network utility.

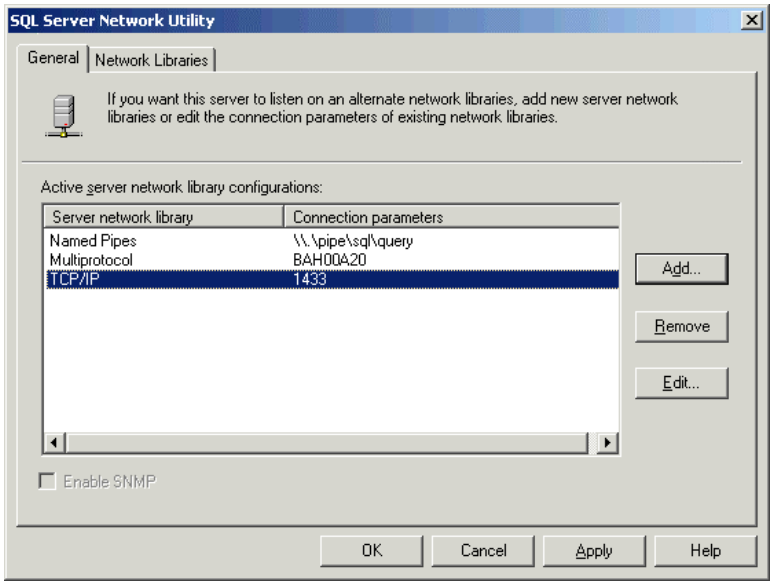


Figure 3.35 – SQL Server Network Utility User Interface

   b. Notice how the TCP/IP entry in this list is highlighted. This shows that this instance of MSDE is configured to accept connection on TCP port 1433.

7. Remove TCP from communications library list.

   In order to disable the network communications of your installation of MSDE, remove the TCP/IP entry from this list. This will close this network port on your machine.

NOTE: Refer to the warning at the beginning of section 3.2.7 of these instructions for the risk of performing this action.

a. To remove TCP/IP from the network library list, click on the TCP/IP entry and press the remove button as illustrated in the following figure:

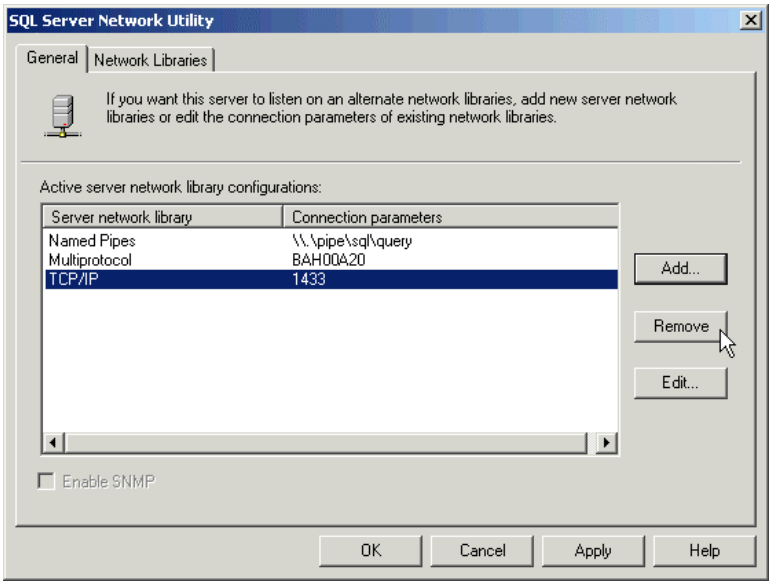


Figure 3.36 – Remove TCP/IP Network Library

b. Once you click the remove button, click the apply button at the bottom of the window to apply the changes you just made.

8. Close network configuration utility

   Once you have removed TCP/IP from the network library configuration list, you can close the Network Utility. The changes will take effect immediately.

When these steps are completed, you have successfully disabled TCP communications for your MSDE installation.

NOTE: Once you remove the TCP/IP library from the SQL Server Network Utility, you must restart the MSDE service for this action to take effect. You can restart the service in any one of the following three ways:

1. *Click on the MSDE server icon in the task bar. If the icon is not on the task bar, select* ***Start>Programs>MSDE>Service Manager****. Select* ***MSSQLServer-Stop****, then* ***MSSQLServer-Start****.*

2. *You may restart your computer to restart the MSDE service.*

3. *From the command prompt, you can use the following syntax to restart the service:* ***C:\C:\MSSQL7\Binn\scm – Action 2***

4 Using ASSET – System

Most of the functionality associated with ASSET supports the creation and modification of individual system self-assessments. This manual steps the user through the process of completing a self-assessment. ASSET has the capability to generate reports based on the information collected for the self-assessment. While useful for highlighting the status of security related to a system, the reports are only as accurate as the information provided. ASSET does not conduct analysis or validate the information provided in the self-assessment.

Data stored within the ASSET application is stored in a database that is created when you install ASSET. The database is accessed whenever you request system information that has been previously stored or when you wish to save the information you have entered. System data can be stored locally on the database or exported to a file for either backup purposes or for transfer to other users of ASSET.

NOTE: Each of the two modules of ASSET (System and Manager) has their own separate database.

NOTE: Data is stored to a database only when you request that the file be saved to the database (see Section 4.7).

A top-level view of the ASSET architecture is shown in the following figure. In this figure, the user has collected and stored data for nine systems using ASSET and stored them locally on the ASSET database. The user has also chosen to create an .xml export file containing three of the nine systems. Since the user is actively working on system two, ASSET automatically backs up every three minutes to a .dat file in case the application abruptly shuts down.

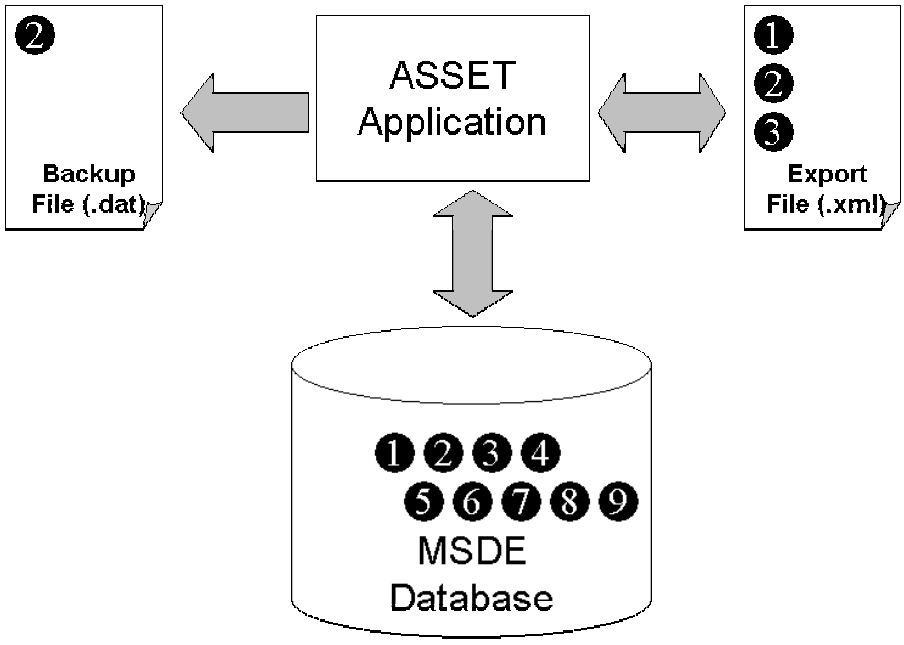


Figure 4.1 – Top-level ASSET Architecture

4.1 Login

Before you can use ASSET, you must login to the system. The login screen requires your full name (first name, followed by last) and your e-mail address. The login screen is intended to serve as identification, not authentication. By logging in and starting a new assessment, ASSET will identify you as the primary assessor.

NOTE: The XML format used for transferring data files between ASSET System and ASSET Manager uses certain command characters in the XML language. Using these specific characters in any text or comment field will not allow that file to be re-imported into ASSET. These special characters include: &, <, >, and %.

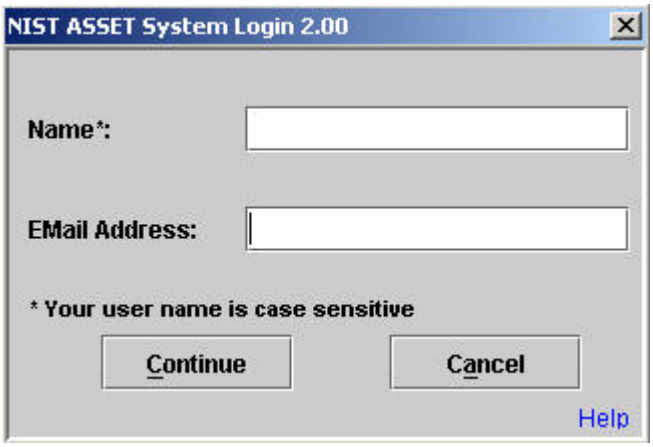


Figure 4.2 – Login Screen

NOTE: By default, the person who logs in will be labeled the primary assessor for a new assessment when it is created. If another person later logs in, they will be considered an alternate assessor for existing assessments and a primary assessor for new assessments that they create.

Figure 4.3 – Completed Login Screen

NOTE: Login names are case sensitive. Therefore, assessor names can be listed more than once if different font cases are used.

After entering primary assessor information, select **Continue**. This will lead to an empty screen (Figure 4.4). From this screen, you can:

- Create a new assessment
- Open an existing assessment
- Save an assessment.

Figure 4.4 – Post Login Screen

ASSET consists of five main parts: Assessment Identification, System Identification, Policy, Assessment Questions, and Summary.

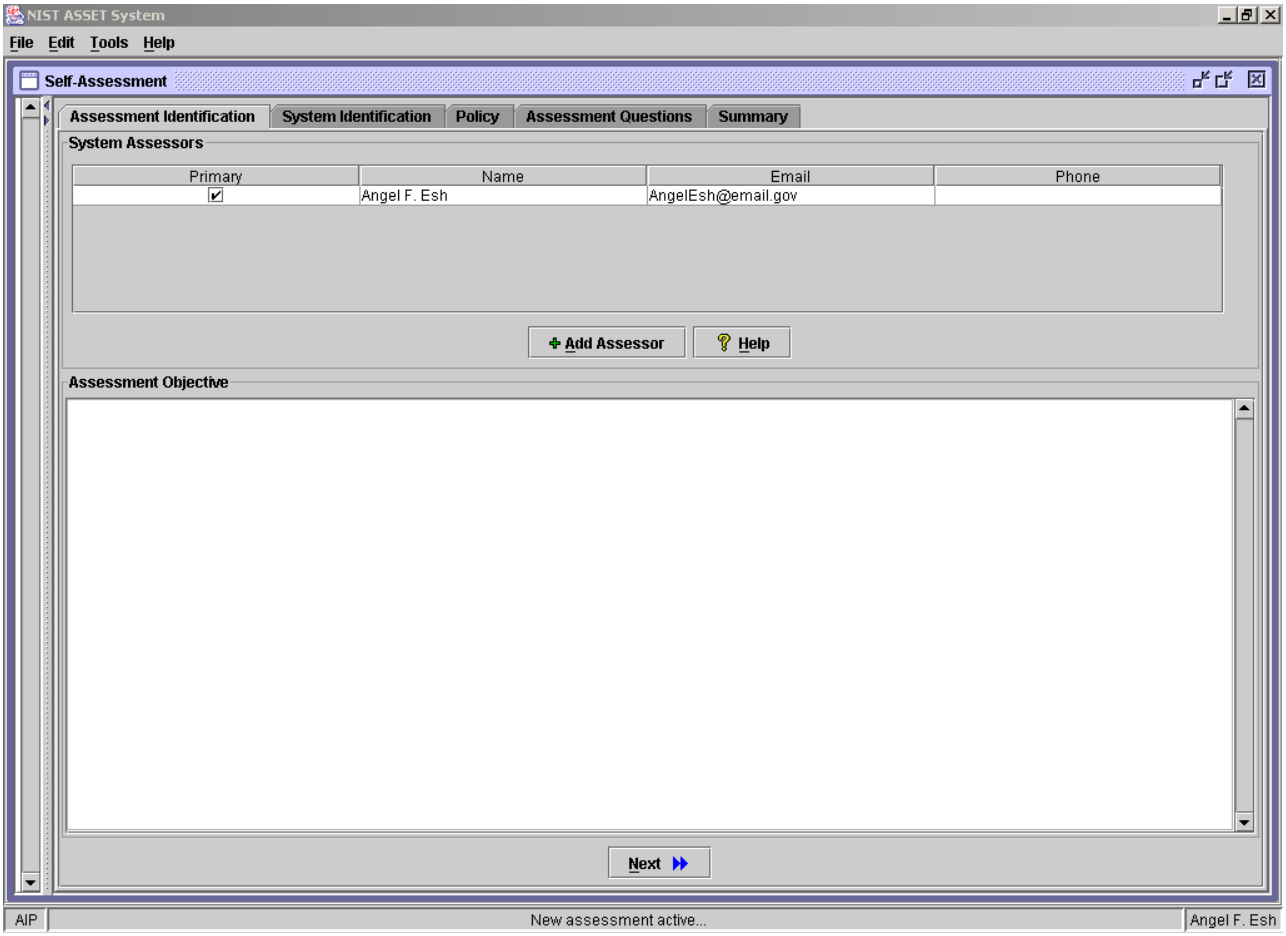


Figure 4.5 – Assessment Identification Tab

The Assessment Identification tab allows you to enter all system assessors and their contact information as well as the assessment objectives that have been established. The System Identification tab provides information related to the identification of a system, the system's criticality, and all interconnected systems. The Policy tab allows the user to indicate whether policy has been established for all the control objectives. The Assessment Questions tab is the start of the assessment. It displays each assessment question and allows the user to enter a response. The Summary tab displays the user's current assessment progress and the critical element response table, which displays the responses generated for each critical element.

4.2 Help Files

Help files are included within ASSET for each of the major processes associated with the tool. Additionally, tool tips are provided. Tool tips are small boxes that appear on the screen automatically when the cursor is placed over certain action buttons. The tool tips provide insight into the functionality of the button without having to press the button.

NOTE: Help files are in html; however, Internet connectivity is not required.

To use the built-in help files, select help from the toolbar or press the yellow question mark button that is located throughout the application. The intent of the help files is to provide limited online help with the application. Detailed guidance can be found in this user manual.

Since help files are provided in html format, they will be opened using your computer's default web browser. If you wish to change your default web browser, you may do so by selecting **Help** and then **Change Default Browser**.

4.3 Navigation

There are multiple ways to navigate through ASSET. The two primary ways to navigate between tabs and assessment questions are to use the buttons located at the bottom of the screen or to use the assessment map that is located on the left side of the screen. To move between questions using the assessment map, highlight the specific question in the assessment map. Once you have selected a question, it will then be displayed on the Assessment Questions tab.

NOTE: When navigating between tabs and after completing a question, it is important to use the navigation buttons at the bottom of the screen. This will ensure that your data is properly written to its file. After you have moved to the next tab or question, you may then use the assessment map to jump to another question.

NOTE: When navigating the first time between the System Identification tab and the Policy tab, users should always use the navigation button, 'Proceed to Assessment' at the bottom of the screen to ensure that ASSET builds the assessment map and policy screens correctly.

Basic Edit Commands

Copy, paste, and cut functions are available using both the Edit toolbar and keyboard commands.

To copy information, highlight the text you wish to copy and use Ctrl+C.

To paste information, position the cursor and use Ctrl+V.

To cut information, highlight the text you wish to cut and use Ctrl+X.

4.4 Create New Assessment

After logging in, you can create a new assessment. To create a new assessment, you can go to **File** and then select **New**, or you can use Ctrl + N.

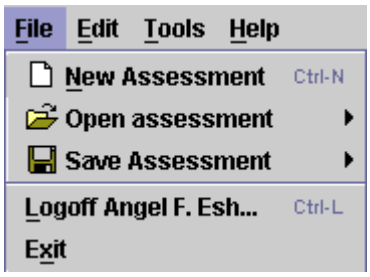


Figure 4.6 – File Drop Down Menu

Once you have selected New Assessment, the main self-assessment window will open (see Figure 4.5).

ASSET will start each new assessment on the Assessment Identification tab, which is shown in a lighter color. The Assessment and Identification tabs are the equivalent of the cover sheet used for the self-assessment in NIST SP 800-26.

4.4.1 Assessment Identification

To begin a new assessment, a few fields need to be completed. These fields will allow the system being assessed to be uniquely identified and, at the same time, provide a baseline of who will be involved with the assessment.

The Assessment Identification section is the first tab that should be completed. The primary assessor is indicated with a check mark next to that person's name and is the individual responsible for the completion of the questionnaire.

4.4.1.1 Add an Assessor

If you anticipate that other people will be providing answers to assessment questions, you can add them as assessors as well. However, they will be identified as alternate assessors because the box in the primary column will not contain a check mark.

To add an assessor, select **Add Assessor** in the **Assessment Identification** tab (Figure 30).

Once **Add Assessor** has been selected, a dialog box like the one below will appear giving you two choices: add a new assessor or add an existing assessor. The **Add New Assessor** tab will always be the first tab displayed.

To add an assessor, enter the new assessor's first and last name, phone number, and e-mail address.

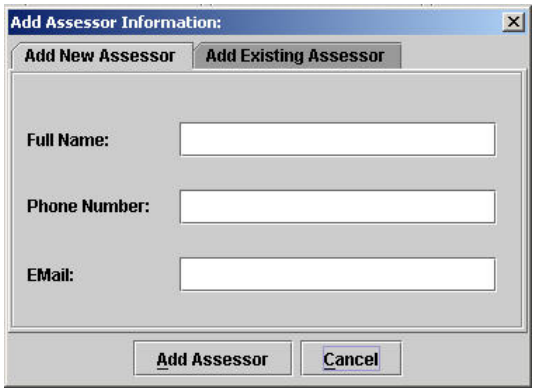


Figure 4.7 – Add New Assessor

Once this information has been entered, select **Add Assessor**. This will take you back to the Assessment Identification tab where you will see that the assessor has been added and that the name now appears in the system assessor table.

NOTE: An alternate way to add an assessor is to do so when on an assessment question (see Section 4.4.4.3.. By adding assessors from within each question, you ensure the right individual is assigned responsibility for answering the question and you avoid adding assessors that will never be used in an assessment. If an added assessor is not assigned to a question, ASSET will not add it to the database when you log off. For this reason, the preferred way to add an assessor is at the time you are answering questions.

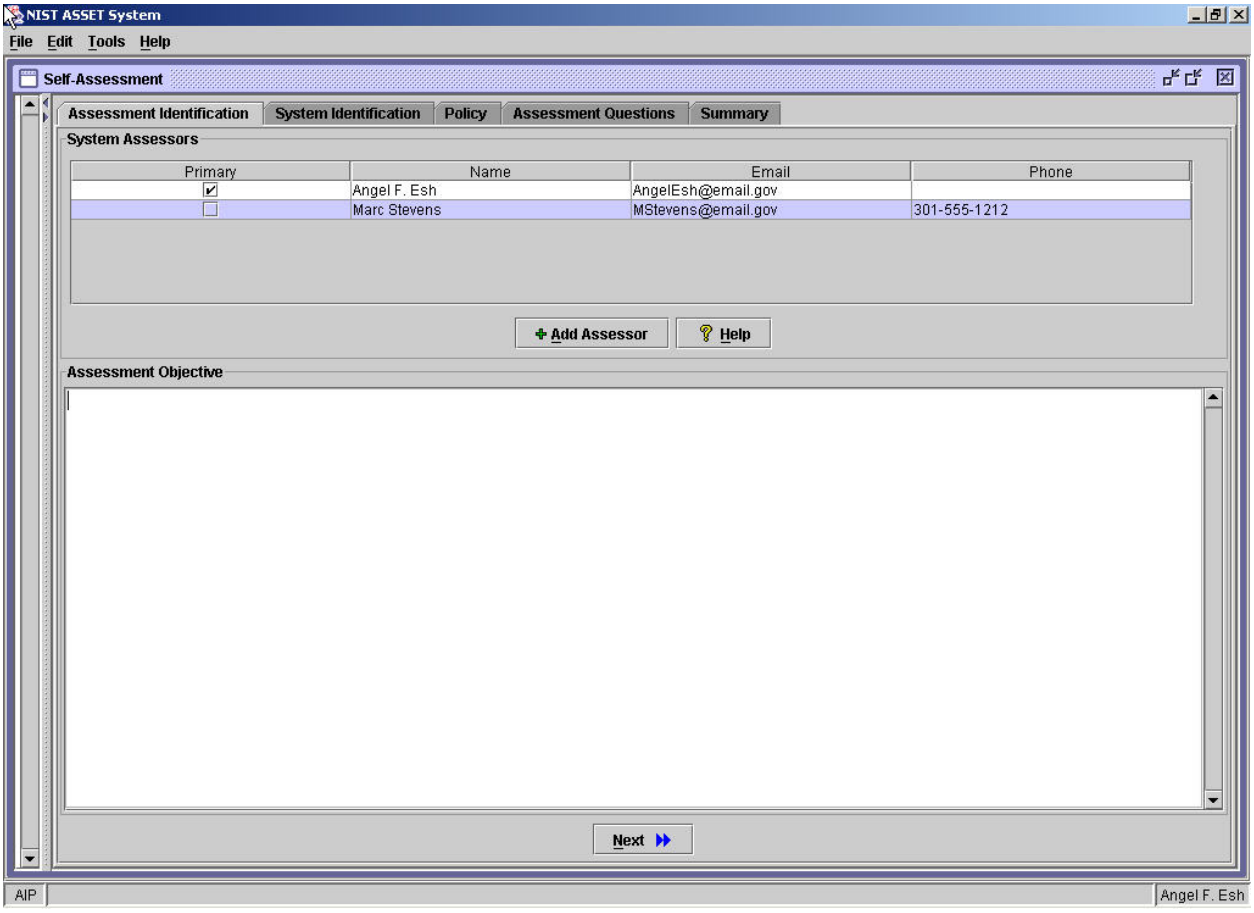


Figure 4.8 – Completed Add Assessor Screen

An existing assessor is someone who has been used in another assessment and is currently in the database. Other assessors are added to the database when they are entered during other system assessments. If you would like to add an existing assessor, select **Add Assessor**, then select the tab that says **Add Existing Assessor**. This tab will display a table that has been populated with all of the assessor names that are in the database. Select the name you want and click on **Add Assessor**.

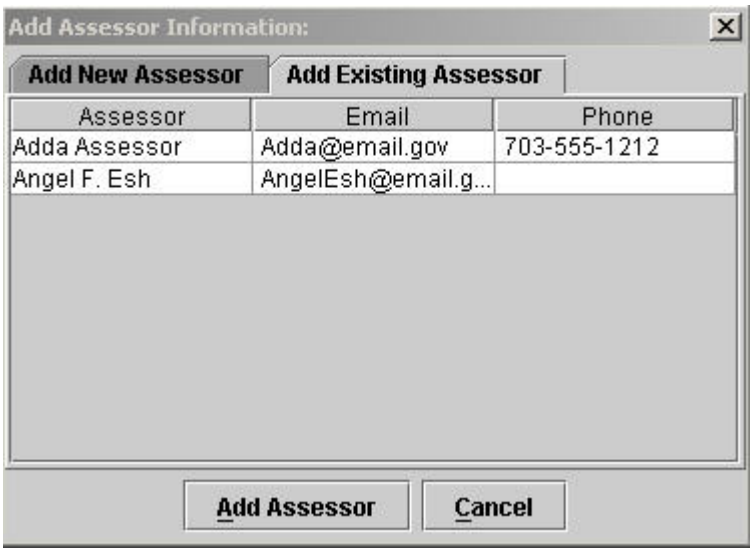


Figure 4.9 – Add Existing Assessor

To void an entry, select **Cancel**.

Once the data has been entered, the new assessor will appear in the assessor table. However, this person will not be considered the primary assessor and will not have a check mark by their name. You can repeat this process as many times as required.

*NOTE: After adding assessors, navigate forward using the **Next** and **Proceed to Assessment** buttons. Do not navigate using the tabs at the top of the window.*

4.4.1.2 Modify an Assessor's Information

To modify an assessor's information, from the Assessment Identification tab highlight the cell you want to edit and double click on the cell holding the assessor's information. After selecting the cell, the cursor will appear inside the cell. Enter the correct information.

