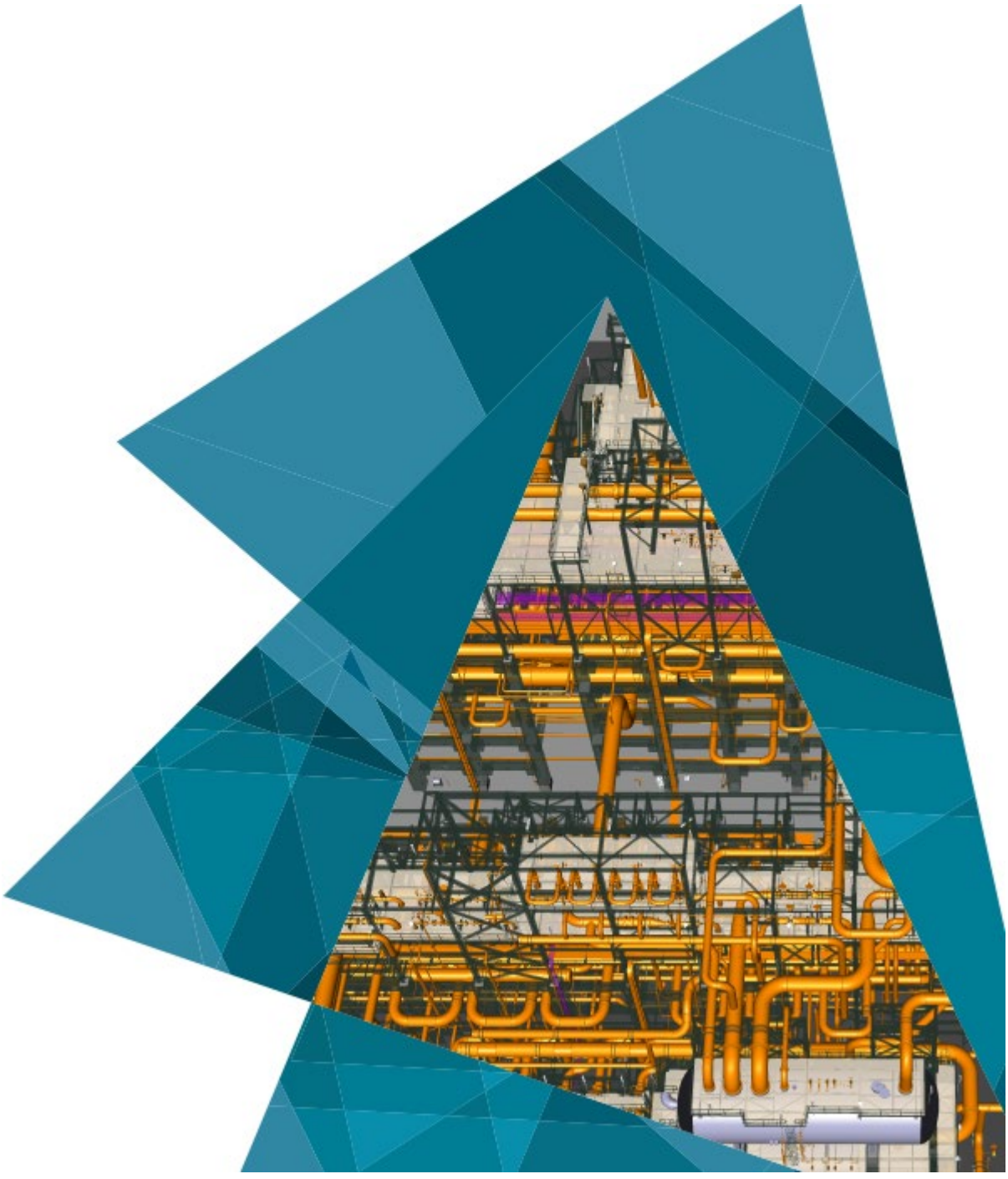
HEXAGON

DOC4000

Administration Guide

2023 (7.3)
February 2023



Contents

SECTION 1

Initial Setup

This section outlines the installation-related configuration tasks for initially setting up DOC4000. After you complete the tasks outlined in the *Installation Guide*, which includes many of the tasks in this section, you may need to perform some of these tasks again to adjust and customize your configuration. Additional configuration information for other customization tasks and capabilities is available in the remaining sections of this guide.

Admin Utility Overview

When you install DOC4000, the Admin Utility is installed on the DOC4000 server. This utility allows an administrator to perform a variety of administrative and configuration functions, such as validating the product license and defining user authentication. Run this utility only on the server where DOC4000 is installed. The left pane of the Admin Utility provides access to each configuration area. When you click a link in the left pane, that window is displayed in the right pane.

Consider the following helpful topics for using the Admin Utility:

- *Running the Admin Utility as an Administrator* (page 7)
- *Starting the Admin Utility* (page 7)
- *Clearing the IIS Cached Configuration Information* (page 7)

Running the Admin Utility as an Administrator

You need to run the DOC4000 Admin Utility as an administrator. You can add the **Run as administrator** property to the Admin Utility shortcuts in your Start menu and on your desktop.

To set the Admin Utility shortcuts to run as administrator:

1. Right-click on the Admin Utility shortcut, and then click **Properties**.
2. Click **Properties** to display the Admin Utility Properties window.
3. Click **Advanced**.
4. Select the **Run as administrator** check box.
5. Click **OK** to close the Advanced Properties window.
6. Click **Apply**, and then click **OK** to close the Admin Utility Properties window.

Starting the Admin Utility

The DOC4000 Admin Utility allows you to perform many configuration and administration tasks. Run this utility only on the server where DOC4000 is installed, and run it as an administrator. For more information, see *Running the Admin Utility as an Administrator* (page 7). The installation program creates a shortcut to this utility on the desktop.

DOC4000 supports Application authentication and Windows authentication modes. You choose which authentication mode to use when you install the product. For more information, see *Configuring User Authentication and Validation* (page 23). When you start the Admin Utility, the authentication mode determines whether you need to log in with an DOC4000 administrator account.

To start the Admin Utility:

1. Click Windows **Start > All Programs > PAS >** DOC4000.
2. Right-click **Admin Utility**, and then click **Run as administrator**.
3. If Application authentication mode is selected, you are prompted to log in. Specify your DOC4000 administrator user name and password, and then click **OK**.

Clearing the IIS Cached Configuration Information

IIS caches the DOC4000 configuration information. Some changes you make through the Admin Utility, such as adding assets, may not be available through DOC4000 until you clear the IIS cache. You can reset IIS (by running `iisreset`) to clear the cache, but this command impacts all users connected to the web server.

An administrator can use the Admin Utility to restart the DOC4000 web application without restarting IIS. This approach disconnects only DOC4000 users.

NOTE Users who are connected to the DOC4000 web application are redirected to the login page. Any unsaved data will be lost.

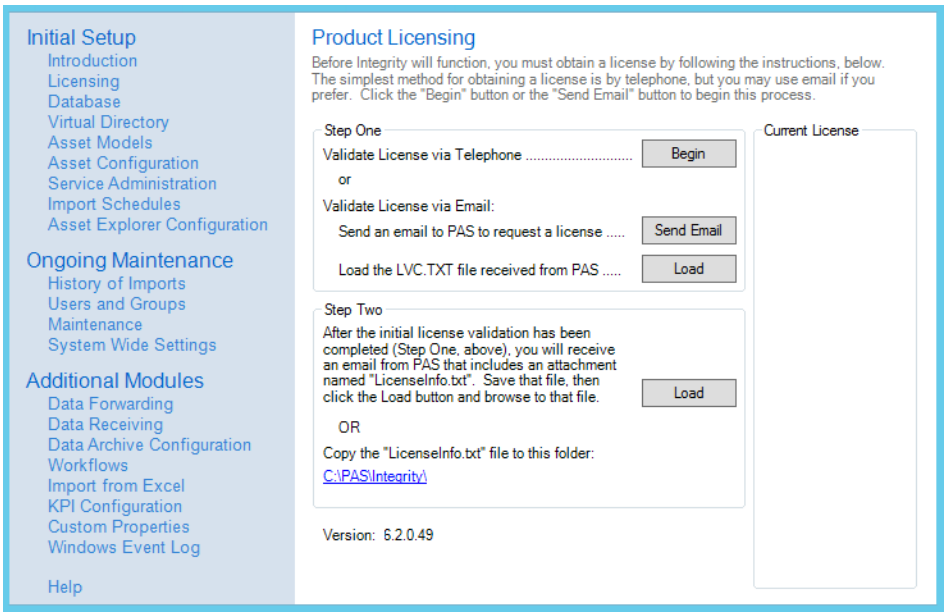
To restart the DOC4000 web application:

1. In the Admin Utility, click the **Maintenance** link.
2. In the **Web Application** section on the right, click **Restart**.

Validating Your License

Your license defines which functions are available for you and which asset models you can import and use. Once you install DOC4000, you need to validate your license.

The **Licensing** link in the Admin Utility opens the Product Licensing window. This window allows you to view your current license information and update your product license.



The Product Licensing window helps you validate your license, which you can complete by telephone or email. License validation is available 24 hours a day, seven days a week.

NOTES

- If your permanent DOC4000 license is in place, your current license information is displayed on the Product Licensing window.
- If DOC4000 is not currently licensed, you can click either **Begin** or **Send Email** to validate your license by telephone or email. For more information, see *Validating Your License by Telephone* (page 8) or *Validating Your License by Email* (page 9).

Validating Your License by Telephone

When you validate your license by telephone, you will provide a validation code to the technical support representative. Then, you will receive a permanent license file (`LicenseInfo.txt`) to add to your DOC4000 server.

To validate the license by telephone:

1. In the Admin Utility, click the **Licensing** link.

2. Click **Begin**. Several windows help you complete the temporary license process.
   a. Click **I Agree** to accept the terms of the license agreement, and click **Next** to see the telephone number to call to validate the license.
   b. Click **Next**.
   c. After reading the code to the technical support representative, type the validation code in the field provided, and click **Next**.
   d. A confirmation is displayed when a valid code has been entered.
3. In the meantime, you receive an email that includes a permanent license file called `LicenseInfo.txt`.
   a. Save the `LicenseInfo.txt` file to the folder where you installed DOC4000, `C:\Program Files (x86)\PAS\Integrity` by default.
   b. Close and reopen the Admin Utility before proceeding with DOC4000 configuration.

Validating Your License by Email

When you validate your license by email, you need to send a request for a license validation file. You will receive a reply, including two license files.

To validate the license by email:

1. In the Admin Utility, click the **Licensing** link.
2. Click **Send Email**.
3. Click **I Agree** to accept the terms of the license agreement, and click **Next** to type your **Name**, **Company Name**, **Telephone Number**, and **Comments**. Then, click **Next**.
4. You may send the email in one of two ways. Follow the directions on the **Send Email** window to either send the email automatically, or you can send the email manually.
   a. On the **Send Email** window, click **Send Now** and the default email program sends the message automatically.
   b. If you choose to send the email manually, follow the instructions for composing the email.

      NOTE You need to attach the `IID.txt` file located in the installation folder if sending manually.
5. Click **Close**.
6. Technical Support sends an email that includes the `LicenseInfo.txt` and `LVC.txt` files.
   a. Save both files in the folder where you installed DOC4000, `C:\Program Files (x86)\PAS\Integrity` by default.
   b. In the Admin Utility, click the **Licensing** link.
   c. Follow the directions in the email from PAS to load the files.
   d. Close and reopen the Admin Utility before proceeding with configuration.

Managing Your Databases

During the installation process, you configure the DOC4000 database. This section provides the initial configuration and upgrade information, as well as other options that include enabling asset roll back and using multiple databases. For more information, see the following topics:

- *Creating a Database* (page 10)
- *Changing the Configuration for an Existing Database* (page 11)
- *Understanding and Enabling Asset Roll Back* (page 12)
- *Working with Multiple Databases for Enterprise Deployments* (page 12)

DOC4000 can also use multiple *project* databases so you can segment information, if needed, for a short-term consulting project. In the Admin Utility, these databases, along with their virtual directories, are managed as *projects*. For more information, see *Working with Project Databases* (page 16).

Creating a Database

The **Database** link in the Admin Utility is used either to create a new Microsoft SQL Server database for DOC4000 or to change the configuration for an existing database. The account used to create the database (your Windows account if you choose Windows authentication or the SQL Server account you specify if you choose SQL Server authentication) must have at least the dbcreator server role on the SQL Server where the DOC4000 database will be created. For more information about service account and database permissions, see *Defining Your Service Accounts* (page 19).

To create a new database:

1. In the Admin Utility, click the **Database** link.
2. Click the **Yes** option to specify that a new database will be created.
3. If you want a location other than the default location for the database files, specify the new location in the **Location** field. The default location depends on the Microsoft SQL Server installation location.
4. In the **Database Connection** area, indicate the **Computer name** (SQL Server name) and **Database name**. If the Microsoft SQL Server installation where the DOC4000 database will be located is a named instance, type the server name followed with a backslash and the instance name in the **Computer Name** field, such as *Server**Instance*.

   The database name must begin with a letter or underscore. Database names can contain only letters, numbers, underscores, dashes, and periods. No special characters can be used.
5. In the **Authentication** area, indicate whether DOC4000 should log in to Microsoft SQL Server using your Windows account or a specified SQL Server user ID and password. If you select **SQL Server mode**, type the user ID and password defined within SQL Server.

   NOTE For either authentication mode, the user account must have the **dbcreator** (min) or **sysadmin** fixed server role and must be assigned the **db_owner** database role. Use SQL Server Management Studio to assign the **db_owner** database role to the account you specify.

6. If you want to enable DOC4000 to support a large number of users, check the **Enable SQL Server managed session state** check box in the **Additional Configuration** section. The default setting is unchecked.
7. If you want to enable import roll back, check the **Enable Asset Roll Back** check box in the **Additional Configuration** section. Then, click **Yes** on the Confirm Creating Additional Database window.

   Asset Roll Back allows administrators to roll back to a previously imported set of data in the event that the most recent import of data is old, invalid, or corrupted. For more information, see *Understanding and Enabling Asset Roll Back* (page 12).
8. Click **Save**.
9. Click **OK** on the Database Creation confirmation message window. The Database ID window is displayed.
10. If you want to use multiple databases, specify a unique ID number for the database. If this database is the only database, leave the value set to **1**, which identifies the primary database. For more information, see *Working with Multiple Databases for Enterprise Deployments* (page 12).
11. Click **OK** to close the Database ID window and create the database. When the process finishes creating the database, a confirmation message is displayed.
12. Click **OK** to close the confirmation window.
13. If a message is displayed that indicates the DOC4000 services must be restarted, complete the following steps:
    a. Click **OK** to close the restart services message window.
    b. Click the **Service Administration** link.
    c. In the **Select a Service** area, select **IntegrityDataCollector2**, and restart it.
    d. In the **Select a Service** area, select **PAS WebFileService**, and restart it.

Changing the Configuration for an Existing Database

The Admin Utility allows you to change how an existing database is configured. For example, you can enable asset roll back or managed session state.

To change the configuration for an existing database:

1. In the Admin Utility, click the **Database** link.
2. Click the **No** option to specify that an existing database should be modified.
3. In the **Database Connection** area, indicate the **Computer name** (SQL Server name) and **Database name**. If the Microsoft SQL Server installation where the DOC4000 database will be located is a named instance, type the server name followed with a backslash and the instance name in the **Computer Name** field, such as *Server**Instance*.
4. In the **Authentication** area, indicate whether DOC4000 should log in to Microsoft SQL Server using your Windows account or a specified SQL Server user ID and password. If you select **SQL Server mode**, type the user ID and password defined within SQL Server.

NOTE For either authentication mode, the user account must have the **dbcreator** (min) or **sysadmin** fixed server role and must be assigned the **db_owner** database role. Use SQL Server Management Studio to assign the **db_owner** database role to the account you specify.

5. If you want to enable DOC4000 to support a large number of users, check the **Enable SQL Server managed session state** check box in the **Additional Configuration** section. The default setting is unchecked.
6. If you want to enable import roll back, check the **Enable Asset Roll Back** check box in the **Additional Configuration** section. Then, click **Yes** on the Confirm Creating Additional Database window.

   Asset Roll Back allows administrators to roll back to a previously imported set of data in the event that the most recent import of data is old, invalid, or corrupted. For more information, see *Understanding and Enabling Asset Roll Back* (page 12).
7. Click **Save**.
8. If a message is displayed that indicates the DOC4000 services must be restarted, complete the following steps:
   a. Click **OK** to close the restart services message window.
   b. Click the **Service Administration** link.
   c. In the **Select a Service** area, select Integrity**DataCollector2**, and restart it.
   d. In the **Select a Service** area, select **PAS WebFileService**, and restart it.

Understanding and Enabling Asset Roll Back

Asset Roll Back allows administrators to roll back the data for an asset to a previously imported set of data in the event that the most recently imported data is old, invalid, or corrupted. To give administrators this capability, you need to use the Admin Utility to configure the database and check the **Enable Asset Roll Back** check box in the **Additional Configuration** section of the Configure Database Connection Parameters window. For more information, see *Changing the Configuration for an Existing Database* (page 11).

If Asset Roll Back is enabled, DOC4000 retains a maximum of three of the most recent restore points in an additional database with the **Rollback_** prefix followed by the name of the database. When you enable Asset Roll Back, the user identified through the **Authentication** section of the Configure Database Connection Parameters window must have SQL Server permissions to create the additional database.

With Asset Roll Back enabled, when you import data for an asset, DOC4000 first creates a restore point of the existing data for that asset and stores it in the roll back database. Then, the new data is imported into DOC4000. The History of Imports window in the Admin Utility allows you to view past import events and their related summary and event log information. On the History of Imports window, you can also select a restore point for an asset and roll back to that data. For more information, see *History of Data Imports* (page 42).

Working with Multiple Databases for Enterprise Deployments

Based on your deployment requirements, you can configure DOC4000 to work with multiple databases. How the databases work together depends on the type of deployment you select. For example, various levels within your organization may need to view DOC4000 information. While users at the site level are involved in day-to-day operations and change management of their local systems, the centralized engineering group may want to view consolidated information from

multiple sites. If the amount of data permits, you can use data forwarding to make the data available both at the site level and at the corporate level. For more information, see *Understanding Data Forwarding and Receiving* (page 64).

In other deployments, multiple databases allow you to segment larger amounts of data and view the consolidated data as needed. Each site can have a secondary database, and the centralized engineering group can have the primary database to view information across the databases. To use multiple databases, an administrator uses the Admin Utility to create the primary database with the database ID set to 1. Next, the administrator creates one or more additional, secondary databases with unique database IDs. Then, the administrator configures DOC4000 to recognize these databases and to coordinate data requests for assets stored in secondary databases.

To make sure the DOC4000 services and utilities work properly with multiple databases, the pasIntegrityDB and IntegrityDataCollector2 services on the DOC4000 server for the primary database need to run using a domain account. This domain account allows the pasIntegrityDB service to see the assets in the secondary databases for multiple database services to perform correctly. You also need to modify the `.config` file for DOC4000 and each utility to identify the domain account you set up for the services to use. For more information, see *Defining Your Service Accounts* (page 19).

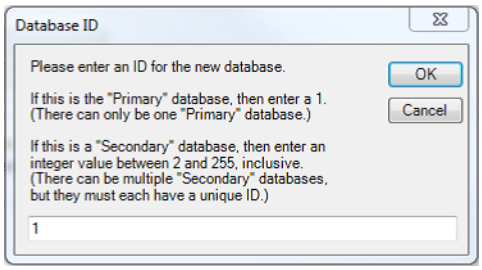
When you use multiple databases, some features may require additional configuration and considerations for the primary database. For more information, see Configuring Baselines with Multiple Databases.

NOTES

- If the password for the service account is changed in the future, you must also change the service configuration or the service will no longer work.
- The names of the assets across all databases must be unique.

To configure multiple databases:

1. Create one primary database using the Admin Utility and set the database ID to **1**. Only one primary database can exist. For more information, see *Creating a Database* (page 10).



2. Create one or more secondary databases using the Admin Utility and set the database ID for each secondary database to a value other than **1**. For a secondary database, the database ID can be an integer value between 2 and 255, and the database ID must be unique.
3. On the DOC4000 server for the primary database, which will be the web server, open the DOC4000`MOCRoot.XML` file in the folder where you installed DOC4000, `C:\Program Files (x86)\PAS\`**Integrity** by default.

4. Copy the `<IMOCConnStr>` line, and then paste and rename the line as `<MainDB>`, and shown in the following image.

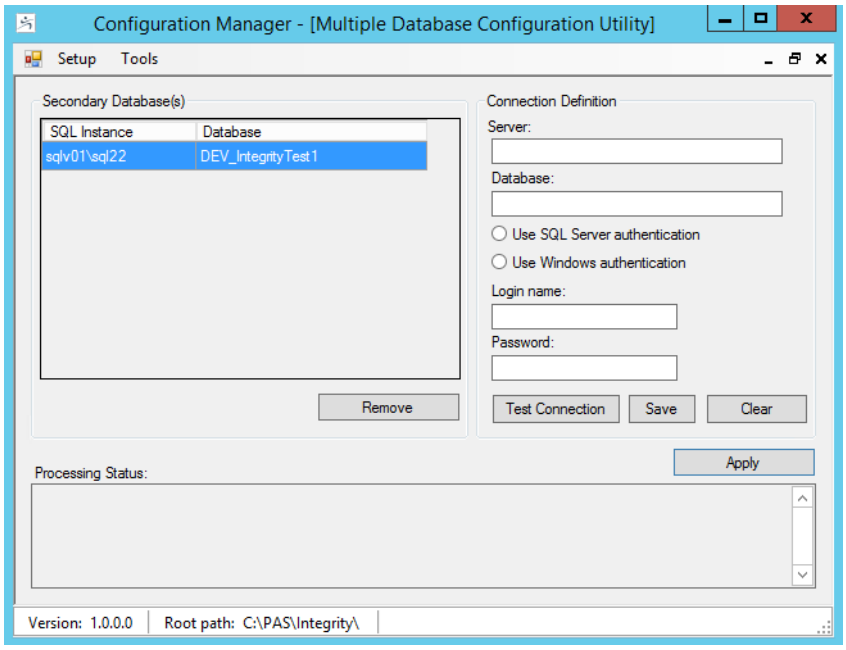
```
<?xml version="1.0" encoding="utf-16"?>
<IntegrityMOC>
  <IMOCConnStr>QiFsD5wLIZU4jMv8qjA7raD==</IMOCConnStr>
  <MainDB>QiFsD5wLIZU4jMv8qjA7raD==</MainDB>
  <IMOCAuthType>Windows</IMOCAuthType>
  <IMOCNoUserValidation>False</IMOCNoUserValidation>
```

5. In each secondary database, import the needed asset models and create the assets for that database using unique names across all databases. Then, import the data for each asset in each database.

6. Open Configuration Manager on the DOC4000 server for the primary database. To open Configuration Manager, run the following file:

   InstallPath`\DataCollector\ConfigurationManager.exe`

7. Click **Tools > Multiple Database Configuration**.



8. For each of the secondary databases, complete the following steps:

   a. Type the connection information for the secondary database, including server name, database name, authentication type, and login credentials.

   b. Click **Test Connection** to make sure the connection information is correct.

   c. Click **Save**.

9. Click **Apply**. Then, click **OK**. DOC4000 adds the data owners from the secondary databases to the primary database data owner table.

10. Close Configuration Manager.

11. Identify a domain account to use for the **pas**IntegrityD**B** service, IntegrityDataCollector2 service, and the DOC4000 configuration utilities. For more information, see *Defining Your Service Accounts* (page 19).
12. On the DOC4000 server for the primary database, configure the services to use the identified domain account by completing the following steps:
    a. Click Windows **Start > Run**.
    b. Type `services.msc`, and then click **OK**.
    c. Right-click the **pasIntegrityDB** service, and then click **Properties**.
    d. Click the **Log On** tab, and then select the **This account** option. Type the domain account user name and password.

       NOTE If the password for this account is changed in the future, you must also change this specified value or the service will no longer work.

    e. Click **Apply**, and then click **OK**.
    f. If the service is not running, click **Start the service**.
    g. Repeat these steps (a-f) for the **IntegrityDataCollector2** service.
13. Verify the **pasIntegrityDB** service has started correctly and is running by completing the following steps:
    a. Open the *InstallPath*`\DataCollector\pasIntegrityDB.txt` file, where *InstallPath* is the folder where you installed DOC4000.

       NOTE If the `pas`IntegrityD`B.txt` file does not exist, the service never started.

    b. Verify no major errors exist.
14. On the DOC4000 server for the primary database, specify the identified domain user account in the `.config` files for DOC4000 and its configuration utilities by completing the following steps:
    a. Use Notepad to edit the following files:
       - *InstallPath*`\web.config`
       - *InstallPath*`\DataCollector\AdminUtility.exe.config`
       - *InstallPath*`\DataCollector\AMDK.exe.config`
       - *InstallPath*`\DataCollector\AssetModelBuilder.exe.config`
       - *InstallPath*`\DataCollector\IDC.exe.config`
       - *InstallPath*`\DataCollector\IntegrityDataCollector2.exe.config`
       - *InstallPath*`\DataCollector\WFSAlerts.exe.config`

a. Find the `<userPrincipalName value="`*domain*`\`*username*`" />` tag in each file.

```
      </netNamedPipeBinding>
    </bindings>
    <client>
      <endpoint address="net.pipe://localhost/" binding="netNamedPipeBinding" bindingConfigurat
        <identity>
          <userPrincipalName value="domainname\username" />
        </identity>
      </endpoint>
    </client>
  </system.serviceModel>
</configuration>
```

b. Change *domain* to the domain name of the primary DOC4000 server and change *username* to the domain account name associated with the **pasIntegrityDB** and **IntegrityDataCollector2** services.

c. Save the files, and then close Notepad.

15. Open Configuration Manager on the DOC4000 server for the primary database. To open Configuration Manager, run the following file:

    InstallPath`\DataCollector\ConfigurationManager.exe`

16. Build the asset hierarchy so you can manage assets from secondary databases. You can drag and drop assets to **Asset Explorer** to define the hierarchy for Asset Explorer in the DOC4000 web interface, or you can use Microsoft Excel to specify your asset hierarchy, and then copy and paste that data to the object grid. For more information about defining your asset hierarchy, see Understanding and Defining Your Asset Hierarchy.

NOTES

- When using multiple databases, use Configuration Manager instead of the Admin Utility to define the asset hierarchy. Since the Admin Utility focuses on one database, the Asset Explorer Configuration window can be missing assets when using multiple databases. If you select **Asset Explorer Configuration** in the Admin Utility, your asset hierarchy may need to be rebuilt using Configuration Manager.
- Certain core asset models need to be imported into specific databases to function correctly. For example, the Baselines asset model should be imported into the primary database. For more information, see Configuring Baselines with Multiple Databases.
- The source asset models, such as PAS Recon or Honeywell EPKS, should be imported into the appropriate secondary databases, where needed. For more information, see the *Implementation Guide* for each source asset type.

Working with Project Databases

The Admin Utility typically works with a single database for DOC4000. However, based on licensing, you can configure the Admin Utility to work with multiple *project* databases.

You can use *projects* to configure and maintain multiple databases and associated web applications, such as for segmenting information for a short-term consulting project. In the Admin Utility, these databases, and their virtual directories, are managed as *projects*.

When your license supports projects, the **Maintain Projects** link is available in the **Additional Modules** section of the Admin Utility. For more information, see the following topics:

- *Creating a Database* (page 10)

Admin Utility Differences When Using Multiple Project Databases

In project mode, all links on the Admin Utility window work the same as described *except* the following links:

- **Database** - When working with multiple project databases, database names must begin with a letter or underscore, and they can contain only letters, numbers, underscores, and periods. No special characters or dashes can be used. Spaces in database names are replaced with underscores. For example, if you type `Production Database` for the database name, the created database is named `Production_Database`.

  NOTE When you change from one database to another, you need to stop and restart the **PAS WebFileService** service.

- **Virtual Directory** - When working with multiple project databases, the virtual directory names for the DOC4000 web interface match the database names and cannot be edited. The fields on this window are disabled.
- **Import Asset Models** - When you select an asset model to load (import) and click the **Import** button, DOC4000 loads the asset model into all projects.
- **Maintain Projects** - In project mode, this additional link is available in the Admin Utility. Click this link to view and maintain all projects in DOC4000.

In addition, users can connect only to existing databases (not create them), so the link called **Database** for an administrator is called **Configure Database** for users. After an administrator creates a database (project), the user can connect to the project by clicking the **Configure Database** link, and then manage the assets within the project.

Deleting a Project in Multiple Database Mode

As an administrator, the Project Maintenance window in the Admin Utility allows you to delete projects, databases, and virtual directories. If you have only a single project, you cannot delete it and the **Delete** button is not available.

You cannot delete a database and project you are connected to. Use the **Database** link in the **Initial Setup** section of the Admin Utility to change to a different database, if needed.

To delete a project, database, or virtual directory:

1. In the Admin Utility, click the **Maintain Projects** link to open the Project Maintenance window. This link is not available unless you are licensed for multiple project databases.
2. In the **Projects** table, click the project to delete.
3. If you want to delete the database as well as the project, check the **Delete database** check box.
4. If you want to delete the virtual directory for the project, as well as the project, check the **Delete virtual directory** check box. If a virtual directory has not been created for a database, the **Virtual Directory** field in the **Projects** table is set to **None** and the **Delete virtual directory** check box is not available.

NOTE If you delete a project, but you do not delete the database and virtual directory for it, the project entry is no longer available on the Project Maintenance window. However, the database and virtual directory still exists. If this situation occurs, you can manually delete the database and virtual directory using Microsoft SQL Server and IIS.

5. Click **Delete**.
6. Click **OK**.

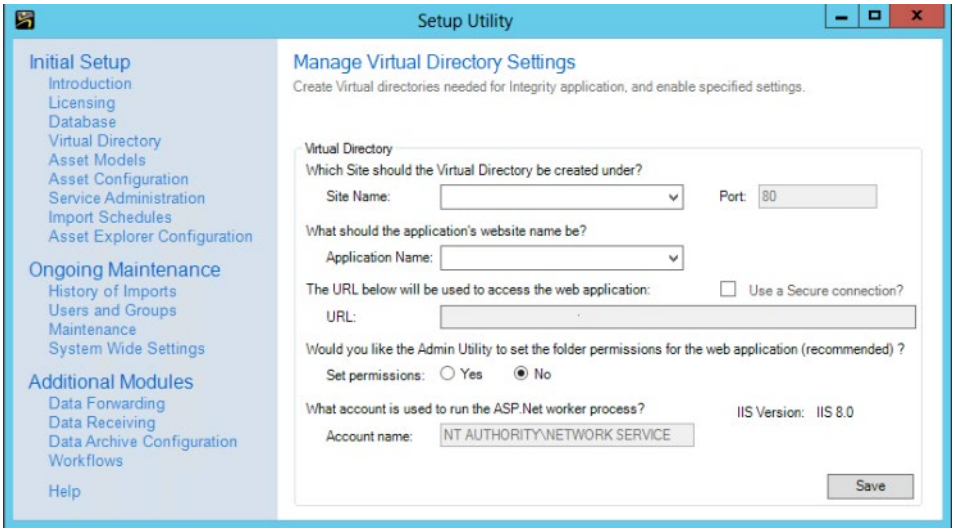
Defining the Web Application (DOC4000 Web Interface)

The **Virtual Directory** link in the Admin Utility is used to configure several options including the virtual directory for the DOC4000 web interface. The Admin Utility also allows you to restart the DOC4000 services and define trusted domain credentials. For more information about managing the web application, see the following topics:

- *Configuring the Web Application* (page 18)
- *Restarting the Web Application* (page 19)
- *Integrating the PAS Dashboard* (page 53)
- *Using the DOC4000 Maintenance Features* (page 50)

Configuring the Web Application

When you click the **Virtual Directory** link in the Admin Utility, the Manage Virtual Directory Settings window displays. This window allows you to configure the virtual directory, folder permissions, and more for the DOC4000 web interface.



To configure the web application:

1. In the Admin Utility, click the **Virtual Directory** link.

2. Use the **Site Name** and **Port** fields to select a site and port for the DOC4000 web interface, or use the default web site and port 80.
3. In the **Application Name** field, type the name for the virtual directory to be used by IIS for user access to DOC4000. This field defaults to the database name (DOC4000). If DOC4000 is in multiple database mode, this field is unavailable and it must match the database name.
4. If you want to use a secure connection (HTTPS), check the **Use a Secure connection** check box and make sure IIS is set up for https support.
5. Note the URL for users to access DOC4000. The URL is the server name and the virtual directory name, such as `http://`*Server*/*VirtualDirectory*.
6. Click **Yes** for the **Set permissions** option to grant the permissions necessary for the ASP.NET account to access the virtual directory.

   For DOC4000 to run properly, permissions must be granted to the virtual directory for the account under which IIS runs. This account is referred to as the ASP.NET worker process account. The name of the account used for running IIS must be entered into the ASP.NET worker process **Account name** field on the Manage Virtual Directory Settings window. If you select **No** for the **Set permissions** option, you need to manually set the directory permissions appropriately.

   If your company security policies require that these accounts provided by the .NET Framework be disabled or deleted, you need to create another system account that has the following permissions:

   - Read and Write permission on the DOC4000 application (DOC4000) folder.
   - Read and Write permissions on the `Reports` folder on the same level as the DOC4000 application folder. The `Reports` folder does not exist until a report is run from the DOC4000 web interface.
7. Click **Save**.

Restarting the Web Application

The administrator can click the **Restart** button on the Maintenance window to restart the web application. This capability can help you resolve a program fault, slow server performance, or entry errors.

NOTE Before you click **Restart**, make sure users are logged off. DOC4000 web interface users will be redirected to the login page. *Any unsaved data will be lost*.

To restart the DOC4000 web application:

1. In the Admin Utility, click the **Maintenance** link.
2. In the **Web Application** section on the right, click **Restart**.

Defining Your Service Accounts

DOC4000 uses several services to provide various features. The **Service Administration** link in the Admin Utility displays the Configure the Services window. This window allows you to start and stop each service. You can also specify the account user name and password for each service to use. These services should run under valid domain accounts, and the permissions required for

these accounts depend on whether you chose to use **Windows authentication mode** or **SQL Server mode** to access the DOC4000 database:

IntegrityDataCollector2

Provides data import and management capabilities. This service must run on each DOC4000 data collector or server where asset data is imported. The account you specify for this service must have access to the data to be imported into DOC4000. This data can reside in files, folders, or databases, and can be located on computers other than the DOC4000 server or data collector. Because this service can run only as a single account, the various data locations must be configured to allow read access to this account.

By default, this service runs under the SYSTEM account. If the DOC4000 data files, the DOC4000 database, and the DOC4000 server are all on the same server, and the service is running under Local System, you do not need to specify an account for this service on this window.

If the DOC4000 database is on a separate server and you chose **Windows authentication mode**, this service account must have the db_owner role on each primary and secondary database. When using multiple databases, if a secondary database is on a separate server from the primary database, this service account must also have the setupadmin role on the primary database to create a database link.

pasIntegrityDB

Provides data management for multiple database deployments. This service is not needed for single database deployments. When using multiple databases, this service must run on the DOC4000 server for the primary database. The account you specify for this service must be a valid domain account. In addition, you need to specify this account in the *InstallPath*`\DataCollector\*.exe.config` files on the DOC4000 server for the primary database.

PAS WebFileService

Provides features for the DOC4000 web interface, such as email notifications and reporting capabilities. This service must run on the DOC4000 server that provides the DOC4000 web interface. Depending on your site security, the account you specify for this service could be a local user account or a domain user account and have read and write permissions to the folder where you installed DOC4000 and its subfolders. If you have specified a local user account and experience issues, specify a domain user account. For email notifications, this service uses the settings specified through **Maintenance > Configure Email Settings** in the Admin Utility.

pasWindowsEventLog

Provides Windows event log data processing and management. This service must run on each DOC4000 data collector or server where Windows event data is imported. The account you specify for this service must have read permissions to the folder where you installed DOC4000. This account must also have read and write permissions to the folder and subfolders where event log data to import is stored. DOC4000 stores Windows event log data in a separate database named PASWindowsEventLogs.

If you collect Windows event log data, the account used to connect to the database (SQL login for **SQL Server mode** or the pasWindowsEventLog service account for **Windows authentication mode**) must have the following roles:

- dbcreator and serveradmin server roles

- If you chose Windows authentication mode, the pasWindowsEventLog service account must also have the db_owner role for the SQL Server where the DOC4000 database is stored and the db_datareader role for the DOC4000 database.

If you collect Windows event log data and if you chose **Windows authentication mode**, the administrator who uses the Admin Utility to create the Windows event log collection database must have at least the dbcreator role on the SQL Server where the DOC4000 database is stored.

PAS Integrity Scheduler

Provides features for the DOC4000 web interface, such as email notifications and scheduled tasks. This service is required if you want to apply normalization rules as you modify or add them and to perform risk analysis activities. The first time you run the service, DOC4000 creates a new database (PASScheduler) on the DOC4000 data collector server.

Ensure that the PAS Integrity Scheduler service is running on the DOC4000 web server (the IIS server hosting the DOC4000 web interface). If the connection to the DOC4000 database is using **Windows authentication mode**, the PAS Integrity Scheduler service needs to run as a domain account that has db_creator on the server and datareader on the DOC4000 database. If the connection to the DOC4000 database is using **SQL Server mode** for login authentication, the SQL Server login account used for the web interface needs the db_creator server role on the SQL Server instance.

PAS Integrity Integration

Provides features for the DOC4000 web interface, such as integrations with third-party applications. This service must run on the DOC4000 server that provides the DOC4000 web interface.

Review the following additional considerations for the account you specify for each service to use and related Windows accounts:

- If the DOC4000 database uses Windows authentication, these services can run as Local System only if the DOC4000 data files, the DOC4000 database, and the DOC4000 server are all on the same server.
- If the DOC4000 database uses Windows authentication, some of these services need to use accounts that have permissions to access the SQL Server database.
- For each account you specify, if the password for that account is changed, you must also change the password through the **Service Administration** link in the Admin Utility or through the service configuration itself.
- By default, SQL Server uses the NETWORK SERVICE Windows account for many functions. Set the NT AUTHORITY/NETWORK SERVICE Windows account to have permissions to the DOC4000 database.
- Maintenance jobs require the SQL Server agent service to be active and running under a Windows account that has permissions to the DOC4000 database. Set the SQL Server agent service to run under the NT AUTHORITY/NETWORK SERVICE Windows account and to start automatically.

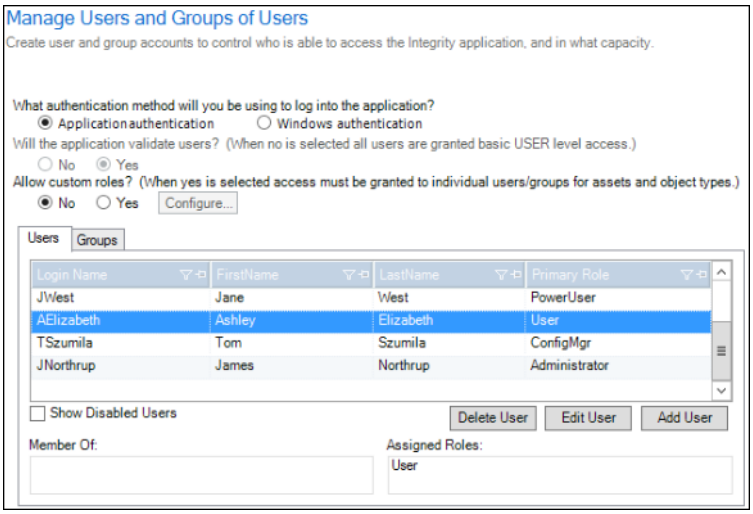
To specify the service accounts:

1. In the Admin Utility, click the **Service Administration** link.
2. In the **Service name** field, select the service to configure.

3. Type the user name and password for an account that has the required permissions for the service. Click **Get Accounts** to view all accounts on the server.
4. To preface the account name with the domain name and backslash, check the **Add Domain to Username** check box.
5. Click **Save**.

Configuring Users and Groups

The **Users and Groups** link in the Admin Utility allows you to specify the authentication method used for accessing the Admin Utility and the DOC4000 web interface. You can also define the users and groups, and create custom roles if needed.



DOC4000 provides access control using the following definitions:

Sets of tasks that can be performed

DOC4000 provides built-in roles that allow users with those roles to perform the tasks associated with those roles. For example, a user with the Administrator role can perform all tasks in the Admin Utility and in the DOC4000 web interface. However, a user with the PowerUser role has a more limited set of tasks available. For more information, see *Understanding Built-In Primary Roles* (page 24).

Sets of assets that can be accessed

DOC4000 allows you to define sets of assets using custom roles. Then, if you assign a custom role to a user, that user has access to only that set of assets. The type of access is defined by the built-in role assigned to the user for that set of assets. However, if you choose to use custom roles, you need to define sets of assets for all users and groups.

> You can also use Configuration Manager to define your asset hierarchy and then give access to assets using the hierarchy. For more information about defining your asset hierarchy and using it to delegate access, see Assigning Roles and Access through the Asset Hierarchy.

DOC4000 provides the flexibility you need to grant or deny individual users or groups of users access to sensitive areas. With the combination of built-in roles, custom roles, and asset hierarchy, you can limit which tasks a user can perform on sets of assets you define.

Consider the following topics for more information about managing users and groups and delegating permissions for sets of assets:

Configuring User Authentication and Validation

In most cases, you should use Windows authentication. This authentication method allows you to rely on Windows users and groups, which can simplify user and group management. A number of features in DOC4000 allow you to assign work to users, such as workflow cases and punch lists. These features are easier to manage with Windows users and groups. In addition, other features like baselines and vulnerability management use the workflow support.

To configure user authentication and validation:

1. In the Admin Utility, click the **Users and Groups** link.
2. Select the authentication method:
   - **Application authentication**: When users open the DOC4000 web interface or the Admin Utility, they are prompted to log in with a user ID and password defined in the Admin Utility. If you select this option, an administrator must define every user account in this window. If you want to run DOC4000 remotely without Active Directory available for authentication, select this option.

     NOTE If you integrate the PAS Dashboard with the DOC4000 web interface, the PAS Dashboard also uses Windows pass-through authentication when displaying non-precalculated data. For more information, see the *PAS Dashboard User Guide*.
   - **Windows authentication**: When a user opens the DOC4000 web interface or the Admin Utility, the current Windows user account determines whether the user is authorized. This method allows you to use Windows users and groups to assign roles in DOC4000 and it simplifies user management. Several features, such as Document Manager and workflows, require or work best with Windows authentication. For more information, see *Understanding Active Directory Integration* (page 24).
3. If you chose to use Windows authentication, select whether to validate users (**Will the application validate users?**):
   - **Yes**: Requires you to add one or more Windows users or groups in DOC4000, and assign a role to each user or group who should have DOC4000 access. If you select **Yes**, users who do not have defined roles cannot access DOC4000.

- **No**: Allows all Windows users to access DOC4000 automatically without adding Windows groups and their members. If you select **No**, all users who are not defined as administrators have the permissions associated with the User role.

NOTE Make sure you have at least one user defined as an administrator before you close the Admin Utility.

Understanding Active Directory Integration

Windows authentication allows you to use Windows users and groups to assign roles in DOC4000 and it simplifies user management. Several features, such as workflows, punch lists, and Document Manager, require or work best with this user authentication method.

If you have a large number of users and groups, or if remote access to the Active Directory causes performance delays, DOC4000 provides a utility to allow you to collect and store user and group membership information. If you choose to use this utility, you should use Windows Task Scheduler to run this utility each night to get the latest changes from the Active Directory. If you want changes in the Active Directory to be available before the scheduled run, you can manually run this utility.

The DOC4000`ADUserTool.exe` utility in the *InstallPath*`/DataCollector` folder allows you to synchronize this information and uses the following syntax:

`DOC4000ADUserTool.exe` *`updateDB updateCases`*

The options are defined as follows:

- *updateDB* specifies whether to update the member list of each group saved in DOC4000. You can specify `true` or `false` for this option.
- *updateCases* specifies whether to update cases to reflect changed group members. When this option is `true`, the utility updates the cases with the current approvers. You can specify `true` or `false` for this option.

Understanding Built-In Primary Roles

The primary role for a user defines the tasks the user can perform on the assets to which the user has access. Typically, an administrator assigns roles when creating a new user or group. The following table summarizes the built-in primary roles.

Role	Permissions
User	Can perform read-only operations and many common tasks. Cannot suppress vulnerabilities, edit or delete public notes, or delete punch lists and punch list items.
PowerUser	Can perform read and write operations the user cannot, but cannot perform administrative operations such as adding or editing user groups and accounts.
ConfigMgr	Can perform all operations a PowerUser can, as well as several configuration tasks. Can view history, view maintenance function, configure workflows and custom properties, and define additional vulnerability matching rules. Cannot add databases or users.

Role	Permissions
Administrator	Can perform all operations.

Creating Custom Roles

Custom roles allow an administrator to define sets of assets. Then, when you assign a primary role to a user, which specifies the tasks the user can perform, you can also select custom roles to allow or deny access to specific assets.

NOTES

- If you choose to use custom roles, be sure to create at least one with all assets and use it to give access to those assets to users with the User, PowerUser, or ConfigMgr role. Otherwise, users will not have access to any assets. Administrators have access to all assets regardless of custom roles and the asset hierarchy.
- If a user is assigned more than one custom role with opposing access permissions for a specific asset, the **Deny** access permission applies. This access can be allowed or denied through custom roles or through the asset hierarchy defined in Configuration Manager. For example, a user is a member of GroupA and GroupB. GroupA has **Allow** access for AssetA. GroupB has **Deny** access for AssetA. In this example, the user does *not* have access to AssetA.

To add a custom role:

1. In the Admin Utility, click the **Users and Groups** link.
2. For **Allow custom roles**, click **Yes**.
3. Click **Configure**.
4. On the Custom Role Settings window, click **New**.
5. In the **Role** field, type a name for the custom role, and then click **OK**.

   The **Asset Permissions** area identifies the specific assets users of this role can access. By default, each custom role has **Deny** permissions for all assets.
6. If you want to grant users of this role access to only a limited set of assets, complete the following steps for each asset:
   a. In the **Asset** field, select a single, specific asset.
   b. In the **Access** field, click **Allow**.
   c. Click **Add**.
7. If you want to grant users of this role access to ALL EXCEPT a limited set of assets, complete the following steps:
   a. In the **Asset** field, select **<All Assets>**.
   b. In the **Access** field, click **Allow**.
   c. Click **Add**.

d. For each asset you want to deny access, select the asset in the **Asset** field, select **Deny** in the **Access** field, and click **Add**.

8. Click **Save**.
9. Click **Close** to close the Custom Role Settings window.

Creating Groups

Administrators can create multiple groups and assign users or groups of users to them. These assigned users assume any additional permissions associated with the group. For example, if a user is assigned to the User role through his or her user account, but the user is also a member of a group with the PowerUser role, the user has the permissions associated with the PowerUser role.

To create a group:

1. In the Admin Utility, click the **Users and Groups** link.
2. Click on the **Groups** tab.
3. Click **Add Group**.
4. Type a name for the group, and click **OK**.
5. If you want to disable this group, check **Disable Group**.
6. To select the role for this group, complete the following steps:
   a. Click **Choose Roles**.
   b. In the **Select Primary Role** field, select one of the roles for this group.
   c. If you want to assign one or more custom roles to this group, select those roles in the **All Custom Roles** list, and then click the right arrow (**>**). Custom roles allow you to limit permissions to a set of assets defined by the custom role. For more information, see *Creating Custom Roles* (page 25).
   d. Click **OK**.
7. If you want to add existing users defined in DOC4000, complete the following steps:
   a. Click **Choose Users**.
   b. In the **All Users** list, select the DOC4000 users to include, and then click the right arrow (**>**) to add them to the **Group Members** list.

      NOTE After saving the group, you can create users, and then edit the group to assign users to it.

   c. Click **OK**.
8. If you want to add Windows groups or users, complete the following steps:
   a. Click **Choose Windows Groups**.
   b. In **Select Computer/Domain**, select the computer or domain, and then click **Go** to display a list of Windows groups available for the selected computer or domain.
   c. In the **Windows groups** list, select the Windows groups to include, and then click the right arrow (**>**) to add them to the **Selected groups** list.

d. If you want to add an individual Windows user account, type the user name, prefixed by the domain, in the **Type Group Name** field (*domain\user*), and then click **Add**. This account must be a domain user account, not a local machine user account.

e. When all desired Windows groups and users are in the **Selected groups** list, click **OK**.

9. Click **Save**.

Creating Users

If **Application Authentication** was selected during installation, an administrator should create multiple user accounts for DOC4000 access. Users are required to type the user name and specified password on the Login window when they open the DOC4000 web interface or the Admin Utility. The administrator also needs to specify a valid email address for each user to support features that can be assigned to users, such as workflow cases and punch lists.

To create a user account:

1. In the Admin Utility, click the **Users and Groups** link.
2. Click on the **Users** tab.
3. Click **Add User**.
4. Type a login name for the user. Login names must begin with one alphabetic character followed by additional alphabetic and/or numeric characters. Some special characters, such as hyphen (-) and underscore (_), are permitted. Login names are not case sensitive.
5. Edit the following information as needed for the user:
   - **Disable user**: Allows you to disable and re-enable the defined user.
   - **Rating weight**: Specifies the rating for documents imported with Document Manager. The default value is **1**. If applicable, you can increase this value to increase the effective influence of document ratings for this user.
   - **First name**: Specifies the first name for the user.
   - **Last name**: Specifies the last name for the user.
   - **Email address**: Specifies the email address to associate with the user.
   - **Roles**: Specifies the primary role for this user. To change the primary role, and select custom roles if needed, click **Choose Roles**.
   - **Account Locked**: Allows you to lock and unlock the defined user.

1. To set the password for the user, complete the following steps:
   a. Click **Set Password**.
   b. Type the case-sensitive password. A password can contain alphabetic and numeric characters, it must be a minimum of six characters, and it cannot be blank.
   c. If you want the user to be able to change his or her password, check the **Allow user to change password** check box.
   d. Click **OK**.
2. Click **Save**.

Changing and Resetting User Passwords

If **Application Authentication** was selected during installation, an administrator needs to create users for DOC4000 access. By default, a new user password is set to password. After you add users, they should log in to DOC4000 and change their password.

NOTE Passwords can contain alphabetic and numeric characters and must be a minimum of six characters. Passwords are case sensitive and cannot be blank.

Users can change their password by clicking the **Change Password** icon in the upper right of the DOC4000 web interface.

For more information, see the DOC4000 *User Guide*.

Administrators can use the Admin Utility to reset a user's password. An administrator can also prevent a user from changing his or her password.

To reset a password for a user:

1. In the Admin Utility, click the **Users and Groups** link.
2. Click on the **Users** tab.
3. Select the desired user.
4. Click **Edit User**.
5. Click **Set Password**.
6. In the **New password** field on the **Set New Password** window, type the new case-sensitive password, with 6-10 alphanumeric characters.
7. If you want to prevent the user from changing his or her password, clear the **Allow user to change password** check box.
8. Click **OK**.
9. If the user account is locked, clear the **Account Locked** check box.
10. Click **Save**.

Unlocking a Locked User Account

If DOC4000 is configured to use **Application Authentication**, administrators can unlock user accounts that are locked. If a user types the wrong password five times, their DOC4000 account is locked for security purposes.

To unlock a locked DOC4000 user account:

1. In the Admin Utility, click the **Users and Groups** link.
2. Click on the **Users** tab.
3. Select the desired user.
4. Click **Edit User**.
5. Clear the **Account Locked** check box.
6. Click **Save**.

Disabling and Re-enabling User Accounts

If DOC4000 is configured to use **Application Authentication**, administrators can disable and re-enable user accounts. This section describes how to disable and enable user accounts using the Admin Utility. Administrators can also use the **Settings** area of the DOC4000 web interface to disable and enable user accounts.

To disable an existing user account:

1. In the Admin Utility, click the **Users and Groups** link.
2. Click on the **Users** tab.
3. Select the desired user.
4. Click **Edit User**.
5. Check the **Disable User** check box.
6. Click **Save**.

Disabled user accounts are not listed by default on the Users window in the Admin Utility.

To re-enable a user account:

1. In the Admin Utility, click the **Users and Groups** link.
2. Click on the **Users** tab.
3. Check the **Show Disabled Users** check box.
4. Select the desired user.
5. Click **Edit User**.
6. Clear the **Disable User** check box.
7. Click **Save**.

Exporting a List of Users or Groups

DOC4000 allows you to export the list of users or groups defined in the Admin Utility. You can save this list to an Excel file. The exported list includes both enabled and disabled users or groups.

To export the list of users or groups:

1. In the Admin Utility, click the **Users and Groups** link.
2. Select whether you want to export the list of users or groups:
   - To export the list of users, click on the **Users** tab.
   - To export the list of groups, click on the **Groups** tab.
3. Click **Export to Excel**.
4. Type the name for the Excel file, and then click **Save**.
5. Click **OK** on the confirmation window.

SECTION 2

Identifying Assets and Importing Data

This section outlines how to add assets and their related configuration data to DOC4000. You can also define a custom asset hierarchy for your asset explorer. This information helps you understand how DOC4000 works with assets of all types and gives you an overview of the import and configuration process. For more information about a specific asset type or asset model, see the *Implementation Guide* for that asset model.

Understanding Assets, Data Owners, and Asset Models

DOC4000 provides a wide array of asset models to allow DOC4000 to incorporate data from many types of systems. Each asset model helps collect configuration data from specific types of systems, such as Honeywell EPKS, and use that information in DOC4000. With this data, DOC4000 displays inventory information, identifies configuration discrepancies, detects unauthorized changes due to malicious attack or inadvertent engineering updates, and enables sustained compliance with regulatory or corporate standards. An asset model is available to DOC4000 customers who purchase a license for the asset model and configure that model. You can also create or customize your own asset models using the Asset Model Development Kit (AMDK). For example, you can create defect checks that verify control system configuration data and viewer tabs that allow you to review or modify configuration data as needed. For more information, run the *InstallPath*`\DataCollector\AMDK.exe` file as an administrator, and then click **Help**.

Once you load an asset model, you can create one or more assets of the type defined by that asset model. In most cases, such as for ICS systems, each DOC4000 asset represents one system. For example, each Honeywell EPKS asset represents one Honeywell EPKS system. However, in some cases, such as for the Network Devices and Recon asset models, you create an asset that represents a group of systems such as network devices or Windows computers. In these cases, the term data owner is often used in place of asset. A data owner is the asset you create in DOC4000 that is associated with a set of data collected for the asset model. Therefore, these two terms often mean the same thing.

The *Implementation Guide* for an asset model provides information about that version of the asset model as well as detailed guidance for installing and configuring that model. For most asset models, the general implementation process involves:

1. Verify the system requirements for the asset model.
2. Collect the needed data from each system of the type supported by the model. Each model often provides collection utilities and scripts.
3. Load the asset model. This task is also called importing the asset model.
4. Create an asset for each group of collected data, such as per data owner.
5. Configure each asset to identify the location of the collected data. Depending on the asset model, the location can be an import folder or a database connection.