NOTE: You can only modify an existing assessor's e-mail and phone number. There is no "undo" button. If you wish to change a person's name, you will need to add a duplicate entry.

4.4.1.3 Delete an Assessor

Deleting existing assessors is not supported in this version of ASSET. If you add an assessor with an incorrect or blank name, you will not be able to delete it.

4.4.1.4 Assessment Objective

As described in NIST SP 800-26, the intent of the assessment objective is to identify the purpose and objectives of the assessment. Enter the objective in the space provided. You can use the cut and paste feature for adding the objective.

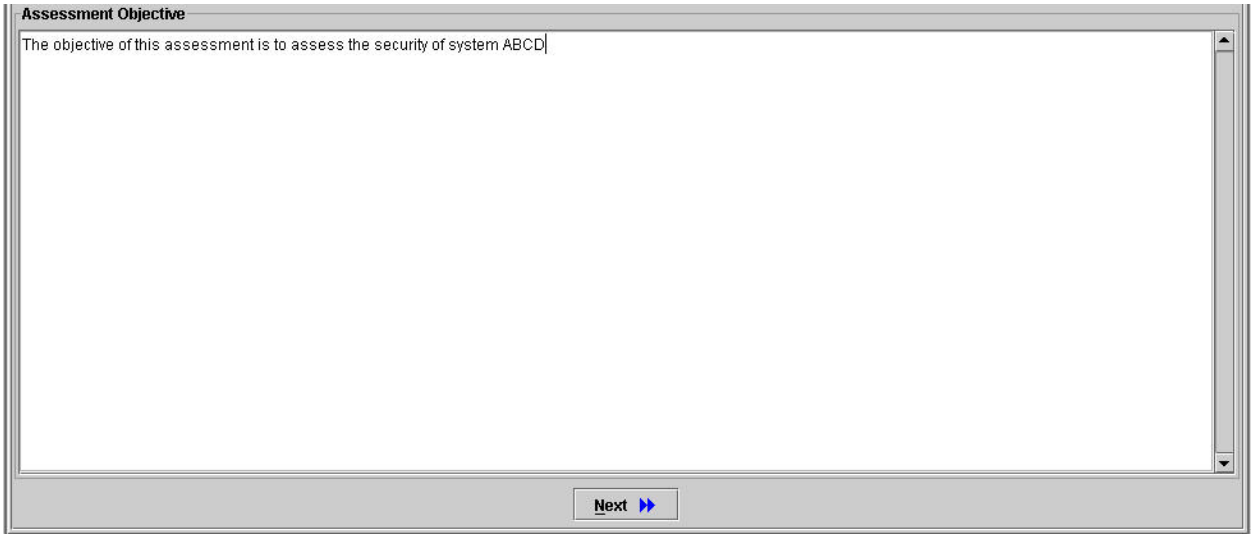


Figure 4.10 – Assessment Objective

4.4.2 System Identification

To proceed to the **System Identification** tab select **Next** . This tab is divided into three main areas: System Identification, System Criticality, and Inter-Connected Systems.

NOTE: When navigating the first time between the System Identification tab and the Policy tab, always use the navigation button, 'Proceed to Assessment,' at the bottom of the screen to ensure that ASSET builds the assessment map and policy screens correctly.

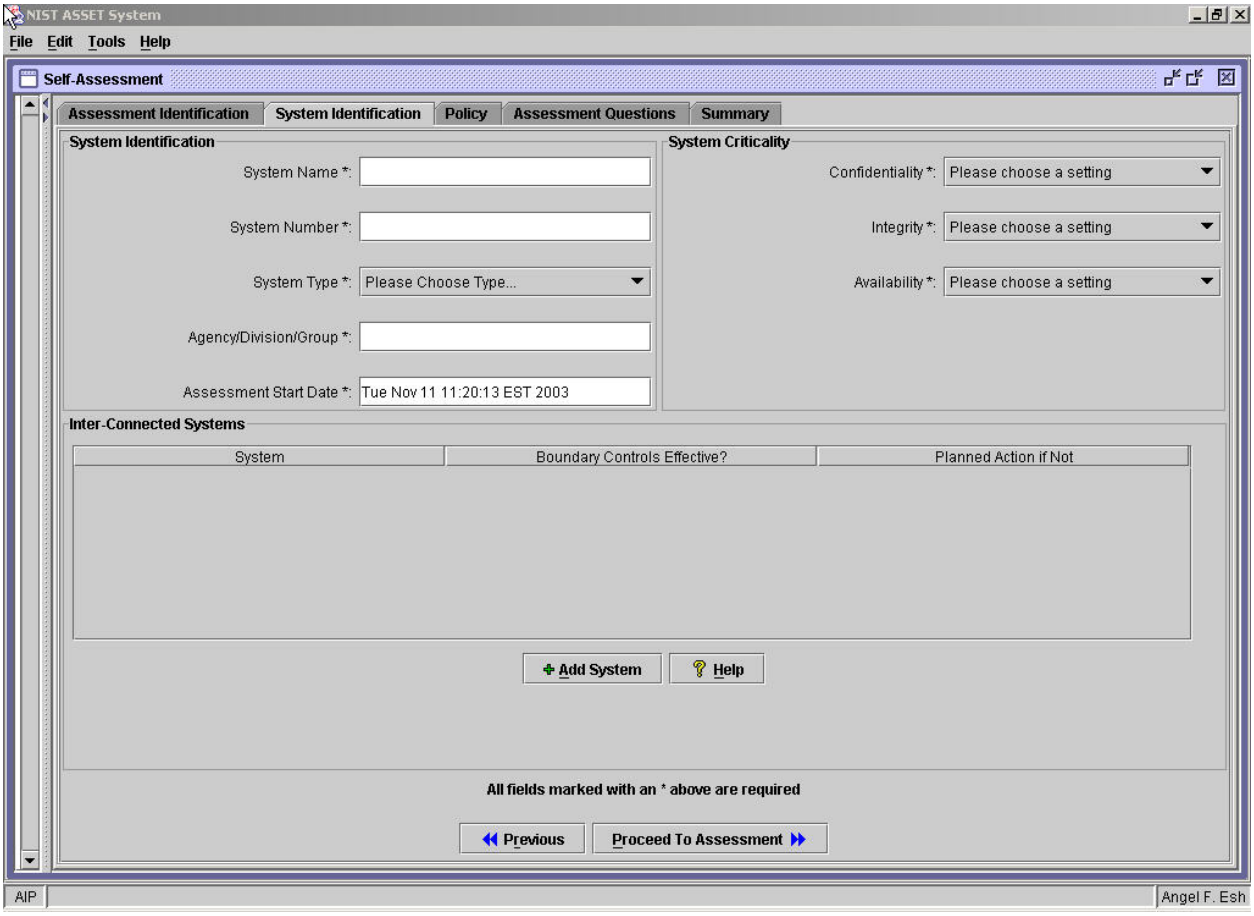


Figure 4.11 – System Identification Tab

4.4.2.1 Identification

System Identification allows you to enter all of the pertinent information that is unique to the system such as: system name, system number, system type, location of the system, and the assessment start date. The system name and number are based on the unique identifiers that your agency has chosen for each system. The system type refers to whether the system is a major application, a general support system, or other. If other is selected, an explanation can be provided in the **Assessment Objective** text box on the Assessment Identification tab. The agency/division/group refers to the physical location where the system resides. The Assessment Start Date is determined by when you first logged into ASSET and created the assessment.

NOTE: System Name and Number should only be expressed using letters, numbers, and dashes.

*NOTE: If you are unsure of how to identify your system and system number, check with your agency's guidance. Version 1.0 of ASSET has limited customization capabilities. If your organization uses a different nomenclature to describe your systems, you should provide clarification in the **Assessment Objective** text box. Prior to beginning an assessment, check any organization guidance that addresses the identification of systems. Future versions will support additional customization capability.*

4.4.2.2 Criticality

The second area on the System Identification tab is System Criticality. This section enables you to rate the sensitivity of the system int three areas on a scale from high to low[7]. The areas of the sensitivity assessment are: confidentiality, integrity, and availability. These categories are discussed in NIST SP 800-26.

Each protection category has a drop down list, which you can use to select the level of criticality. To do so, select the desired level from the drop down menu.

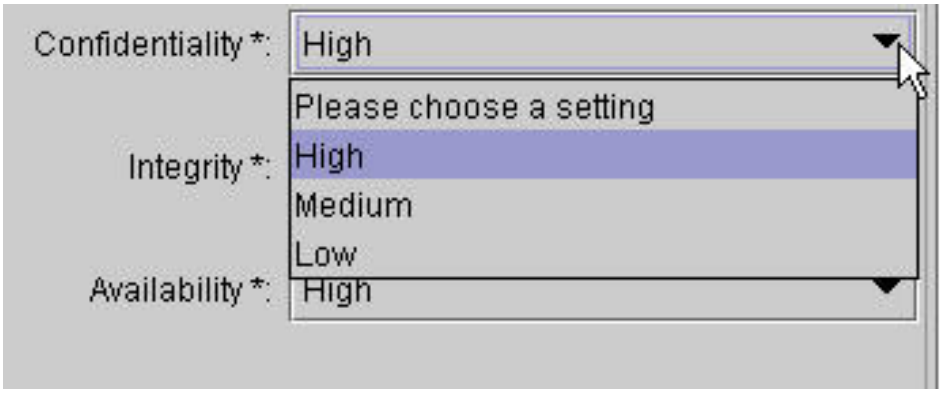


Figure 4.12 – Sensitivity Levels

[7] See NIST Special Publication 800-26 for an expanded discussion of the sensitivity assessment.

4.4.2.3 Inter-connected System

Inter-Connected Systems is the last area on the System Identification tab. This area allows you to add, modify, or delete a connected system.

4.4.2.1.1 Add an Inter-Connected System

To add a connected system, first select **Add System from the System Identification tab**.

Once selected, a dialog box will open that contains two tabs: one for adding a new system and the other for adding a current system that is already in the database. Systems may be in the ASSET database if an assessment already exists for that system, either because it was created on your computer or you imported it from another ASSET user.

If the system has not been previously entered, select **Add New System**

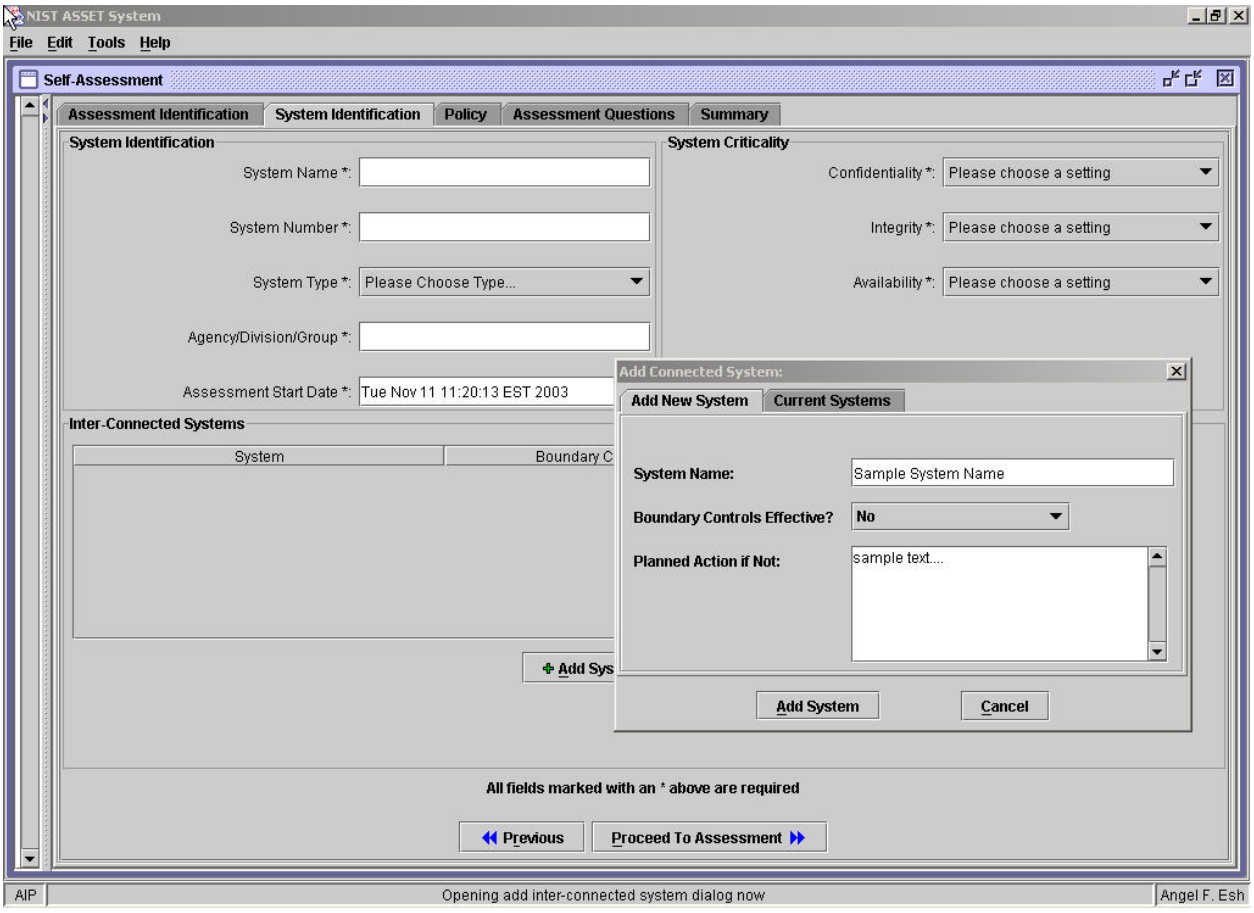


Figure 4.13 – Add New Inter-Connected System

Add the name of the system that connects to your IT system. After completing the connected system information, select **Add System**. The Add Connected Systems window will close. Repeat this process as many times as needed. There is no limit to the number of inter-connected systems you can add within ASSET.

NOTE: When entering an interconnected system, use the unique identifier for that system. If you need to cancel at any point, select "Cancel."

4.4.2.1.2 Modify an Inter-Connected System

The name of the inter-connected system cannot be changed once it is entered. If you need to change the "boundary controls effective" or "planned action" at any point, highlight the cell you want to edit and double click on it. The cursor will appear inside the cell. Type the changes directly into the cell.

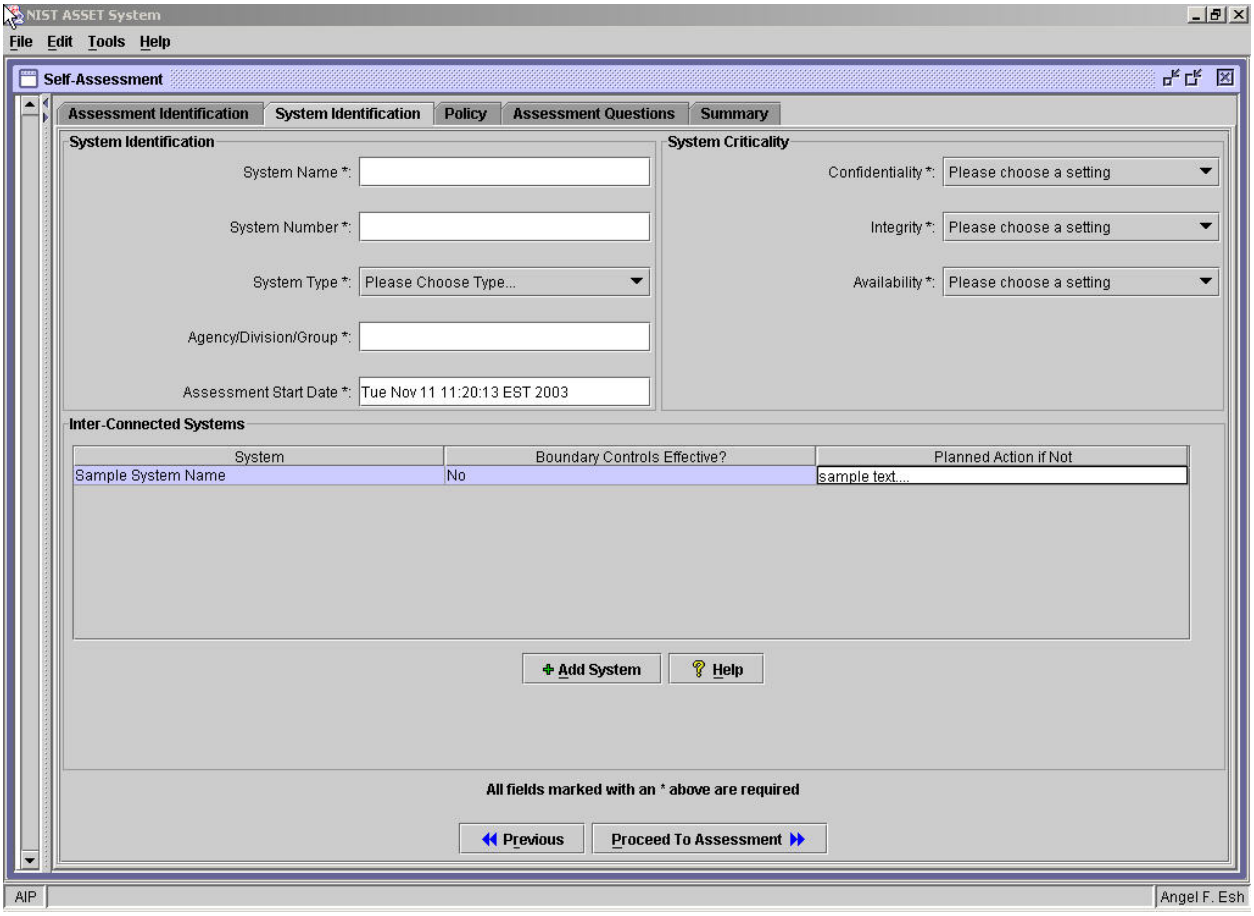


Figure 4.14 – Modify an Inter-connected System

4.4.2.1.3 Delete an Inter-Connected System

Deleting an inter-connected system is not supported in this version of ASSET.

After completing the information in the System Identification tab, select **Proceed to Assessment.** Do not use the navigation bar at the top of the screen because it may not build the assessment map or policy screens correctly.

*NOTE: You must complete the Assessment Identification and System Identification tabs and press **Proceed to Assessment** in order for ASSET to save the information that has been entered.*

4.4.3 Policy

Documented policy is the first level of effectiveness described in NIST SP 800-26. Determining whether policy meets the criteria described in Appendix C of NIST SP 800-26 should be an agency-level decision.

NOTE: Based on the guidance received from management, select each of the areas where policy has been documented and disseminated in your agency.

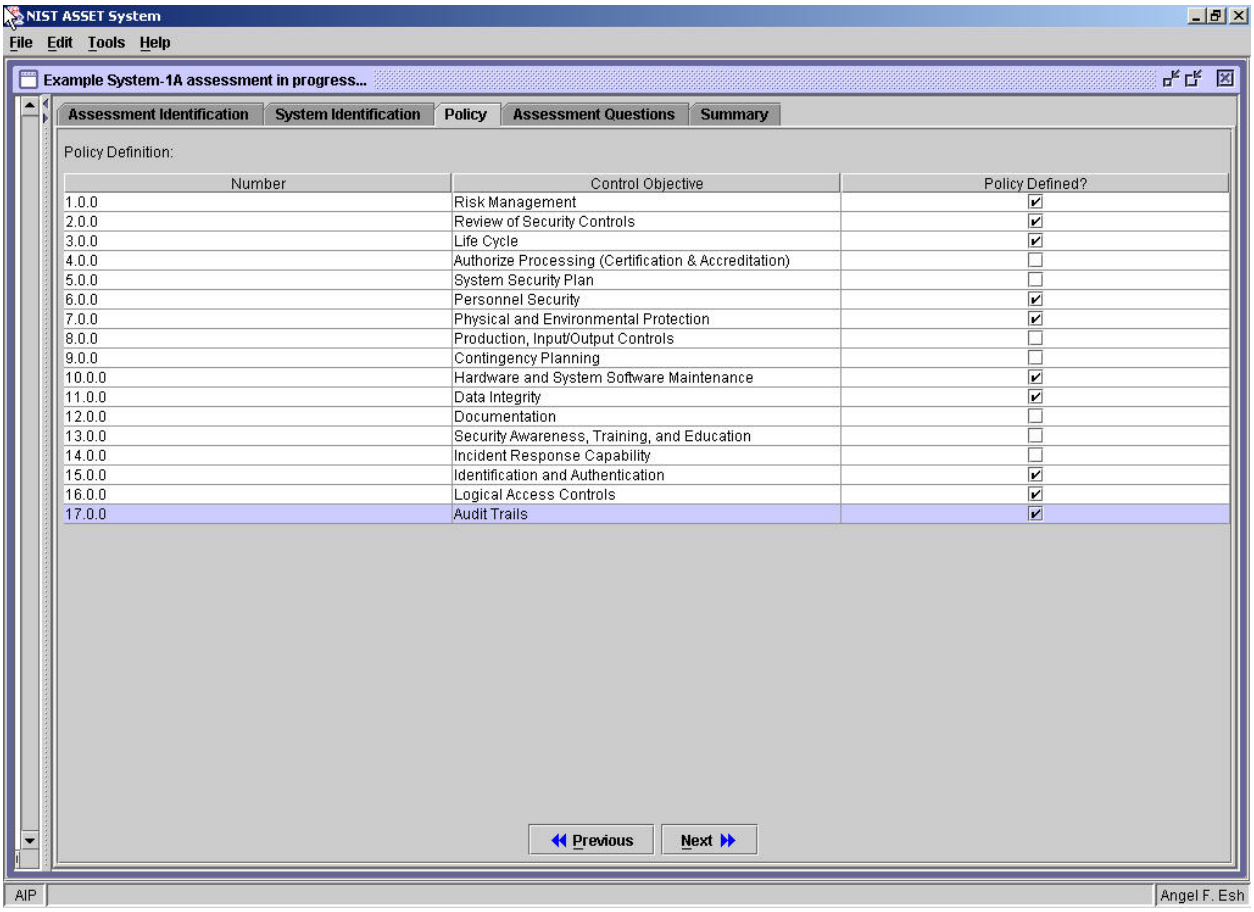


Figure 4.15– Policy Tab

Select each box to the right where policy exists for your organization. If you check the wrong area, you can deselect the box by checking it again.

If there is no policy documented and disseminated for at least one of the 17 topic areas, the questions (controls/objectives) for the topic areas can be answered but the answers do not appear in the assessment summary. ASSET allows you to answer the questions even if you do not have policy because of the possibility that policy will be developed and completed at a later date. The assessment questions would not have to be answered at a later date, just the policy area would have to be updated to reflect the creation of policy.

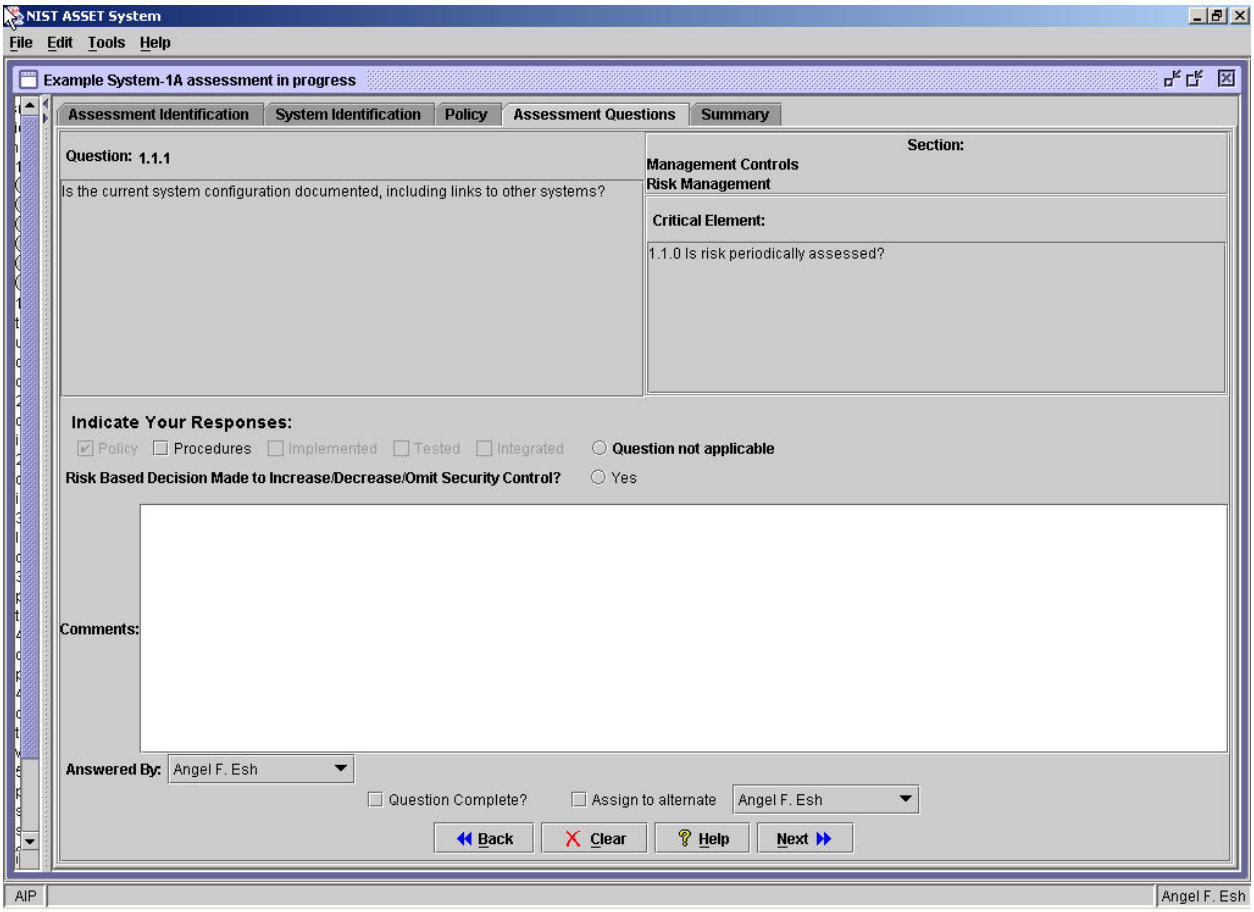
After completing policy control objectives, select **Next**. "Next" will lead you to **Assessment Questions.**

NOTE: The Previous button will move you back one screen at a time.

4.4.4 Assessment Questions

The Assessment Questions tab has one main function— to collect all the responses to the self-assessment questions. The questions are structured identically to the questions listed in Appendix A of NIST SP 800-26. In ASSET, the critical element effectiveness level (policy, procedures, implementation, tested, and integrated) is derived for you by calculating the lowest effectiveness level of the subordinate questions (control objective/techniques). For example, if the three subordinate questions of critical element 2.1 were answered with two of the questions (control objectives/techniques) being implemented and one of the questions only containing procedures. The critical element for 2.1 would be at the procedures effectiveness level.

Based on the business rules of ASSET, after the policy effectiveness level, all other levels must be checked in sequence. Non-consecutive effectiveness levels cannot be selected, i.e., the tested level cannot be checked if the procedures and implemented levels have not been selected[8].



[8] For other business rules, see Appendix C.

Figure 4.16 – Assessment Questions

There are two main ways to move from question to question. The first way to navigate is to use the **Back** and **Next** buttons located at the bottom of the screen. The second method is to use the assessment map that is located on the left side of the screen. The assessment map displays and rolls up questions and allows you to move from question to question by highlighting the desired question and then double clicking on it.

4.4.4.1 Assessment Map

There are two screen view options when completing the assessment questions – full screen and split screen. Full screen allows you to focus solely on the questions. Split screen allows you to see questions and the assessment map.

To view the assessment map, you must first open the split screen.

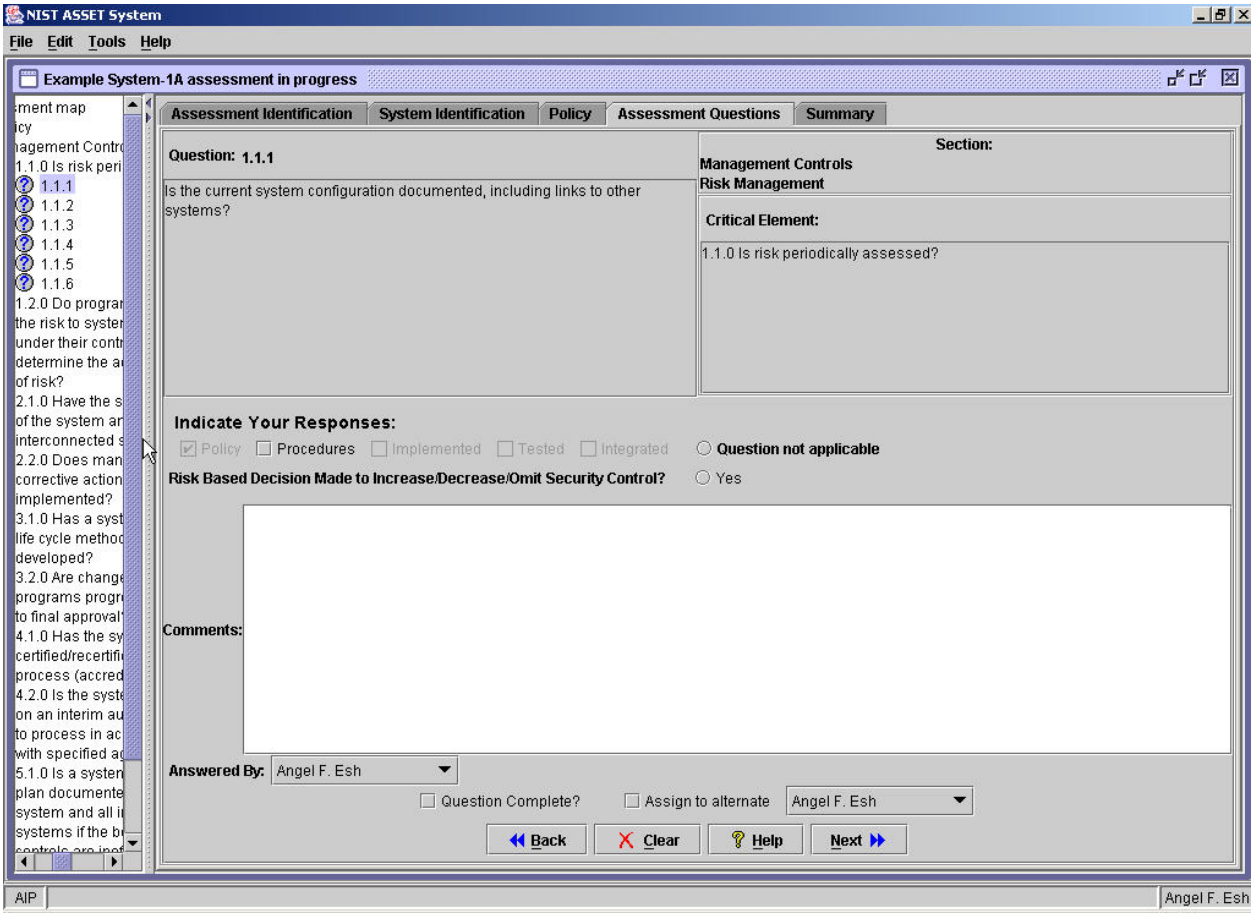


Figure 4.17 – Assessment Map

To open the assessment map, click and drag the arrows on the left side of the screen until the assessment map is completely visible. The map displays all questions in the self-assessment. The split screen enables you to see the assessment map and questions. To view all 17 control areas, select the Management, Operational, and Technical Controls folder icons.

4.4.4.2 Indicate Your Response

For each question, the question number (which maps to the number in SP 800-26), the section (which contains Management, Operational, or Technical area, and the Topic Area), the critical element, and the question itself is displayed. Your responses to each question are provided in the section called Indicate Your Responses. Once you have finished, you must indicate that the question is either complete or assign the question to an alternate assessor. Use the assessment map or the **Next** button to proceed to the next question.

If the question does not apply, do not check any levels of effectiveness and check the “Question Not Applicable” box. If you have checked the levels of effectiveness that apply to your system or application, you may identify whether a risk-based decision has been made related to that security control. If the answer is yes or if the question is ‘not applicable,’ you will be required to explain your decision. Without an explanation, you will not be able to continue to other questions.

Under the assessments questions, there is a comments section. You can use the comments section to write any remarks or supporting data on why the question was answered the way it was. It may also be used as a place to write comments to another assessor who has been assigned the responsibility to answer the question.

NOTE: If you do not make a risk-based decision, you are not required by the application to provide comments. However, if you make a risk-based decision or answer ***Question Not Applicable****, you must provide comments.*

After entering the level of effectiveness for the question (control objective/technique), the **Answered By**: field will display the name of the person logged on as the assessor who answered the question. If someone else other than the assessor who is logged on answered a question, choose the assessor from the list of assessors already created or enter a new assessor.

4.4.4.4 Assign Responsibility to an Assessor

If a question cannot be completed initially because someone else needs to provide input, select whom the assessor will be. To assign responsibility for answering a question to another assessor, check the box that says **Assign to alternate** and select the name of an assessor who is responsible for answering the question.

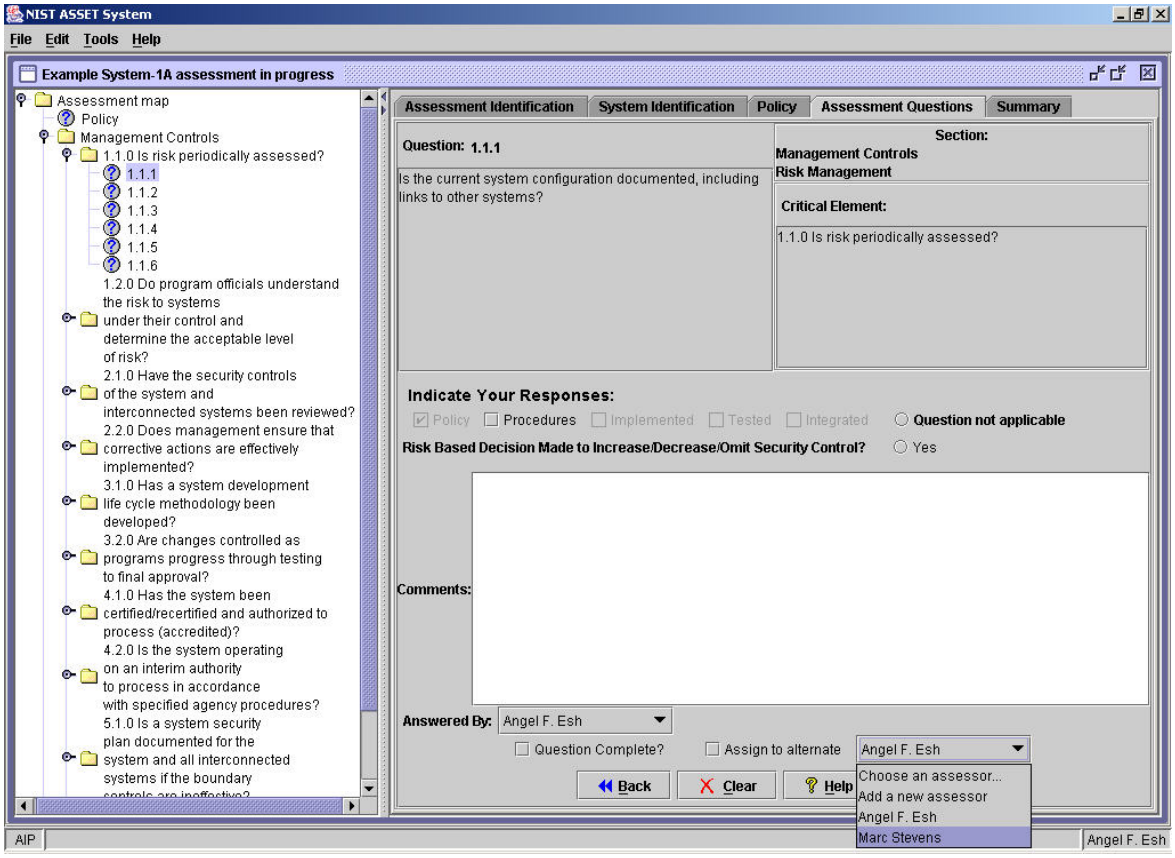


Figure 4.18 – Assign to Alternate

The drop box has been populated with all the assessor's names that have been entered in on the Assessment Identification tab. If the assessor's name is not listed, highlight **Add a new assessor**. A dialogue box will appear where you can choose to either **Add a new assessor** or an existing assessor.

NOTE: If three assessors are listed on the drop down box, the last assessor on the list may be masked by the Windows toolbar at the bottom of the screen. If this happens, you can navigate to that name using the down arrow on the keyboard. Adding a fourth assessor to the list will position the drop down menu so that all assessors can be viewed properly.

Completion of a question requires you to select the box **Question complete** or **Assign to alternate**. However, if you cannot answer a question and you want to continue, you can assign it to an alternate assessor. If the box **Assign to alternate** is selected, you will need to select who will be the alternate (either yourself or another assessor).

NOTE: If you know that you will answer the question at a later date but do not have information available to you at the time you are completing the assessment, choose yourself as an alternate assessor so the question will be flagged for later review.

4.4.4.4 Edit a Response

To edit a response that you made to a question, use either the assessment map or the **Back** button located on the bottom of the screen to locate the question you wish to modify. Once you have found the question, you can change your response. You can return to the last question that you were on or move around elsewhere in the assessment.

NOTE: If any mandatory field has not been completed for a question, you will receive an error message. You cannot move forward until you address the mandatory fields.

NOTE: You must answer or scroll through the subordinate questions within a critical element to save the responses. You can still move randomly through the critical elements.

4.4.5 Summary Tab

The Summary tab is the final tab and can be accessed at any time while answering the assessment questions. The Summary tab displays a summary of all critical elements and the levels of effectiveness. As long as one of the questions is not answered for the critical element, the critical element effectiveness level will not be computed and the critical element is not displayed in the Summary Tab.

NOTE: The effectiveness level of the critical elements in the summary section is based on the weakest supporting question. This approach is consistent with the concept that the security is only as strong as the weakest link.

In the figure following, you can determine the following from the system being assessed:

- Critical elements 1.1.0 to 3.2.0 have been completed.
- Of the questions in critical element 2.1.0, at least one of them has been answered 'not applicable.'
- Of the questions in critical element 2.1.0 and 3.1.0, at least one question in each critical element has been answered by selecting 'risk-based decision.'

- Critical elements 1.1.0 and 1.2.0 have the highest rated element at ‘integrated.’
- Critical elements 2.1.0, 2.2.0, and 3.2.0 have the lowest rated elements.

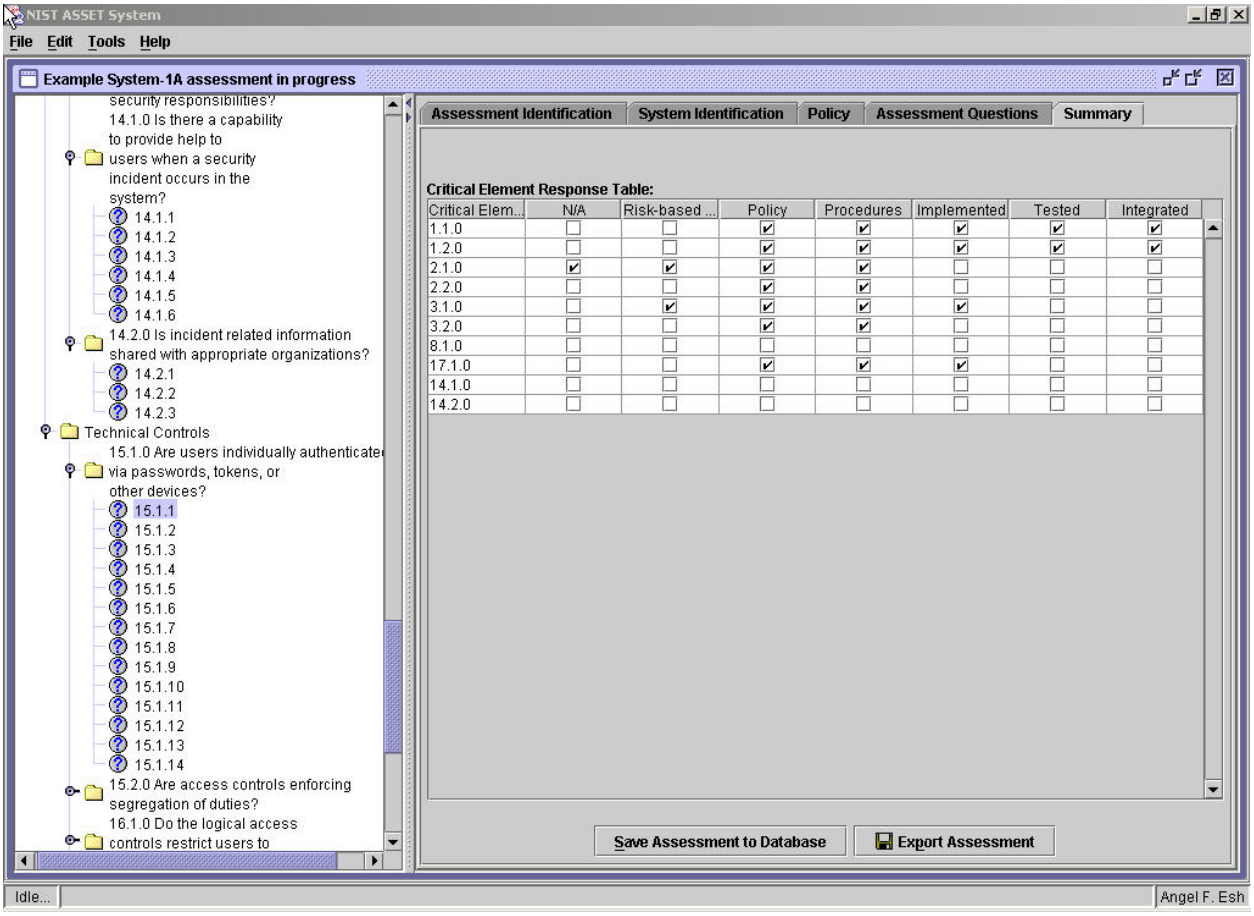


Figure 4.19 – Summary Tab

4.5 Edit an Assessment

Text can be edited directly for most parts of ASSET. Use either the assessment map or the **Back** button located on the bottom of the screen to locate the screen upon which the edit will be made. Identify the element that requires a change and type directly into the area.

4.6 Save an Assessment

There are two different formats for saving assessments. One method is to save the assessment as a file. The other method is to save a file to the database. In addition to actively saving an assessment, ASSET automatically stores all data from an open assessment to a back-up file every three minutes. The back-up file is stored under ASSET data folder. Importing back-up files should be attempted only if a system crashes in the middle of a session. In addition to different formats for saving assessments, there are multiple ways to save an assessment.

4.6.1 Save an individual assessment as a file

To save an assessment as a file, select **File** from the menu bar and then **Save**. Save has two options: **Save assessment to database** or **Save assessment to file**. Select **Save assessment to file**.

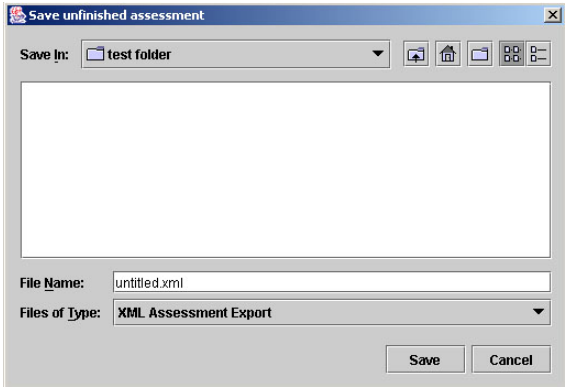


Figure 4.20 – Saving a File

After selecting Save assessment to file, a window will appear. Select the location in which to save the assessment and then name the assessment. Include the .xml extension on the file name. Once you have chosen the location and given it a name, select **Save**.

Another way to save an assessment is by using Export Assessment button on the Summary tab. On the bottom of the tab there are two buttons: **Save assessment to database** and **Export Assessment**. Export Assessment requires you to save the file in XML in the location of your choice (Section 4.8). Save assessment to database will save the current assessment to the database.

4.6.2 Save individual assessment to the database

To save an assessment to the database, select **File** from the menu bar and then **Save**. Select **Save assessment to database**.

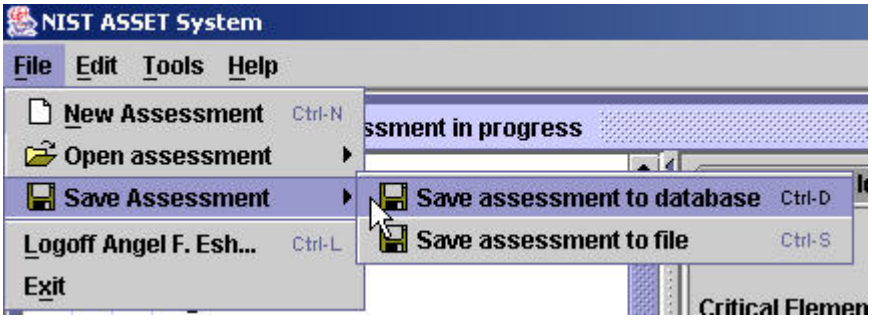


Figure 4.21 – Save Assessment to the Database

The save is automatically executed. You will see a confirmation window when the save to database is complete.

Another method for saving an assessment to the database is to go to the summary tab. Click on the **Save Assessment to Database** button to save the assessment to the database.

NOTE: It is important to save to database periodically as there is no automatic saving function to the database. Only back-up assessments are saved as files (see 4.1.6.1). All assessments are stored locally on the MSDE database engine, as installed with ASSET.

4.6.3 Save more than one assessment as a file

To save multiple assessments as a single file, you need to export the assessments into one XML file.

Select **File, Open assessment, Open assessment from database**. Check the boxes under the Export? column for all assessments that you want to save into the XML file.

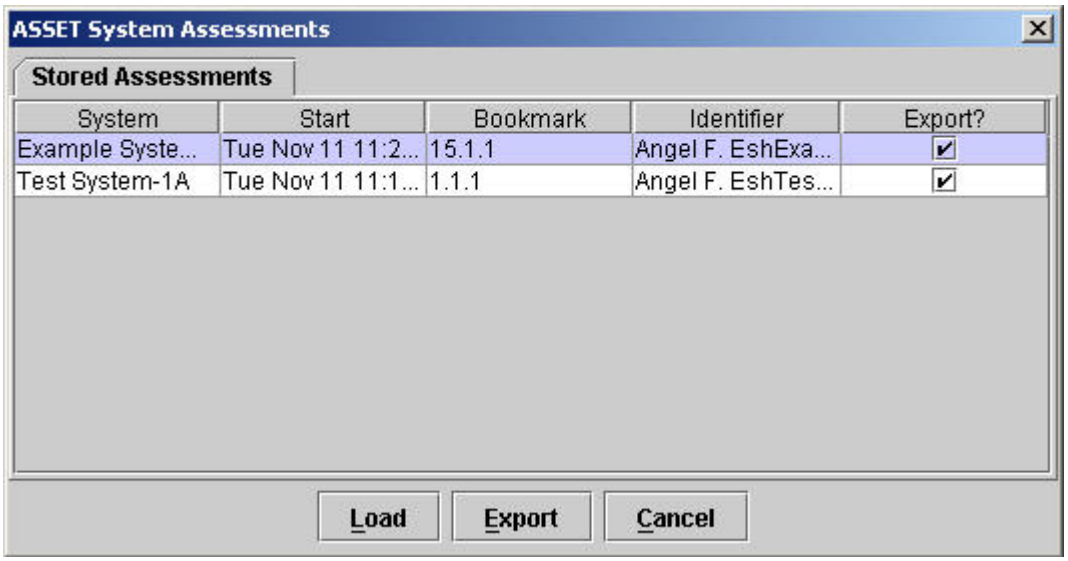


Figure 4.22 – Export Files to XML

Once assessments are chosen, select export. The Choose file to export assessment results dialog box opens. Select the location for the file, name the file (including the .xml file extension), and then click **Save**. The XML file exports to the ASSET system folder located on your hard drive by default or to the location you selected.