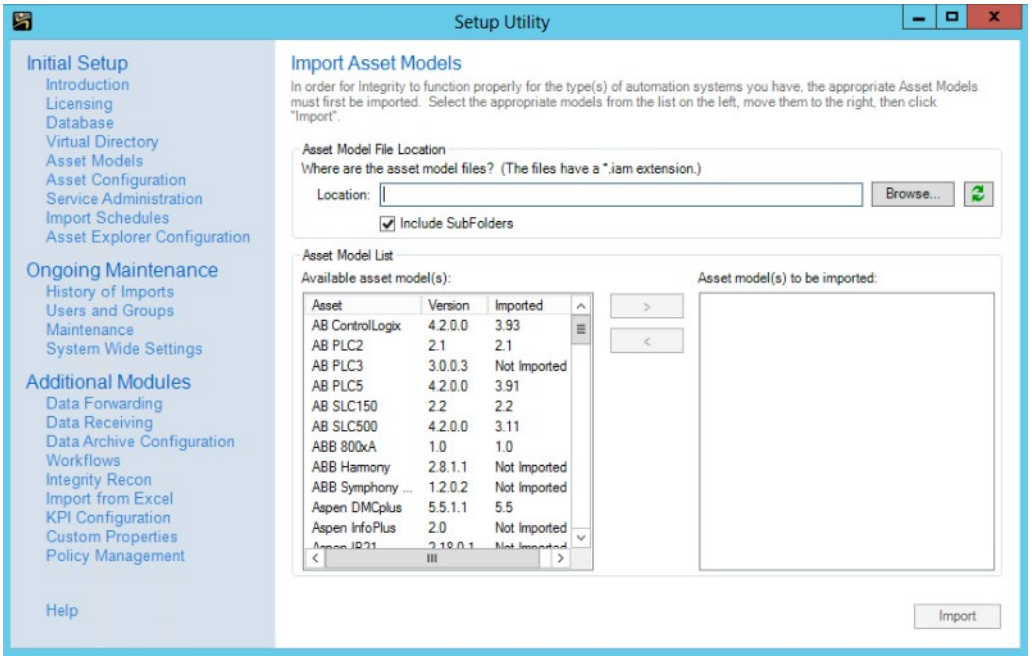
6. Configure additional properties to support references for other assets. For example, some Honeywell EPKS systems may reference other systems, such as Honeywell TPS systems or other Honeywell EPKS systems.
7. Import the collected data and verify the results.
8. Schedule data collection and import to keep the data in DOC4000 up to date.

Loading (Importing) Asset Models

The **Asset Models** link in the Admin Utility opens the Import Asset Models window. From this window, you can load the DOC4000 asset models you have purchased. This process allows DOC4000 to understand details for specific types of distributed control systems, historians, programmable logic controllers, and more. The **Asset Models** link in the Admin Utility is available only if a database exists as specified through the **Database** link.

The Import Asset Models window allows you to select one or more asset models to load. The **Version** column in the **Available asset model(s)** list indicates the version of the asset model and whether it is available. The **Imported** column in the **Available asset model(s)** list indicates whether an asset model was previously loaded and the version that was loaded.

This window does not allow you to add asset models already listed in the **Asset model(s) to be imported** list. In addition, if an asset model is listed in the **Version** column as **Not Licensed**, you cannot add it to the **Asset model(s) to be imported** list.



To load an asset model:

1. In the Admin Utility, click the **Asset Models** link.
2. Click the **Browse** button to locate the model files provided with your installation, or type the path to the asset models to be loaded, such as *InstallPath*`\DataCollector\Asset`

`Models`. Since the DOC4000 server or data collector cannot access files on mapped drives, use only Universal Naming Convention (UNC) paths.

3. From the **Available asset model(s)** list, click on a model to load and then click the **>** button to move the asset model to the **Asset model(s) to be imported** list.
4. Click the **Import** button. DOC4000 displays a message to confirm success.

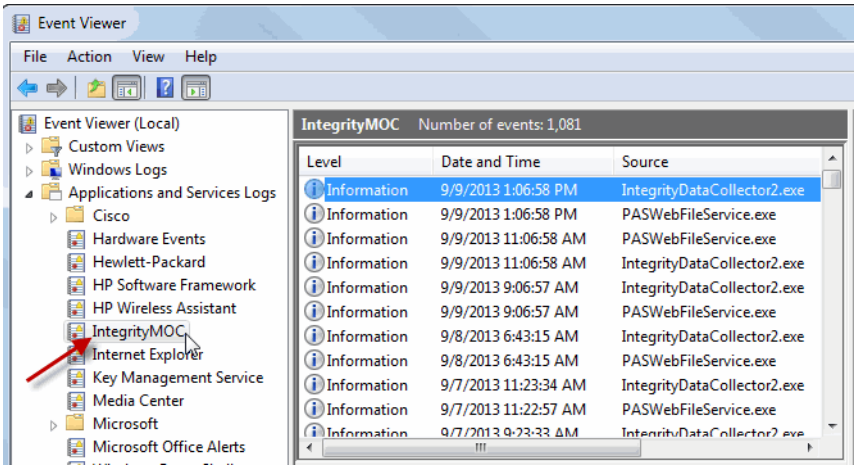
NOTE After you load an asset model, view the Windows event log to verify that no errors occurred during the loading process. For more information, see *Viewing the Event Log for Asset Model Loading Errors* (page 33).

Viewing the Event Log for Asset Model Loading Errors

After you load an asset model, check the DOC4000**MOC** section in the Windows Event Viewer to verify that no errors occurred during the loading process.

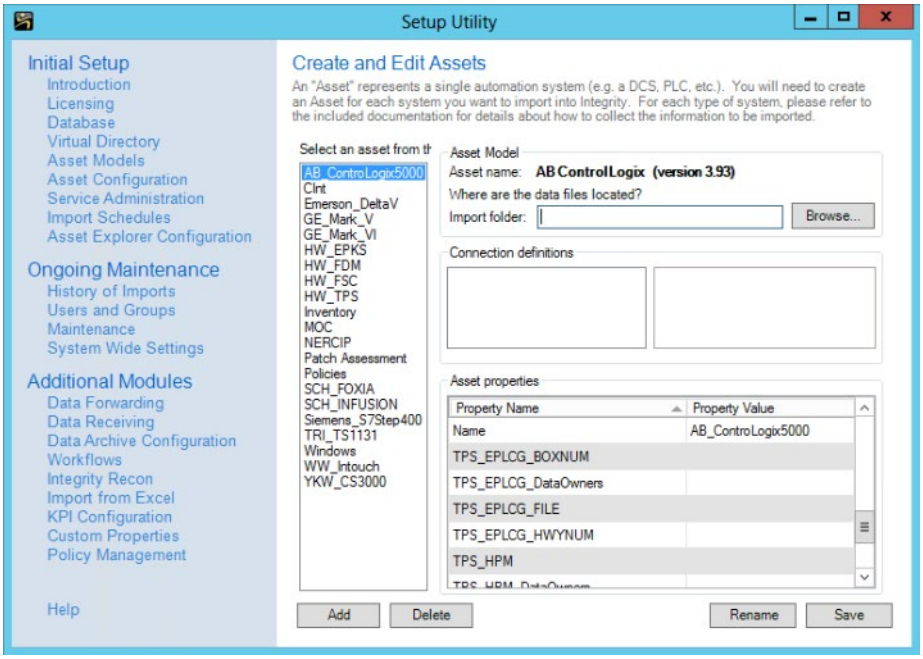
To open the Windows Event Viewer:

1. Click Windows **Start > Run**.
2. Type `eventvwr` and click **OK**.
3. Click DOC4000**MOC** in the left pane to view the event log. Notice whether errors from the time period associated with the asset model loading have occurred.



Adding, Modifying, and Deleting Assets (Data Owners)

Once you load an asset model, you can create one or more assets (data owners) for that type of system. The **Asset Configuration** link in the Admin Utility allows you to create new assets and configure the properties for existing assets. You can also rename existing assets and delete those assets.



Before you add assets and schedule imports for a type of system, see the *Implementation Guide* for the associated asset model. Each *Implementation Guide* provides detailed information and configuration instructions specific to that asset model. For more information about using the Create and Edit Assets window, see the following topics:

- *Adding an Asset (Data Owner)* (page 34)
- *Configuring an Existing Asset (Data Owner)* (page 35)
- *Deleting an Asset (Data Owner)* (page 35)

Adding an Asset (Data Owner)

After you load an asset model, you can create one or more assets (data owners) for that type of system. The **Asset Configuration** link in the Admin Utility allows you to create new assets and configure the properties for existing assets. For more information about a type of system, see the *Implementation Guide* for the associated asset model, which provides detailed information and configuration instructions specific to that asset model.

To add an asset:

1. In the Admin Utility, click the **Asset Configuration** link.
2. Click **Add**.

3. Type a unique name for the asset and select the asset model for this asset type. Asset (data owner) names can have a maximum of 50 characters.
4. Click **OK**.
5. If this asset type imports files from a folder, in the **Import folder** field, either type the location of the data files collected from the system associated with this asset, or click **Browse** to browse to the location.
6. If this asset type imports data using a data source connection, in the **Connection definitions** field, specify the connection to that data as needed.
7. If this asset type requires additional properties, type the values in the **Asset properties** field as needed. These properties can define many different aspects of the associated asset, such as connections to other systems. For more information about these properties, see the *Implementation Guide* for that asset model.
8. Click **Save**.

Configuring an Existing Asset (Data Owner)

The **Asset Configuration** link in the Admin Utility allows you to create new assets and configure the properties for existing assets. For more information about a type of system, see the *Implementation Guide* for the associated asset model, which provides detailed information and configuration instructions specific to that asset model.

To configure an existing asset:

1. In the Admin Utility, click the **Asset Configuration** link.
2. Select the asset in the list that you want to configure. The Create and Edit Assets window displays the properties and values for the selected asset.
3. If this asset type imports files from a folder, in the **Import folder** field, you can type the location of the data files collected from the system associated with this asset, or click **Browse** to browse to the location.
4. If this asset type imports data using a data source connection, in the **Connection definitions** field, you can specify the connection to that data as needed.
5. If this asset type requires additional properties, you can type the values in the **Asset properties** field as needed. These properties can define many aspects of the associated asset, such as connections to other systems. For more information about these properties, see the *Implementation Guide* for that asset model.
6. Click **Save**.

Deleting an Asset (Data Owner)

The **Asset Configuration** link in the Admin Utility allows you to delete existing assets. When you delete an asset, you also delete all the data for that asset in the DOC4000 database. However, DOC4000 does not delete the workflow cases associated with the asset.

You may also want to delete the import folder or data sources associated with that asset. Before you delete an asset, identify the locations of the import folder and data sources. For more information about a type of system, see the *Implementation Guide* for the associated asset model.

To delete an asset:

1. In the Admin Utility, click the **Asset Configuration** link.
2. Select the asset in the list that you want to delete. The Create and Edit Assets window displays the properties and values for the selected asset.
3. Click **Delete**.
4. Click **Yes** on the confirmation message to indicate you want to delete all data in the DOC4000 database for that asset.

Scheduling Data Imports

After you have collected the data files from your systems, loaded the related asset models, and added the assets in DOC4000, you can run or schedule a data import for those assets. For each asset, you need to direct DOC4000 to perform the data import and subsequent processing of the data. Typically, this procedure runs on a regular schedule that coincides with potential periodic updates in newly collected data.

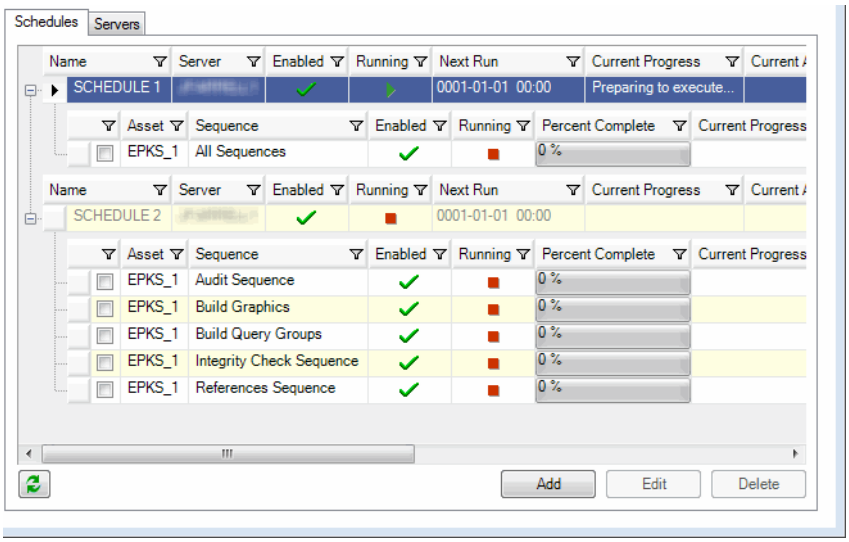
NOTE When you first install DOC4000, you need to complete the data import process to make data available in the DOC4000 web interface. If you load a new version of an asset model, you may also need to complete the data import process for those type of assets to use the updated processing of the data defined by the asset model.

You can schedule data imports through the Admin Utility and monitor their progress. You can also use Windows Task Scheduler to schedule and run data imports from the command line. For more information, see the following topics:

Scheduling and Running Data Imports with the Admin Utility

The **Schedules** link in the Admin Utility opens the Schedule Imports and Monitor Progress window. This window allows you to create one or more schedules for importing or exporting data from one or more data sources. You can create one schedule for multiple assets, or you can create multiple schedules, such as one for each asset type. You can also run a schedule now and then review the results. DOC4000 also allows you to create an **Auto** schedule, which checks the import folder for a `NewFiles.txt` file, and when this file exists DOC4000 imports the data in that folder.

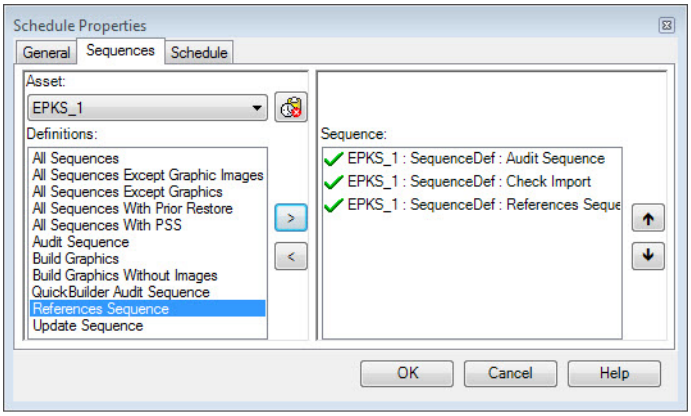
This window also allows you to view the status of all data imports. The **Schedules** link is available only when the database exists as specified through the **Database** link.



To import data now or on a scheduled basis:

1. In the Admin Utility, click the **Schedules** link.
2. Click **Add** to open the Schedule Properties window and add a new schedule.
3. Click on the **General** tab to name the import schedule and identify which DOC4000 server or data collector will import the data. Complete the following steps:
   a. In the **Schedule Name** field, type a descriptive name for the import schedule.
   b. In the **Server run on** field, type the name of the DOC4000 server or data collector that will import the data.
   c. If you want to disable this schedule, clear the **Enabled** check box. By default, this check box is selected so the import starts at the scheduled time.
4. Click on the **Sequences** tab to specify the data import tasks (sequences) and their order. This tab allows you to select sequence definitions for one or more assets in a single schedule. For each asset you want to include in this schedule, complete the following steps:
   a. In the **Asset** field, select an asset. To view a list of assets that have not been scheduled, you can click the **Schedule** button next to the **Asset** field.

b. In the **Definitions** list, select one or more sequences you want to run. Most asset models support an **All** sequence. Other sequences are available for testing and troubleshooting purposes, as well as for coordinating connected assets and cross references. In most cases, these other sequences should be used only when working with Technical Support. For more information, see the *Implementation Guide* for the associated asset model.



c. Click the **>** button to move the selected sequences to the **Sequence** list.

d. Use the up and down arrow buttons to adjust the order of the sequences. The tasks are run one at a time starting at the scheduled start time.

5. Click the **Schedule** tab to specify the frequency and start time for the import.

6. If you want to run the defined import now, complete the following steps:

   a. In the **Perform schedule** field, select **One Time Only**.

   b. Check the **Run now** check box.

   c. Click **OK**.

7. If you want to run the defined import when a NewFiles.txt file is in the import folder, complete the following steps:

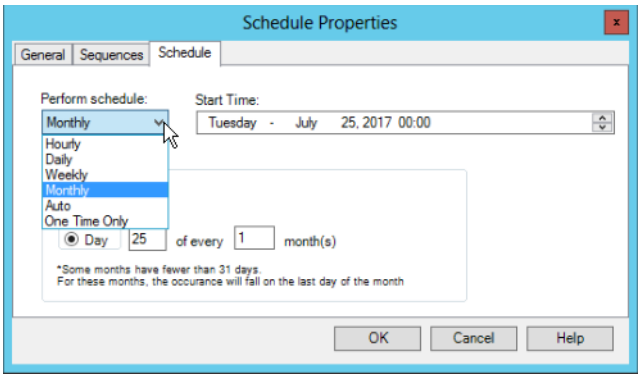
   NOTE DOC4000 can use a `NewFiles.txt` file to indicate new data is available. Several DOC4000 utilities that support data collection and transport create and use this file to continue the data processing on the next system.

   a. In the **Perform schedule** field, select **Auto**.

   b. Click **OK**.

8. If you want to schedule the defined import, complete the following steps:

a. In the **Perform schedule** field, select how often you would like the defined import to run, such as **Daily** or **Weekly**. Additional fields are displayed in the **Details** section.



b. Use the fields in the **Details** section to define the schedule you want.

c. In the **Start Time** field, refine the start time for the next scheduled import to begin.

d. Click **OK**.

Repeat these steps until you have scheduled all data imports and they are listed on the Schedule Imports and Monitor Progress window. You can click the plus sign (**+**) next to each import schedule to see the import tasks included in it. Notice the **Percent Complete** column for each task. Wait until the initial data imports have successfully finished before you open the DOC4000 web interface to view the data.

Running a Defined Data Import

DOC4000 allows you to run a defined data import without waiting for the scheduled time. This capability allows you to collect data, as needed, and import it to update the displayed information.

NOTE Make sure the IntegrityDataCollector2 service is running on the DOC4000 server or data collector where the data will be imported. If this service is not running, the **Run Now** option is not available.

To run a defined data import:

1. In the Admin Utility, click the **Schedules** link.
2. Right-click the schedule name for the schedule you want to run, and then click **Run Now**.

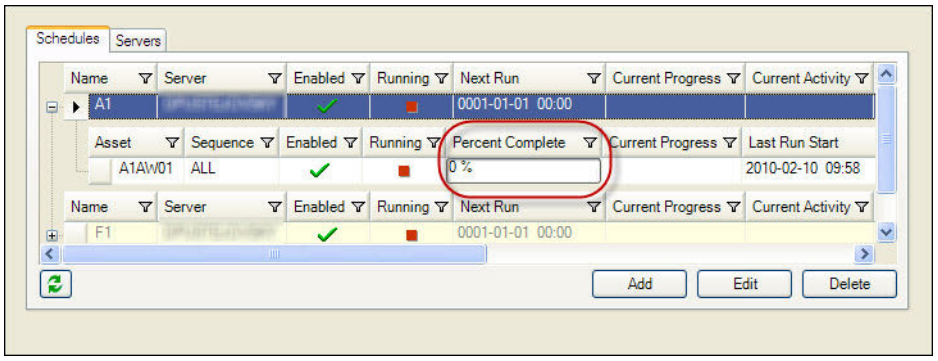
Monitoring the Status and History of Scheduled Data Imports

The **Schedules** link in the Admin Utility opens the Schedule Imports and Monitor Progress window. This window allows you to monitor the progress of an import and to view the import log, if needed. You can also view the history for a scheduled import.

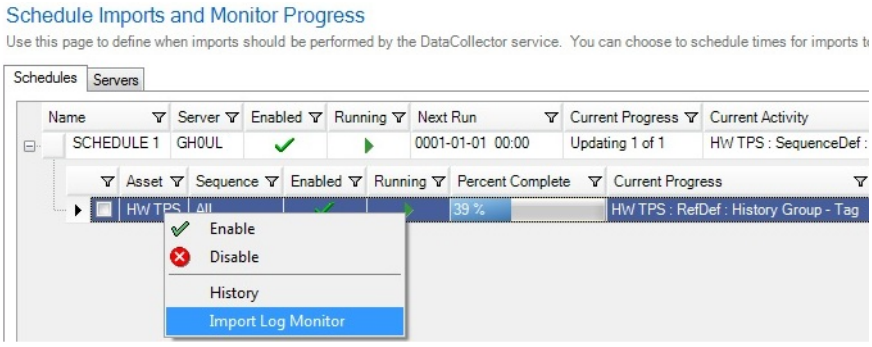
DOC4000 also provides the Review a History of Imports window, which displays information concerning imported data for any asset model. Through the Review a History of Imports window, you can view more details about the imported data and roll back to a previous set of imported data if the database is configured to support data roll back. For more information about the Review a History of Imports window, see *History of Data Imports* (page 42).

To monitor an import:

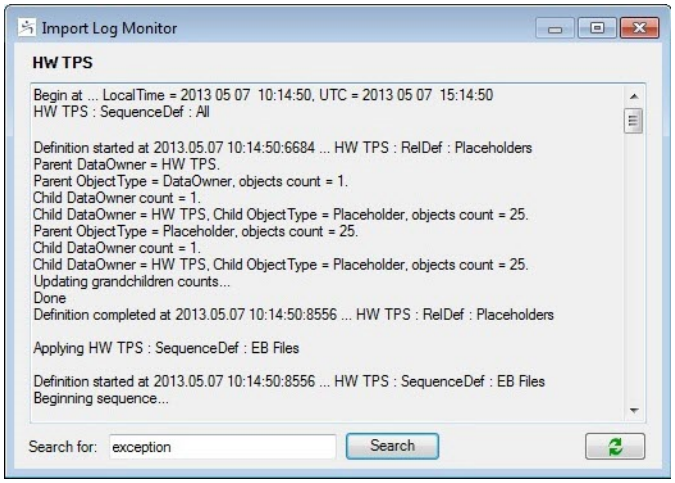
1. In the Admin Utility, click the **Schedules** link.
2. On the Schedules tab, click the plus sign (**+**) next to an import schedule to see the import tasks included in it. The **Percent Complete** column for each task provides progress information.



3. If you want to view the import log for a running import, right-click on an asset row, and select **Import Log Monitor**.



The Import Log Monitor window displays the contents of the import log, which you can scroll to view all the text. You can click **Refresh** to update the contents as the import progresses. To search the import log, type the criteria in the **Search for** field, and then click **Search**. The search text defaults to `exception` to search for errors in the log.



4. If you want to view the history for an import schedule, right-click on a scheduled import row in the Schedule Imports and Monitor Progress window, and select **History**. The Update

Summary window is displayed with details about the imported data for the selected asset. For more information about this window, which is similar to the Review a History of Imports window, see *History of Data Imports* (page 42).

Copying a Data Import Schedule

You can select sequences within an import schedule to copy to a new import schedule. Then, you can modify the new import schedule for your specific needs. This task is helpful when a sequence within an import schedule has an error and you want to run that sequence again to resolve the issue. The **Save Selected As New** option is available only if the IntegrityDataCollector2 service is running on the DOC4000 server or data collector specified in the import schedule you want to copy.

To copy a data import schedule:

1. In the Admin Utility, click the **Schedules** link.
2. Expand the schedule to be copied by clicking the plus sign (**+**) next to the schedule name.
3. Check the check box next to each sequence that you want to copy to the new schedule.
4. Right click on the schedule name, and click **Save Selected As New**.

The list of schedules is disabled while DOC4000 creates the new import schedule with the selected sequences. When finished, the new import schedule is added to the Schedules tab and the schedule name is set to **Copy_of_***originalschedulename*. You can then modify the new import schedule as needed. For more information, see *Modifying a Data Import Schedule* (page 41).

Modifying a Data Import Schedule

You can modify an existing data import schedule, including the import sequences and their order, as well as the frequency and start time. Once you create a data import schedule, you cannot change the schedule name. For more information about the options and tabs of the Schedule Properties window, see *Scheduling and Running Data Imports with the Admin Utility* (page 36).

To modify a data import schedule:

1. In the Admin Utility, click the **Schedules** link.
2. Right-click the schedule name for the schedule you want to modify, and then click **Edit**.
3. Change the properties as needed on the tabs of the Schedule Properties window, and then click **OK**.

Enabling or Disabling a Data Import Schedule

You can enable or disable a data import schedule as needed.

To enable or disable a data import schedule:

1. In the Admin Utility, click the **Schedules** link.
2. If you want to enable a disabled data import schedule, right-click the schedule name for the schedule you want to enable, and then click **Enable**.

3. If you want to disable an enabled data import schedule, right-click the schedule name for the schedule you want to disable, and then click **Disable**.

Deleting a Data Import Schedule

If you no longer need a data import schedule, you can delete it.

To delete a data import schedule:

1. In the Admin Utility, click the **Schedules** link.
2. Right-click the schedule name for the schedule you want to delete, and then click **Delete**.
3. Click **Yes** on the Delete Confirmation window.

Scheduling Data Imports from the Command Line

The `RunDefinition.exe` utility allows you to import data for an asset from the command line. You can also use Windows Task Scheduler to import newly-collected data by running this command on a scheduled basis. The syntax of this command is:

"InstallPath`\DataCollector\RunDefinition.exe"`"*Asset* `: SequenceDef :` *Seq"*

- *InstallPath* - Specifies the location where you installed DOC4000, such as `C:\Program Files (x86)\PAS\Integrity`.
- *Asset* - Specifies the name of the asset (data owner) in DOC4000, such as `ABSLC500-Unit1`.
- *Seq* - Specifies the name of the import sequence defined by the asset model for this asset, such as `All`.

For example, to import the data for the `TPS1` asset using the `All` import sequence with DOC4000 installed in the `C:\PAS\Integrity` folder, enter the following command:

```
"C:\PAS\Integrity\DataCollector\RunDefinition.exe" "TPS1 : SequenceDef : All"
```

History of Data Imports

The **History of Imports** link in the Admin Utility opens the Review a History of Imports window, which displays information concerning imported data for any asset. This window allows you to perform many tasks related to imported data for assets, such as viewing details about the imported data and restoring a previous set of imported data. This link is available only if a database exists as specified through the **Database** link.

DOC4000 also provides the Schedule Imports and Monitor Progress window, which allows you to monitor the progress of an import and to view the import log, if needed. For more information about the Schedule Imports and Monitor Progress window, see *Monitoring the Status and History of Scheduled Data Imports* (page 39).

For more information about using the Review a History of Imports window, see the following topics:

- *Viewing Details about Imported Data* (page 43)

Viewing Details about Imported Data

You can view summary information about imported data and the detailed import log file for that import. You can also export the summary information or log file.

To view information about a data import for an asset:

1. In the Admin Utility, click the **History of Imports** link.
2. In the **Assets** field, select the asset you want to view. The **Import Events** list displays the import events for the selected asset.
3. In the **Import Events** list, click a row to select that import event.
4. If you want to view a summary of the selected event, click **Show Summary**. The information for the selected event is displayed in the **Summary** field.
5. If you want to view the log file with details of the import, click **Show Log File**. The log file for the selected event is displayed in the **Log file** field.
6. If you want to save the summary or log file, complete the following steps:
   a. Display the summary information or log file you want to save.
   b. Click **Export File**.
   c. Select the folder where you want to save the text file, and click **OK**. Then, click **OK** to close the confirmation window.

Restoring a Previous Version of Imported Data (Roll Back)

The asset roll back feature allows you to restore a previous version of imported data for an asset. This feature is available only if the database was configured to enable it. For more information, see *Understanding and Enabling Asset Roll Back* (page 12).