4.7 Open an Existing Assessment

To open an existing assessment, select **File** from the menu bar and then **Open**. There are two choices under Open. Depending on the location of the assessment, you can select either **Open assessment from the database** or **Import assessment from file**.

To open an assessment from the database, select **Open assessment from database** from the File open menu.

A window will then appear displaying a table of assessments that have been stored. Select the assessment you would like to open by highlighting the system name and choose **Load**.

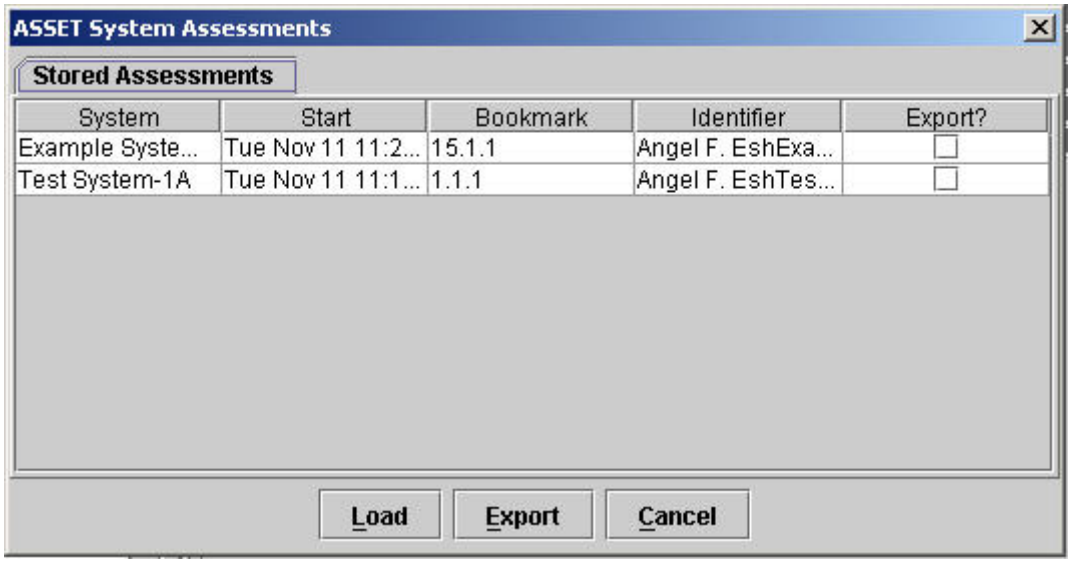


Figure 4.23 – Stored Assessment Window

The assessment will open in the main window.

To open an assessment that is in a file, select **Import assessment from file** from the File open menu. A window will appear where you can choose the file you would like to open and the format (.xml or .dat) for import. Once you have chosen your file, select **Open**.

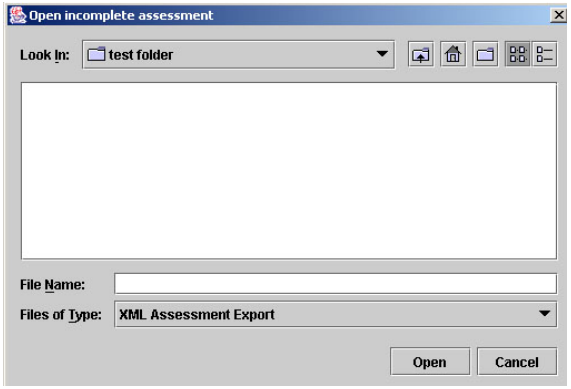


Figure 4.24 – Open an Assessment from a File

Once the file containing the assessment(s) has been imported, a confirmation dialog box will be displayed.

4.8 Export a Completed Assessment

Once you have completed your assessment, you are ready to export the assessment. There are two ways to export an assessment. You can use the Export Assessment button on the Summary tab, which is shown in Figure 4.25, or the Open assessment from database option, which is located under File open menu.

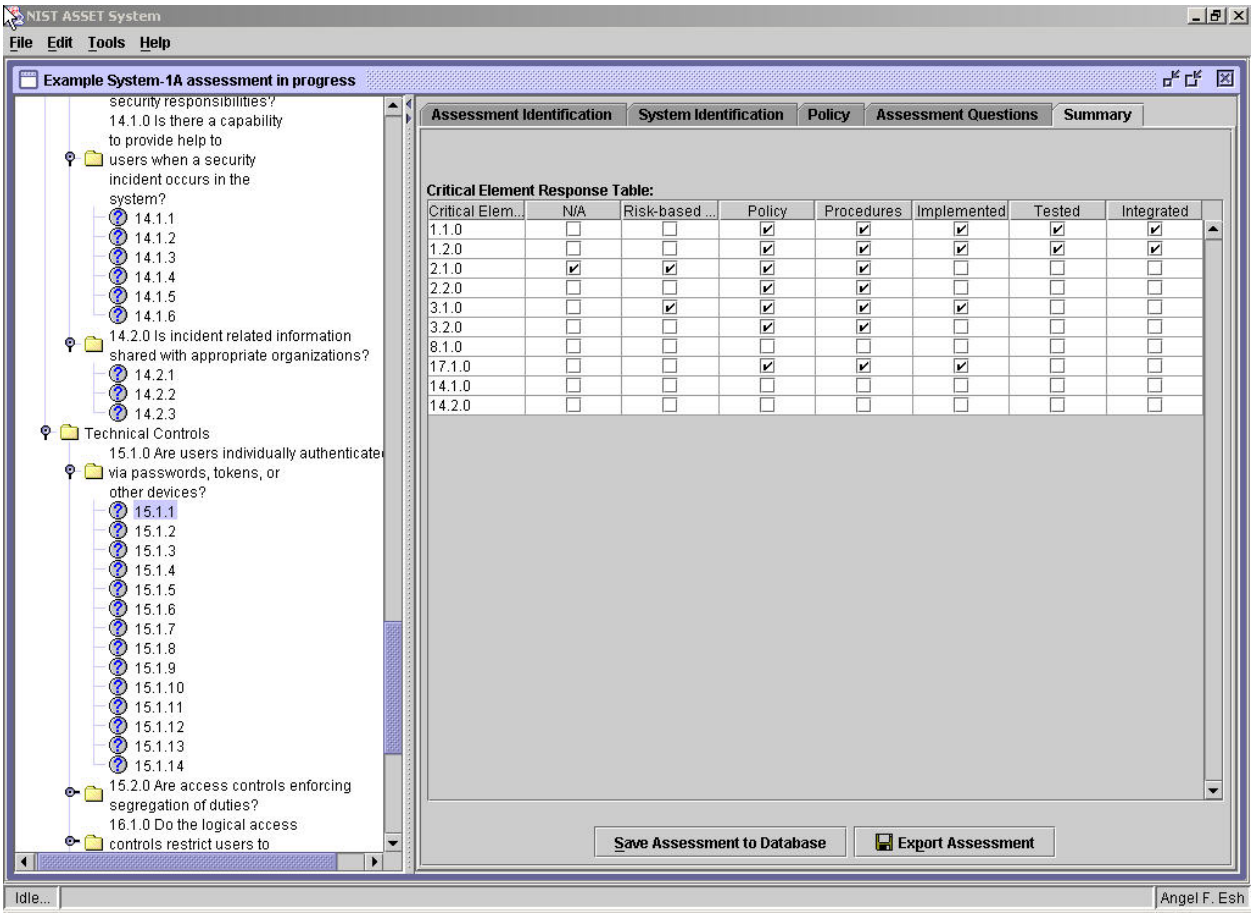


Figure 4.25 – Export an Assessment

Once export assessment has been selected, determine where you would like to save the assessment and the name for the assessment. Once you have determined a name and selected the location to save, select **Export**. The assessment will be exported/saved in XML and is then ready to be transferred via e-mail or disk to the individual in the Reporter role.

The **Open assessment from database** option, which is located under **File** and **Open Assessment**, is another way you can export the assessment. Once Open assessment from database has been selected, a window will show a table with all the assessments that are currently being stored in the database. Select the file that you would like to export by checking off the **Export** box. When the box has been checked off, you may select **Export**. Select the location in which the file will be saved. Name the file, including the .xml file extension, and select **Save**. The assessment will be exported/saved in XML.

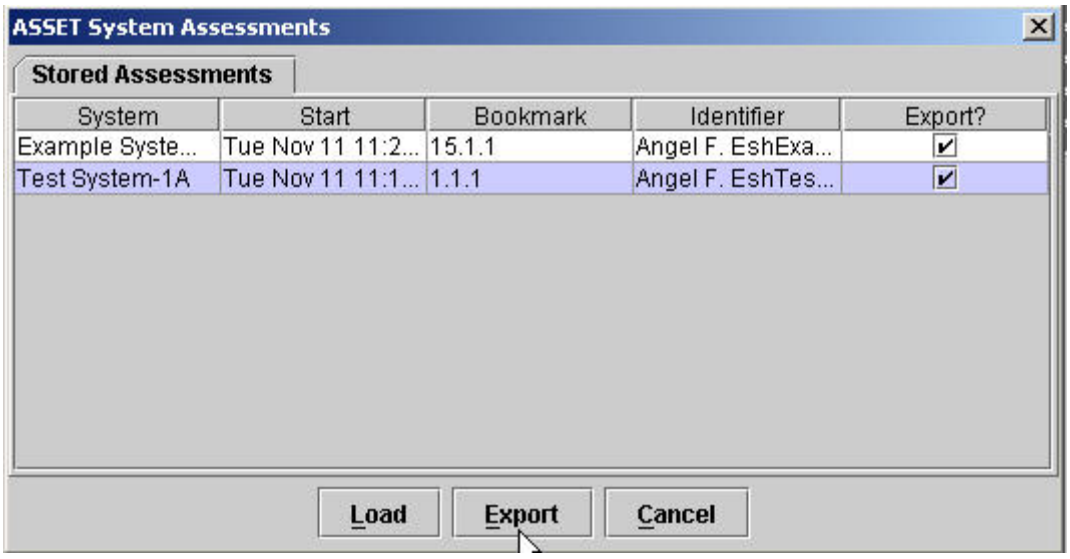


Figure 4.26 – Export Stored Assessments

At this point, the assessment is ready to be transferred via e-mail or disk to the Reporter.

NOTE: The export function saves the assessment to a file. It does not actually send the assessment to another system.

4.9 Reports

To develop and export reports within ASSET – System, select **Tools** from the menu bar and then **Reporting**.

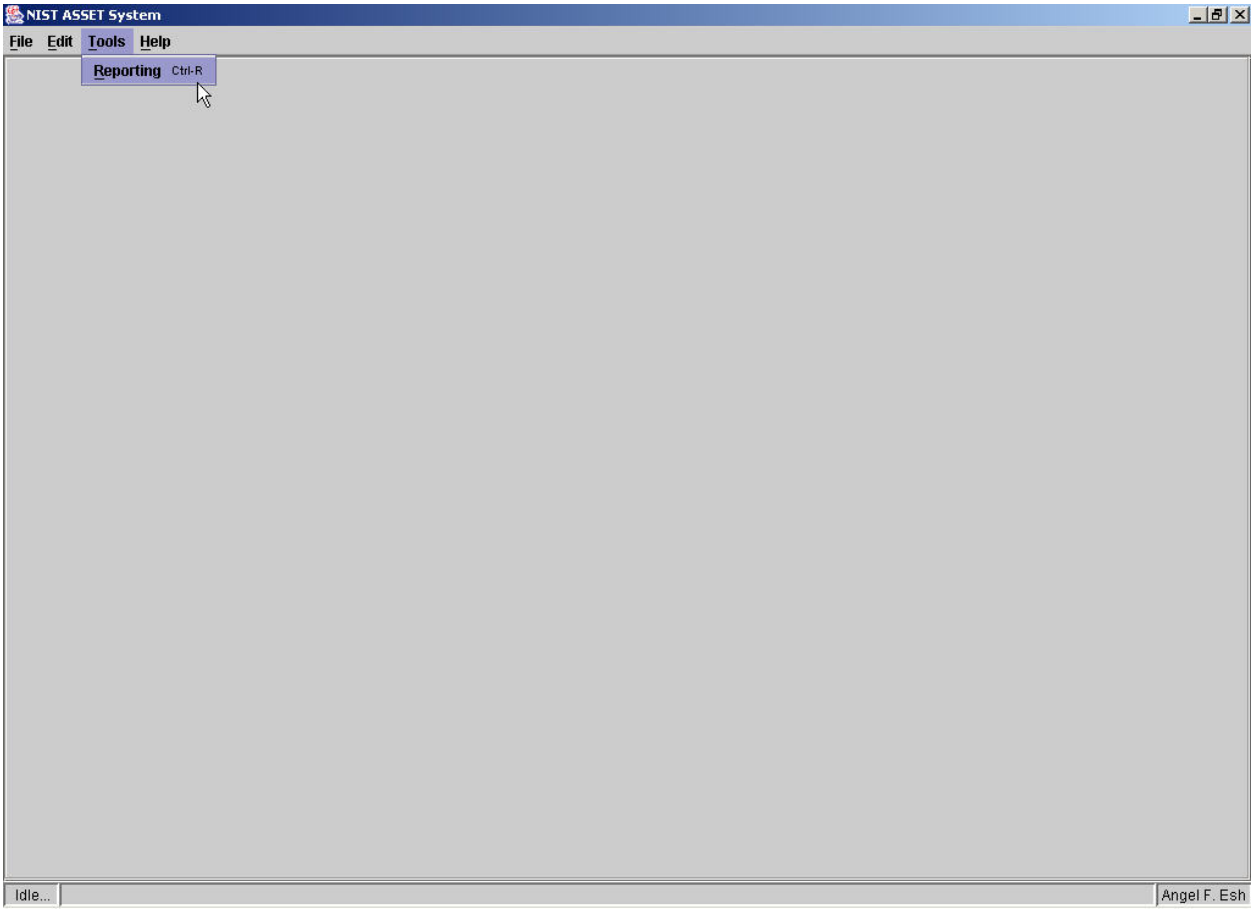


Figure 4.27 – Reports

Once **Reporting** has been selected, ASSET opens the reporting window, which provides a single access point for all reports. If you wish to return to ASSET, you may minimize or close the reporting window. To return to the reporting window, you can either reselect **Reporting** from the **Tools** menu or minimize the ASSET main window and then maximize the **Reporting** window.

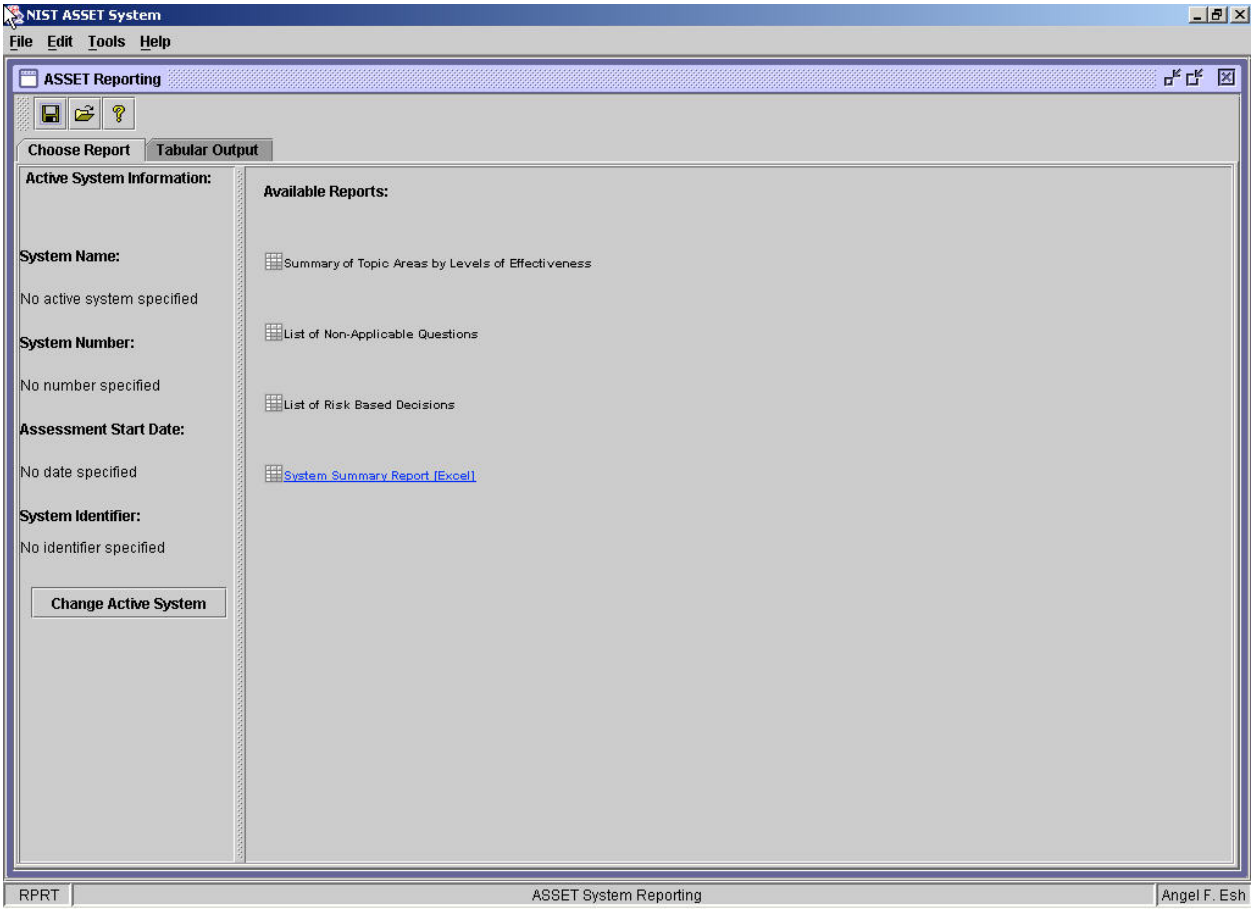


Figure 4.28 – Select a Report

Before you can create a report, you must identify which system among all the systems in the database you wish to view. To do this, you can either select **Change Active System** from within the active reporting window or select the **Open** icon at the top of the reporting window.

NOTE: An assessment must be first saved to the database before it can be viewed as a report.

Once you select the desired system from the Choose Assessment popup window, select **Continue**.

NOTE: You can only access one system at a time to develop and export reports.

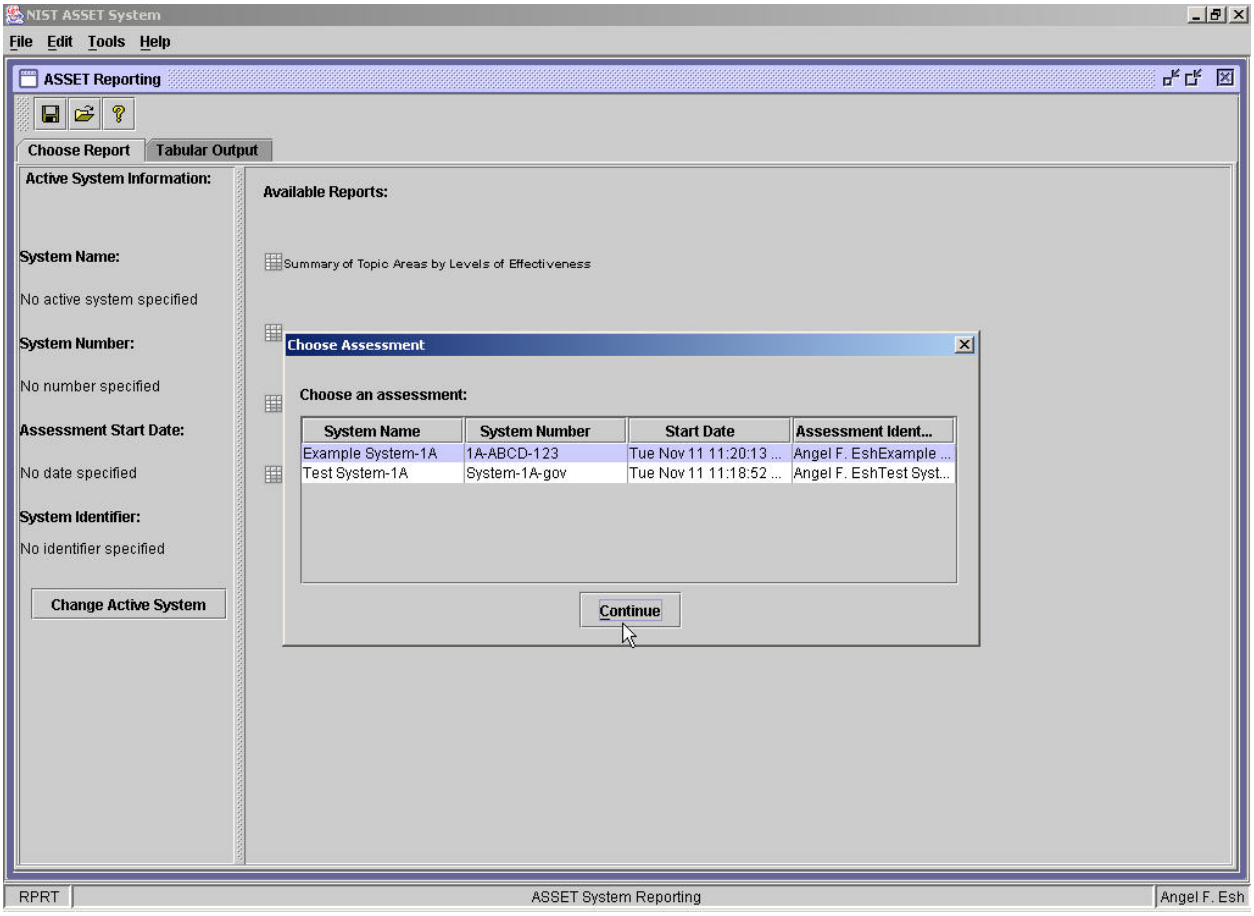


Figure 4.29 – Select Assessment Report

The system you select will be identified in the left windowpane of the reporting window. The four reports available for viewing in ASSET are listed in the right windowpane of the reporting window. They are a summary of topic areas by levels of effectiveness, list of non-applicable questions, list of risk-based decisions, and system summary. To select a report, click on the report title and the report will be displayed. The contents of each report are described below.

- Summary of topic areas by levels of effectiveness
    - Topic Number
    - Topic Area
    - Level of Effectiveness

- List of non-applicable questions
    - Question Number
    - Question Text
    - Comments

- List of risk-based decisions
    - Question Number
    - Question Text

    - Comments

- System summary (four Excel-based worksheets, all in a single workbook)
    - Level of Effectiveness summary worksheet
    - Non-applicable Questions summary worksheet
    - Risk-based Decision summary worksheet
    - System Summary worksheet

NOTE: The 'refer to' column of the system summary report shows questions that were assigned to an alternate assessor.

In general, these four reports will be used to assist you in understanding the state of single system assessments before exporting and sending them to the Reporter.

To move between the reporting window and the active report, the **Choose Report** and **Tabular Output** tabs of the reporting window may be used.

The first three reports can be exported to a tab-delimited text file, which is a text file format compatible with most applications. To export these reports to any spreadsheet, reporting, charting, or word processing application, click on the **Save** icon in the reporting window to save the report as "tab delimited text file." Type in the desired file name, select the desired file location, and select **Save**.

The fourth report exports ASSET data directly to Excel. After selecting **System Summary Report [Excel]**, Excel will be launched. A dialog box will be presented by Excel warning the user of the presence of macros. Macros are a necessarily element of this report and should be enabled when prompted.

In the fourth report, a color-coding scheme is used in the two summary reports to assist the user in identifying areas of improvement. A summary level of effectiveness of Policy, Procedures, or Implemented will generate a yellow color. A summary level of effectiveness of Tested or Integrated will generate a green color. No color represents either no policy or the question is not applicable or the question was not completed.

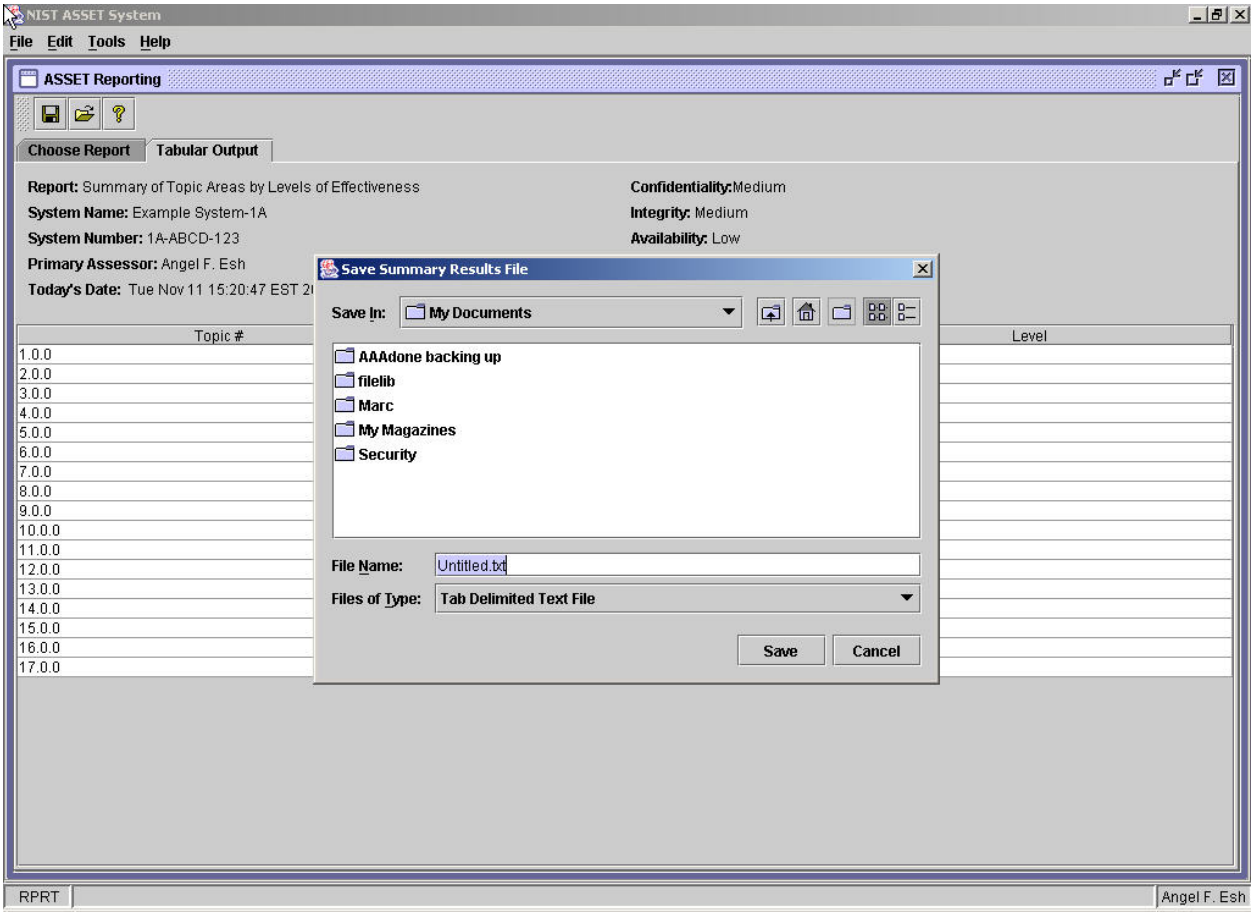


Figure 4.30 – Save as Tab Delimited Text File

To open a saved report from any other application (e.g., Microsoft Excel), open the application, navigate to that file, and open the file. Some applications may prompt with a series of questions to convert the file to a format compatible with that application. The report can then be modified to suit your own individual and unique purposes.

4.10 Printing

Printing directly from ASSET is not currently supported. To print, you must first export the assessment using the reporting functionality described above. Once the assessment has been exported to another application like Microsoft Excel, you can print the assessment and/or any reports that you have created.

4.11 Close ASSET

To exit from ASSET, select file. Then select either logoff or exit.

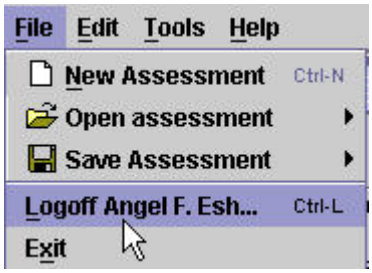


Figure 4.31 – Logoff

5 Uninstalling ASSET

To uninstall ASSET and all the components that were installed when ASSET was installed, you will need to uninstall the ASSET program files, JRE, and MSDE. Each of these uninstallation processes will need to be performed separately.

WARNING: Uninstalling ASSET will delete the database that contains your assessment data! It is important to export all your data to a backup XML file before uninstalling ASSET!

5.1 Uninstalling ASSET Program Files

To uninstall the ASSET Program Files, select **Start Menu** > **Programs > NIST ASSET** > **UnInstall ASSET**. Select **Yes**.

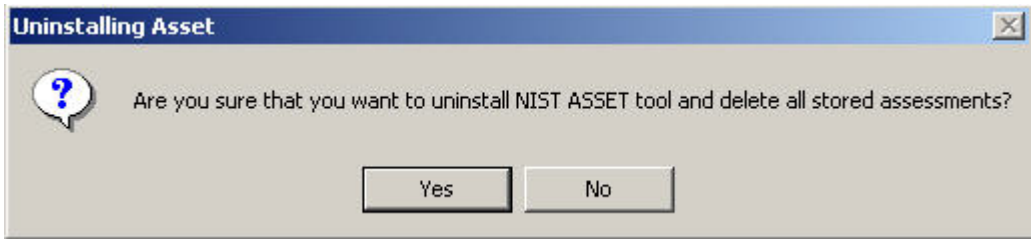


Figure 5.1– ASSET Confirmation Dialog Box

The uninstallation process will delete both the ASSET – System and ASSET – Manager databases. Select **Close** to complete the uninstall process.

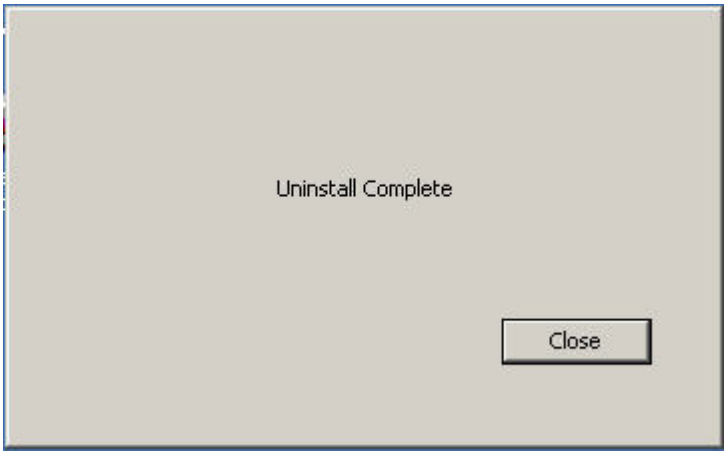


Figure 5.2 – Confirmation of ASSET Program Files Uninstall Completion

If files have been added to the NIST ASSET program folder, the uninstallation process will not delete this folder and any added files. This folder must then be manually deleted to complete the uninstallation process.

5.2 Uninstalling JRE

The process required to uninstall JRE is similar to the uninstall process of other Windows-based applications. Select **Settings**, then **Control Panel**, then **Add/Remove Programs**, from the **Start Menu**. Select **Java 2 Runtime Environment**, and **Change/Remove**.

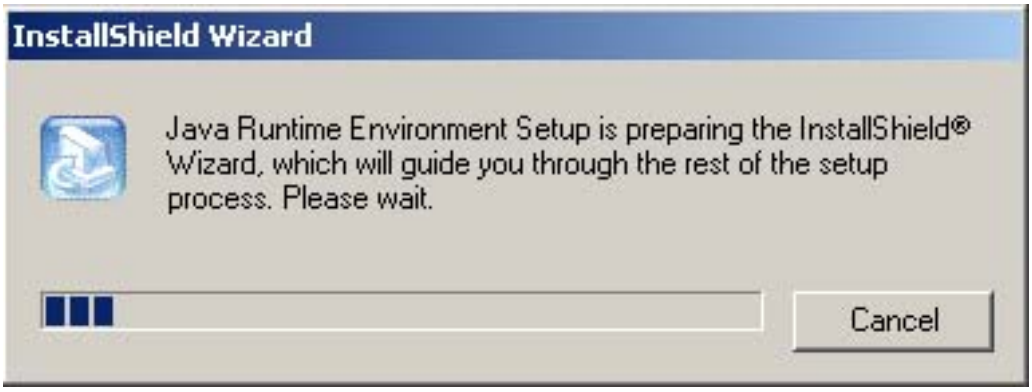


Figure 5.3 – JRE InstallShield Preparation Window

You will then be prompted to uninstall JRE.

Figure 5.4 – JRE Confirmation Dialog Box

Click OK. JRE will then be uninstalled from your system.

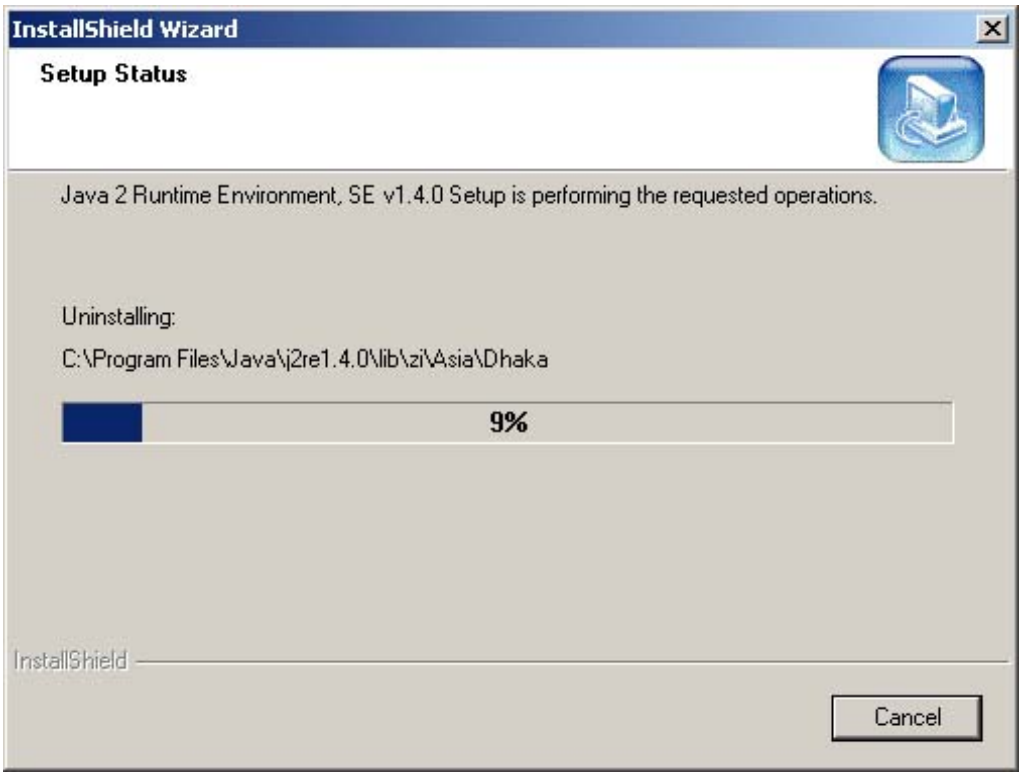


Figure 5.5 – JRE Uninstall Status Window

The JRE installation process installs an application and icon on the desktop entitled 'Java Web Start' which is not used by ASSET. You may uninstall Java Web Start by selecting **Add/Remove Programs**, and selecting Java Web Start.

5.3 Uninstalling MSDE

The process required to uninstall MSDE is similar to the uninstall process of other Windows-based applications.

Before you can uninstall MSDE, the MSDE SQL Server must be disabled. Right click on the SQL Server icon in the task bar located in the lower right corner of the screen (See Section 3.2.7) and select **MSSQL Server – Stop**. Next, right click on the SQL Server icon and select **Exit**. If the SQL Server icon is not displayed on the task bar, select **Program Files** from the **Start Menu**, then **MSDE**, then **Service Manager**, and select **Stop**.

Select **Settings**, then **Control Panel**, then **Add/Remove Programs** from the **Start Menu**. Select **MSDE**, and **Change/Remove**.

*NOTE: You may receive an error message, which restricts your ability to uninstall MSDE. The error message may list a process name that appears to be running. If you receive this message, press **Ctrl-Alt-Delete**, **Task List**, and **Processes**. Select the process name that was listed in the error message and select **End Process**. Close the task list window and continue with the MSDE uninstall process.*

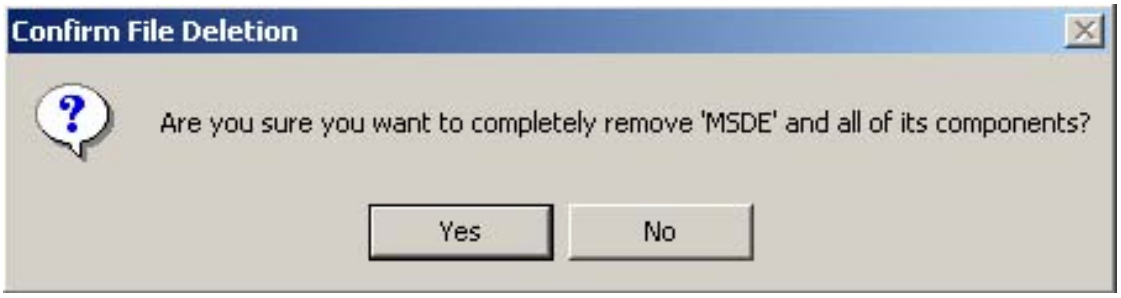


Figure 5.6 – MSDE Confirmation Dialog Box

NOTE: During the uninstallation process, you may be prompted to determine if you want to delete any 'shared files' that other programs may use in addition to MSDE. If you are unsure if you should select Yes, consult your system administrator.

Once the MSDE uninstall process has begun, the progress will be shown. At the end of the MSDE uninstall process, select **OK.**

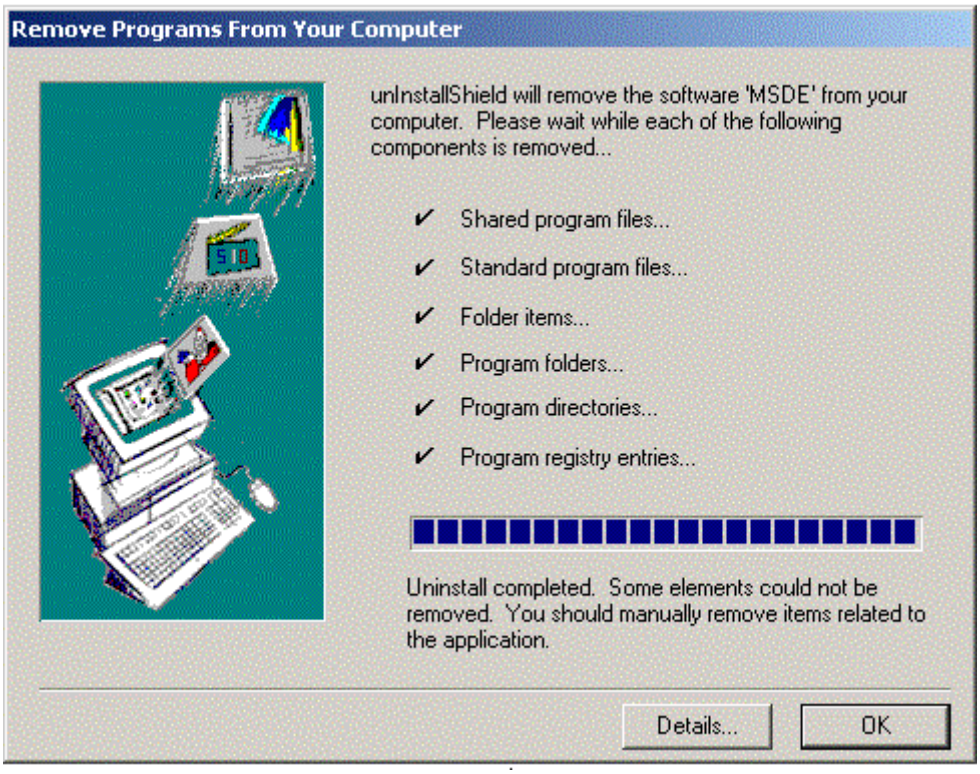


Figure 5.7 – MSDE Uninstall Progress Window

The final step to uninstalling MSDE is to delete the MSSQL7 folder from your hard drive. Open **My Computer**, then **Local Disk (C:)** and delete the MSSQL7 folder.

Appendix A—Glossary

Acceptable Risk	Is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing controls.
Access Controls	Restrict the ability to do something with a computer resource.
Accreditation	Is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security.
Agency/Division/Group	A hierarchical organizational component.
Asset	Is a major application, general support system, high-impact program, physical plant, mission critical system, or a logically related group of systems (in this context, it is not the acronym associated with the Automated Security Self-Evaluation Tool).
Audit Trails	A record of system activity by system or application processes and by user activity.
Authentication	Verifying the identity of a user, process, or device often as a prerequisite to allowing access to resources in a system.
Availability	The information technology resource (system or data) must be available on a timely basis to meet mission requirements or to avoid substantial losses. Availability also includes ensuring that resources are used only for intended purposes.
Availability Protection	Requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.
Awareness, Training, and Education	Awareness programs set the stage for training by changing organizational attitudes towards realization of the importance of security and the adverse consequences of its failure; the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in IT security.
Boundary Controls	The security measures that protect an interconnected system from unauthorized access.

Certification	Is the technical and non-technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements.
Computer Security	The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).
Confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality has three different protection requirements: High, a critical concern of the system; Medium, an important concern, but not necessarily paramount in the organization's priorities; or Low, some minimal level of security is required, but not to the same degree as the previous two categories.
General Support System	Is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
Implemented	Procedures and controls are carried out.
Individual Accountability	Requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.
Information	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.
Information Owner	Is responsible for establishing the rules for appropriate use and protection of the data/information. The information owner retains that responsibility even when the data/information are shared with other organizations.
Integrated	A comprehensive security program that is an integral part of an agency's organizational culture. Decision-making is based on cost, risk, and mission impact.
Integrity	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has when it has not been altered in

	an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
Interconnected System	Any system that is connected to another system.
Logical Access Controls	The system-based mechanisms used to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted.
Major Application	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.
Management Controls	Controls that focus on the management of the IT security system and the management of risk for a system.
Material Weakness	Is used to identify control weaknesses that pose a significant risk or a threat to the operations and/or assets of an audited entity. "Material weakness" is a very specific term that is defined one way for financial audits and another way for weaknesses reported under the Federal Managers Financial Integrity Act of 1982. Such weaknesses may be identified by auditors or by management.
Networks	Include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.
Not Applicable	Question (control objective/technique) does not apply to the system.
Operational Controls	Address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).
Organizational Standards	Required technologies or procedures that are specific to an organization.
Policy	Senior management's directives to create a computer security program, establish its goals, and assign responsibilities.
Primary Assessor	The primary assessor is defined by ASSET as the person who initiated the system assessment. The primary assessor designation

	is determined by the person who logs into the ASSET application at startup.
Procedures	Document the implementation of specific security controls.
Risk	Is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.
Risk-Based Decision	A decision that is made based upon looking at the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity and then weigh it against the impact and the cost of prevention.
Risk Management	Is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.
Sensitive Information	Refers to information whose loss, misuse, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs or the privacy to which individuals are entitled.
Sensitivity	An information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and/or availability that is determined by an evaluation of the sensitivity of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.
System	A generic term used for briefness to mean either a major application or a general support system.
System Assessor	Either a subject-matter expert or someone who knows and uses the system that will answer or help answer questions within the NIST Self-Assessment.
System Criticality	The degree of sensitivity based on the confidentiality, integrity, and availability needs of the system.
System Name	The name assigned to a given system.
System Number	The unique identifier given to a system.
System Operational Status	Operational – System is operating

	Under Development – System is being designed, developed, or implemented Undergoing a Major Modification – system is undergoing a major conversion or transition
System Type	Identifies the type of category the system is: major application or general support.
Technical Control	Focuses on security controls that the computer system executes.
Tested	Evaluates the adequacy and effectiveness of security policies, procedures, and controls.
Threat	An event or activity, deliberate or unintentional, with the potential for causing harm to an IT system or activity.
Vulnerability	A flaw or weakness that may allow harm to occur to an IT system or activity.

Appendix B—ASSET – Manager

B.1 Introduction

ASSET is a tool that was developed to support the NIST SP 800-26 self-assessment questionnaire. ASSET may be used to gather data and generate reports related to the status of the self-assessment. ASSET contains the security control objectives and suggested techniques for measuring the security of a system or group of interconnected systems as explained in NIST SP 800-26. The control objectives are taken from long-standing requirements found in statute, policy, and guidance on security and privacy.

B.1.1 Description of ASSET

ASSET consists of two host-based applications: ASSET – System and ASSET – Manager.

- **ASSET – System** facilitates the gathering of individual system data. It provides a limited reporting capability and allows the user to determine the completeness of an individual system assessment in progress.

- **ASSET – Manager** aggregates individual system assessments created by ASSET – System. It assists managers in developing an organization-wide perspective on the state of IT system security. ASSET – Manager also has the capabilities of ASSET – System built into it to facilitate the gathering of data for a limited number of systems.

The reporting features of ASSET are designed to provide users with a clear picture of the security status of their resources, as specified in NIST SP 800-26. The reports available from ASSET can be generated and interpreted by the users of the application.

ASSET – Manager stores data collected for the each of the individual system self-assessments. The tool generates all the reports that ASSET – System can generate. Additionally, it generates reports that summarize any user-defined group of systems (more than one system). Reports can be exported to any popular spreadsheet or charting program (certain reports are opened directly by Excel). The results of the self-assessment questionnaire can be used as input to a report evaluating an organization-wide IT security program.

NOTE: When ASSET – System and ASSET – Manager are installed on a single computer, each application will have its own unique database installed. ASSET – System can create individual assessments. ASSET – Manager can aggregate these individual assessments but it can also generate new individual assessments. Individual assessments that are created and modified when using ASSET – Manager will not exist in the ASSET – System database, as the two databases (System and Manager) are separate.

Although you can generate new assessments using ASSET – Manager, it is not a good practice as configuration management of data can be difficult if some original assessments are located in ASSET – System and some are located in ASSET-Manager. If necessary, you can view and modify existing assessments in ASSET – Manager. However, the tool bar from ASSET – System will not be available, which limits functionality. Because you can view and modify existing assessments, you will be able to make minor changes to the questionnaire for individual systems from within ASSET – Manager. The detailed instructions for this function are described in Section 4, Using ASSET – System of the ASSET User Manual.

B.1.2 Scope of Appendix B

This appendix provides specific detail about the operation of the ASSET – Manager module. Sections 1 through 3 of this user manual should be reviewed prior to reading this Appendix. Additionally, information has been provided that may be used by assessment managers in developing a strategy for conducting organization-wide system assessments. Each organization has unique issues and concerns that will necessitate an individualized approach to each organization-wide assessment. This appendix captures three generic scenarios that may be encountered by organizations. It should not be considered all-inclusive in the types of strategies that might be employed in performing an effective organization-wide IT security self-assessment.

B.2 Assessment Scenarios

The strategy for planning and conducting an assessment as well as reporting the results of an assessment will be unique to each organization. Each manager responsible for planning an organization-wide assessment must consider a host of factors in developing a strategy that can include: size, locations, and culture of an organization; capabilities and competencies of data assessors; and numbers and complexity of systems under review.

B.2.1 Scenario 1 – Limited Number of Systems

Scenario 1 involves an organization-wide self-assessment with a limited number of systems. Limited is a subjective term but in this scenario, it involves eight systems that a single assessor and reporter assessed. In this case, the data assessor and the reporter is the same person. Although the ASSET – Manager module can access ASSET – System from within its own module, it is important to understand that they are still separate applications. Individual system assessment data is collected using ASSET – System and is then exported to a .xml file. ASSET – Manager can then import that .xml file so that the assessments for the eight systems can be analyzed by developing individual system reports or aggregated system reports of all the eight systems (Figure B.1).