To restore a previous version of imported data:

1. In the Admin Utility, click the **History of Imports** link.
2. In the **Assets** field, select the asset you want to restore to a previous version of imported data. The **Import Events** list displays the import events for the selected asset.
3. In the **Import Events** list, click a row to select that import event.
4. Click **Roll Back Import**.

Setting an Import Time as the Baseline

You can establish a set of imported data as a baseline. This baseline can then be used to compare against for evaluating imported data. These comparisons can help you identify imported data that may have issues. The **Set Import Time as Baseline**. button is available only if you have configured data DOC4000 and the **Import Time Change** option. For more information, see *Data Integrity* (page 58).

To set an import time as the baseline:

1. In the Admin Utility, click the **History of Imports** link.
2. In the **Assets** field, select the asset you want to restore to a previous version of imported data. The **Import Events** list displays the import events for the selected asset.
3. In the **Import Events** list, click a row to select that import event.
4. To set the selected event time as the baseline by which the Import Time Change is compared, click **Set Import Time as Baseline**. For more information about this baseline and the **Number of Changes** and **Import Time Change** options, see *Data Integrity* (page 58).

Configuring Asset Explorer and Rack Settings

The asset explorer tree displays a hierarchical view of your data owners, assets, and related objects for each data owner or asset. By default, the data owners are listed in alphabetical order at the top level of the asset explorer tree, and as you add new data owners to DOC4000, they are automatically added to the top level of this hierarchy. As your list of data owners grows, you may want to organize them in a different way.

You can customize your asset explorer to meet your specific needs. For example, you can create a custom hierarchy that groups data owners by system type, such as Honeywell EPKS, or by plant location, or both. You can also use this custom hierarchy to assign permissions to different objects.

Some asset models, such as the Invensys FoxIA asset model, provide additional configuration options for rack objects and hardware, based on your license. The Rack Configuration tab is available only if an asset model you imported supports it. The asset model determines which objects can be parents of a rack and which objects can be children of a rack.

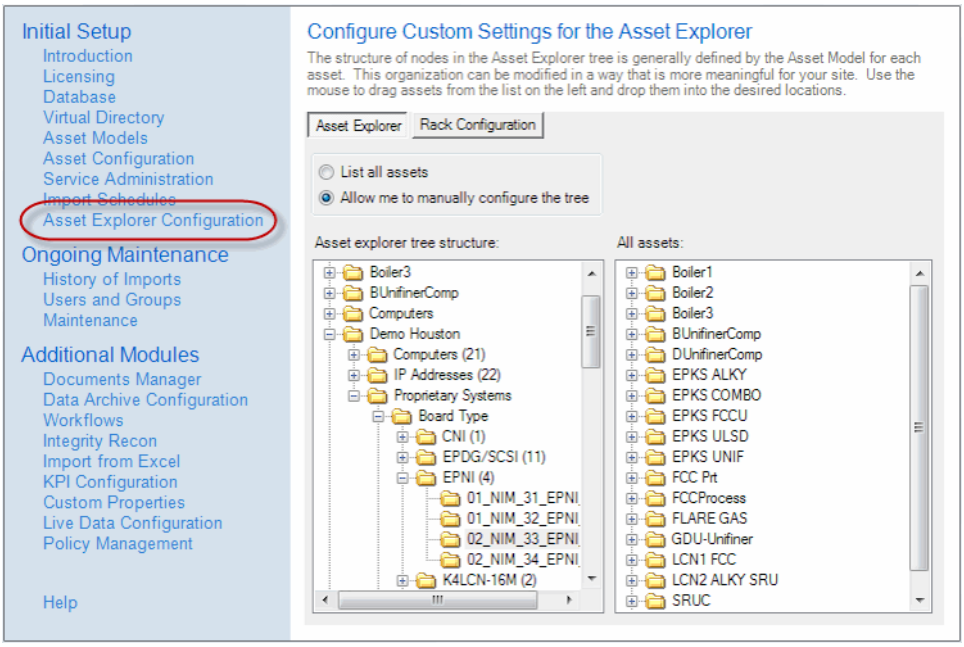
The **Asset Explorer Configuration** link in the Admin Utility opens the Configure Custom Settings for the Asset Explorer window. This window provides tabs that allow you to define settings for the asset explorer tree and for rack objects and hardware. For more information about these options, see the following topics:

- *Configuring the Asset Explorer Tree* (page 44)
- *Rack Configuration* (page 46)

Configuring the Asset Explorer Tree

The **Asset Explorer Configuration** link in the Admin Utility opens the Configure Custom Settings for the Asset Explorer window. This window provides options to override the structure of the asset explorer in DOC4000 and to complete manual rack configuration. For more information about rack configuration, see *Rack Configuration* (page 46).

You should finish adding all data owners prior to configuring the asset explorer tree structure. If you import additional data owners after you configure the asset explorer tree structure, *new data owners are not displayed* in the tree structure in DOC4000 until you manually add them to the tree.



Before you modify your asset explorer tree, review the following considerations:

- You can also use Configuration Manager to define the asset explorer tree structure. If you have Cyber DOC4000, you also need to use Configuration Manager to define an asset hierarchy for Cyber DOC4000. For more information, see Understanding and Defining Your Asset Hierarchy.
- When using multiple databases, use Configuration Manager to define the asset explorer tree. If you select **Asset Explorer Configuration** in the Admin Utility, you may need to rebuild your asset explorer tree using Configuration Manager. For more information, see *Working with Multiple Databases for Enterprise Deployments* (page 12).

To configure the asset explorer tree:

1. In the Admin Utility, click the **Asset Explorer Configuration** link.

   By default, the **List all assets** option is selected, and all assets are displayed in alphabetical order.

2. If you want to customize the asset explorer tree structure, complete the following steps:

   a. Click **Allow me to manually configure the tree**.

   b. If you want to add a grouping node to the asset explorer tree structure, right-click on the **Asset Explorer tree structure** list, or the blank area if no list has been started, and click **Add child node**. Type a title for the node, and then click **OK**. You can repeat this step to add more grouping nodes.

   c. Click on an asset in the **All assets** list, and drag-and-drop it to the desired location in the **Asset Explorer tree structure** list. Then, click **Yes** to confirm the selection and location.

Drop an object on top of a node to nest the object under that node. You can repeat this step to create the structure you want with all your assets.

d. If you want to change a grouping node you created, right-click on a manually-created node in the **Asset explorer tree structure** list and then click **Rename**, **Delete**, or **Change icon** for the node.

3. If you want to use the default asset explorer tree that lists all assets in alphabetical order, complete the following steps:

   a. Click **List all assets**.

   b. Click **Yes** to confirm that you want to show all assets. DOC4000 saves your last manual configuration of the asset explorer tree for the future, if needed.

Rack Configuration

Rack Configuration allows you to insert rack objects and reorganize the hardware overview. This configuration option is available only if an asset model you imported supports it. For example, the Invensys FoxIA asset model supports rack configuration.

The asset model determines which objects can be parents of a rack and which objects can be children of a rack. When a data owner is selected on the Rack Configuration tab, you might see one or more placeholders that display the hardware objects when expanded. Expanding the hardware objects displays the inserted racks and children for that object.

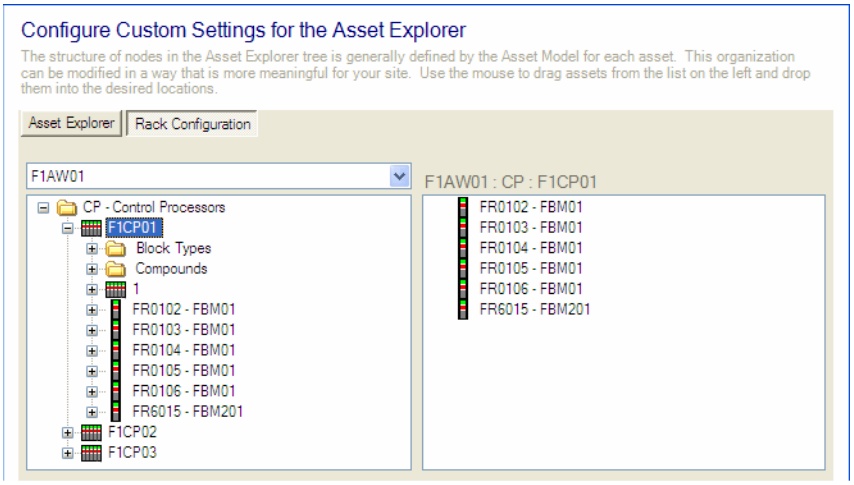
The Rack Configuration window allows you to:

- Insert rack objects for pieces of hardware
- Assign children of the parents to the racks using drag and drop

NOTE You should complete this configuration only once after the first import.

When you perform rack configuration, you should review the following topics:

- *Adding a Rack in Rack Configuration* (page 47)
- *Assigning Objects to a Rack in Rack Configuration* (page 47)



Adding a Rack in Rack Configuration

When you configure the racks for asset models that support it, you need to add rack objects for pieces of hardware. Then, you can assign objects and define parent-child relationships. For more information, see *Assigning Objects to a Rack in Rack Configuration* (page 47).

To add a rack:

1. In the Admin Utility, click the **Asset Explorer Configuration** link.
2. Click the **Rack Configuration** tab.
3. In the list at the top of the Rack Configuration tab, select an asset. The asset model for that asset must support rack configuration.
4. Expand the placeholder nodes to view the objects. Only applicable object types are listed.
5. Right-click on an object, and then click **Add Rack**.
6. On the Add Rack window, specify the **Title**, **Total slots**, and **I/O slots** fields for the rack, such as `1`, `16`, and `12`.
7. Click **OK**. The new rack is listed as a child of the parent object.
8. If you want to modify the rack object, right-click on the rack to view other options, such as **Rename**, **Delete**, and **Change icon**.

Assigning Objects to a Rack in Rack Configuration

After you add the rack objects you need, you can assign objects and define parent-child relationships.

To assign children to a rack:

1. Click the rack's parent object. Only the children for the rack are displayed in the right pane.
2. Select one or more children in the right pane to assign to the rack.
3. Drag-and-drop the children to the designated rack.
4. Click **Yes** to confirm.

   NOTE If a child has already been assigned to a rack and should be assigned to a different rack, it must first be assigned back to the parent prior to assigning it to the new rack.
5. If you want to reassign an object to a different rack, complete the following steps:
   a. Under the rack, select the object to reassign.
   b. Drag-and-drop the object to the parent.
   c. Click **Yes** to confirm.
   d. If you have not exited the Admin Utility from the time of the original object assignment until now, the objects are displayed in the right pane of the window and are available to be reassigned. However, if you have exited the Admin Utility after the original assignment, the objects are not available to be reassigned until after the next data import.

SECTION 3

Maintenance, Settings, and Data Management

After you initially install and configure DOC4000, there are several general maintenance areas that need your attention. DOC4000 also allows you to configure change tracking, email notification, and other features to meet your specific needs. In addition, you may find that you want to adjust your system-wide settings for how data is imported and asset discovery is performed. This section provides topics to help you perform these management and maintenance tasks.

Maintaining DOC4000

When maintaining DOC4000, you need to ensure your data is backed up and protected, your systems are up-to-date, and the features are configured as needed. DOC4000 provides a powerful solution with the flexibility to meet your specific needs.

Review the following topics to ensure your DOC4000 implementation functions well:

- *Antivirus Software, Security Information, and Patches* (page 48)
- *Backing up and Archiving Data* (page 48)
- *Shrinking the Transaction Log* (page 49)
- *Scheduling Maintenance* (page 49)
- *SQL Server Roles and Permissions* (page 50)

In addition, DOC4000 provides several maintenance features to help you keep DOC4000 running efficiently and effectively. For more information, see *Using the DOC4000 Maintenance Features* (page 50).

Antivirus Software, Security Information, and Patches

To keep your DOC4000 and Microsoft SQL Server systems updated and secure, you need to stay informed of current security issues or threats and keep the systems up to date with the latest patches and service packs. You should also install, configure, and maintain an antivirus software program such as Norton Antivirus Corporate Edition or McAfee Security. Some antivirus products can interfere with DOC4000. If you experience any issues, contact Technical Support.

To obtain the latest security information, subscribe to several security-related newsletters and check some of the main Microsoft SQL Server security websites for news and information.

Backing up and Archiving Data

Microsoft SQL Server database backup and restore operations are used to recover from catastrophic hardware or software failure. These operations run against the entire database and are not recommended for simple archival purposes. Microsoft SQL Server includes database maintenance tools that you can use to back up and restore Microsoft SQL Server databases. When backing up your data, review the following considerations:

- The default database name is DOC4000. Periodically store a backup copy of the database in a secure location.
- In some deployment scenarios, you may want to configure DOC4000 to work with multiple databases. In these cases, be sure to back up all your databases. For more information, see *Working with Multiple Databases for Enterprise Deployments* (page 12).
- If you enable asset roll back, DOC4000 creates an additional database with the same name as the DOC4000 database prefixed with Rollback_, such as Rollback_DOC4000. Make sure you also back up this database.
- If you enable event log data collection, DOC4000 creates an additional database named PASWindowsEventLogs. Make sure you also back up this database.

DOC4000 provides several features to help you archive or save data. These features can help you recover from incorrect data collected from one or more systems. You can choose to implement and use any or all of these features:

Asset Roll Back

This feature allows you to roll back the data for an asset to a previously imported set of data in the event that the most recently imported data is old, invalid, or corrupted. For more information, see *Understanding and Enabling Asset Roll Back* (page 12).

Data Archive

This feature allows you to archive the latest data files for an asset following each import for that asset. You can also restore the latest archived data files. These files are stored in a separate location that you specify. For more information, see *Understanding Import Data Archives* (page 75).

Data Forwarding

This feature securely exports and transports data for a set of objects from one DOC4000 site to another DOC4000 site where it can be imported. For more information, see *Understanding Data Forwarding and Receiving* (page 64).

Shrinking the Transaction Log

The Microsoft SQL Server transaction log records transactions and database changes to support features such as individual transaction rollback and recovery of incomplete transactions. In some cases, the transaction log can grow and consume a large amount of disk space. This disk space may be required to perform ongoing data transactions. If you need to reduce the disk space used, you can shrink the transaction log. However, if the transaction log grows again, you may need to make that disk space available for the log.

NOTE Store a backup copy of the database in a secure location before you shrink the transaction log.

Scheduling Maintenance

You should create a schedule for common maintenance tasks. The following table provides a sample and is not intended to supersede your current disaster recovery plan.

Task	Interval
Update Antivirus	Daily
Update Patches Daily and Service packs	Monthly
Database Backup*	Monthly
Shrinking Transaction Log	Monthly
Index Defragmentation	Monthly
RDF Backup*	Semi Annually
Ghost or hard disk clone of application server*	Semi Annually

*This data should be stored in a safe location on another computer.

SQL Server Roles and Permissions

DOC4000 uses several services to provide various features. These services should run under valid domain accounts, and the SQL Server roles and permissions required for these accounts depend on whether you choose to use Windows authentication or SQL Server authentication to access the DOC4000 database. For more information about these requirements, see *Defining Your Service Accounts* (page 19).

For more information about SQL Server roles and permissions, see https://msdn.microsoft.com/en-us/library/aa337562.aspx https://msdn.microsoft.com/en-us/library/aa337562.aspx.

Using the DOC4000 Maintenance Features

The Maintenance window in the Admin Utility allows you to fine-tune your DOC4000 implementation and adjust several key functions:

- *Performing Database Maintenance* (page 51)
  - Rebuild full-text search catalogs and table indexes
  - Enable reservations of spare components
  - Update friendly names that are displayed as labels on objects
- *Configuring Change Tracking* (page 52) and excluding selected properties from being tracked for changes
- *Configuring Email Notifications* (page 52)
- *Accessing DOC4000 with Trusted Domains* (page 53)DOC4000*Accessing DOC4000 with Trusted Domains* (page 53)
- *Integrating the PAS Dashboard* (page 53)

In some cases, you may want to restart the DOC4000 web application to clear the cache or synchronize changes made in Windows Active Directory with those set-in workflow user

assignments. For more information and the issues to consider before restarting the web application, see *Clearing the IIS Cached Configuration Information* (page 7) and *Restarting the Web Application* (page 19).

To access the DOC4000 maintenance features:

1. In the Admin Utility, click the **Maintenance** link in the **Ongoing Maintenance** section.
2. Use the fields in the various sections of the window to perform various maintenance tasks.

For more information about the options on the Maintenance window and additional guidance for specific tasks, see the following sections:

- *Performing Database Maintenance* (page 51)
- *Configuring Change Tracking* (page 52)
- *Configuring Email Notifications* (page 52)
- *Accessing DOC4000 with Trusted Domains* (page 53)DOC4000*Accessing DOC4000 with Trusted Domains* (page 53)
- *Integrating the PAS Dashboard* (page 53)

Performing Database Maintenance

The **Database Maintenance** options on the Maintenance window allow you to rebuild the full-text search catalog and table indexes, identify spare assets, update friendly names, and more. In addition to these options, review the other maintenance considerations for data backup, archiving, and other data maintenance and management tasks. For more information, see *Maintaining DOC4000* (page 48).

To perform DOC4000 database adjustments using the Admin Utility:

1. In the Admin Utility, click the **Maintenance** link in the **Ongoing Maintenance** section. The Maintenance window is displayed.

   The **Database Maintenance** section of the Maintenance window provides rebuild and index options that apply to all assets, as well as other options that apply only to the selected asset.
2. If you want to update full-text search capabilities, click **Rebuild Full-text catalogs**. This option begins a background process to update the full-text catalog used to perform full-text searches. Rebuilding the full-text index can be time intensive, based on the volume of data that needs to be processed, so rebuild the catalog only if you observe issues with the full-text search results. If a user performs a search before this background process finishes, only the results that have been indexed up to that point are returned without indicating the data is incomplete. To use the full-text search in DOC4000, the SQL Full-text Filter Daemon Launcher service must be enabled and running on the Microsoft SQL Server.
3. If you want to view the status of the database table indexes, click **Index Monitor**. This option displays the Database Index Monitor window, which displays the index status for each database table. You can view the status of all indexes or only the fragmented ones. The **Reindex Needed** column identifies the indexes that should be rebuilt. To rebuild indexes, choose whether to rebuild the selected indexes, all fragmented indexes, or only the system-wide indexes (common tables' indexes), and then click **Rebuild Now**. You can sort the displayed information by clicking on a column heading.

4. If you want to update the spare reservations for an asset, select the asset, check the **Spare Reservations** check box, and then click **Run**. This option begins an update of spare reservations that have been filled with objects previously deleted from a prior import.
5. If you want to update the friendly name for an asset, select the asset, check the **Update friendly names** check box, and then click **Run**. This option begins an update of the name displayed for objects of the selected asset.

Configuring Change Tracking

Identifying changes across your organization and their potential impact is vital. DOC4000 provides the ability to view changes to objects. The asset model for each asset type defines properties to track changes for. The links in the **Change Tracking** section of the Maintenance window allow you to configure which changes to exclude.

To configure change tracking:

1. In the Admin Utility, click the **Maintenance** link in the **Ongoing Maintenance** section.
2. If you want to exclude properties from being tracked for changes, click the **Exclude properties from Change Tracking** link in the **Change Tracking** section.
3. In the **Asset Model** field, choose the asset model for the object whose property you want to exclude from change tracking.
4. In the **Object Type** field, choose the type of object whose property you want to exclude from change tracking. The properties currently excluded from change tracking are listed in the **Excluded Properties** list.
5. In the **Property Name** field, type the name of the property to exclude, and then click **Add**. You can use wildcard characters in the **Property Name** field. The following table illustrates how each wildcard character is evaluated.

Wildcard character	Matched characters in property names
?	Any single character
*	Zero or more characters
#	Any single numerical digit (0-9)

6. When you are done adding properties to exclude, click **OK**.

Configuring Email Notifications

To use the various DOC4000 email notifications, you must specify the Email Notifications configuration information. This information defines the email server, port, and other email settings for DOC4000 to use.

To complete the email notification configuration:

1. In the Admin Utility, click the **Maintenance** link in the **Ongoing Maintenance** section.

2. Click the **Configure email notifications** link in the **Email Notifications** section. The Email Notifications Configuration window is displayed.
3. In the **Server** field, type the email server name or the IP address.
4. In the **Port** field, type the port number to use for email delivery.
5. In the **Display Name** field, type the name to display in the **To** field of each email sent by DOC4000. This value is displayed instead of the email address.
6. In the **From Address** field, type the email address from which the email is sent.
7. If you want to use the default user name and password to log into the email server, check the **Use Default Credentials** check box. When this option is selected, the **User Name** and **Password** fields are not available.
8. If you want to log into the email server with a specified user account, clear the **Use Default Credentials** check box, and then specify values in the **User Name** and **Password** fields. However, if the password for this account is changed in the future, you must also change the value on this window or notifications will no longer work until the password value is updated.
9. Click **Send Test Email** to verify the email configuration values you specified.
10. Click **OK** to save the information and return to the Maintenance window.

Accessing DOC4000 with Trusted Domains

In some deployment scenarios, the DOC4000 server may need to authenticate a user who is defined in a trusted domain. For example, if the DOC4000 server is in the DMZ domain and a user from the PCN domain connects to the DOC4000 web interface, the DOC4000 server needs to authenticate that user in the PCN domain. In this case, DOC4000 needs credentials for a valid user in the PCN domain.

The **Users and Groups** section on the Maintenance window allows an administrator to specify a valid user name and password for the other, trusted domain. The DOC4000 server can then connect to the trusted domain and authenticate other users from that domain. Type a valid user account name and password for the trusted domain in the fields in the **Users and Groups** section, and then click **Save**.

NOTE If the password for this trusted domain account is changed in the future, you must also change the password on this window or DOC4000 cannot authenticate a user who is defined in a trusted domain.

Integrating the PAS Dashboard

Honeywell, Inc. provides an advanced dashboard that can be configured to replace the dashboard provided with the Cyber DOC4000 web interface. For more information about installing, configuring, and using the PAS Dashboard, see the *PAS Dashboard User Guide*.

To use the PAS Dashboard in the Cyber DOC4000 web interface:

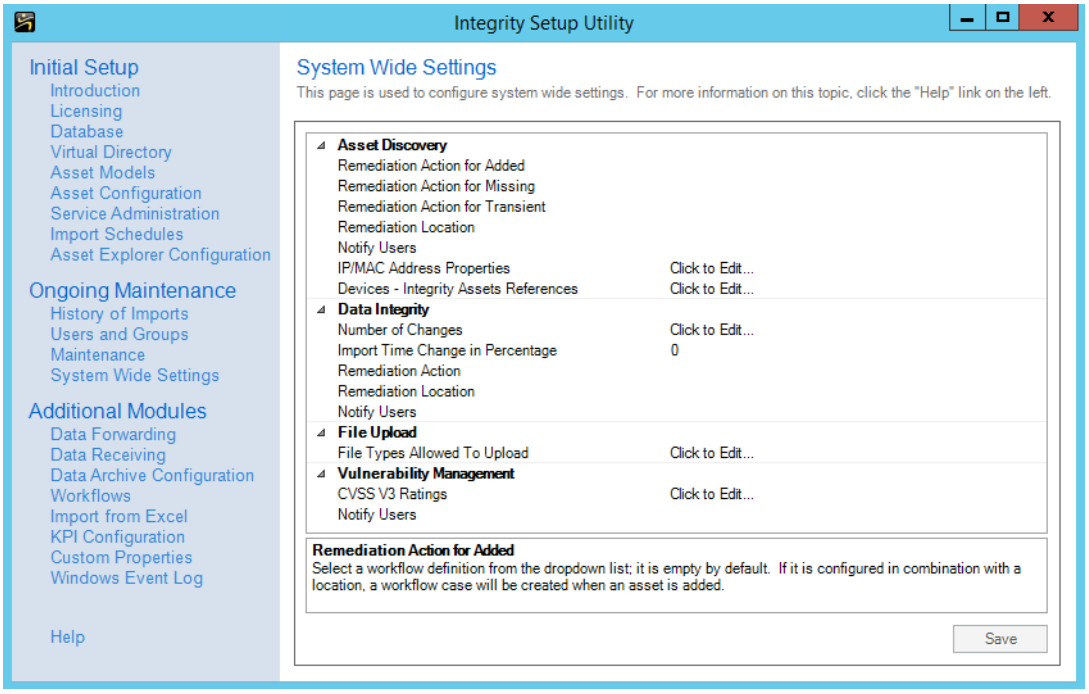
1. In the Admin Utility, click the **Maintenance** link in the **Ongoing Maintenance** section.
2. In the **PAS Dashboard URL** field, specify the URL for the PAS Dashboard installation to integrate with the Cyber DOC4000 web interface, and then click **Save**.

System Wide Settings

System wide settings define several global configuration options for functions. For example, some of these settings determine how imported data is evaluated, how assets are identified, and how uploaded files are managed. The **System Wide Settings** link in the Admin Utility allows you to configure system wide settings for the following areas:

- *Automated Asset Discovery* (page 54)
- *Data Integrity* (page 58)
- *File Upload Restrictions* (page 61)
- *Vulnerability Management* (page 62)

To access these settings, open the Admin Utility, and then click **System Wide Settings** in the **Ongoing Maintenance** section. The System Wide Settings window is displayed.



Automated Asset Discovery

Industrial control systems face growing risk from a malicious or inadvertent change. Hackers have increased their knowledge of industrial control systems and are becoming more coordinated and targeted in their efforts to gain control over process control systems. Mistakes and anomalies can go unnoticed and potentially affect production without automated detection in place.

One way to actively monitor for safety and reliability threats is to maintain a complete inventory of IT and OT assets. To keep an inventory complete and current, it cannot be managed manually. Devices on the Process Control Network (PCN) change as new systems are added, existing systems are removed, and unauthorized devices may connect. To ensure security and compliance, you need to know what assets or devices exist at all times. The only way to do that

efficiently is to automatically discover the assets on the network as well as those assets that are no longer on the network.

To provide this information, DOC4000 gathers data from assets connected to the PCN. By referencing this data, DOC4000 can accomplish the following goals:

- Dynamically detect what is or is not on a PCN.
- Detect previously identified assets or devices that are no longer on a PCN.
- Ensure that the assets or devices on the PCN are being managed.

To use automated asset discovery, you need to implement the following asset models:

- PAS Cyber DOC4000
- PAS Workflows
- PAS Inventory Items
- PAS Network Devices
- PAS Recon

You should also implement the asset models for your other types of systems. For more information, see the *Implementation Guide* for each asset model.

For more information about asset discovery, see the following topics:

- *Understanding the Asset Discovery System Wide Settings* (page 55)
- *Defining Workflow Cases and Notifications for Asset Discovery* (page 56)
- *Improving IP Address and MAC Address Identification* (page 57)
- *Mapping Known Network Devices and DOC4000 Data Owners* (page 57)DOC4000*Mapping Known Network Devices and DOC4000 Data Owners* (page 57)

Understanding the Asset Discovery System Wide Settings

The **Asset Discovery** system wide settings allow you to configure how DOC4000 handles assets added to or removed from the network. These settings are defined as follows:

Remediation Action for Added

Specifies the workflow definition to use to automatically create a case when a new asset is discovered on the network. You can select a different workflow for each remediation condition to customize the process for your specific needs.

Remediation Action for Missing

Specifies the workflow definition to use to automatically create a case when a previously discovered asset has been removed from the network. You can select a different workflow for each remediation condition to customize the process for your specific needs.

Remediation Action for Transient

Specifies the workflow definition to use to automatically create a case when an asset is discovered on the network, then removed, and then discovered again. This condition is identified as transient on the network. You can select a different workflow for each remediation condition to customize the process for your specific needs.