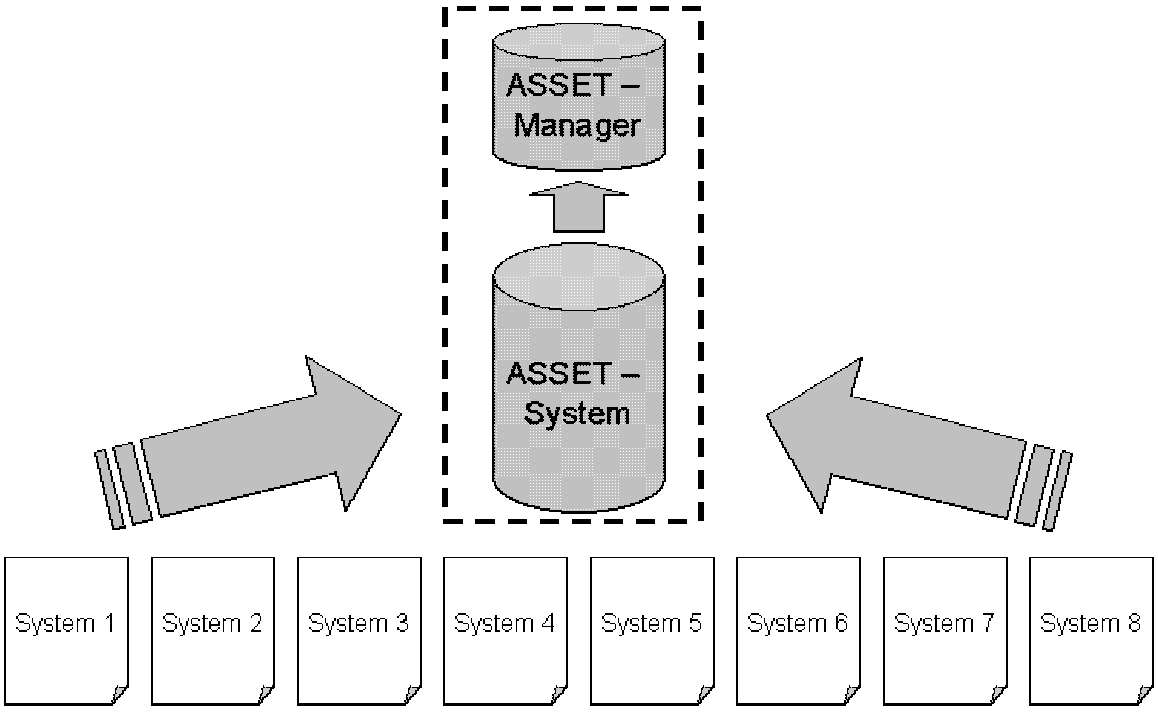


Figure B.1 – Scenario 1 Limited Number of Systems

B.2.2 Scenario 2 – Typical Assessment

A typical assessment occurs when an organization has a significant number of systems organization-wide, but can define logical groupings of systems. A fixed number of Assessors can gather data using ASSET - System for a number of systems, which then export this data for use by ASSET – Manager (Figure B.2). In this scenario, the organization has 16 systems, which are being evaluated by four assessors. Assessor A is evaluating six systems, assessor B is evaluating two systems, and so on. Each of the four assessors ensures that each of the assessments is complete before creating an .xml export file containing all the systems that they are assessing. The reporter then imports each of the four .xml files from each assessor, so that the assessments for the 16 systems can be analyzed by developing individual system reports or aggregated system reports of all the systems.

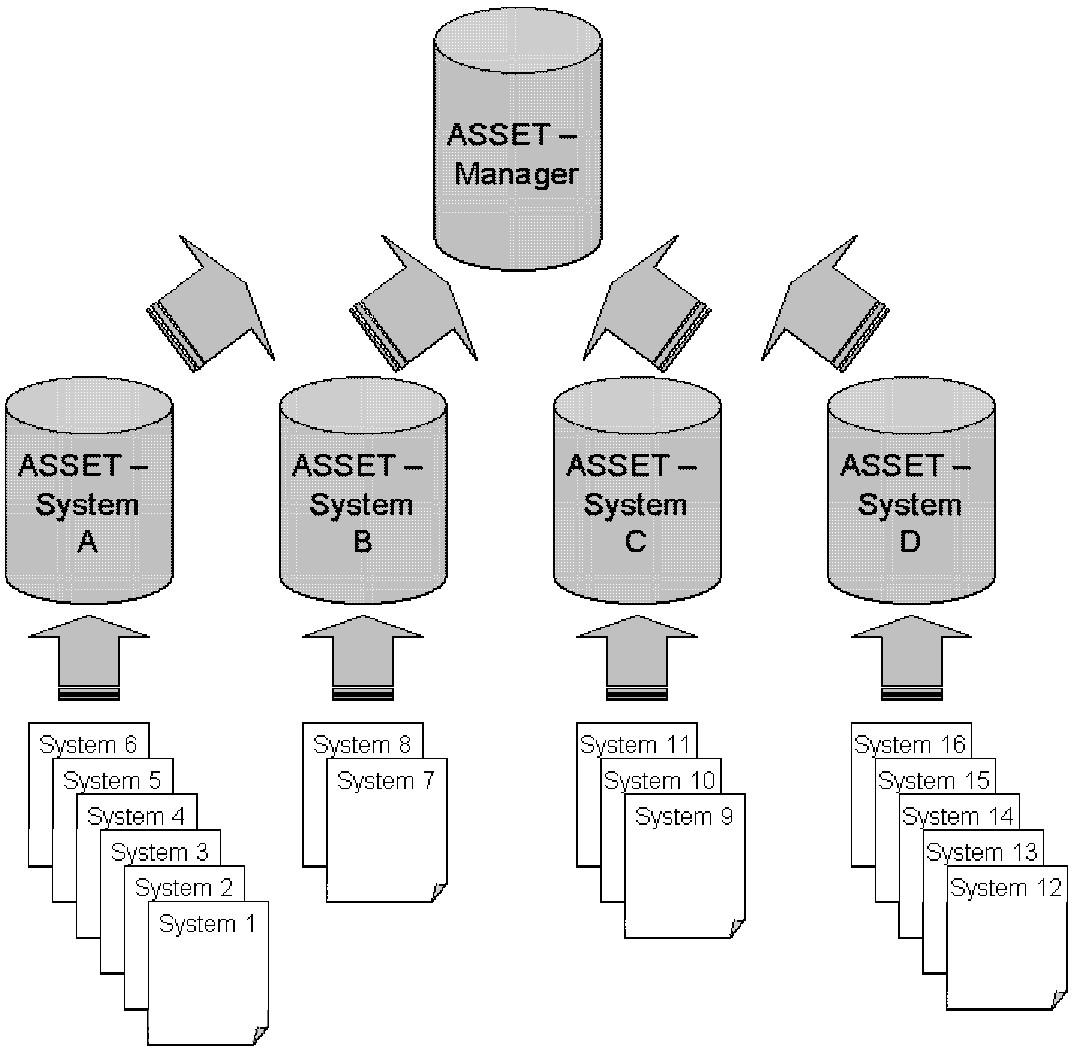


Figure B.2 – Scenario 2 Typical Assessment

B.2.3 Scenario 3 – Large Number of Systems

Scenario 3 involves a very large number of systems across a geographically distributed organization. In this scenario, each geographically distributed organization could be considered its own separate organization from a planning perspective. In this scenario, each sub-organization would gather system data as if it was operating under scenario 2. However, this scenario differs slightly in that system data could be aggregated at an intermediate level (the sub-organization level) by ASSET – System before being passed to ASSET – Manager for organization-wide aggregation (Figure B.3). This scenario is unique in that ASSET – System has the capability of importing into its database, a group of system assessments, although it is unable to view aggregation reports. (See Section 4.6.3 of the ASSET - System User Manual for guidance on exporting system assessments from the ASSET - System database.) This intermediate step only serves to simplify the task of aggregating a very large number of systems across a geographically distributed organization. It is important to note that in any assessment, there can only be one instance of ASSET – Manager, although there can be any number of instances of ASSET – System organized into any hierarchy necessary to perform an organization-wide assessment.

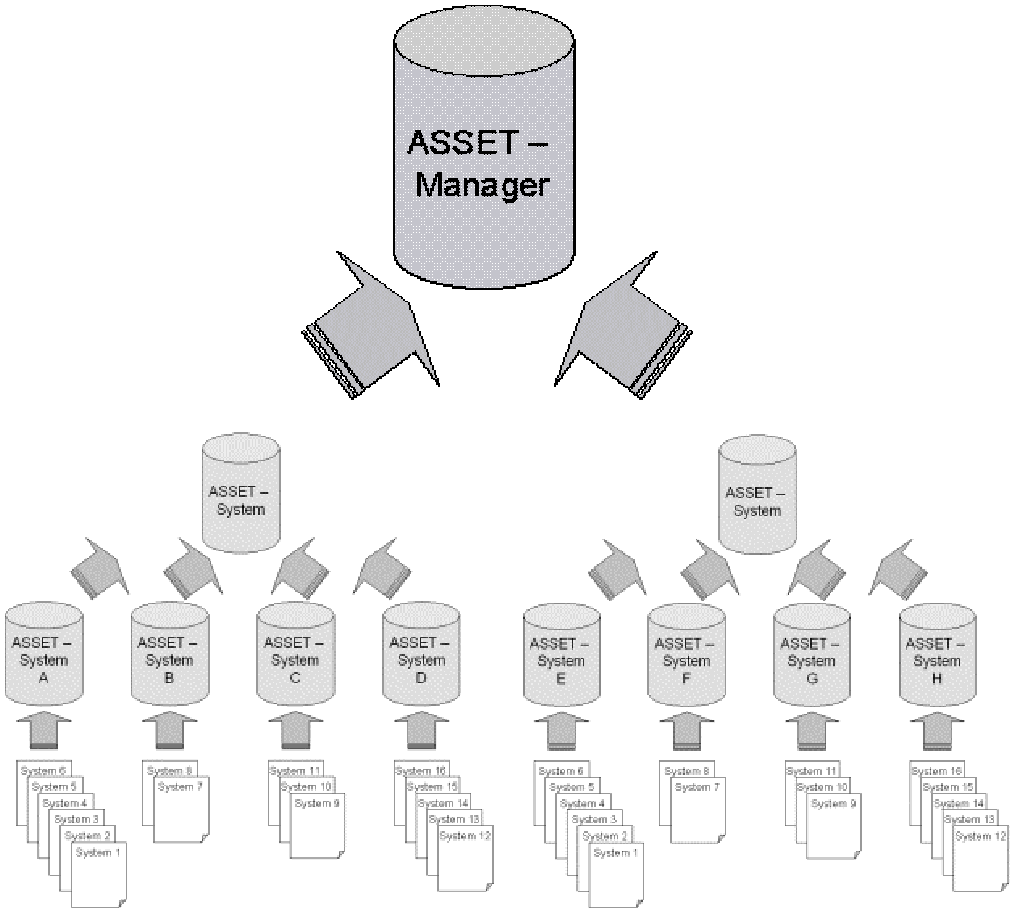


Figure B.3 – Scenario 3 Large Number of Systems

B.2.4 Special Consideration

In many cases, the manager planning an organization-wide assessment may wish to pre-answer a set of questions and then distribute these questions as the baseline questionnaire. For instance, the manager may wish to answer all the Policy questions since policy might be described at the headquarters level.

The following steps should be performed if the manager wishes to distribute a baseline questionnaire:

1. Create a new assessment from within ASSET – System and answer only those questions that will apply to a group of systems. You will need to create 'dummy' system identification data because this information is required by ASSET – System.
2. Export the assessment to an XML file and distribute to all data Assessors.
3. Assessors (those using ASSET – System) should import this questionnaire into their ASSET – System.
4. Assessors should modify the system identification information and save the assessment to the database.
5. Assessors should repeat step 4 as many times as necessary until all systems have been identified using the baseline questionnaire provided by the manager.

When implementing ASSET - System within an organization, there should be guidelines developed for completing the system identification section, i.e., naming conventions for system name/number, system type, agency/division/group, and system criticality. By establishing a standard prior to the completion of the questionnaires, the fields will be easily searched on by ASSET - Manager.

B.3 Using ASSET – Manager

B.3.1 Login

The login process is the same as ASSET – System except that you should double click on the ASSET – Manager icon located in the ASSET – Manager folder or on the Start menu. The rules for login are the same as ASSET – System.

B.3.2 User Interface

Once you login to ASSET – Manager, the Search ASSET – Manager window will open (you should maximize this window to view the available options).

NOTE: Certain incompatibilities may exist with the JRE application that is installed when ASSET is installed on your computer. These incompatibilities do not impact the data that you will create and save, but in a few isolated cases, the screen may not redraw properly. To correct this, maximize and then minimize (or vice versa) the screen.

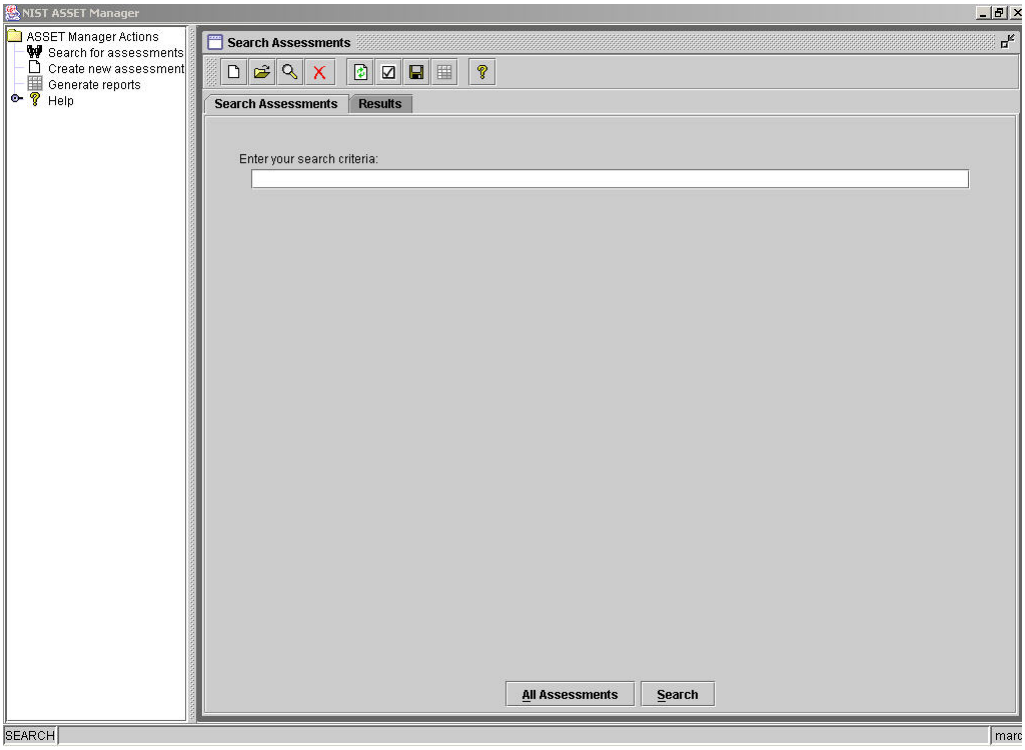


Figure B.4 – ASSET – Manager Search Window

You will be presented with four options on the left pane of the main window: Search for assessments, Create new assessment, Generate reports, and Help. Clicking on any of these options will present you with the selected option by opening the respective window.

NOTE: ASSET – Manager layers the windows as you open them. Reselecting one of the options on the left pane will not bring the option to the front of the window. You must minimize all windows and then reselect your desired window.

You may also use the toolbar at the top of the **Search Assessments** window. The following actions are available:

- Start new assessment: This option duplicates the action, **Create New Assessment**, in the left window (See Section B.3.5).
- Import new assessment: See Section B.3.3.
- Open selected assessment: This option opens a single assessment (ASSET – System view) for the systems that are checked.
- Delete selected assessment: This option deletes the assessments that are checked from the database.
- Refresh original assessment data: Clears all check boxes.
- Select all results: Selects all check boxes.
- Save / Export results to hard drive: Exports the display of systems to a text file so that it can be opened by any compatible application. This option only exports the search results display, not the assessment data.
- Reporting. Open reporting only on those assessments you set as active: Opens the reporting window. For ASSET – Manager reports, the selected systems will be used to generate aggregated reports. You cannot run the ASSET – System reports for multiple systems.
- Help: Provides guidance for each of the major processes.

In many cases, it will be easier to navigate using the toolbar rather than the options in the left window pane. In some cases (Import assessment, Reporting of set(s) of assessments, and Select all assessments), the functionality only exists on the toolbar.

NOTE: The Search Assessments Window is the default window; however, you must import your assessment(s) into the ASSET - Manager database before you can find them using the Search function.

B.3.3 Import Assessments

When you click **Import Assessments** on the tool bar, a dialog box will appear. You can then navigate to the XML file containing one or more assessments created in ASSET – System. Select the appropriate file and press **Open**. A confirmation box will appear. Click **Yes** to continue. Once the assessments have been imported in to the ASSET – Manager database, ASSET – Manager will return to the window that was active when you selected import, the **Search Assessments** window.

NOTE: To display a window appropriately, you may need to maximize the ASSET – Manager window.

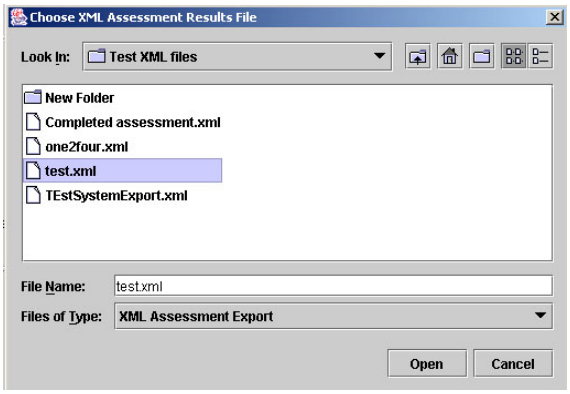


Figure B.5 – Import Assessments

B.3.4 Search for Assessments

The **Search Assessments** window (Figure B.4) allows you to select any subset of systems in the ASSET – Manager database.

To search the ASSET Manager database, the **Search Assessments** window must be active.

You can now perform a search of the assessment database using the search screen. The most common search will be to view the entire list of systems within the database. To view all systems, select **All Assessments** at the bottom of the **Search Assessments** window.

For more complex and specific searches, you must enter a search words into the search criteria box. Once this is done, you must choose a search field in the choose field box. ASSET will search the text boxes within the **Assessment Identification** and **System Identification** tabs. This search is not case sensitive.

Once ASSET – Manager retrieves the subset of systems that match the search criteria, the subset of systems will be displayed in the Results tab. You must then select the systems that you wish to analyze.

NOTE: To select a system, check the select box in the Search Assessments window. This allows you to create management-level reports on all systems checked. To perform an action that requires you to select a single system, for example, reviewing the system questionnaire, check the select box for only that system.

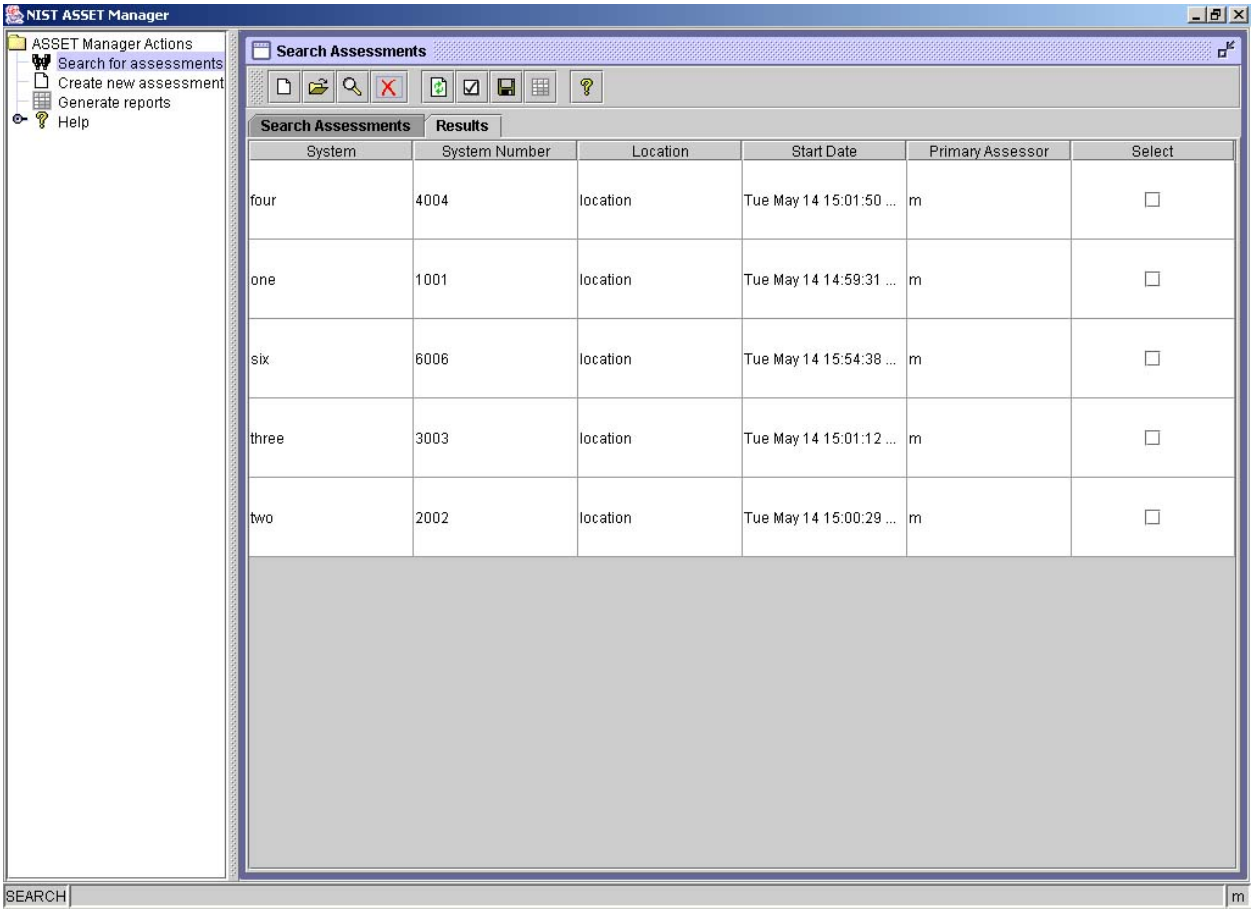


Figure B.6 – Search Assessments Window (Search Results)

Right-clicking on a selected system(s) will provide you with three options:

1. Show Info (provides administrative information about the selected system). This includes system name, number, and type; start date; whether the assessment is complete; primary assessor; and objective.

2. Export Results (exports the displayed table results showing the search results to a comma-separated-value text file)

3. Delete Assessment (deletes selected assessment).

B.3.5 Generate Reports

There are three ways to generate reports. You can generate reports using data from all assessments in the database, data from selected assessments in the database, or data from individual assessments in the database.

The **Generate Reports** button in the left navigation pane is used to generate reports from all assessments in the database.

The **Generate Reports** icon on the toolbar in the **Search Assessments** window is used to generate reports of selected sets of assessments or individual assessments. These reports will display data for the subset of systems checked in the **Search Assessments** window.

Select **Generate Reports** from the left window pane to open the reports window. The following window will appear:

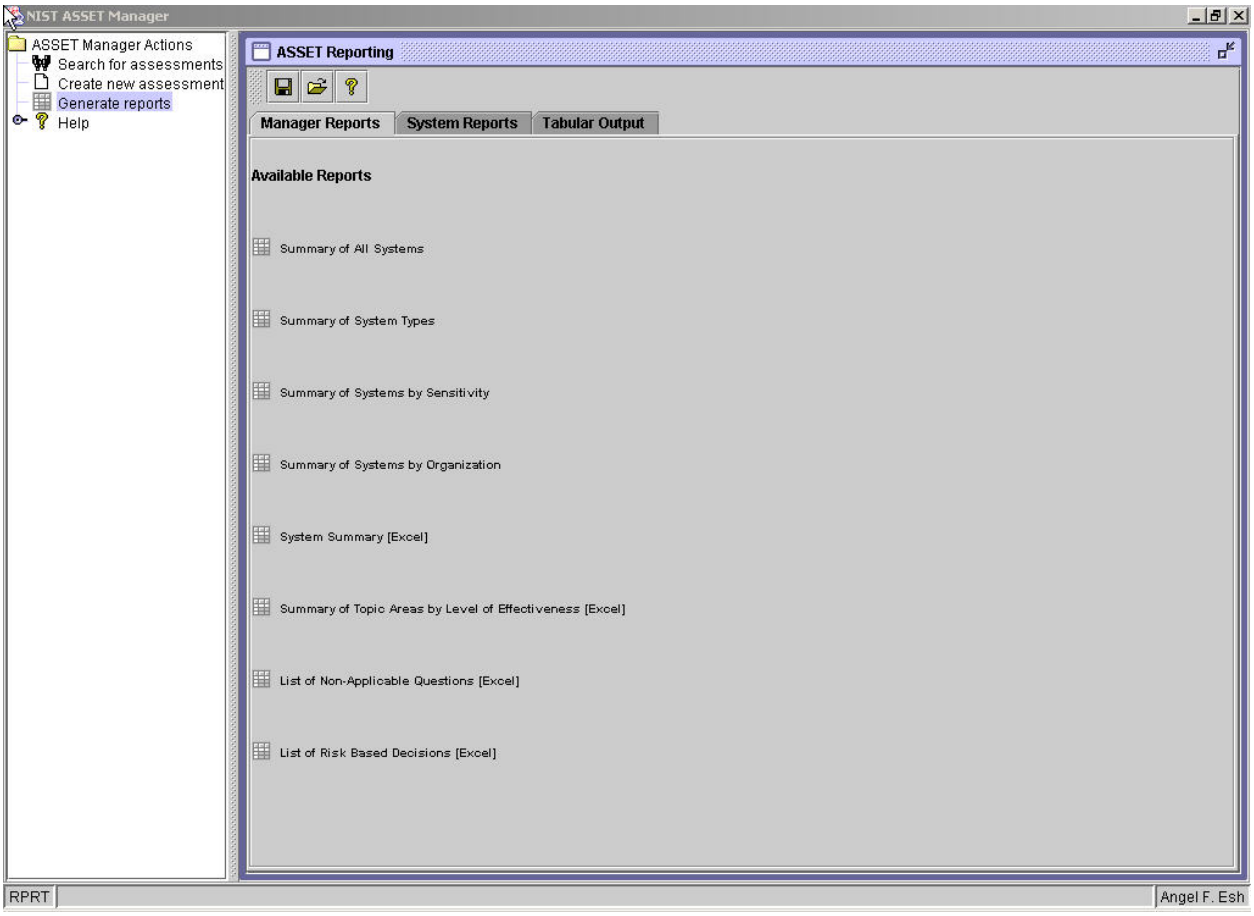


Figure B.7 – Reporting Window

This window is very similar to the reporting window of ASSET – System. For ASSET – Manager, four ASSET – based reports and four Excel – based reports are available under the Manager Reports tab.

The four ASSET – based reports include summaries of: all systems, system types, systems by sensitivity, and systems by organization. The contents of each report are described below.

- Summary of All Systems
    - System Name
    - System Number
    - System Type

    - Organization
    - Primary Assessor
    - Confidentiality Level
    - Integrity Level
    - Availability Level
    - Level of Effectiveness across Control Objective Area
        - Risk Management
        - Review of Security Controls
        - Life Cycle
        - Authorize Processing (Certification and Accreditation)
        - System Security Plan
        - Personnel Security
        - Physical Security
        - Production, Input/Output Controls
        - Contingency Planning
        - Hardware and Systems Software Maintenance
        - Data Integrity
        - Documentation
        - Security Awareness, Training, and Education
        - Incident Response Capability
        - Identification and Authentication
        - Logical Access Controls
        - Audit Trails
    - Assessment Completed?
- Summary of System Types
    - System Name
    - System Number
    - System Type
- Summary of Systems by Sensitivity
    - System Name
    - System Number
    - Confidentiality
    - Integrity
    - Availability
- Summary of Systems by Organization
    - System Name
    - System Number
    - Organization

The four Excel – based reports include system summary, summary of topic areas by level of effectiveness, list of non-applicable questions, and list of risk – based decision. Clicking on any of the links will launch Excel which will then create a formatted workbook suitable for printing that consists of worksheets that correspond to each of the selected assessments. Additionally, a summary report is created as the first worksheet. For instance, if 25 systems are selected, then a workbook will be created that consists of a summary page and 25 pages corresponding to each of the selected systems.

Each of these Excel – based reports uses macros to generate the formatted worksheets. Excel will prompt you to either disable or enable macros. You must enable macros if you wish the worksheets to open properly.

A color coding scheme is used to assist the user in identifying areas of improvement. A summary level of effectiveness of Policy, Procedures, or Implemented will generate a yellow color. A summary level of effectiveness of Tested or Integrated will generate a green color.

The **System Reports** and **Tabular Output** tabs perform identically as described in Section 4 of the ASSET User Manual. The **System Reports** are only available for individually selected assessments.

Appendix C—FISMA Reporting Template

C.1 Introduction

The FISMA reporting template was designed to extract data directly from the ASSET Manager database and provide users with answers to questions required by FISMA that can be derived from the data in ASSET. This template will generate data from ALL assessments in the ASSET - Manager database.

The template can be downloaded from the NIST ASSET website, http://csrc.nist.gov/asset.

C.2 Using the Template

Use of this template requires Microsoft Excel and ASSET – Manager and assessments in the ASSET – Manager database.

The procedure for using the FISMA Reporting Template is a 2-step process and is provided below.

Step 1 - Prepare data in ASSET Manager

Since this template extracts data using ALL the assessments in the ASSET – Manager database, it is important to delete any assessment that you do not wish to be considered by the template.

1. Open ASSET – Manager. Type '*' (no quotes) into the search criteria and select Search.

2. Delete any assessment that you would NOT like to see considered by the FISMA Reporting Template. Select the assessment(s) to be deleted, and select the 'X' command at the top of the window to delete the assessment. [NOTE: Due to a discrepancy in the v1.03 software, only 1 assessment may be deleted at a time. To delete the 2nd and subsequent assessments, this step (step 2) must be repeated. Versions 1.04 and up do not have this discrepancy]

3. Close ASSET – Manager [ASSET – Manager does not need to be open to use the template. The template creates a trusted connection with the ASSET – Manager database and extracts the data directly from the database.]

Step 2 - Using the FISMA Reporting Template

1. Double-click on the file, FISMASubset_Report_Template.xlt

2. Microsoft Excel will ask if you would like to enable macros. Macros must be enabled to use this template.

3. The template will extract the data from the ASSET – Manager database and prepare the template.

4. Save the template using a desired file name.

You now have successfully extracted data from ASSET - Manager using the FISMA Reporting Template.

Appendix D—ASSET Business Rules

ASSET incorporates a number of rules in the application that relate to how the questionnaire is answered and how questions and critical elements are scored when viewed as a group. This appendix describes these rules.

RULE TITLE	RULE DESCRIPTION
Responses to a question	Assessors are constrained to provide the levels of effectiveness in a sequential manner from Procedures, Implemented, Tested, and Integrated. If they do not check Procedures, for example, ASSET will not allow you to check Implemented.
Comments for a question	Comments are required if Not Applicable or Risk-based Decision is checked.
Completing a question	A question is considered complete if the Question Complete box is checked. If a question is not complete, it can be assigned to an alternate assessor. If you would like to answer the question later, you can assign the question to yourself.
Summary tab (first 2 columns)	If Not Applicable or Risk-based decision is checked in the Summary tab, at least one question in the critical element has been identified as Not Applicable or Risk-based Decision, respectively.
Scoring of critical elements	The last 5 columns of the summary tab show the effectiveness level for the critical elements. If Policy has been checked for a particular topic area, then all critical elements in that topic area will have Policy checked. If Policy has not been checked, then no critical element in that topic area will show any subsequent responses (Procedures, Implemented, Tested, Integrated), regardless of their actual responses in the questionnaire. The effectiveness level for the critical element is only as strong as the weakest question. Therefore, if out of six questions, five are answered Integrated, and one is answered Implemented, the critical element is rated as Implemented.
Scoring of topic areas	Like the effectiveness level of the critical elements, the topic areas are only as strong as the weakest critical element.

Appendix E—Considerations for ASSET Versions

Since ASSET was released, there have been four versions: 1.01, 1.03, 1.04, and 2.0. Versions 1.01 and 1.03 are no longer available for download at the NIST website. Significant changes incorporated by versions 1.04 and 2.0 are shown in the following table. A complete list of changes in each version can be found at the NIST ASSET website.

	v1.04	v2.0
ASSET Program	- Cannot use special characters (see user manual). - A number of small discrepancies were fixed (see v1.04 fact sheet at ASSET website). - Assessor names were not properly tracked in v1.03. When upgrading to v1.04, users need to verify that their assessors are properly documented. - Version 1.04 was modified so that multiple System Numbers could not be associated with a single system. Users should verify that their System Numbers are correct in v1.04. - Hard paragraph marks in text fields will result in proper formatting of tab-delimited reports. - Can import v2 XML files. Since v2 accepts special characters, while v1.04 cannot, users will still be required to eliminate any special characters from imported v2 assessments. - Allows more than one assessment in Manager to be deleted at a time.	- Can use special characters (except as noted by section 4). - New reports in both System and Manager that use Excel to draw and format the reports.
JRE	- Java 2 Runtime Environment v1.4.0	- Java 2 Runtime Environment v1.4.0
MSDE	- MSDE 1.0	- MSDE 1.0
Installation Process Notes	- Uses InstallShield Wizard for full install - Application is available to move incrementally from v1.03 to v1.04 - Icons for ASSET are placed on the desktop - ASSET is uninstalled by using the Add/Remove Programs control panel	- Uses a custom installation application - Application is available to move incrementally from v1 (either v1.03 or v1.04) to v2.0 - Must have Microsoft Access, Microsoft Office Server Extensions, or MSDE currently installed.[9] - Icons for ASSET are not placed on the desktop. For incremental installations from v1 to v2, existing icons will remain on the desktop. - ASSET is uninstalled using the Uninstall link located on the Start >Programs>NISTASSET menu

Figure E.1 – Overview of Changes (ASSET v1.04 and v2)

[9] Microsoft Access and Office Server Extensions are available on the Office 2000 installation disk.

Appendix F—Installation Process for Version 1.04

Note to Readers:

This section describes the full installation and uninstallation process for NIST ASSET v1.04. This appendix was adapted directly from NISTIR 6885 2003 ED, Automated Security Self-Evaluation Tool User Manual (version 1.0), sections 3.1 to 3.2.3, and section 5.1. Sections 3.2.4, 3.2.5, 5.2, and 5.3 are not specific to ASSET version number and are retained in the body of this user manual.

It is also possible to incrementally upgrade v1.03 to v1.04. Instructions for this incremental upgrade process can be found at the NIST ASSET website:

http://csrc.nist.gov/asset/

F.1 Requirements for Installing Version 1.04

Microsoft Windows® is the required operating system for ASSET. Much of the organization and logic of the ASSET installation process is similar to that required for other MS Windows application installations. ASSET installation files are available on NIST ASSET website:

NOTE: Internet connectivity is NOT a requirement for use of ASSET.

F.1.1 Hardware

The following are minimum hardware requirements to run ASSET:

- Pentium III – 1.0 GHz processor (or equivalent x86 compatible architecture)
- 256 MB RAM
- 120 MB of free disk space

NOTE: Each completed assessment in ASSET requires an additional 3 megabytes of hard disk space.

F.1.2 Software

The following minimum software is required for ASSET:

- ASSET was designed to operate with Windows 2000 Professional
- JRE version 1.4 installed
- MSDE version 1.0 installed

NOTE: The ASSET installation process will install all required software, including JRE and MSDE.

F.2 Installation Process

When downloading the installation files from the NIST website, follow the instructions on the website for downloading the files. The licensing provisions of this application are described during the installation of ASSET.

The ASSET installation process uses an InstallShield application common to many Windows-based applications. Three major components are installed on your computer during the installation process:

- MSDE
- JRE
- ASSET program files

The ASSET application and its program files are installed in the **Program Files** folder. If your computer has restricted access to this folder, your systems administrator will need to grant you permission to access the **NISTASSET** folder within the **Program Files** folder.

Additionally, the MSDE administrator password must be set and the ASSET database must be initialized. Guidance on completing these actions is provided in following sections of this appendix.

NOTE: The setting of the MSDE administrator password is critical to eliminating one of the identified MSDE vulnerabilities.

One vulnerability with MSDE exists because MSDE is designed to allow your computer to act as a database server. The final action that you should perform in the installation process, which is not done during the InstallShield process, is to turn off this MSDE network functionality. (See Section 3 of the user manual for instructions on how to turn off MSDE network functionality.)

NOTE: Turning off MSDE network functionality is not required by ASSET but it eliminates a number of MSDE vulnerabilities. If your computer requires MSDE network functionality, you should not perform this last installation process. If you are unsure if you need this functionality, consult your network administrator. MSDE vulnerabilities can be mitigated in other ways should you need to have MSDE network functionality. Examples include additional host-based or network-based security.

F.2.1 Installing ASSET and its Required Components

To install ASSET, double click the **setup.exe** file located in the NIST ASSET installation folder (disk). Click on the **Next** button to proceed with the installation.

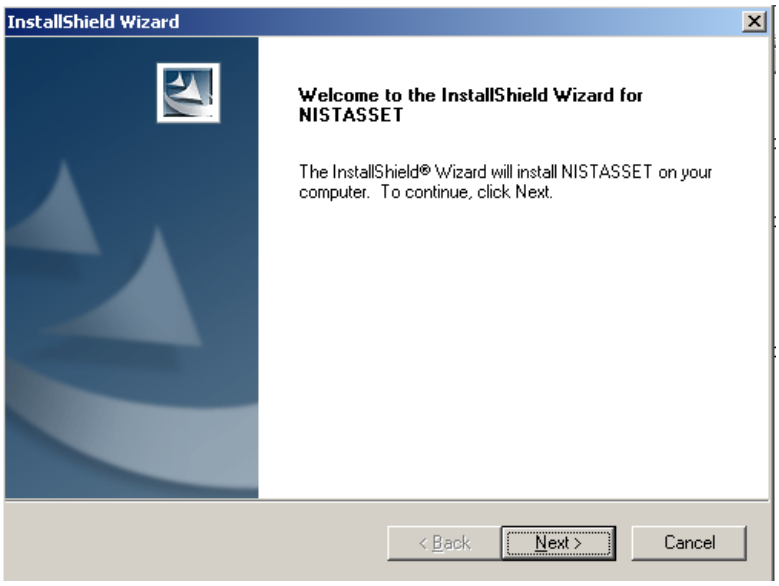


Figure F.1 – ASSET Installation Start Screen

The licensing provisions of ASSET will be displayed. If you agree, select **Yes**. You must agree to the licensing provisions of ASSET if you wish to proceed with installation.

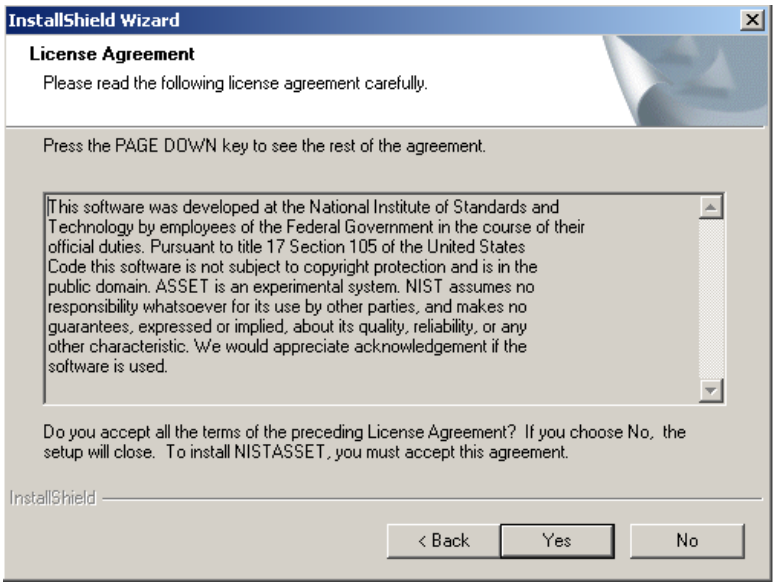


Figure F.2 – License Agreement

Two options are available for installation: install ASSET – System only or install both ASSET – System and ASSET – Manager. In all options, all necessary components (MSDE and JRE) will be installed.

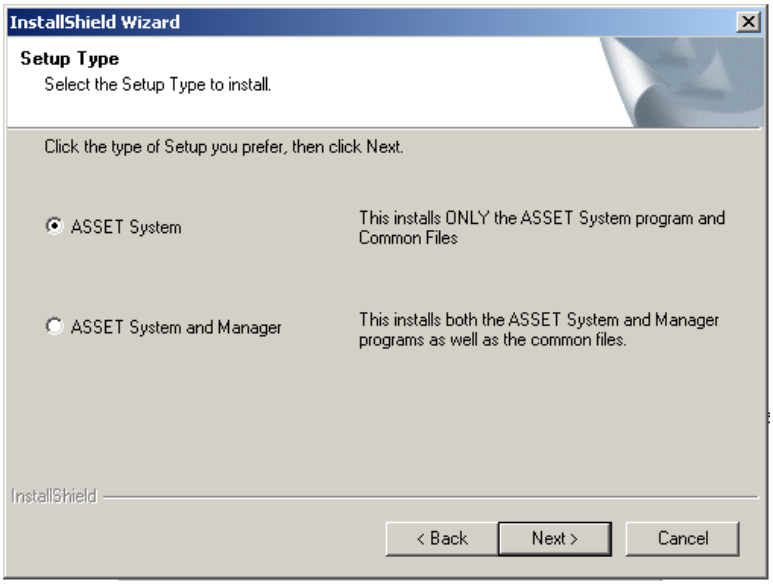


Figure F.3 – Installation Types

NOTE: If you install only ASSET – System and later want to add ASSET – Manager, you will need to backup / export your data, uninstall ASSET – System and then install both ASSET – System and Manager.

NOTE: Once you reach this point in the installation process, the installer application will reach 73-87% (depending on the type of installation) progress very quickly. It may then take up to 5 additional minutes to complete the next step in the installation process.

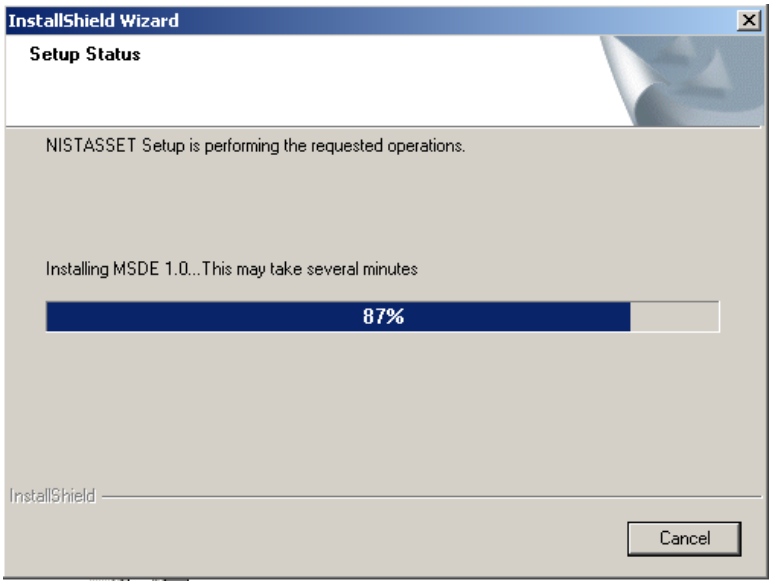


Figure F.4 – Setup Status

An error may be displayed in the installation process that states the ‘Service has not been started.’ You should press OK to proceed with the installation.

The InstallShield wizard will then walk you through the installation of JRE.

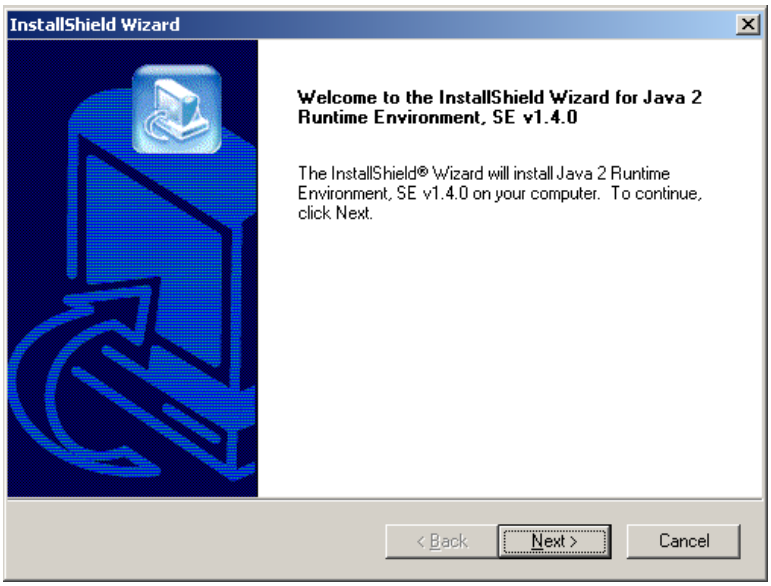


Figure F.5 – JRE Installation

You will then be prompted to accept the JRE license agreement. You must accept this agreement to proceed with installation.

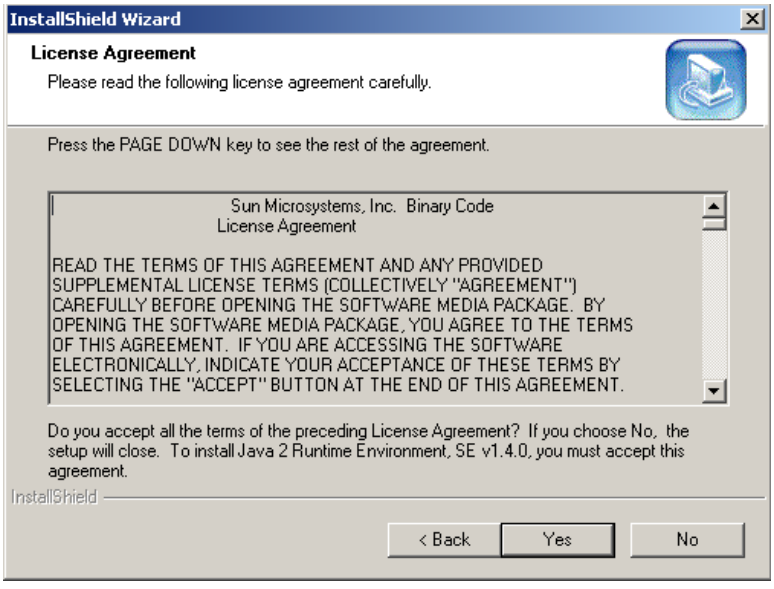


Figure F.6 – JRE Installation License Agreement

You will be prompted to select the location of the JRE files.

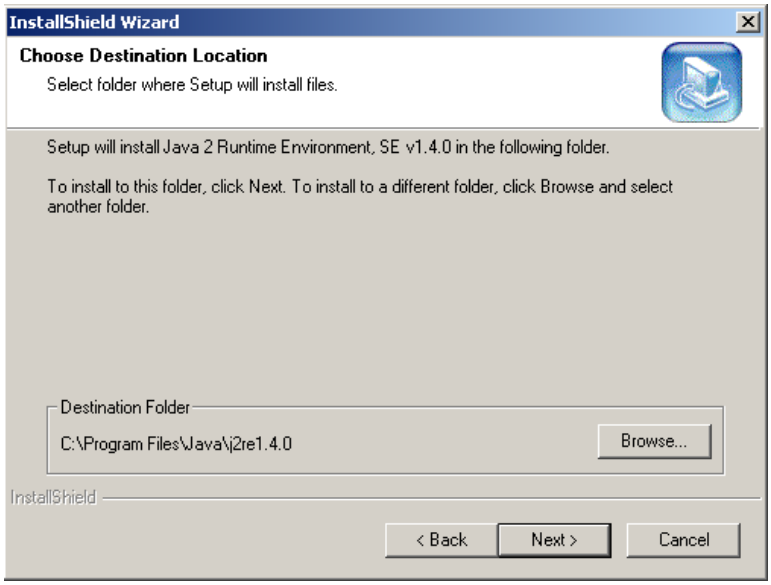


Figure F.7 – JRE Destination Location

At this point in the installation process, you will be asked to select the browsers for use with JRE (ASSET).