Remediation Location

Specifies the location to set in the workflow case created when as asset is added, missing, or transient. This setting works with the **Remediation Action** settings to correctly create the workflow case. The **Remediation Location** allows you to notify the correct set of users, specific to a location within the asset hierarchy, through the workflow case. The email notification includes a link to the case that was automatically initiated. The default value is blank.

Notify Users

Specifies one or more email addresses to notify when an asset is added, removed, or identified as transient on the network. The first email address you specify is the owner for the workflow case. Use a comma as the delimiter between two email addresses. The default value is blank.

IP/MAC Address Properties

Specifies property names to associate with IP addresses or MAC addresses. The matching of MAC address and IP address within asset discovery is done using a specific format. In most cases, DOC4000 can discover assets with no issue. In some cases, however, DOC4000 may not be able to make a match. For those cases, you can configure DOC4000 to look at different property name formats. This configuration setting indicates what to look for to match the MAC address and IP address with what DOC4000 finds in the system. For more information, see *Improving IP Address and MAC Address Identification* (page 57).

Devices - DOC4000 Asset References

Specifies the known DOC4000 asset names associated with each network device identified on the network. Assets that are discovered across multiple network segments may share the same IP address, which can create false matches. This system wide setting allows you to resolve this issue by mapping DOC4000 assets to a known network device by name. For more information, see *Mapping Known Network Devices and DOC4000 Data Owners* (page 57).

Defining Workflow Cases and Notifications for Asset Discovery

Several of the **Asset Discovery** system wide settings work together so you can specify the workflow case to create and the users to notify when an asset is added, removed, or identified as transient on the network. For more information about each setting, see *Understanding the Asset Discovery System Wide Settings* (page 55).

To define cases and notifications for asset discovery:

1. In the Admin Utility, click the **System Wide Settings** link in the **Ongoing Maintenance** section.
2. In **Remediation Action for Added**, select the workflow definition to use to create a case when a new asset is discovered on the network.
3. In **Remediation Action for Missing**, select the workflow definition to use to create a case when a previously-discovered asset is not found on the network.
4. In **Remediation Action for Transient**, select the workflow definition to use to create a case when an asset is discovered on the network, then removed, and then discovered again.

5. In **Remediation Location**, select the location to set in the workflow case created when as asset is added, missing, or transient. This location in the asset hierarchy allows you to notify the correct set of users through the workflow case.
6. In **Notify Users**, specify the email addresses to notify when an asset is added, removed, or identified as transient on the network. You can specify multiple email addresses by separating each email address with a comma. The first email address you specify is the owner for the workflow case.
7. Click **Save**.

Improving IP Address and MAC Address Identification

Asset discovery uses MAC addresses and IP addresses to identify unique assets on the network. In most cases, DOC4000 discovers assets and their MAC address and IP address using a common format without an issue. In some cases, however, DOC4000 may not be able to identify these values and find a match. For those cases, you can configure DOC4000 to look at different properties for the MAC address and IP address.

To specify other properties to use for IP address or MAC address:

1. In the Admin Utility, click the **System Wide Settings** link in the **Ongoing Maintenance** section.
2. In the **IP/MAC Address Properties** field, click the ellipsis (**...**) button.
3. In the **Property names associated with IP Address** field, specify the names of properties to use as the IP address for discovered assets.
4. In the **Property names associated with MAC Address** field, specify the names of properties to use as the MAC address for discovered assets.
5. Click **Save**.

Mapping Known Network Devices and DOC4000 Data Owners

Assets that are discovered across multiple network segments may share the same IP address, which can cause false matches to DOC4000 assets. To resolve this issue, you can define mappings to improve matching. For each known network device, you can identify the DOC4000 data owners associated with that network device.

To specify references that match a known network device to DOC4000 assets:

1. In the Admin Utility, click the **System Wide Settings** link in the **Ongoing Maintenance** section.
2. In the **Devices -** DOC4000 **Asset References** field, click the ellipsis (**...**) button.
3. In the **Device Name** field, type a network device name or select one from the list. The list of devices is available only after network device asset data has been imported.
4. In the DOC4000 **Asset Names** field, type the names of DOC4000 data owners associated with that network device. You can specify multiple names by specifying a comma between the names.
5. Click **Save**.

When saved, the grid view is populated with the mapping information.

Data Integrity

DOC4000 customers import data from their systems on a set schedule. For example, some customers import data from their Distributed Control System (DCS) or Supervisory Control and Data Acquisition (SCADA) systems into DOC4000 daily or weekly, while others may import data monthly or quarterly, depending on how often their systems change. Since this data is imported into DOC4000 using a schedule you configure, you need to know if something goes wrong during the import and what specifically went wrong. Knowing your scheduled import finishes successfully allows you to be more confident in the validity and consistency of the data imported into DOC4000.

To increase the consistency and validity of the data being imported, you need to define a set of standards that are used to evaluate the imported data and the import process itself. These standards are the thresholds used during the evaluation, and how deviations in the following measurements are handled:

- Number of changes identified in the imported data
- Amount of time required to import the data

To evaluate data integrity using these data import threshold values, you need to implement the PAS Workflows asset model. You also need to implement the asset models for your systems from which you import data. For more information, see the *Implementation Guide* for each asset model.

For more information about data integrity, see the following topics:

- *Understanding the Data Integrity System Wide Settings* (page 58)
- *Defining the Workflow Case and Notifications for Data Integrity* (page 59)
- *Defining the Expected Number of Changes During Data Imports* (page 60)
- *Defining the Expected Length of Time for Data Imports* (page 61)

Understanding the Data Integrity System Wide Settings

The **Data Integrity** system wide settings allow you to configure the thresholds by which the validity of data imports is measured. You can also specify the workflows and notifications used when deviations are identified. These settings are defined as follows:

Number of Changes

Defines the range (minimum and maximum number) of total object changes considered normal for each asset model during an import. When the total number of changes in the current import is within the threshold range, no action occurs. If the total number of changes is outside the threshold, more than the maximum or less than the minimum, the workflow case specified in the **Remediation Action** field is created and a Number of Changes notification is sent to the email addresses specified in the **Notify Users** field. For more information, see *Defining the Expected Number of Changes During Data Imports* (page 60).

Import Time Change in Percentage

Defines how much the time to import the data can vary from one import to another and be considered normal. When the time required to import data during the current import is within the threshold percentage specified, no action occurs. If the time required to import data during the

current import increases or decreases from the previous import by more than the percentage specified, the workflow case specified in the **Remediation Action** field is created and an Import Time Change in Percent notification is sent to the email addresses specified in the **Notify Users** field. For more information, see *Defining the Expected Length of Time for Data Imports* (page 61).

NOTE You need to specify an import sequence per asset model in the Number of Changes window so the import time change check is performed for the specified sequence for that asset model.

Remediation Action

Specifies the workflow definition to use to automatically create a case when the number of changes or the time required to import the data for the current import are outside the threshold values you specified. The default is blank (none).

Remediation Location

Specifies the location to set in the workflow case created when a defined threshold for a data import is exceeded. This setting works with the **Remediation Action** field to correctly create the workflow case. The **Remediation Location** allows you to notify the correct set of users, specific to a location within the asset hierarchy, through the workflow case. The email notification includes a link to the case that was automatically created. The default value is blank.

Notify Users

Specifies one or more email addresses to notify when a defined threshold for a data import is exceeded. The first email address you specify is the owner for the workflow case. Use a comma as the delimiter between two email addresses. The default value is blank.

Defining the Workflow Case and Notifications for Data Integrity

Several of the **Data Integrity** system wide settings work together so you can specify the workflow case to create and the users to notify when a defined threshold for a data import is exceeded. For more information about each setting, see *Understanding the Data Integrity System Wide Settings* (page 58).

In the System Wide Settings for **Data Integrity**, the **Remediation Action**, **Remediation Location**, and **Notify Users** fields define how potential data import issues are handled. You specify values in these fields that are used when imported data includes too few or too many changes, or when the import process takes too little or too much time to finish. These conditions can indicate an issue with the imported data.

To define cases and notifications for data integrity:

1. In the Admin Utility, click the **System Wide Settings** link in the **Ongoing Maintenance** section.
2. In **Remediation Action**, select the workflow definition to use to create a case when a data import is outside the expected thresholds and identified as unusual.
3. In **Remediation Location**, select the location to set in the workflow case created when a data import is identified as unusual. This location in the asset hierarchy allows you to notify the correct set of users through the workflow case.

4. In **Notify Users**, specify the email addresses to notify when a data import is outside the expected thresholds and identified as unusual. You can specify multiple email addresses by separating each email address with a comma. The first email address you specify is the owner for the workflow case.
5. Click **Save**.

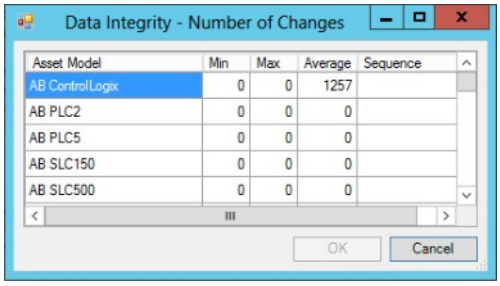
Defining the Expected Number of Changes During Data Imports

In the system wide settings for Data Integrity, the **Number of Changes** values define the range (minimum and maximum number) of total object changes considered normal for each asset model during an import. When the total number of changes in the current import is within the threshold range, no action occurs. If the total number of changes is outside the threshold, more than the maximum or less than the minimum, the workflow case specified in the **Remediation Action** field is created and a Number of Changes notification is sent to the email addresses specified in the **Notify Users** field.

The results of the Number of Changes comparison are recorded in the **History of Imports** table in the **Import Issues** column noted by an icon. For more information, see *History of Data Imports* (page 42).

To specify the expected number of changes values:

1. In the Admin Utility, click the **System Wide Settings** link in the **Ongoing Maintenance** section.
2. In the **Number of Changes** field, click the ellipsis (**...**) button. The **Data Integrity - Number of Changes** window is displayed.



3. Specify the minimum and maximum number of changes you expect by completing the following steps for each asset model:
   a. Review the **Average** column value, which indicates the average number of changes for the most recent data import for all assets of that type.
   b. Click on the cell in the **Min** column of the asset model, and then select the minimum number of changes for that threshold. The default value is 0.
   c. Click on the cell in the **Max** column of the asset model, and then select the maximum number of changes for that threshold. The default value is 0.

      NOTE If you do *not* select a minimum or maximum value, the Data Integrity feature is not activated.

   d. In the **Sequence** column, select the import sequence you selected when you scheduled the data imports of that asset type, such as **All** or **All Sequence**. The import sequence defines what data DOC4000 imports. When an import using the selected sequence

occurs, DOC4000 checks the number of changes and the time required to complete the import.

NOTE If you do *not* select a sequence for an asset model, DOC4000 does not check the number of changes or the import time for those assets.

4. Click **OK**.
5. Click **Save** on the System Wide Settings window.

Defining the Expected Length of Time for Data Imports

In the system wide settings for Data Integrity, the **Import Time Change in Percentage** value defines how much the time to import the data can vary from one import to another and be considered normal. When data is imported into DOC4000, the amount of time to import the data is compared to the amount of time required to import the data during the previous import. When the time required to import data during the current import is within the threshold percentage specified, no action occurs. If the time required to import data during the current import increases or decreases from the previous import by more than the percentage specified, the workflow case specified in the **Remediation Action** field is created and an Import Time Change in Percent notification is sent to the email addresses specified in the **Notify Users** field.

NOTE You need to specify an import sequence per asset model in the Number of Changes window so the import time change check is performed for the specified sequence for that asset model. For more information, see *Defining the Expected Number of Changes During Data Imports* (page 60).

The results of the Import Time Change in Percentage comparison are recorded in the **History of Imports** table in the **Import Issues** column noted by an icon. For more information, see *History of Data Imports* (page 42).

To specify the import time change value:

1. In the Admin Utility, click the **System Wide Settings** link in the **Ongoing Maintenance** section.
2. In the **Import Time Change in Percentage** field, select a value from 0 to 100. The default value is zero (0).
3. In the **Number of Changes** field, click the ellipsis (**...**) button. The Number of Changes window is displayed.
4. Make sure an import sequence is specified in the **Sequence** column for each asset model. Then, click **OK**.
5. Click **Save** on the System Wide Settings window.

File Upload Restrictions

DOC4000 allows users to upload files, such as when attaching a file to a note or to a checklist in a workflow case. The **File Upload** system wide settings allows you to specify which file types users can upload from the DOC4000 web interface.

DOC4000 always allows users to upload files with the standard Microsoft Office file extensions or common image file formats that include `.DOC`, `.DOCX`, `.XLS`, `.XLSX`, `.PPT`, `.PPTX`, `.BMP`, `.JPG`, `.JPEG`, `.ICO`, `.IMG`, `.SVG`, `.PDF`, `.XML`, `.TIFF`, `.GIF`, `.TIF`, `.PNG`, `.VSD`, `.VSDX`, and `.TXT`. If you specify a list of file extensions in the **File Types Allowed to Upload** field, users can upload

those types of files in addition to files with the standard Microsoft Office or common image file extensions.

To add to the list of acceptable file extensions:

1. In the Admin Utility, click the **System Wide Settings** link in the **Ongoing Maintenance** section.
2. In **File Types Allowed to Upload**, click the ellipsis (**...**) button.
3. Type a comma-delimited list of file extensions for files that can be uploaded, and then click **Save**. Files with any other extension, except the standard Microsoft Office and common image file extensions, will *not* be accepted and uploaded.

Vulnerability Management

Identifying and remediating or mitigating known ICS vulnerabilities is one of the best ways to prevent industrial compromises. Given the sophistication and effectiveness of recent industrial incidents, it is more important than ever to implement effective ICS vulnerability management. Cyber DOC4000 provides robust vulnerability and patch management capabilities for complex, multi-vendor industrial facilities. Honeywell, Inc. collects the latest known vulnerability and patch information, and makes it available for you to automatically download and use within Cyber DOC4000.

The system wide settings for vulnerability management allow you to specify a list of email addresses to notify if the import of the latest vulnerability and patch information is not completed successfully. For comprehensive information about vulnerability and patch management, and other Cyber DOC4000 features, see Understanding Vulnerability and Patch Management.

To use vulnerability and patch management, you need to implement the following asset models:

- PAS Cyber DOC4000
- PAS Workflows
- PAS Vulnerability Management
- PAS Patch Management

You should also implement the asset models for your other types of systems. For more information, see the *Implementation Guide* for each asset model.

For more information about vulnerability management, see the following topics:

- *Understanding the Vulnerability Management System Wide Settings* (page 62)
- *Defining Notifications for Vulnerability and Patch Management Data* (page 63)
- Understanding Vulnerability and Patch Management

Understanding the Vulnerability Management System Wide Settings

The **Vulnerability Management** system wide settings allow you to specify a list of email addresses to notify if the import of the latest vulnerability and patch information is not completed successfully. These settings are defined as follows:

CVSS V3 Ratings

Defines the severity level Cyber DOC4000 displays for a vulnerability based on the Common Vulnerability Scoring System (CVSS) score of that vulnerability. The default severity levels are set as shown in the following table. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

Severity Level	Default Minimum	Default Maximum
Low	0.0	3.9
Medium	4.0	6.9
High	7.0	8.9
Critical	9.0	10.0

Notify Users

Defines the list of email addresses that are sent notifications in the event the import of the latest PAS Vulnerability Management or PAS Patch Management asset model are not completed as expected. The latest vulnerability management file should be imported once every 24 hours. The latest patch management file should be imported once every month. Use a comma as the delimiter between two email addresses. The default value is blank. For more information about automating the download and import of the latest vulnerability and patch management information, see Understanding Vulnerability and Patch Management.

Additional DOC4000 settings allow you to refine the risk scores Vulnerability Management displays by customizing impact factors and groups for your environment.

For more information, see the *User Guide*.

Defining Notifications for Vulnerability and Patch Management Data

The PAS Vulnerability Management and PAS Patch Management asset model provide the latest vulnerability and patch information. To provide this information, these asset models are updated and published on a regular basis. The latest vulnerability management file should be imported once every 24 hours. The latest patch management file should be imported once every month. You can automate the download and import of these files. For more information about automating the download and import of the latest vulnerability and patch management information, see Understanding Vulnerability and Patch Management.

In the system wide settings for vulnerability management, the **Notify Users** setting allows you to specify the list of email addresses that are sent notifications in the event the import of the latest PAS Vulnerability Management or PAS Patch Management asset model are not completed as expected.

To define the notifications for vulnerability and patch management data:

1. In the Admin Utility, click the **System Wide Settings** link in the **Ongoing Maintenance** section.

2. In **Notify Users**, specify the email addresses to notify when a data import is not completed within the expected time range. You can specify multiple email addresses by separating each email address with a comma.
3. Click **Save**.

Understanding Data Forwarding and Receiving

Companies have different requirements at various levels within their organizational structure and operational demands:

- While those at the site level are involved in day-to-day operations and change management of their local systems, the centralized engineering group might want to view consolidated information from multiple sites.
- Some groups might want to centrally maintain a complete operational inventory or check what sites have systems that could be susceptible to a particular vulnerability. Operationally, Cyber DOC4000 enables your ability to comprehend and resolve vulnerabilities at both the enterprise and the site levels.
- The central team might want to know which sites have specific control systems when renewing maintenance contracts.

The process of data forwarding securely exports and transports normalized data from each of the source (affiliate/site) DOC4000 installations to one or more destination (enterprise) installations. The destination installations can then receive and import the data.

Use data forwarding and receiving to consolidate various types of information from across your DOC4000 installation. DOC4000 can forward the following types of information:

- Vulnerability information as one or more `CFF` files
- Inventory information as `CFF` and `CSV` files
- Normalization settings as `CFF` files
- System settings (rare)

Data forwarding enables large corporations to consolidate data from site-level installations of DOC4000 into one or more enterprise-level installations. DOC4000 provides two scenarios to implement data forwarding and receiving:

Inventory and Vulnerability Management data (optimized method): data can be processed at the site or enterprise level and forwarded; however, wherever the processing takes place, all of the source objects must be present (where you imported the data).

Inventory data only: data can be exported from either the site or enterprise level and forwarded to the enterprise level for viewing and further processing.

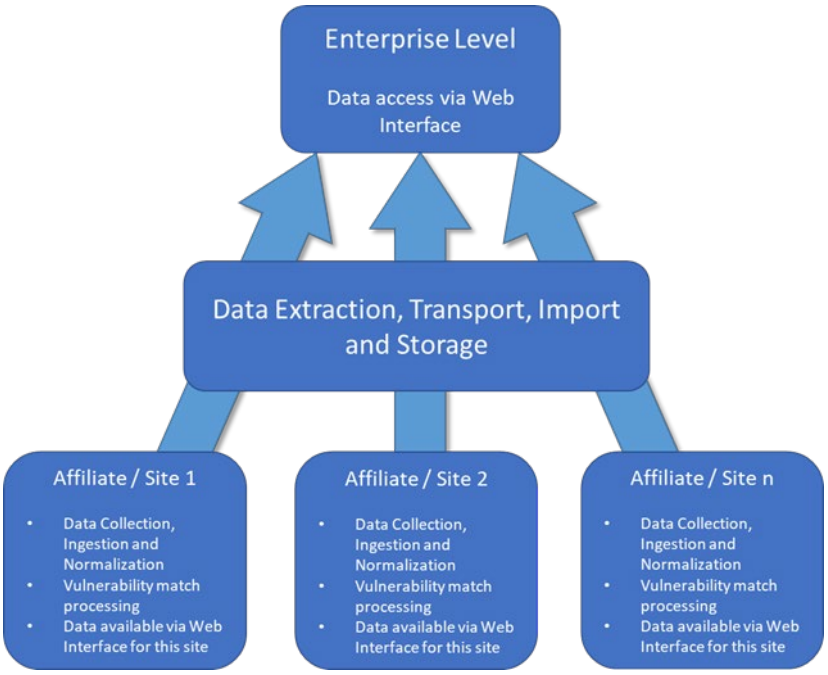
This functionality ensures these deployment scenarios are more easily implemented in a reliable manner, and that no special scripts or customization are required.

Understanding Data Forwarding and Receiving Scenarios

When you configure data forwarding, you define sets of data to export. Each set of data is known as a data group, and it includes data for the assets you define. After transferring the files to the destination DOC4000 installation, you then use data receiving to import the data from a data group to the receiving destination DOC4000 installation.

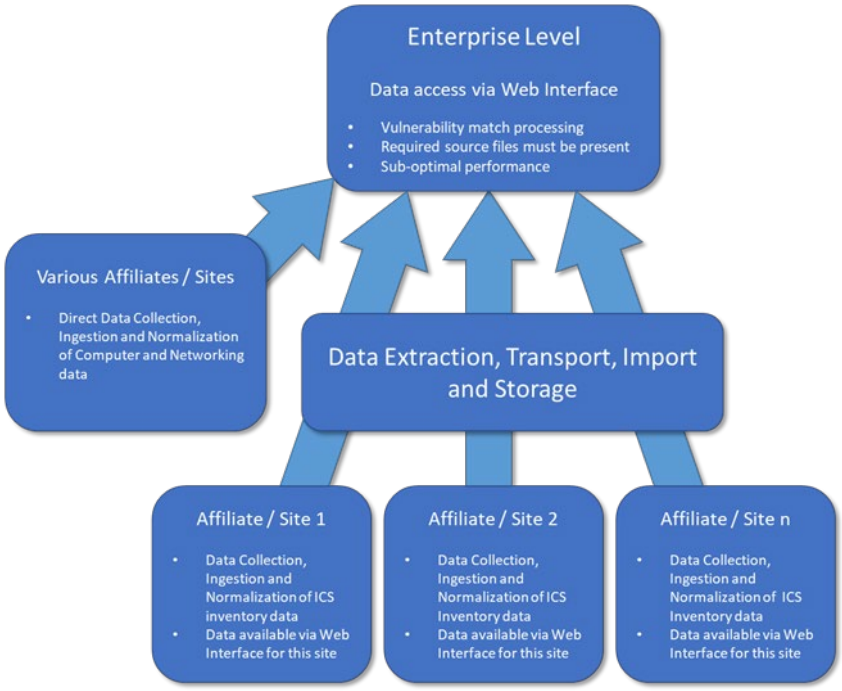
Inventory and Vulnerability Management Data

Your organization might want site-level data forwarded to an enterprise installation of DOC4000. Some forwarded data contains inventory information, and some forwarded data contains processed vulnerability information. Vulnerability data must be processed at the level where the source objects are present.



Inventory Data Only

Your organization might want site data forwarded to an enterprise installation of DOC4000. In this scenario, collect Automation DOC4000 and PCN data for all ICS assets and send `CFF` and `CSV` files to the receiving server. Even if your site uses Vulnerability Management, processing the vulnerability data takes place at the enterprise site after receiving inventory data.



Understanding Forwarded Data

DOC4000 can forward the following types of data:

- Vulnerability data as one or more `CFF` files
- Inventory data as `CFF` and `CSV` files
- Normalization settings as `CFF` files
- System settings (rare)

Vulnerability data

Cyber DOC4000 collects information about your assets and compares it to the latest known vulnerability and patch information, identifying assets to investigate.

Inventory data

An inventory item is an asset or component of an asset, such as an installed software product or a hardware component. The PAS Inventory Items asset model uses information from the other asset models and assets to build a set of inventory items in Cyber DOC4000.

Normalization settings

You can define a single, normalized, name or value when manufacturers, products, or engineering units are represented in different ways in your data. For example, some products in your environment could be represented by Microsoft or Microsoft, Inc. Also, you might have different versions of the same product that you want to see as a single unit.

Normalization rules allow you to identify these multiple variations and set a single, normalized value that represents all the variations. Normalized values apply to search results in Vulnerability Management, Inventory, and Sensor Data Integrity.

You can export and import normalization rule sets to maintain consistency between sites with different DOC4000 servers. To accomplish this scenario, export the rule set to a `CFF` file using data forwarding steps, and then import the rule set from the `CFF` file using data receiving steps.

System settings

Some information you may want to forward is system information, which is not associated with an asset model. To select this information in the Data Forwarding window on the source DOC4000 installation, check the **System** check box and select **System** in the **Assets** list. Then, you can select the object types and properties you want to forward.

To receive system information on the destination DOC4000 installation, you need an asset to associate with the import. Since system information is not associated with an asset model, you can create any type of asset on the destination DOC4000 installation, and then import the data by selecting the correct import folder that contains the system data files. The system information is stored in the correct way on the destination DOC4000 installation regardless of the asset associated with the data import on that installation.

Data Forwarding and Receiving Prerequisites

Data forwarding and receiving has the following prerequisites:

- DOC4000 7.3 or later.

  NOTE If you have configured data forwarding and receiving in DOC4000 7.2 or earlier, your scheduled imports will continue to function. If you need to modify the imports after upgrading to DOC4000 7.3 or later, you should recreate your data forwarding and data receiving configuration, along with any changes to it, using the latest version of the Admin Utility.

- Cyber DOC4000 must be configured. For more information, see Steps for Configuring Cyber DOC4000.
- The asset names must match in both environments and databases.
- The Cyber DOC4000 hierarchy from the enterprise level must include all forwarded assets from the site level.
- The enterprise and site installations should use the same asset model versions for forwarded data.
- For Inventory Items select both assigned and native properties to forward.
- If you are using the Vulnerability Management module in your deployment, when you configure data forwarding and receiving you must use a specific folder structure to ensure that the enterprise level receives vulnerabilities from all the sites. For more information, see *Vulnerability Management Folder Structure Requirements* (page 68).

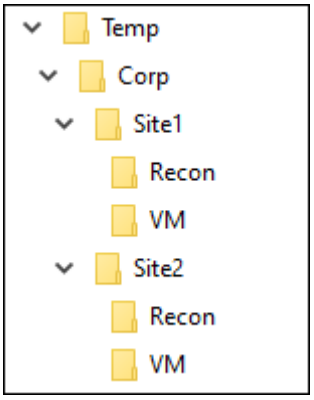
Vulnerability Management Folder Structure Requirements

If your Cyber DOC4000 deployment includes site and enterprise DOC4000 installations that are not connected to each other, and you are using the Vulnerability Management module, you must set up a specific folder structure of files for your data forwarding and receiving. This ensures that the enterprise level Cyber DOC4000 installation accurately reflects all vulnerability data from each site.

You must export the vulnerability data from each site to its own folder for that site, and then import the data to the enterprise site. Segmenting the vulnerability data under each site's folder structure and importing the site data using a single data receiving schedule preserves the data from multiple sites to give your enterprise site an accurate representation of all vulnerabilities.

For example, you have an enterprise site, named Corp, and two remote sites, named Site1 and Site2, that all have Cyber DOC4000 installed with the Vulnerability Management module licensed and running. In this case, you must configure the remote sites to export their vulnerability data to a folder that sits inside the overall site folder that is collecting data to forward to the enterprise site.

To preserve the VM data from each site, import all sites to a single data receiving folder with each site in a separate folder under the corporate data receiving folder.



Planning for Data Forwarding and Receiving

When you configure data forwarding, you define sets of data to export. Each set of data is known as a data group, and it includes data for the assets you define. After transferring the files to the destination DOC4000 installation, you then use data receiving to import the data from a data group to the receiving destination DOC4000 installation.

Data Forwarding Planning

If your DOC4000 deployment consists of sites that are disconnected from the enterprise level DOC4000 installation, you can configure data forwarding and receiving if you want to transfer data from the sites to the enterprise level.

When you configure data forwarding, you define a data group for each site that you want to forward to the top level installation of DOC4000 in your environment. In the data group, you define the assets and object types you want to forward. DOC4000 creates and writes a set of `CFF` files and a `NewFiles.txt` file to the export folder using the data group name as a subfolder. Some assets or object types might create additional files, such as `CSV` files. Copy everything from the data forwarding folders to the destination DOC4000 installation. After transferring the files to the

destination DOC4000 installation, you can import those files to the other DOC4000 server or data collector where you configured data receiving for that set of assets.

NOTES

- If you are using data forwarding in a multi-site environment (site and enterprise), the following requirements apply:
  - The asset names must match in both environments and databases.
  - The Cyber DOC4000 hierarchy from the enterprise level must include all forwarded assets from the site level.
  - The enterprise and site installations should use the same asset model versions for forwarded data.
  - For Inventory Items select both assigned and native properties to forward.
- If you are using the Vulnerability Management module in your deployment, you must use a specific folder structure to ensure that the enterprise level receives vulnerabilities from all the sites. For more information, see *Vulnerability Management Folder Structure Requirements* (page 68).

One step in your planning is to decide on a method to securely and regularly transfer the files from sites to destinations. Some options to consider include:

- Use a secure file transfer application, such as Data Collection Control Center or Data Transfer Utility
- Write a script to transfer files using SFTP
- Manually transfer files or use an in-house application

The **Data Forwarding** link in the Admin Utility allows you to configure the properties for forwarding data from a source installation of DOC4000. For each data group you create, you select the assets, object types and properties to forward and specify where to store those files. DOC4000 creates the schedule for creating those data files. Then, you enable the schedule and make any needed changes.

The **Data Receiving** link in the Admin Utility allows you to configure the properties for receiving forwarded data at a destination installation of DOC4000. For each destination, create a data group and define the location where you plan to copy data forwarding files. DOC4000 creates the schedule for importing those data files. Then, you enable the schedule and make any needed changes. After you enable the schedule, DOC4000 imports the latest data files when it detects the `NewFiles.txt` file in the configured folder location. In most cases, you should need a single data receiving schedule to import data from separate sites or plants. In a few cases, you might have multiple schedules to accommodate importing data that is collected a different intervals. If you have more than one schedule for data receiving, make sure to allow enough time for each schedule to complete.

The last step is to implement your chosen method to transfer the files from sites to destinations.

Data Receiving Planning

After you configure data forwarding, you create a data group (schedule) in each destination installation of DOC4000 where you want to consolidate asset data you forward from the source DOC4000 installations. Use the **Data Receiving** link in the Admin Utility on the destination installation of DOC4000 to create a data group and define the folder where the source data is stored. The data for the assets is a set of folders containing `CFF` files and a `NewFiles.txt` file. Some assets or object types might create additional files, such as `CSV` files. Copy everything from

the data forwarding folders to the destination DOC4000 installation. DOC4000 creates the import schedule as disabled and with the schedule set to **Auto**, which checks for the `NewFiles.txt` file, and imports the data when it finds that file after you enable the schedule.

In most cases, you should need a single data receiving schedule to import data from separate sites or plants. In a few cases, you might have multiple schedules to accommodate importing data that is collected at different intervals. If you have more than one schedule for data receiving, make sure to allow enough time for each schedule to complete.

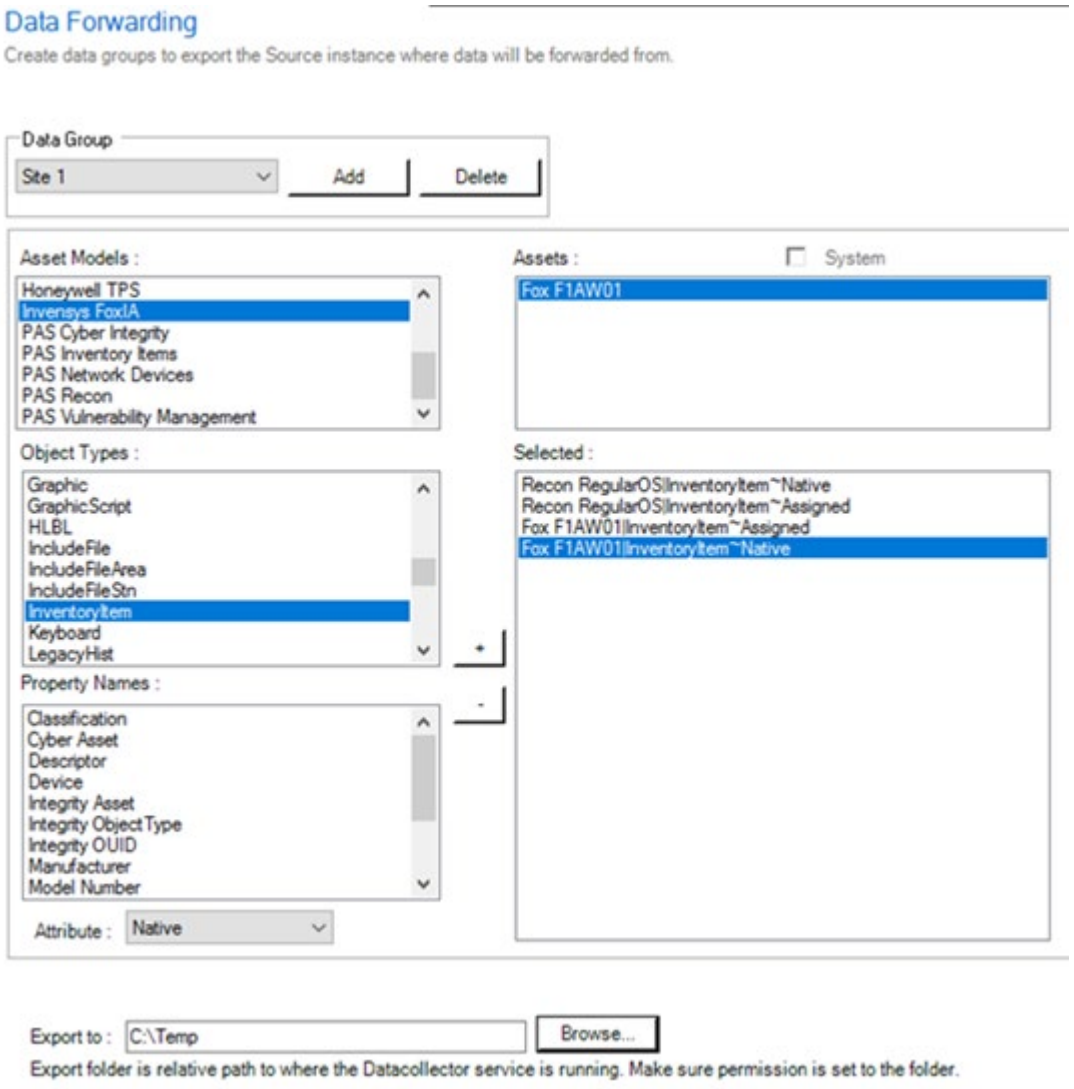
NOTES

- If you are using data forwarding in a multi-site environment (site and enterprise), the following requirements apply:
  - The asset names must match in both environments and databases.
  - The Cyber DOC4000 hierarchy from the enterprise level must include all forwarded assets from the site level.
  - The enterprise and site installations should use the same asset model versions for forwarded data.
- If you are using the Vulnerability Management module in your deployment, you must use a specific folder structure to ensure that the enterprise level receives vulnerabilities from all the sites. For more information, see *Vulnerability Management Folder Structure Requirements* (page 68).

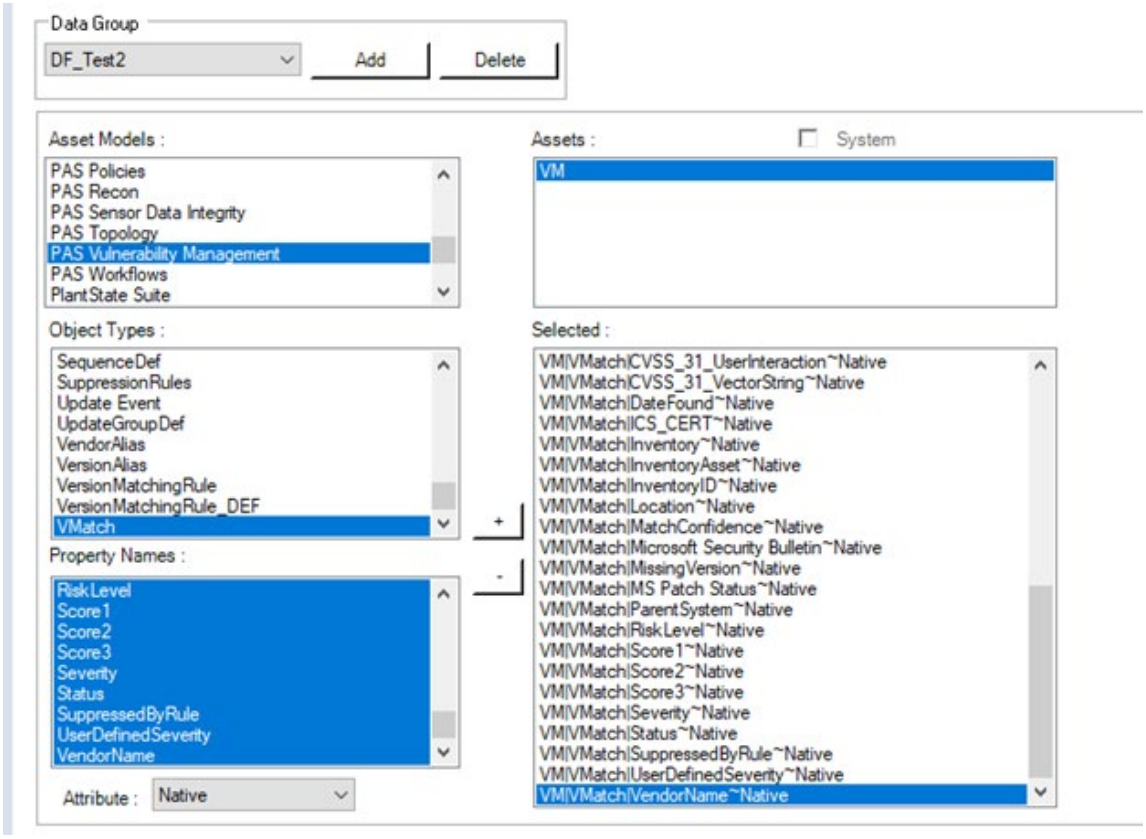
Configuring Data Forwarding

The following images show examples of data forwarding configuration.

Inventory forwarding example



Vulnerability forwarding example



Use this procedure for step-by-step guidance:

1. In the Admin Utility on the source DOC4000 server, click the **Data Forwarding** link in the **Additional Modules** section. The **Data Forwarding** window is displayed.
2. Click **Add**.
3. Type the name for the data group, and then click **OK**. Since each data group is for a site, you should name the group in a way that identifies the site and its data.
4. In **Asset Models**, select the type of asset, such as Invensys FoxIA or PAS Vulnerability Management.
5. In **Assets**, select the specific asset whose data you want to forward, such as PAS Inventory or VM.

   NOTE If you want to forward system information, which is not associated with an asset model, check the **System** check box, and then select **System** in **Assets**.
6. In **Object Types**, select an object type whose data you want to forward. For example, select **InventoryItems** to forward inventory data and select **VMatch** to forward vulnerability data.
7. If you want to select only some properties to forward, in **Property Names**, select one or more properties whose data you want to forward.

   NOTE If you want all the properties, do *not* select any properties.
8. In **Attribute**, select whether you want to select **Native** or **Assigned** properties. Assigned properties are defined by the asset model. In most cases, select **Native**.

NOTE For Inventory Items select both assigned and native properties to forward.

9. Click the plus sign (**+**).
10. In **Export to**, type the path or browse to the folder where you want to create the `CFF` files for the selected data group.

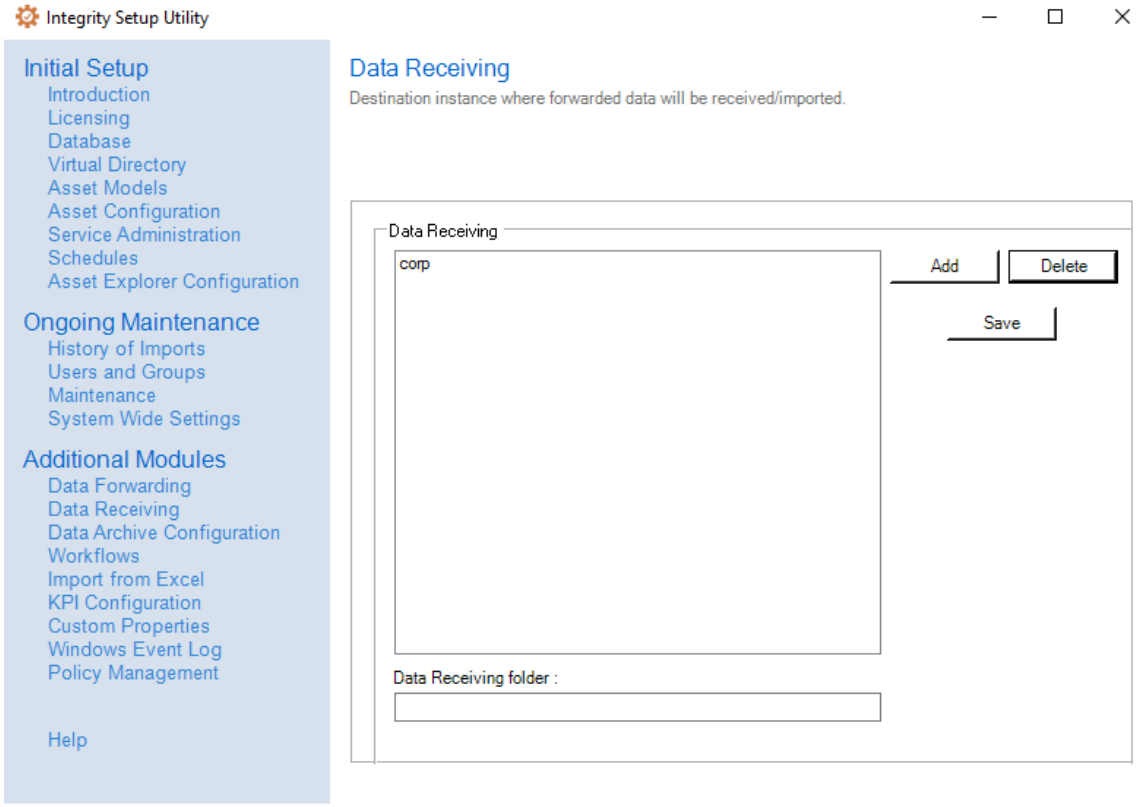
    NOTE Each data group contains separate folders named for the assets selected for the data group.
11. Click **Save**.
12. Click **OK** on the Data Forwarding message window. This message indicates a schedule has been created for generating the data files. By default, the schedule is disabled so you can edit the schedule to run on the interval you want.
13. Click **Schedules** in the left pane of the Admin Utility. The Schedule Imports and Monitor Progress window is displayed. The data forwarding schedule is listed with the name `Schedule-`*datagroup*.
14. Select the schedule that was created, and then click **Edit**.
15. On the General tab, check **Enabled**.
16. On the Schedule tab, specify the interval you want to use for creating the data files, such as once a week, and then click **OK**. You can choose **One Time Only** and **Run Now** to test the schedule and review the generated files.

    NOTE Some assets depend on regular imports to run to gather data. Make sure you consider these assets and their required imports when setting the data forwarding schedule. For more information, see the *Implementation Guide* for each asset.
17. After you have the generated files, move them to the folder on the destination DOC4000 installation associated with the group you created on the destination to receive the data.

Configuring Data Receiving

Use this procedure for step-by-step guidance:

1. In the Admin Utility on the destination DOC4000 server, click the **Data Receiving** link in the **Additional Modules** section. The Data Receiving window is displayed.



2. Click **Add**, and then enter a name for the data receiving schedule and the folder where the data receiving files reside.

   NOTE In most cases, you should need a single data receiving schedule to import data from separate sites or plants. In a few cases, you might have multiple schedules to accommodate importing data that is collected at different intervals. If you have more than one schedule for data receiving, make sure to allow enough time for each schedule to complete.

3. In **Data Receiving folder**, review the folder specified for the selected asset and make sure the data files (`*.CFF` and `NewFiles.txt`) for the data group from the source DOC4000 installation are in that folder.

   NOTE Some assets or object types might forward additional files, such as `CSV` files.

4. Click **Save**.
5. Click **OK** on the Data Receiving message window. This message indicates a schedule has been created for importing the data files. By default, the schedule is disabled so you can edit the schedule to run as you want.
6. Click **Schedules** in the left pane of the Admin Utility. The data receiving schedule is listed with the name `Schedule-`*data receiving group*, where *data receiving group* is the name of the schedule you defined for data receiving on the destination DOC4000 installation.
7. Select the schedule that was created, and then click **Edit**.
8. On the **General** tab, check **Enabled**.

9. On the **Schedule** tab, specify the interval you want to use for importing the data files, and then click **OK**. By default, the schedule is set to **Auto**, which means that after you enable the schedule, the import occurs automatically when there is a `NewFiles.txt` file in the specified data receiving folder.

Understanding Schedules for Data Forwarding and Receiving

When you configure data forwarding, DOC4000 creates an export schedule with a name that matches the data group on the source DOC4000 installation. This schedule is disabled by default to allow you to set the frequency and start time to meet your needs before you enable the schedule. For example, if you have inventory imports that run on a regular schedule, you might want to set the data forwarding schedule to run after those imports complete. This flexibility allows you to meet your specific needs and transport the files to the destination together or separately.

When you configure data receiving, DOC4000 creates an import schedule named with the configured data receiving names on the destination DOC4000 installation. This schedule is disabled by default to allow you to set the frequency and start time to meet your needs before you enable the schedule. These schedules allow you to import the forwarded data files as you need. In most cases, you should need a single data receiving schedule to import data from separate sites or plants. In a few cases, you might have multiple schedules to accommodate importing data that is collected a different intervals. If you have more than one schedule for data receiving, make sure to allow enough time for each schedule to complete.

Understanding Import Data Archives

DOC4000 allows you to archive data files after each data import to assist you with disaster recovery. After data files are processed for an asset during an import, DOC4000 can create a zip file of those data files and store the zip file in the location you specify. DOC4000 also saves the latest zip file for each asset in a database. You specify the number of zip files you want to save. For example, DOC4000 can save the last three sets of data files imported for each asset.

The **Data Archive Configuration** link in the Admin Utility opens the Archive Data window, which allows you to configure import data archiving, as well as restore a set of data files to a folder you specify so you can review the data files for an asset.

When you first open the Archive Data window, DOC4000 detects whether a database for import data archiving has been created. If not, you can specify the database to create or use and the credentials for accessing the database.

After you define the import data archive database, you can enable data archiving, configure the number of import data archive zip files to save and where to store your primary archive, and you can check how many import data sets you have archived for each asset.

After you have archived at least one set of import data files, you can restore a set of import data files to the folder you specify. This restore feature allows you to review and recover data files you collected for an asset and imported into DOC4000.

If you have multiple data collectors managing assets and you enable data archiving, you must configure data archives for each data collector to have complete archives for your environment. On each data collector, use the Admin Utility to configure the data archive settings for the assets that are set to import to DOC4000 from that data collector. For example, your TPS asset data imports run on data collector Alpha, while your DeltaV asset data imports run on data collector

Beta. You must configure the data archive settings on both data collectors to create the archives for your TPS and DeltaV assets.

For more information about import data archives, see the following topics:

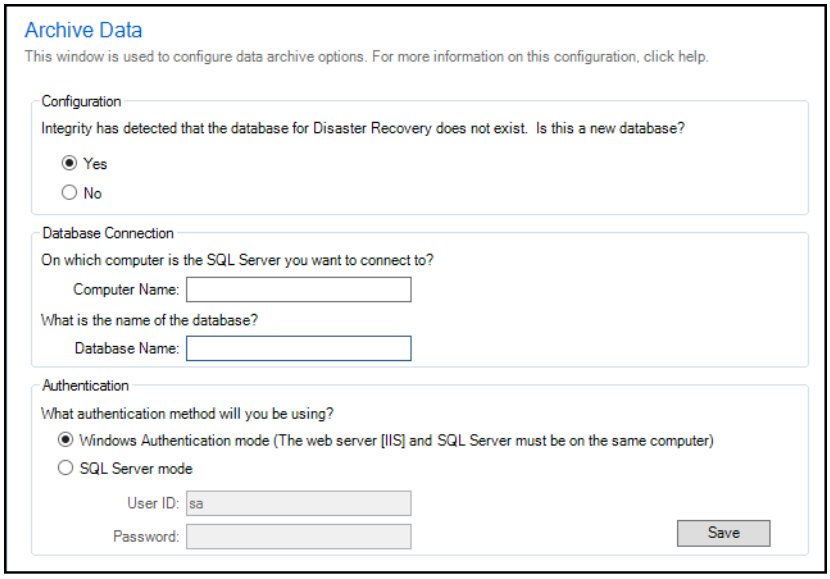
- *Creating the Database for the Import Data Archive* (page 76)
- *Configuring the Import Data Archive* (page 77)
- *Checking the Status of the Import Data Archive* (page 78)
- *Restoring an Import Data Archive* (page 78)

Creating the Database for the Import Data Archive

DOC4000 uses a database to track import data archiving and to store the latest import data archive zip file for each asset. You need to specify the database to create or use for import data archiving, and the authentication method and credentials for accessing the database.

To create the import data archive database:

1. In the Admin Utility, click the **Data Archive Configuration** link. DOC4000 detects whether a database for import data archiving has been created. If a database has not been specified, the Archive Data window is similar to the following image.



2. In **Configuration**, specify whether you want to create a new database (**Yes**) or use an existing database (**No**).
3. In the **Database Connection** area, indicate the **Computer Name** (SQL Server name) and **Database Name**. If the Microsoft SQL Server installation where the import data archive database will be located is a named instance, type the server name followed with a backslash and the instance name in the **Computer Name** field, such as Server*Instance*.

   The database name must begin with a letter or underscore. Database names can contain only letters, numbers, underscores, dashes, and periods. No special characters can be used.

4. In the **Authentication** area, indicate whether DOC4000 should log in to Microsoft SQL Server using your Windows account or a specified SQL Server user ID and password. If you select **SQL Server mode**, type the user ID and password defined within SQL Server.

   NOTE For either authentication mode, the user account must have the **dbcreator** (min) or **sysadmin** fixed server role and must be assigned the **db_owner** database role. Use SQL Server Management Studio to assign the **db_owner** database role to the account you specify.

5. Click **Save**.

After the database is created and defined, the Archive Data window displays different options so you can configure import data archiving. For more information, see *Configuring the Import Data Archive* (page 77).

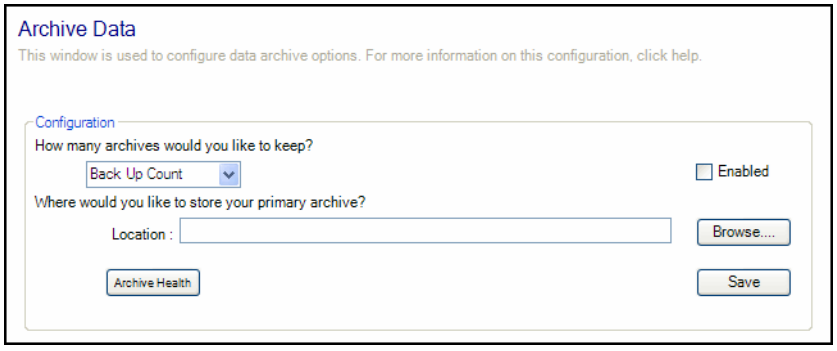
Configuring the Import Data Archive

After you define the import data archive database, you can enable data archiving, configure the number of import data archive zip files to save, and define where to store your primary archive zip files. You can also check the health of the import data archive. For more information, see *Checking the Status of the Import Data Archive* (page 78).

After you enable data archiving and specify a data archive location, DOC4000 automatically archives the data files from all imports after each import finishes. Following each successful import for each asset, a folder with the asset name is created in the location you specified if that folder does not already exist. Then, a zip file containing a copy of the imported files is added to the folder. The zip file name identifies the asset name and the date and time of the import. If more zip files for the asset exist than you specified to keep, the oldest zip file in that asset folder is deleted.

To configure the import data archive:

1. In the Admin Utility, click the **Data Archive Configuration** link. DOC4000 detects whether a database for import data archiving is defined. For more information, see *Creating the Database for the Import Data Archive* (page 76). If a database is defined, the Archive Data window is similar to the following image.



2. In the **How many archives you would like to keep** field, select the number of import data zip files (1-10) you want to store for each asset. When the number of data import archive zip files for an asset reaches this number, the oldest archive is deleted before the latest zip file is stored. Increasing this number increases the amount of disk space required to store these archive files.

3. In the **Location** field, type the folder location where you want to store the import data archive zip files. You can also browse to the location. The folder you specify must already exist and DOC4000 must have full read and write permissions. Avoid mapped drives, which are defined

by user. When a data import for an asset finishes, the zip file is stored in the folder for this asset.

4. Check the **Enabled** check box to enable the data archive process. Then, click **Save**.

Checking the Status of the Import Data Archive

After the import data archive database is defined and you start archiving the import data for your assets, you can check the health of the import data archive. This information includes the amount of disk space used by the archive zip files, the remaining amount of disk space available, and the number of import data sets archived for each asset.

To view the status of the import data archive:

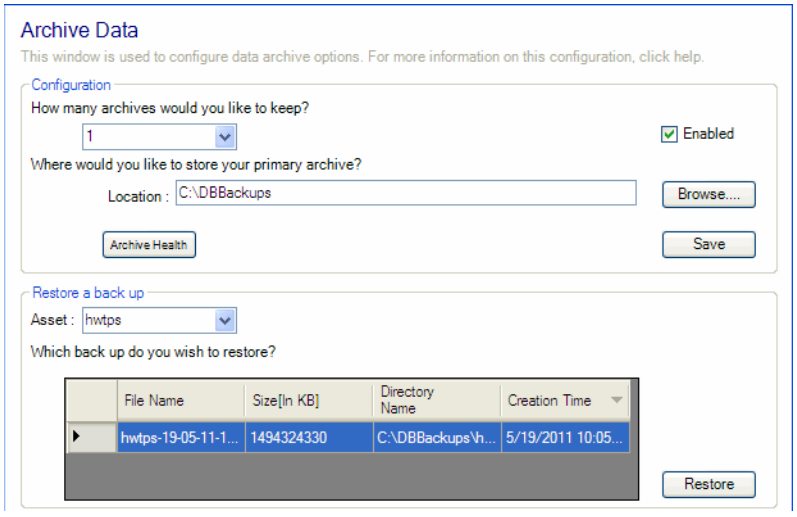
1. In the Admin Utility, click the **Data Archive Configuration** link.
2. Click **Archive Health**.
3. If you want to review the archive size and count for a specific asset, select the asset in the **Asset Specific** field.

Restoring an Import Data Archive

After you have archived at least one set of import data files, you can restore a set of import data files to the folder you specify. This restore feature allows you to review and recover data files you collected for an asset and imported into DOC4000.

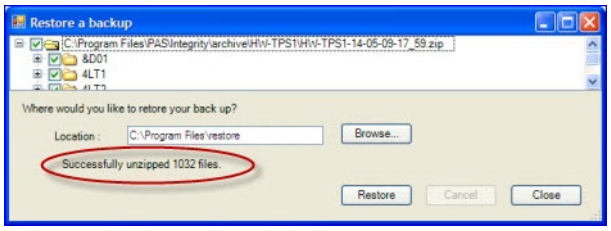
To restore an archived set of import data:

1. In the Admin Utility, click the **Data Archive Configuration** link.
2. In the **Restore a backup** section, select the asset in the **Asset** field. The **Restore a backup** section is not available until at least one import is completed and its import data is archived.