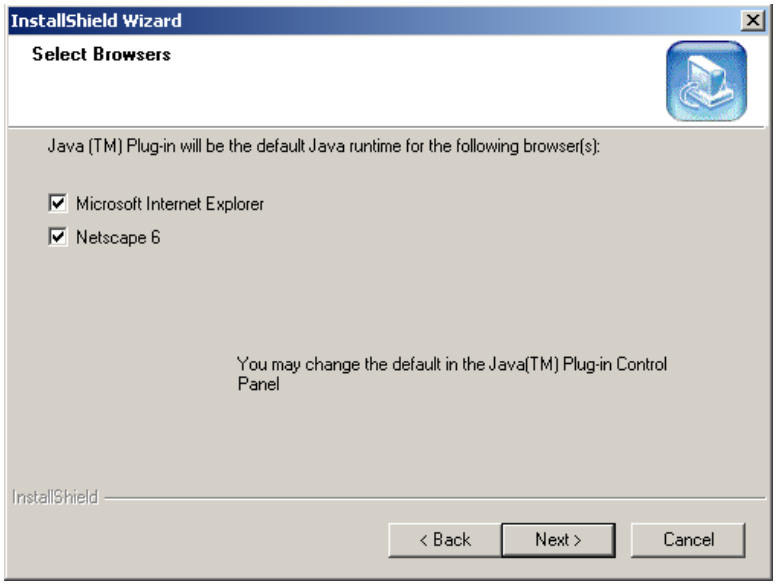


Figure F.8 – JRE Browsers

At this point in the installation process, InstallShield will create the necessary databases for ASSET – System and ASSET – Manager.

F.2.2 Setting ASSET Administrator Database Password

This section describes the operation of the ASSET Database Password Utility (ADPU). This utility is designed to change the default password of the MSDE database system that powers the NIST ASSET application. The default installation of MSDE creates an account with a username of "sa" and no password. Several vulnerabilities have been known to exploit this blank password to gain access to a system with MSDE installed.

The operation of the ADPU depends on user interaction. You will be prompted to interact with the ADPU during the installation process or you may access it later (**NISTASSET Program Files > ASSETPassword.jar**) to change the password.

If you decide to choose your own password, you will need to confirm the password before you can change it with the MSDE system.

NOTE: It is not necessary to remember this password as it will only be used once and you will not be required to enter it again.

The ADPU user interface is displayed in the following figure:

Figure F.9 – ADPU User Interface

NOTE: If only installing ASSET – System, the installation process will default to the Advanced tab of the ADPU user interface. You should select the Change Password tab to continue with the installation process.

Manual selection of password. You have the option to choose a password. If you wish to choose a password, enter it into the text box in the ADPU user interface. There is no limit on the password that you choose. The only requirement is that the maximum length of the password must be less than 128 characters.[10]

[10] Asterisks are indicated as a security feature to mask the password.

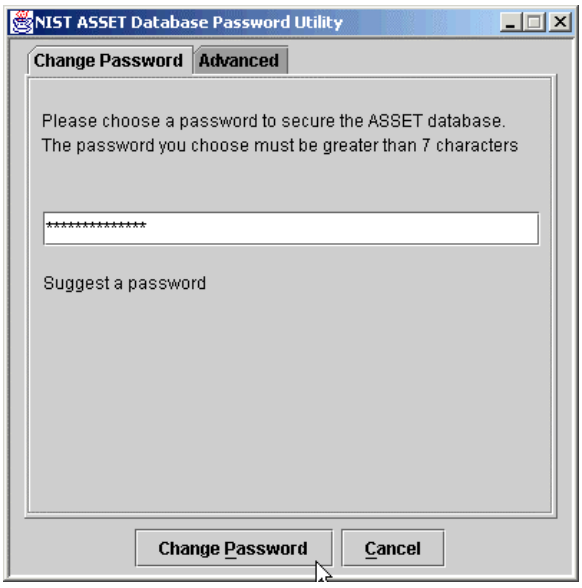


Figure F.10 – ADPU Password Textbox

Once you have entered a password once, you must press the Change Password button in order to initiate the password change. In order to confirm the password you entered, you will be required to enter the password again. The following figure shows the ADPU program requiring you to re-enter the password.

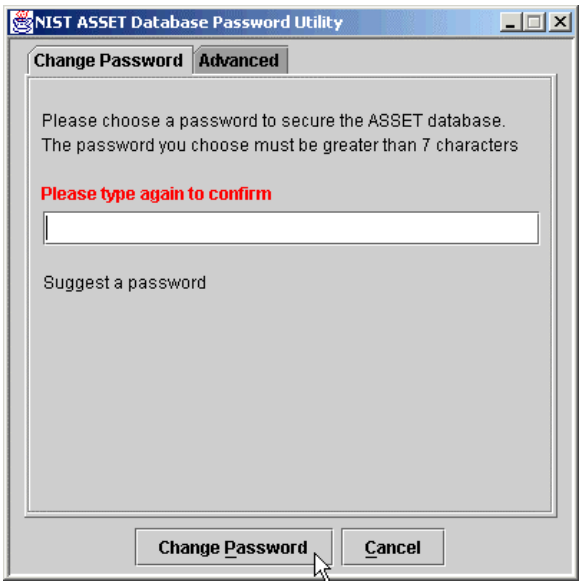


Figure F.11 – ADPU Password Confirmation

Automatic selection of password. The ADPU program can suggest a random password. To have ADPU suggest a password, click on the **Suggest a Password** link. The following figure shows an example of having the ADPU program suggest a password for you.

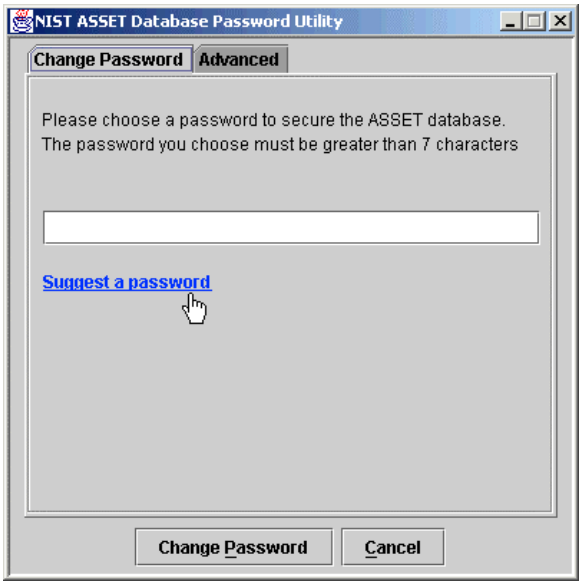


Figure F.12 – APDU Automatic Password Selection

NOTE: Once you choose a password or have one suggested for you by the APDU program, you need to submit the changed password by clicking on the ***Change Password*** *button.*

Depending upon which ASSET applications you have installed, you may see either one or both of the following figures.

Figure F.13 –ASSET System Password Changed Dialog Box

Figure F.14 –ASSET Manager Password Changed Dialog Box

Click on **OK** to close the dialog boxes. Once you have followed these steps, the password of the ASSET application has been changed. If your organization password policy requires routine password changes, the ADPU control panel can be accessed later (**Start Menu>Programs>NIST ASSET>Change Password**)

NOTE: Do not modify any of the settings on the Advanced property page without consulting your network administrator.

F.2.3 ASSET Installation Completion

The ASSET installation process is now complete. You will not be prompted to restart your computer.

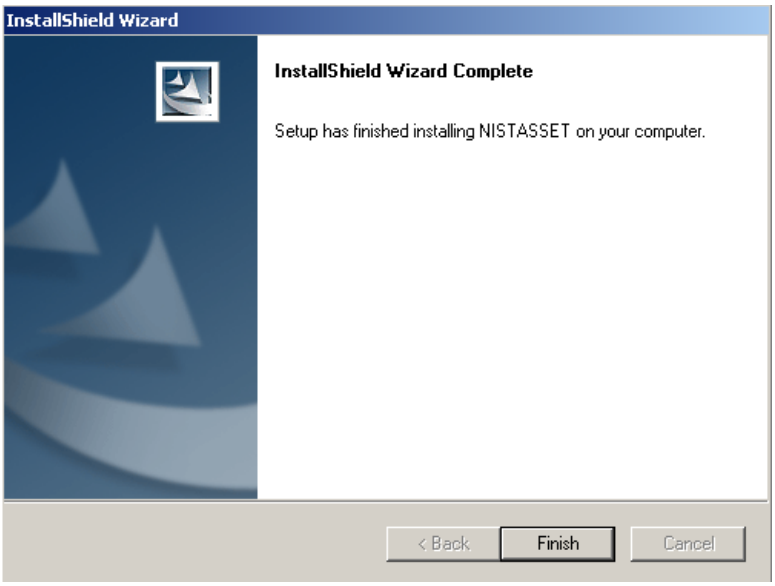


Figure F.15 – ASSET Installation Complete

Once the ASSET installation process is complete, you may locate the ASSET program files in the NISTASSET folder within your Program Files folder.

NOTE: Shortcuts for ASSET, the user manual, and NIST SP 800-26 are placed on the Start menu. Shortcuts for ASSET are placed on your desktop.

NOTE: Although restarting your computer is not necessary after ASSET is installed, it is a good practice to restart once installation is complete.

*NOTE: It is highly recommended that you now install the latest service pack for MSDE, which is in the **Service Packs** folder.*

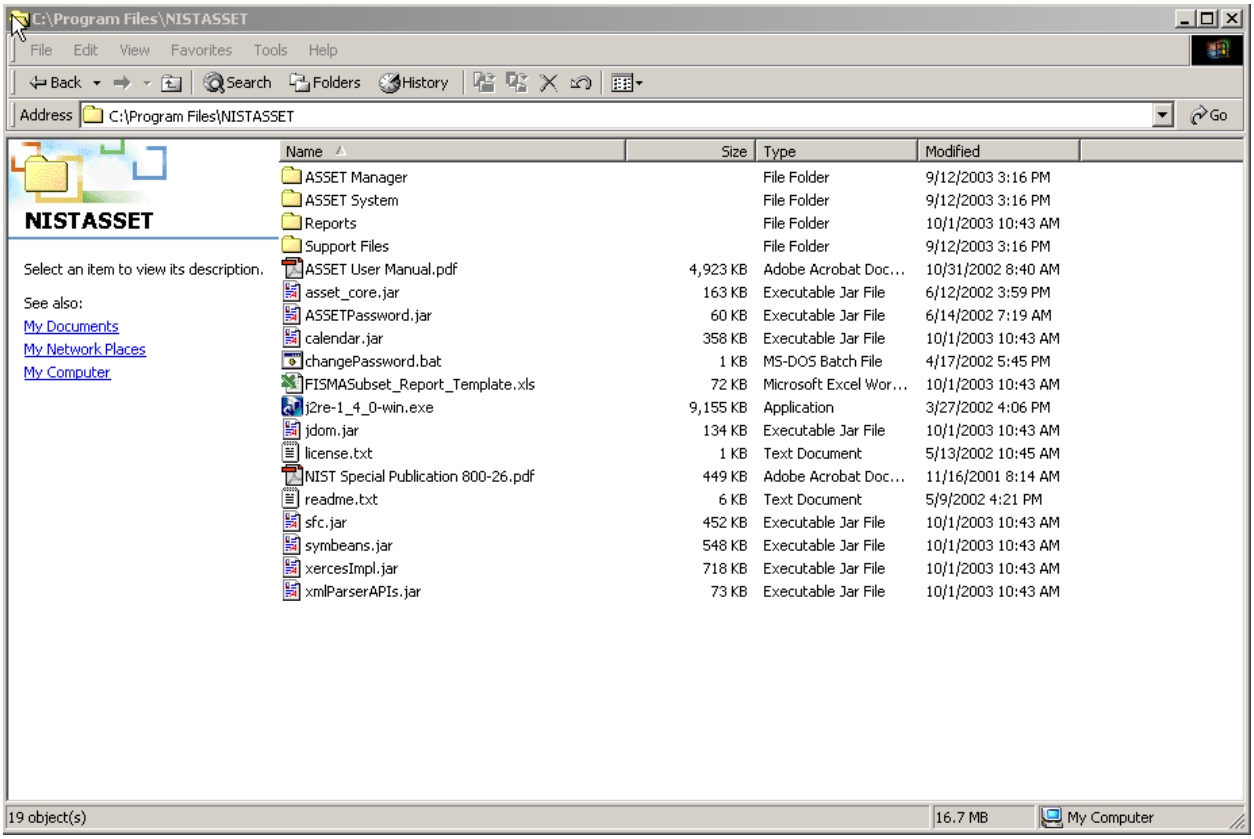


Figure F.16 – ASSET Folder Structure

To uninstall ASSET and all the components that were installed when ASSET was installed, you will need to uninstall the ASSET program files, JRE, and MSDE. Each of these uninstallation processes will need to be performed separately.

WARNING: Uninstalling ASSET will delete the database that contains your assessment data! It is important to export all your data to a backup XML file before uninstalling ASSET!

F.3 Uninstalling ASSET Program Files

The process required to uninstall ASSET is similar to the uninstall process of other Windows-based applications. Select **Settings**, then **Control Panel,** then **Add/Remove Programs**, from the **Start Menu**. Select **NISTASSET** and **Change/Remove,** then **OK**.

Figure F.17 – ASSET Confirmation Dialog Box

The uninstallation process will delete both the ASSET – System and ASSET – Manager databases. Click **OK** to close the dialog boxes.

Figure F.18 – Confirmation of ASSET – Manager Database Deletion

Figure F.19 – Confirmation of ASSET – System Database Deletion

The progress of the ASSET uninstallation will be shown in a progress window.

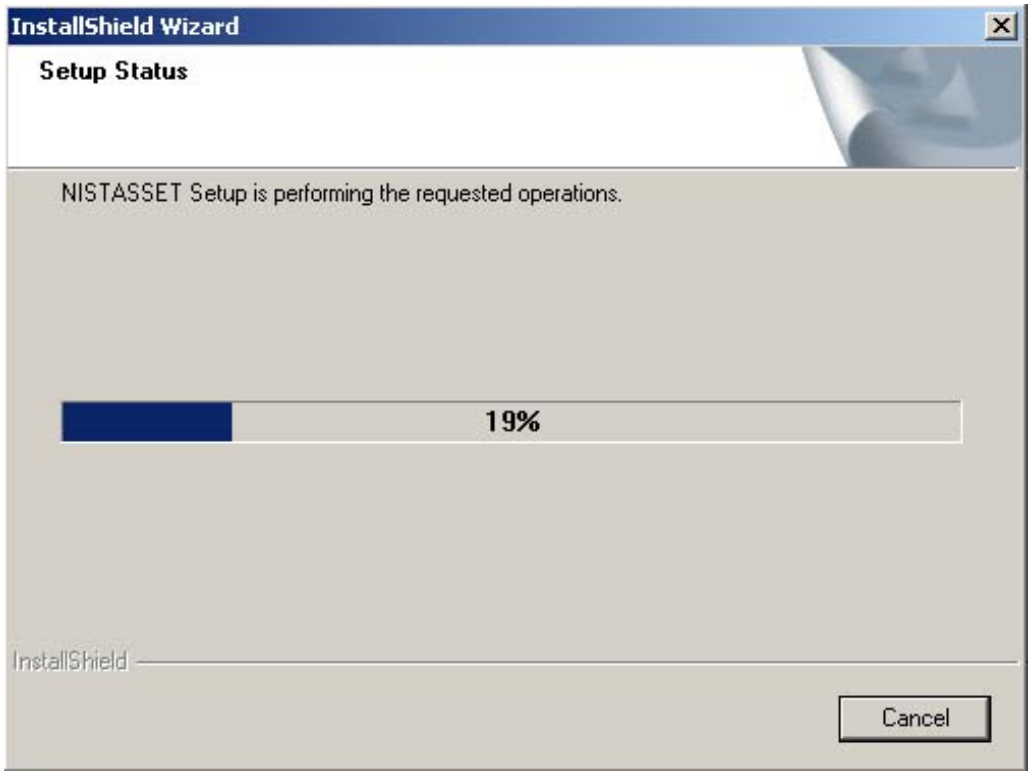


Figure F.20 – ASSET Uninstall Status Window

Once the ASSET uninstall process is complete, you will need to select **Finish**.

If files have been added to the NIST ASSET program folder, the uninstallation process will not delete this folder and any added files. This folder must then be manually deleted to complete the uninstallation process.

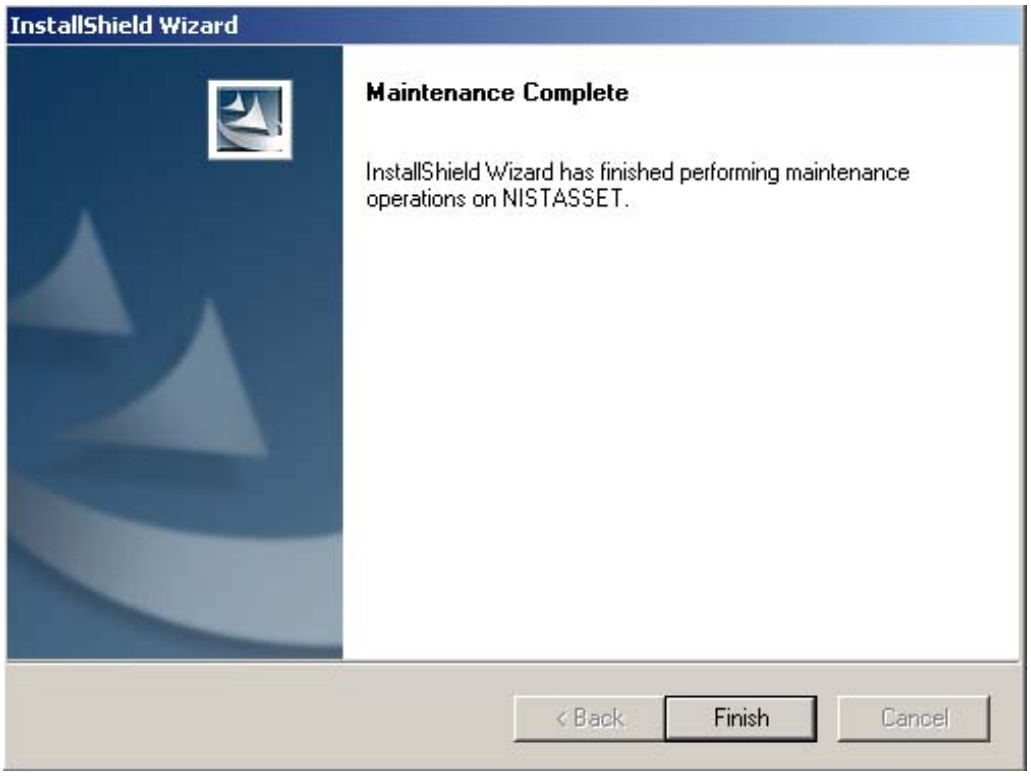


Figure F.21 – ASSET Uninstall Complete Window

Appendix G—Version 1 to 2 Upgrade Process

Once you determined whether you will use the upgrade or full installation path, there are several steps to follow to ensure a successful installation. The following two flowcharts provide a visual description of the steps involved with a full or upgrade installation.

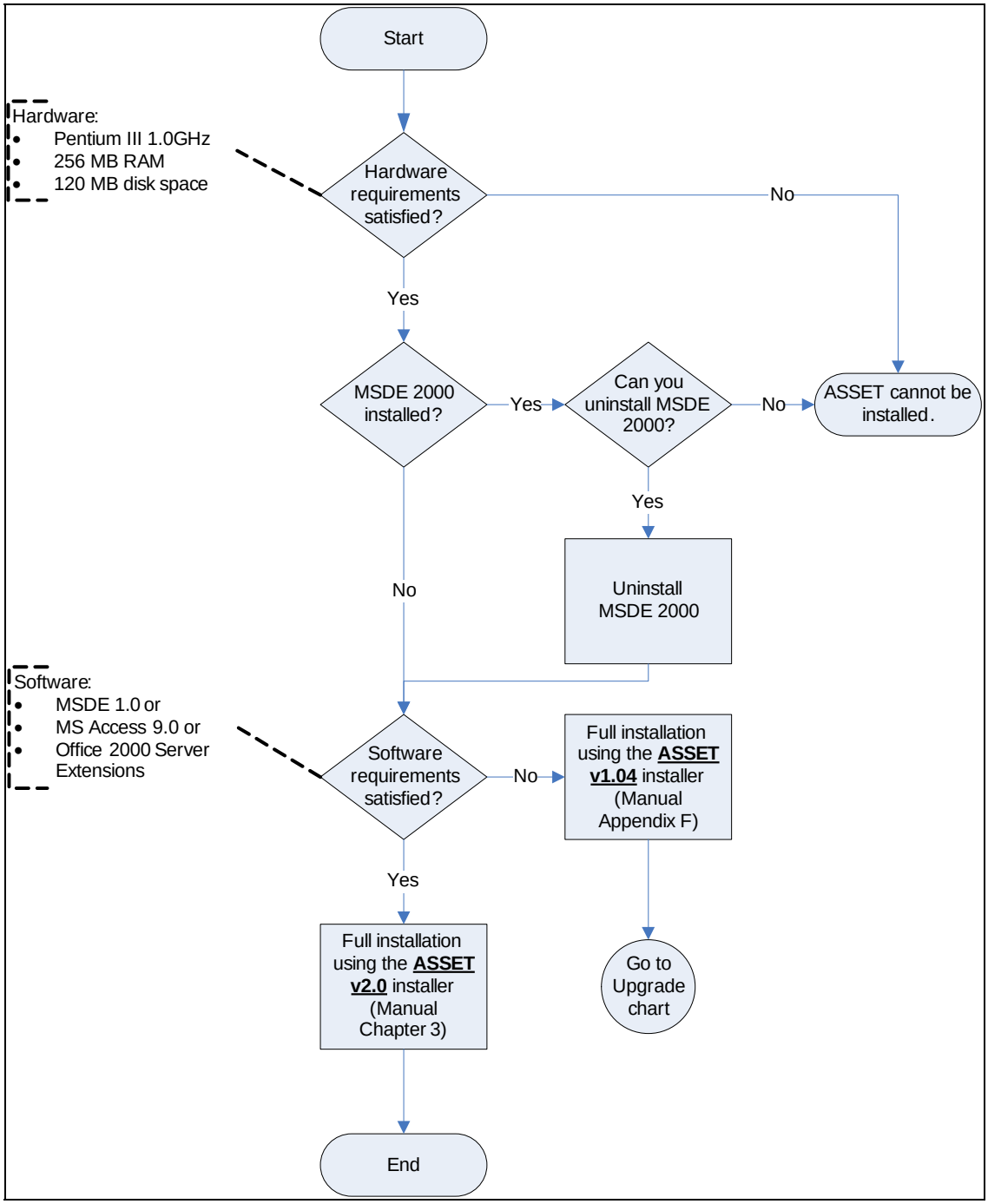


Figure G.1 – Full Installation Process

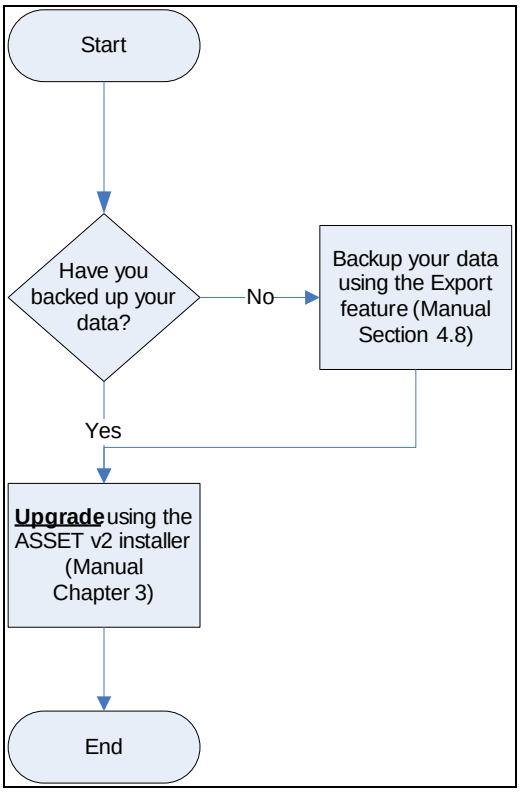


Figure G.2 – Upgrade Installation Process