3. In the **What backup do you wish to restore** table, select the zip file to restore by clicking in the column to the left of the **File Name**.
4. Click **Restore**.

5. On the Restore a Backup window, select the check box next to the zip file name to restore all files in the backup. To restore individual folders or files in the backup, click the plus sign (**+**) to expand folders if needed, and then select a subset of the archived files.
6. In the **Location** field, type the folder location where you want the files to be restored. You can also click **Browse** to browse to the location. The folder you specify must already exist and DOC4000 must have full read and write permissions. Avoid mapped drives, which are defined by user, unless you have full read and write permissions on the mapped drive.
7. Click **Restore**. A status bar is displayed during the restore process and a message is displayed when the files have been successfully restored.



8. Review the restored files, and if needed, import the data to DOC4000 using the appropriate data collector per asset for any asset data that you need to recover.

SECTION 4

Creating and Configuring Workflow Definitions

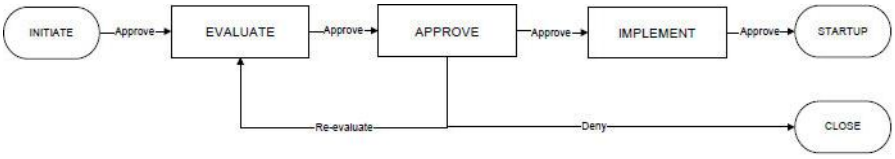
Workflow definitions identify the information required to support common work processes associated with managing and responding to information in DOC4000. A workflow definition identifies each step (state) in the process and it determines whether the process is ready to move to the next step. Once configured, a user can create a case based on a workflow definition. The case provides a set of fields, known as common fields, that describe the work to be completed and allow the user to add information about the work. The case uses the states, checklists, and transitions defined by the workflow definition to follow the work process.

For more information about workflow definitions, see the following topics:

- *Understanding States, Transitions, and Checklists* (page 80)
- *Sample Workflow Templates* (page 81)
- *Understanding Workflow Case Numbering* (page 82)
- *Steps for Workflow Configuration* (page 83)

Understanding States, Transitions, and Checklists

Each workflow definition includes a *beginning* workflow state, one or more additional states, one or more transitions per state, and one or more *end* states. The states defined for a workflow definition are the major steps in the process, such as Initiate, Evaluate, and Implement. For example, consider the following example process.



Each workflow has one beginning state, which is the first state you add to a workflow definition. Each workflow can have only one beginning state. In the previous example, Initiate is the beginning state.

Each workflow has a set of states that identify the desired path. These states and the transitions along the desired path are known as the normal path. In the previous example, Initiate, Evaluate, Approve, Implement, and Startup are the normal path.

You can include additional states and transitions in a workflow to define alternate paths. When you view the progress indicator for a workflow, states in an alternate path are indicated by an alternate color.

Each workflow definition can have one or more end state. Once a workflow case reaches an end state, the case is complete and excluded from the list of active workflows. In the previous example, Startup and Close are end states.

A transition provides a link from one state to the next state. Transitions identify the benchmarks or milestones achieved so the process is ready to advance. Transitions are assigned a *From* state and a *To* state. You can also configure email alerts for each transition with notes pertaining to the transition. In the previous example, an Approve transition for the Initiate state links to the Evaluate state and indicates that once the Initiate state is completed and approved, the evaluation process can begin. The Approve state has the following possible transitions: Approve, Re-evaluate, and Deny.

To document the transition from state-to-state, you can create a checklist that must be completed prior to a state being completed. Each checklist can include a variety of items, such as check boxes, radio buttons, text fields, and signatures. When a case is assigned to a user, that user completes the checklist for the current state and can indicate when it is ready for approval.

Sample Workflow Templates

Workflows allow you to document work processes involved with configuration management for your industrial control system (ICS) and other assets managed within the configuration database. You can start a workflow case manually or based on condition changes within the database. You can also associate a workflow with changes.

For example, you can configure a workflow to detect changes within the configuration database. To ensure each change is reviewed and approved, you can link an asset change to an administrative approval of a workflow reconciliation.

DOC4000 provides several sample workflow templates to meet security best practices and common compliance criteria. To avoid overwriting a sample template, save a template as a new workflow definition, and then modify the new definition.

To use a sample workflow template, you need to complete several configuration tasks. The following list summarizes the sample workflow templates:

Asset Disposal Workflow

Documents the chain of custody of handling an asset as it is removed from service. The workflow is active until all sensitive information on the device is wiped and the supporting evidence of the destruction of the information is documented and attached to the Asset Disposal case number.

Configuration Change, Implementation

Documents the process to implement a change in a production system. This process includes the configuration change and any related configuration policy changes. If a **Configuration Change, Testing** case initiated the **Configuration Change, Implementation** case, the testing case number is included in the implementation case notes.

Configuration Change, Testing

Documents the process to test a proposed change and capture the test results for compliance requirements. If the proposed change identifies a defect in the configuration policies, the workflow covers the modification to the configuration policy and the approval steps for the policy change. If a workflow case has an associated configuration policy, a **Configuration Change, Implementation** case is created when the **Configuration Change, Testing** case is closed. The implementation case covers all assets that are monitored by the configuration policy, and it is associated with each location.

Periodic Review

Notifies owners of documents, reports, and lists that need to be reviewed at a certain frequency. For an example Annual Review, when there are 30 days left before the anniversary of the last approval date, the workflow starts a case, runs the report, and sends the report to the owner for review. The trackable case is associated with the review, and once the review has been completed, the next review date is set.

Security Incident Response

Documents security incidents based on your specific incident response procedure. The workflow incorporates all internal and regulatory notifications, captures the following steps, and includes the ability to document the lessons learned while updating the mitigation steps and incident response procedures:

- **Assessing**: Identifying and investigating an issue to determine whether there is an incident based on a set of configurable rules.
- **Classifying**: Identifying the threat level and severity of the incident.
- **Declaring**: Notifying the stake holders about the incident.
- **Containing**: Performing the steps to contain the threat and stop the attack.
- **Restoring**: Performing the steps required to return to normal operations.

Vulnerability Assessment

Guides patch management tasks, including evaluating and applying patches to mitigate vulnerabilities.

Understanding Workflow Case Numbering

By default, DOC4000 provides a unique, generated number as the case number. The case number must be unique, so DOC4000 uses the current date and an index number to create the default case number.

With the PAS Workflows asset model version 2.5.1 or later, the `CreateCaseID` function provides additional case numbering support for a prefix value and a manually specified case number. If you are using a previous version of the PAS Workflows asset model, contact Technical Support for assistance with updating your `CreateCaseID` function.

You can also modify the case numbering function to create the case numbering you want. The `CreateCaseID` function definition in the PAS Workflows asset model can be modified through Asset Model Builder. When you modify the `CreateCaseID` function, you can also incorporate common fields with names that you define.

Prefix for the Case Number

When you define a workflow, you can specify a prefix for all cases that use that workflow. On the Workflows page in the Admin Utility, select the workflow and then specify the prefix value in the **Prefix** field in the **Workflow Details** area of the window. If you leave the **Prefix** field blank, DOC4000 does not use a prefix for cases that use that workflow. DOC4000 applies the prefix value to the case number using the following format:

prefix-YY-*number*

- *prefix* - Identifies the prefix for the workflow. If you do not specify a prefix, DOC4000 does not include the prefix or the hyphen at the start of the number.
- `YY` - Indicates the two-digit year, such as 18 for 2018.
- *number* - Identifies the unique number for the case. If you choose to use a manually specified case number, this portion of the case number is controlled by the rules for that specified value.

Manually Specified Case Number

If you want to allow users to manually specify the case number for a new case, you can create a **Case Entry #** common field. The name of the common field must be **Case Entry #** and you must check the **Case Type filter when starting a new case** check box for that field. You can create one global **Case Entry #** common field, or you can create a category-specific **Case Entry #** common field in one or more categories. For more information, see *Defining Common Fields* (page 84).

When a user creates a case, DOC4000 can prompt the user for the **Case Entry #**. The user can specify an alphanumeric value, up to 100 characters, and DOC4000 then uses the specified value as the case number. If the specified value is not unique, DOC4000 appends a three-digit index number to the end of the specified value to make it unique.

If you do not specify a prefix and you use the default case numbering without the **Case Entry #** common field, or if the user does not specify a value in the **Case Entry #** common field, DOC4000 sets the case number to a unique numeric value without hyphens.

NOTE If a user specifies a **Case Entry #** value of more than 100 characters, processing errors can occur.

Steps for Workflow Configuration

To make workflows available in the DOC4000 web interface, you need several items:

- Your DOC4000 license must include workflows.
- An administrator needs to load the PAS Workflows asset model. This model is a customer model, which stores implementation details within the model. Therefore, once you load and configure the PAS Workflows asset model, you should not upgrade this asset model. For more information, see *Loading (Importing) Asset Models* (page 32).
- An administrator must create and configure one or more workflow definitions using the Admin Utility.

The following list guides you through the remaining topics in this section to create the specific workflow definitions you need.

1. Identify your work processes for which you want to use workflow cases to document, track, and streamline the process. In some areas, such as change tracking, the product can use workflows to extend the functionality. For more information about configuring workflows for specific features, see the following topics:
   - *Configuring Change Tracking Workflows* (page 103)
   - *Configuring Patch Management Workflows* (page 107)
   - *Configuring a Vulnerability Management Workflow* (page 116)
   - *Configuring Baseline Workflows* (page 118)

1. Define common fields to use in workflow cases. The common fields describe the work to be completed and allow the user to add information about the work. You must at least define a location field. For more information, see *Defining Common Fields* (page 84) and *Defining the Location Common Field for Workflows* (page 87).
2. Review the default workflow case numbering. If you want to customize this numbering, define the common fields you need. You can also modify the `CreateCaseID` function to meet your specific needs. For more information, see *Understanding Workflow Case Numbering* (page 82).
3. Create checklists to use for completing specific states (stages) within workflows. For more information, see *Creating Checklists for Workflows* (page 89).
4. If you want to use PSS data within a workflow definition, specify the PSS server in the DOC4000 configuration file. For more information, see *Using PlantState Integrity (PSI) Data within Workflow Definitions* (page 92).
5. Create the workflows you need. For more information, see *Creating a Workflow Definition* (page 93).
6. If you want to use case type selection fields to determine which workflow to use when creating a case, set the values for each case type common field that are associated with a defined workflow. For more information, see *Configuring Case Type Selection Properties* (page 95).
7. Specify which users and groups are assigned to checklists and transitions. For more information, see *Assigning Users to Transitions and Checklists* (page 96).
8. Set up email notifications. For more information, see *Configuring Email Message Templates* (page 97), *Configuring Email and Approval Rules* (page 98), and *Configuring Email Notifications for Errors* (page 99).
9. Select the types of objects that can be associated with a case. For more information, see *Associating Object Types with a Case* (page 101).

The following topics provide additional information about workflows:

- *Viewing the Transition Event Log* (page 102)
- *Viewing the Email Queue* (page 103)
- *Configuring Change Tracking Workflows* (page 103)
- *Configuring Patch Management Workflows* (page 107)
- *Configuring a Vulnerability Management Workflow* (page 116)
- *Configuring Baseline Workflows* (page 118)

Defining Common Fields

When a user creates a case, the user can select a workflow definition for the case. Then, the case can be updated as each state of the workflow is achieved. The **Define Common Fields** link on the Workflows window in the Admin Utility allows you to create and define fields that can be displayed and updated as part of the case. You can also define some of these fields to be included in Request for Approval emails and Notification emails.

When you add a field, you can add it as a **Global field** or a **Category-specific field**. Global fields are shared and displayed in all cases, regardless of the workflow category. Category-specific fields are displayed only in workflow cases of that category.

NOTE To create an additional category, you need to create a workflow, type the new category in the **Category** field, and then save that workflow.

In addition to the fields you create for your specific needs, DOC4000 allows you to create fields it uses for case management, such as case numbering and location. You need to select the proper options for these fields:

Case numbering

DOC4000 provides a unique, generated number as the case number. You can modify the case numbering feature to create the case numbering you want. For more information, see *Understanding Workflow Case Numbering* (page 82).

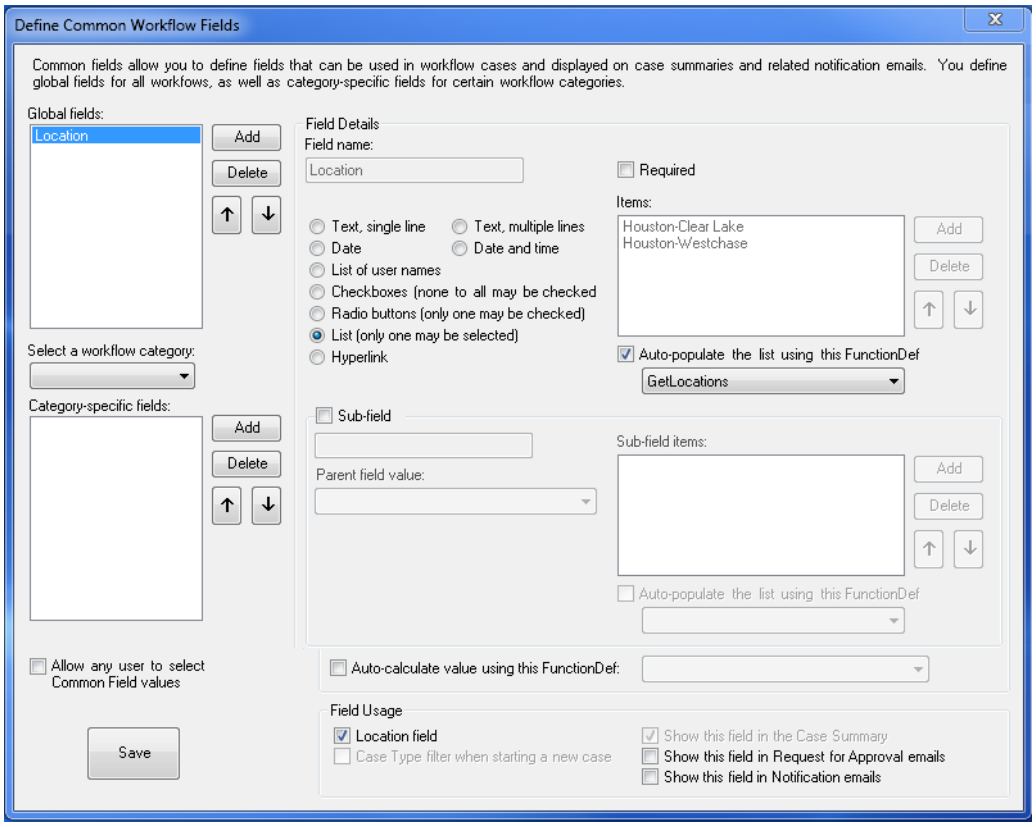
Case location

DOC4000 requires the location for a case, and you must define a location field as a **Global field**. To set a field as the location field, check the **Location field** check box for that field. The field should be a list of values to select. You can also use the `GetLocations` function definition in the PAS Workflows asset model to list the location values defined through Asset Model Builder for that function. This function can also get these locations from objects in your asset hierarchy. For more information about defining the location field, see *Defining the Location Common Field for Workflows* (page 87).

To define a common field:

1. In the Admin Utility, click the **Workflows** link.

2. On the Workflows window, click the **Define Common Fields** link in the **Workflow-related Tasks** area. The Define Common Workflow Fields window is displayed.



3. Select which type of field you want to create:
   - To create a field for all categories of workflow cases, click **Add** next to the **Global fields** list.
   - To create a field for one category of workflow cases, select the category in the **Select a workflow category** field, and then click **Add** next to the **Category-specific fields** list.
4. Type a name for the field, and then click **OK**. Make sure the name indicates the type of information for the user to type. The new field should be selected in its list.
5. In the **Field Details** area, select the type of data for the field, such as **Text**. If you select **Hyperlink**, any URL the user types in this field, starting with `http://` or `https://`, will be a link to that URL.
6. If you want the field to be required, check the **Required** check box.
7. If you selected Check boxes, Radio buttons, or List as the data type, you need to specify the values for the selected field type by adding them to the **Items** list:
   a. If you want to manually add values, click **Add** next to the **Items** list, type the value, and then click **OK**. You can add as many items as you need.
   b. If you want to use a function definition to define the values, you can associate the field with a function definition in the PAS Workflows asset model. To create or modify a FunctionDef in the PAS Workflows asset model, use Asset Model Builder. Then, check the

Auto-populate the list using this FunctionDef check box and select a FunctionDef from the list.

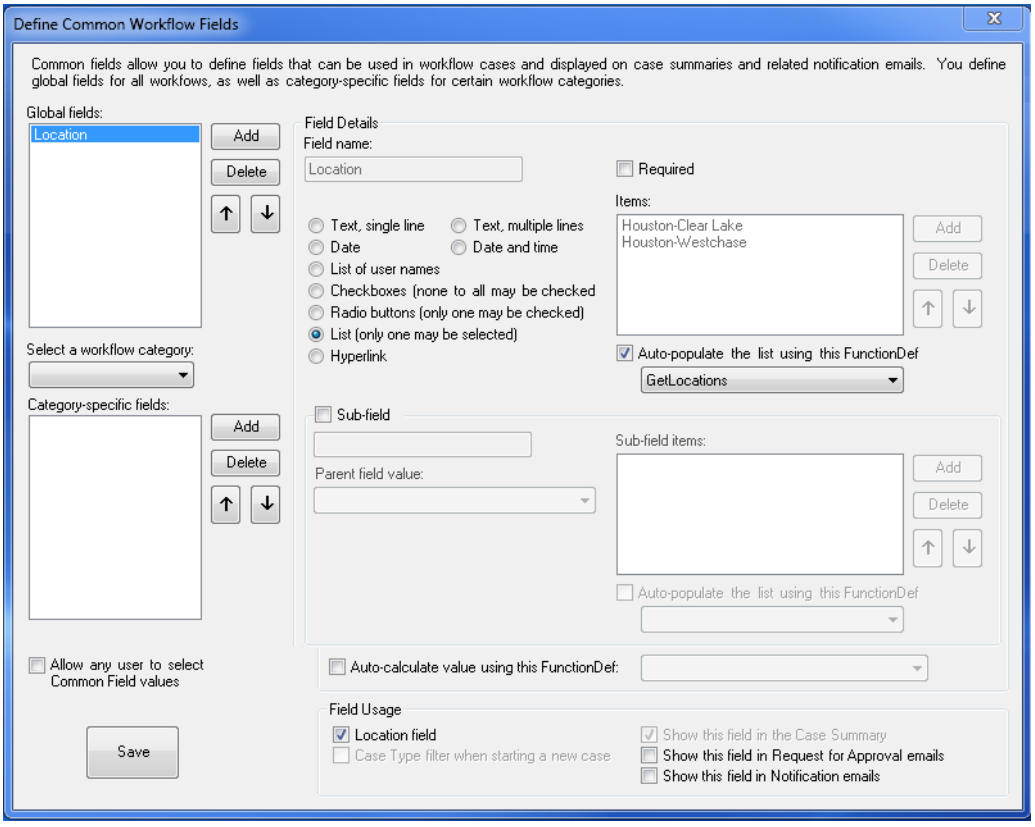
NOTE For more information about creating or modifying a FunctionDef with Asset Model Builder, see *Defining the Location Common Field for Workflows* (page 87) or contact Technical Support.

8. If you would like to add sub-fields for a List field, complete the following steps:
   a. Click **Save** to save the current field definition.
   b. Check the **Sub-field** check box and type a name in the text box.
   c. Select a **Parent** field value.
   d. Click **Add** next to the **Sub-field items** list, type the value, and then click **OK**. You can add as many sub-field items as you need. You can also use a function definition to define the values as you can do for the parent list items.
9. If you want to use the field for case management, such as setting the case location, select the appropriate option in the **Field Usage** area:
   - **Location field**: Identifies the location for a case. The field must be a **Global field** and can be a text box or a list of values to select. You can use the `GetLocations` function definition to populate the list values. You must create one field to be a location field for all categories of cases.
   - **Case Type filter**: Displays the field when the user creates a new case. This type of field cannot be modified after a case is created unless you also check the **Required** check box. Check this option for the **Case Entry #** field, which is used for manually specified case numbers. For more information, see *Understanding Workflow Case Numbering* (page 82).
   - **Show this field in...**: Identifies where this field is used, such as in the **Case Summary** or in **Request for Approval** or **Notification** emails.
10. Click **Save**.

Defining the Location Common Field for Workflows

Workflows, including those used in Cyber DOC4000, require you to define the **Location** common field. You can configure the **Location** common field to auto-populate its values using the `GetLocations` function definition. You may have previously configured this common field if you are using workflows for other purposes. This function can pull values from your asset hierarchy.

Before you perform this task, you should have your asset hierarchy defined. For more information about your asset hierarchy, see Creating New Object Types for the Asset Hierarchy, and Understanding and Defining Your Asset Hierarchy.



To auto-populate the list of items for the Location common field:

1. In the Admin Utility, click the **Workflows** link under **Additional Modules**.
2. In the **Workflow-related Tasks** area, click **Define Common Fields**.
3. If a Location field does not exist in the Global fields list, complete the following steps:
   a. Next to the **Global fields** list, click **Add**.
   b. Type `Location` as the name for the new field, and then click **OK**.
4. In **Global fields**, click **Location**.
5. In **Field Details**, click **List**.
6. Under the **Items** list, check the **Auto-populate the list using this FunctionDef** check box, and then select **GetLocations** from the list below the check box.
7. In **Field Usage**, check the **Location field** check box.
8. Click the **Save** button.
9. Close the Define Common Workflow Fields window.
10. Edit the GetLocations function to display values from your asset hierarchy by completing the following steps:

a. Open the Asset Model Builder on the DOC4000 server. To open the Asset Model Builder, run the following file:

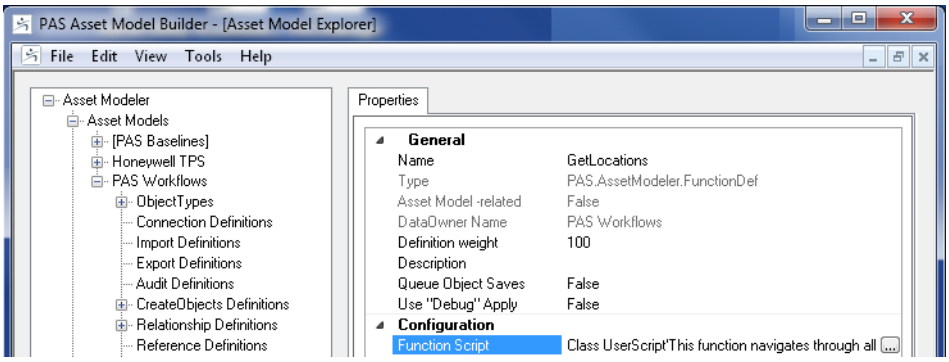
InstallPath\DataCollector\AssetModelBuilder.exe

b. Click **Edit** > **Asset Model Explorer**.

c. In the left pane, click the plus sign next to the following nodes to expand these nodes: **Asset Models**, **PAS Workflows**, and **Function Definitions**.

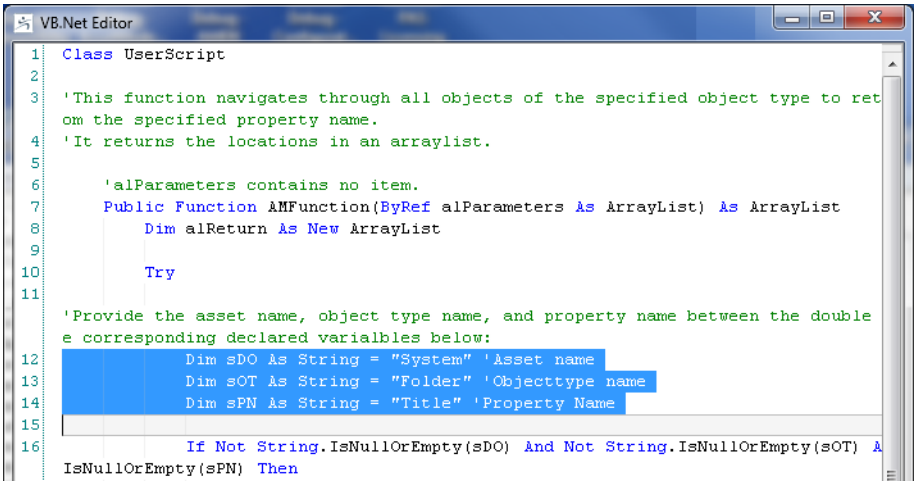
d. In the left pane, click **GetLocations**. The right pane displays the properties.

e. In the right pane, click **Function Script**.



f. Click the ellipses button (**...**) to edit the script. The VB.Net Editor window is displayed.

g. Specify the appropriate values between the double quotes on lines 12-14 of the script. For example, the following figure shows how to set the location values to include all system folders in your hierarchy.



h. Click **Save** on the script editor window.

i. Click **Save** on the Properties tab of the Asset Model Explorer window.

j. Close Asset Model Builder.

Creating Checklists for Workflows

When a case is created, the case is assigned a workflow definition. The case is then updated as each state of the workflow definition is achieved. To document the transition from state-to-state,

you can create a checklist that must be completed prior to a state being considered complete. Each checklist can include a variety of items on the checklist:

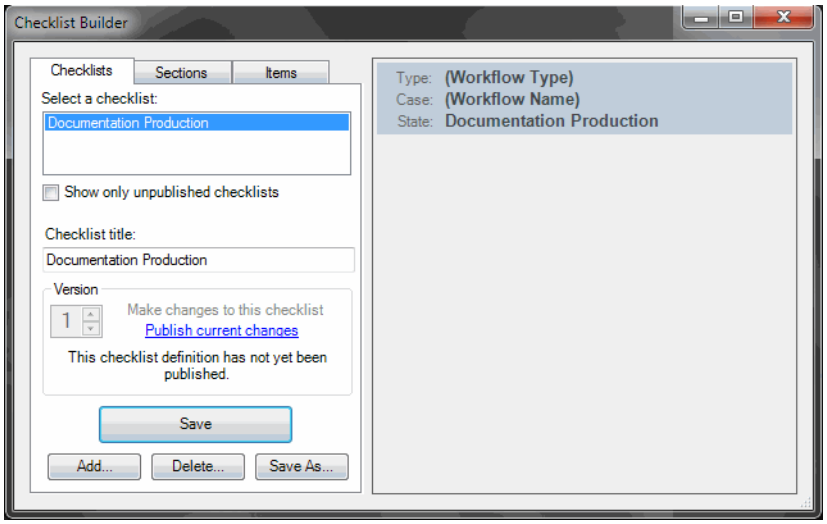
- Check Box - a true/false item that the user can check to indicate completion.
- Radio Buttons - an item that has multiple choices, but the user can select only one.
- Text Entry - an item that includes a text box to allow the user to type information.
- Fixed Text - an item that can provide a heading, description, or identification for other items.
- Hyperlink - an item that the user can click to open a web page when provided with the proper URL.
- Dropdown List - an item that includes a drop-down arrow to allow the user to select a single value from the list.
- Date Selector - an item that includes a calendar to allow the user to select a date.
- Attach File - an item that includes a **Browse** button to allow the user to upload a file.
- Signature - an item that includes a check box to indicate a signature.
- Reconciled Changes - an item that allows the user to type additional comments about changes.
- Proposed Changes - an item that allows the user to identify proposed value and setting changes. You can customize this item to provide a grid with multiple columns. You can specify the header text and data type for each column, as well as predefined values if you select a drop-down list data type. To use data from PSI in checklists and workflows, you need to provide the PSI web server name. For more information, see *Using PlantState Integrity (PSI) Data within Workflow Definitions* (page 92).
- Equipment - an item that identifies equipment state information. To use data from PSS in checklists and workflows, you need to provide the PSS web server name. For more information, see *Using PlantState Integrity (PSI) Data within Workflow Definitions* (page 92).
- Transition Approvals - an item that allows the user to reassign the case to other approvers of the state. This functionality is replaced by the **Reassign Approvers** button on the detail viewer for a case.
- Policy & Current Version Selector - an item that allows the user to select the policy name and current version. This item is used by the default Test workflow for patch management.
- Policy & New Version Selector - an item that allows the user to select the policy name and new version. This item is used by the default Test workflow for patch management.
- Policy Details - an item that allows the user to select the policy name, current version, new version, and a link to the associated test case. This item is used by the default Implementation workflow for patch management.

You can identify which items are required. The checklist displays a red asterisk next to each required item to indicate to users which items are required. A single item, **Check Box** or **Signature**, can designate that the section is complete.

If you want to add a section that provides lines of instruction and is not required to complete the checklist, select the section, and then check the **This section is for information only** check box at the top of the Sections tab.

To create a checklist:

1. In the Admin Utility, click the **Workflows** link.
2. On the Workflows window, click the **Create and Edit Checklists** link in the **Workflow-related Tasks** area.
3. In the Checklist Builder window, click **Add** to create a new checklist.
4. Type a name for the checklist in the **Checklist title** field, and click **Save**.



5. If you want to create a section, complete the following steps:
   a. Click the **Sections** tab.
   b. Click **Add**, and then click on the new section in the right pane.
   c. In the **Section title** field, type a name for the section.
6. If you want to add items to a section, complete the following steps:
   a. In the right pane, select the section you want to add items to. The section should be expanded in the right pane.
   b. On the Sections tab, click the arrow button next to the item you want to add to the checklist section. Available items include instructions (fixed text), check boxes, radio buttons, text boxes, and more.
   c. In the right pane, click on the new item to open the **Items** tab so you can type a label for the item and specify other options, such as values if you are creating a list.

      NOTE If you specify a value in the optional **Item Name** field, that item is displayed as a column in the case summary, unless the value is enclosed in square brackets. Some features, such as patch management, use square brackets and specific names to identify items with values to use within that feature.
7. Make sure each section, other than informational sections, has a check box or a signature field to indicate the section is complete. In each section, click the appropriate check box or signature field in the right pane, and check the **Indicates that the Section is complete** check box on the Items tab.
8. On the **Checklists** tab, click **Save**.
9. Click the **Publish current changes** link to finalize the checklist so that it can be assigned to a state.

10. Click **Yes** to confirm publication of the checklist.

Using PlantState Integrity (PSI) Data within Workflow Definitions

You may want to use PSI data, such as D&R information, in workflows. For example, the **Proposed Changes** item can be added to checklists to identify proposed value and setting changes. For more information about this checklist item and others, see *Creating Checklists for Workflows* (page 89).

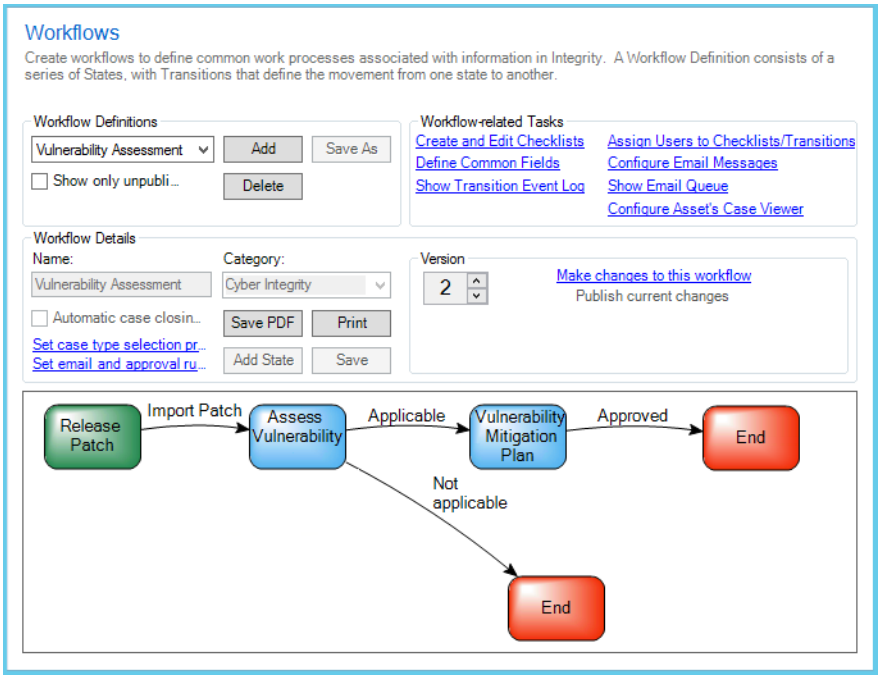
To allow DOC4000 to connect to PSS:

1. Edit the `IntegrityMOCRoot.xml` file. This file is located in the root folder of the application, such as `C:\PAS\Integrity\`.
2. Find the following tags in the `IntegrityMOCRoot.xml` file:

   `<PSSWebServerName> </PSSWebServerName>`
3. Specify the name of the PSI web server in these tags, such as `<PSIWebServerName>`*ServerName*`</PSIWebServerName>`
   where *ServerName* is the computer name. In some cases, you may need to specify the IP address.
4. Save and close the `IntegrityMOCRoot.xml` file.

Creating a Workflow Definition

Once you import the PAS Workflow asset model, the **Workflow** link in the Admin Utility is available. The **Workflow** link opens the Workflows window, which allows you to define workflows with checklists to be assigned to cases for management of change (MOC). For more information about the complete workflow configuration process and the related tasks and requirements, see *Steps for Workflow Configuration* (page 83).



Instead of creating a workflow from scratch, you may want to copy an existing workflow and the modify it to meet your specific needs. For more information, see *Copying a Workflow Definition* (page 94) and *Modifying a Workflow Definition* (page 95).

To create a workflow definition:

1. In the Admin Utility, click the **Workflows** link.
2. In the **Workflow Definitions** area, click **Add** to define a new workflow.
3. Type the name for the new workflow, and then click **OK**.
4. In the **Workflow Details** area, type or select the category in the **Category** field. When you type a new category and save the workflow, the new category is added to this list for use when defining workflows and common fields.
5. If you want cases that use this workflow to be closed automatically when they move to the normal end state, check **Automatic case closing upon completion**.

   When a case transitions to the normal end state, DOC4000 checks whether that state has a checklist. If there is no checklist and you checked **Automatic case closing**, DOC4000 closes the case. If the normal end state has a checklist, DOC4000 cannot close the case. Once the checklist is completed and signed, DOC4000 closes the case.
6. In the **Workflow Details** area, click **Add State** to define the beginning state.

7. Type the name for the state, and then click **OK**.
8. Click on the state to open the **State Details** area and drag the state to where you want it within the workflow area.
9. Type a description for this state.
10. Check the **This is the beginning state** check box. A workflow can have only one beginning state.
11. Add additional states as needed by repeating Steps 6-9. In the **State Details** area, each state defaults to the *normal path*. For states that are *not* in the normal path, clear the **This state is in the normal path** check box.
12. When you are finished adding states, click the end state and check the **This is the end state** check box to designate it as the final state.
13. Connect the states by clicking on the edge of a state and dragging the cursor to the edge of the state to which the connection should be formed. A line with an arrow should be displayed from the one state to the next. Then, type a name for the transition and click **OK**.
14. Click on each transition arrow and type a description for that transition in the **Transition Details** section of the window. If the transition requires an approval to proceed to the next state, check **This transition requires approval**. A transition that does not require an approval is approved by the current case owner.

    NOTE At least one transition in the workflow, such as the transition to the final state, must require an approval or you cannot publish the workflow.
15. If you want to assign a checklist to a state, complete the following steps:
    a. Click on the state to assign a checklist to.
    b. In the **State Details** area, select the checklist to assign to the state. For more information about checklists, see *Creating Checklists for Workflows* (page 89).
16. In the **Workflow Details** area, click **Save**.
17. If you want to make the workflow available for use, publish the workflow by completing the following steps:
    a. In the **Version** area, click **Publish current changes**.

       If you attempt to publish a workflow without setting at least one transition to require approvals, DOC4000 displays a red exclamation point next to the **Publish Workflow** button and displays an error message. If this occurs, click **OK** to close the error message and make sure at least one transition requires an approval.

       If you have unsaved changes, you will be prompted to save your changes before proceeding. If this occurs, click **OK** to close the message, and then click **Save**.
    b. Click **Yes** to confirm publication of the workflow.

Copying a Workflow Definition

You can duplicate an existing workflow definition and then modify the new workflow as needed.

To copy an existing workflow definition:

1. In the Admin Utility, click the **Workflows** link.

2. In the **Workflow Definitions** area, select a workflow.
3. In the **Version** area, click **Make changes to this workflow**.
4. In the **Workflow Definitions** area, click **Save As**.
5. Type a name for the new workflow definition, and then click **OK**.
6. In the **Workflow Definitions** area, select the original workflow definition.
7. In the **Version** area, click **Publish current changes**, and then click **Yes**.

Now, you can select the new workflow, modify it as needed, and then save and publish the new workflow. For more information, see *Modifying a Workflow Definition* (page 95).

Modifying a Workflow Definition

To make changes to a workflow, you must first click the **Make changes to this workflow** link in the **Version** area. Then, you can modify the workflow, save your changes, and publish your changes as a new version.

To modify a workflow definition:

1. In the Admin Utility, click the **Workflows** link.
2. In the **Workflow Definitions** area, select a workflow.
3. In the **Version** area, click **Make changes to this workflow**.
4. Change the workflow as needed.
5. In the **Workflow Details** area, click **Save**.
6. If you want to make the workflow available for use, publish the workflow by completing the following steps:
   a. In the **Version** area, click **Publish current changes**.

      NOTE If you attempt to publish a workflow without setting at least one transition to require approvals, DOC4000 displays a red exclamation point next to the **Publish Workflow** button and displays an error message. If this occurs, click **OK** to close the error message and make sure at least one transition requires an approval.

   b. Click **Yes** to confirm publication of the workflow.

Configuring Case Type Selection Properties

You can configure DOC4000 to display a set of fields when a user starts a case. Then, based on the values selected for those fields, DOC4000 can determine which workflow definition to assign to the case. These types of common fields are known as case type filter fields.

You must first create one or more common fields that have the **Case Type filter** check box checked. Then, this task allows you to specify which values for these fields are associated with each workflow definition. When a user starts a new case and sets the case type filter fields to the values you specified, the case is assigned to the appropriate workflow definition for those values. Once a case is assigned to a workflow definition, the case can then be updated as each state of the workflow is achieved.

The **Set case type selection properties** link on the Workflows window in the Admin Utility allows you to specify which fields and values are associated with each workflow definition. You need to

select the fields and values for each workflow definition you want to use based on a set of case type filter fields and their values.

To set the case type selection properties and values for a workflow:

1. In the Admin Utility, click the **Workflows** link.
2. On the Workflows window, select a workflow definition in the **Workflow Definitions** area.
3. In the **Workflow Details** area, click **Set case type selection properties** link.
4. On the Workflow Definition Properties window, select the common field and type or select the value to be used as the filter. Repeat this step for additional fields.
5. Click **Save**.

Assigning Users to Transitions and Checklists

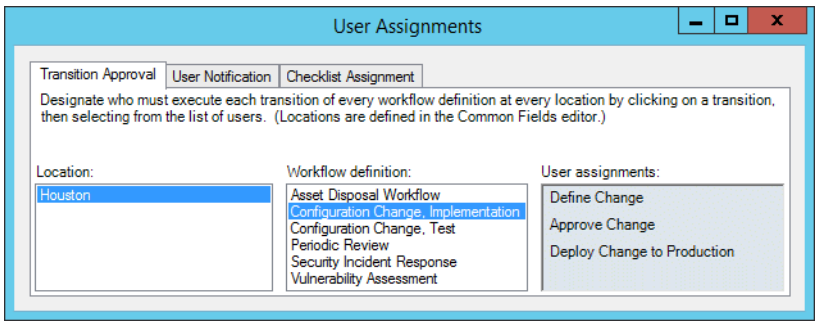
In many cases, work processes have team members who are assigned to review or approve the work at various stages. DOC4000 allows you to specify which users can approve cases so the cases can transition from one state to the next. You can also specify which users are assigned to checklists in cases.

The **Assign Users to Checklists/Transitions** link on the Workflows window in the Admin Utility allows you to assign users to transitions or checklists.

To assign users to transitions or checklists:

1. In the Admin Utility, click the **Workflows** link.
2. On the Workflows window, click the **Assign Users to Checklists/Transitions** link in the **Workflow-related Tasks** area. The User Assignments window is displayed.
3. Select the tab for the type of assignments you want to define:
   - **Transition Approval**: Allows you to specify who can approve a case transition from one state to the next. For each location and workflow definition, select one or more users for each of the listed transitions. When a case requires approval to transition from one state to the next, an email is sent to the users selected for the transition, location, and workflow definition of that case.
   - **User Notification**: Allows you to specify who receives an email when a case transitions to the next state. For each location and workflow definition, select one or more users for each of the listed transitions. When a case transitions from one state to the next, an email is sent to the users selected for the transition, location, and workflow definition of that case. The case owner automatically receives this notification, so you do not need to add the owner.
   - **Checklist Assignment**: Allows you to specify who is assigned to checklists in a case. For each location and workflow definition, select one or more users for each of the listed checklists. When a case transitions to a state with a checklist, an email is sent to the users selected for the checklist, location, and workflow definition of that case. You can also limit checklist updates and signing to the users you selected for that checklist, location, and workflow definition.

4. Click on a location, and then a workflow definition.



5. In the **User assignments** list, click on a transition or checklist.
6. On the Select Users window, add users to the appropriate lists.
7. Select **All primary users must approve** or **Any user(s) must approve**. If you select **Any user(s) must approve**, type the number of users to approve in the text box.
8. Click **Save**.
9. Repeat Steps 5-8 for all transitions and checklists you want assigned users.
10. If you want to enforce checklist assignments and not allow other users to update or sign checklists, on the Checklist Assignment tab, check the **Only assigned users can complete checklist** check box.

Configuring Email Message Templates

As cases advance from state to state within a workflow definition, the work can shift to different team members. For example, an approval may be needed, or the case may need to be assigned to a different team member. DOC4000 allows you to configure email notifications to streamline the work process and notify team members when needed.

NOTE To send email messages, you must first configure the email server by clicking the **Configure email notifications** link on the Maintenance window in the Admin Utility. You also can click the **Configure email server information** link at the bottom of the Email Message Configuration window.

The **Configure Email Messages** link on the Workflows window in the Admin Utility allows you to create templates for many types of email notifications:

- Requests for approval
- Checklist assignment notifications
- New case owner notifications
- Case owner updates
- Approval no longer required
- General notifications
- Tacit approval and disapproval emails sent to request approval or notify users of actions needed

To configure email message templates:

1. In the Admin Utility, click the **Workflows** link.
2. On the Workflows window, click the **Configure Email Messages** link in the **Workflow-related Tasks** area. The Email Message Configuration window is displayed.
3. Click the link on the left for the template you want to configure, such as **Request for approval**.
4. In the **Subject** field, type text to include in the subject line of each email. You can include the Case ID and Description in the subject line of each email by typing `<Case>` and `<Description>` in the **Subject** field. You can include common fields that are viewable in the Case Summary in the subject line by typing the field name in angled brackets, such as <*fieldname*>.
5. In the **Body** field, type the text of the email message.
6. Repeat Steps 3-5 to configure additional email templates.
7. Click **Save**.

Configuring Email and Approval Rules

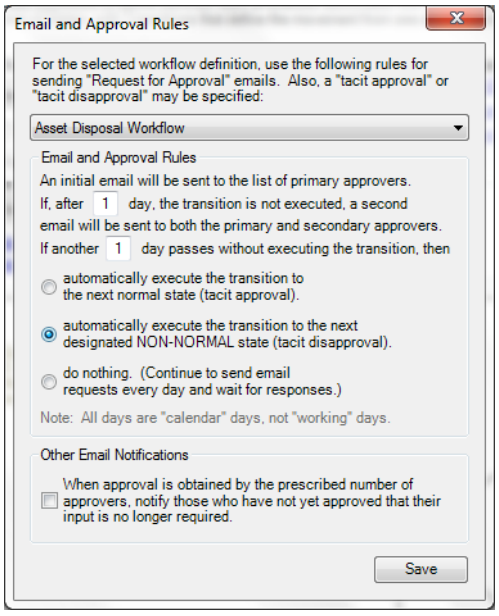
DOC4000 allows you to configure how often email notifications are sent or resent. You can also specify what to do if no one takes action following the email notification. For example, you can send an email notification when an approval is needed for a case to transition to the next state. If the case is not approved or updated within a specified period of time, you can configure DOC4000 to send another email or to automatically transition the case to the next state.

The **Set Email and approval rules** link on the Workflows window in the Admin Utility allows you to configure the intervals when requests for approval emails are sent and whether the transition is executed automatically when no users interact.

To configure email and approval rules:

1. In the Admin Utility, click the **Workflows** link.

2. On the Workflows window, click the **Set email and approval rules** link in the **Workflow Details** area.



3. On the Email and Approval Rules window, select a workflow definition from the list.
4. In the **Email and Approval Rules** area, type the number of days when a follow up email will be sent to both the primary and secondary approvers if the transition is not executed after the initial email was sent.
5. Type the number of days and select an option for what will happen after these days pass without executing the transition.
6. For additional workflow definitions, repeat Steps 3-5.
7. If you want to send notifications when approval is obtained, check the **Other Email Notifications** check box.
8. Click **Save**.

Configuring Email Notifications for Errors

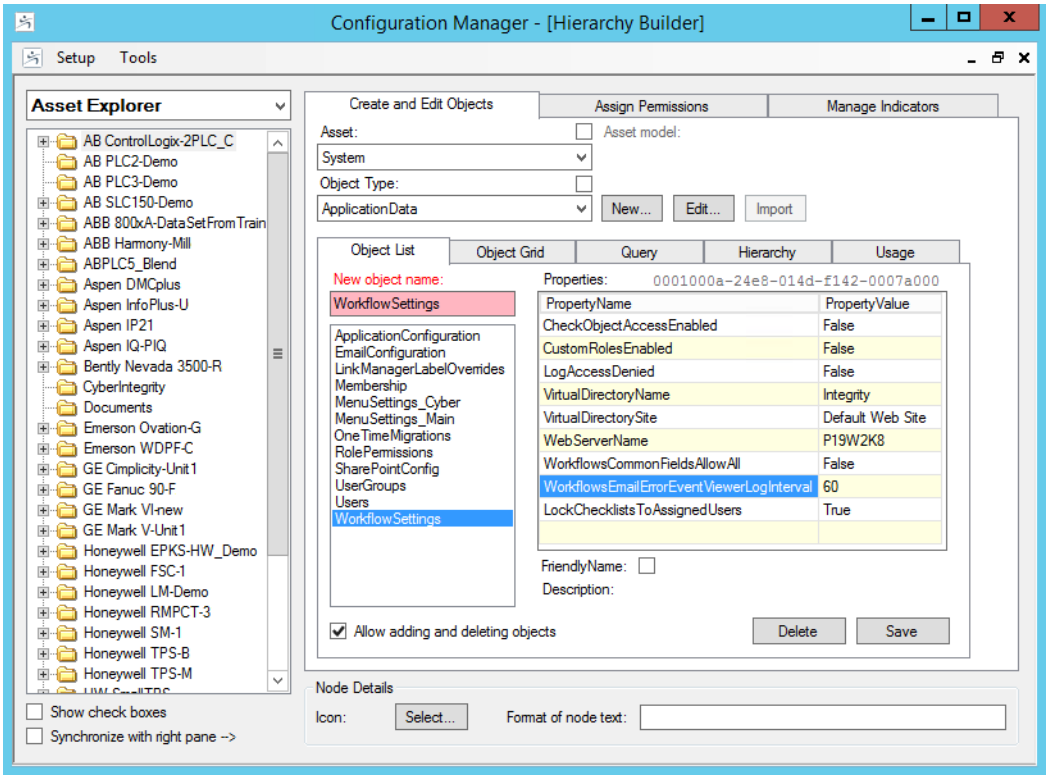
DOC4000 provides several email notifications and log entries when the following error cases or potential issues are identified:

- When a user assigned to a transition in a workflow is removed, DOC4000 sends a request for approval to the case owner once every 60 minutes. DOC4000 also creates a log in Windows Event Viewer once every 60 minutes.
- If the DOC4000 server loses its connection to the Exchange Server, DOC4000 creates an error in the Windows Event Viewer once every 60 minutes by default but does not attempt to email the case owner.

You can use Configuration Manager to change the default value of 60 minutes for these emails and error reporting.

To change the default email and error event viewer interval:

1. Open Configuration Manager on the DOC4000 server by running the following file: *InstallPath*\DataCollector\ConfigurationManager.exe.
2. Click the Create and Edit Objects tab.
3. In **Asset**, select **System**.
4. In **Object Type**, select **ApplicationData**.
5. On the Object List tab, check the **Allow adding and deleting objects** check box.
6. In **New object name**, type `WorkflowSettings`, and then click in an empty area of the list below the **New object name** field.
7. Click **Save**. The **WorkflowSettings** object is added to the list of objects and its properties are displayed in the **Properties** list.



8. In the blank **PropertyName** field, type the following property name:

   `WorkflowsEmailErrorEventViewerLogInterval`

9. In the associated **PropertyValue** field, type how often, in minutes, you want email notifications and error logging for an unresolved error to occur.
10. Click **Save**.

NOTE Type the exact names for the **New object name** and **PropertyName** values.

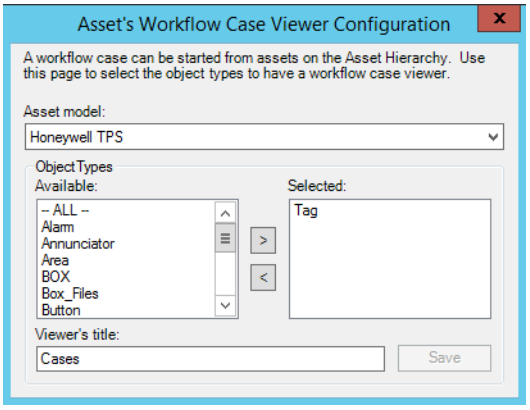
Associating Object Types with a Case

You can select the types of objects that users can associate with a case. When a user selects an object of a selected object type, the DOC4000 web interface displays the case viewer (Case tab) in the right pane to provide information about the cases with which the object is associated.

To select the object types that can be associated with a case:

1. In the Admin Utility, click the **Workflows** link.
2. In the **Workflow-related Tasks** area of the Workflows window, click **Configure Asset's Case Viewer**.

   The Asset's Case Viewer Configuration window is displayed. This window allows you to view the object types supported by each asset model, and you can select which object types can be associated with a case.



3. For each asset model with types of objects you want to be able to associate with a case, complete the following steps:

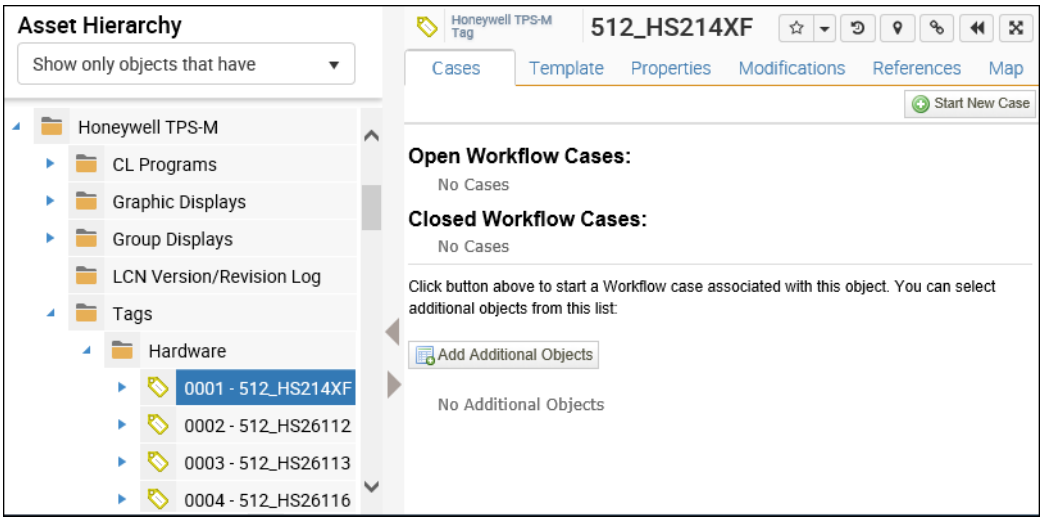
   a. In **Asset model**, select the asset model for that type of object.

   b. In the **Available** list, select the object types you want, and then click the **>** button to add them to the **Selected** list.

   c. In **Viewer's title**, type the name you want for the tab, such as `Cases`, and then click **Save**.

4. Click the red **X** button to close the window.

When a user selects an object in the DOC4000 web interface, and that object type was configured, the asset's case viewer is available as a tab to provide the information of the cases that the object is associated with. The following figure shows an example of an object selected and the Cases tab available for that object.

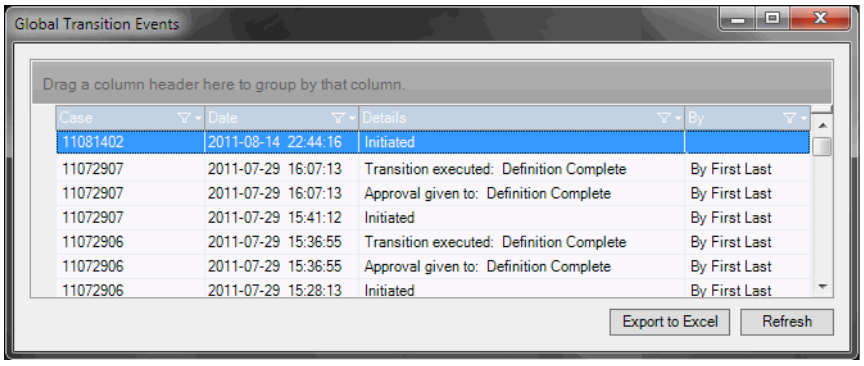


Viewing the Transition Event Log

As workflow cases transition from state to state, DOC4000 tracks and logs this activity. The **Show Transition Event Log** link on the Workflows window in the Admin Utility allows you to view a summary of the transition events for all cases. You can also export this log to an Excel file.

To view the transition event log summary:

1. In the Admin Utility, click the **Workflows** link.
2. On the Workflows window, click the **Show Transition Event Log** link in the **Workflow-related Tasks** area.



3. Click **Refresh** to update the table with the most recent transitions.
4. If you want to export the log to an Excel file, complete the following steps:
   a. Click **Export to Excel**.
   b. Navigate to the folder where you want to save the file, specify the name for the file, and then click **Save**.

Viewing the Email Queue

You can configure DOC4000 to send email notifications for workflow cases. If a user does not receive an email notification, you may want to view the email queue. This queue allows you to view any approval or notification emails that have not yet been sent. The **Show Email Queue** link on the Workflows window in the Admin Utility allows you to display this email queue.

To view the email queue:

1. In the Admin Utility, click the **Workflows** link.
2. On the Workflows window, click the **Show Email Queue** link in the **Workflow-related Tasks** area.
3. Click **Refresh** to update the table with the most recent information.

Configuring Change Tracking Workflows

You can use workflow cases to assign and record the resolution of identified changes. DOC4000 allows you to categorize changes to individual object properties. Then, for changes that are categorized as **Security** changes, DOC4000 can automatically create a workflow case for each of those changes. You can define the workflow to use for the case and the time period to wait before the case is created.

The following list guides you through the configuration tasks to support using workflows for change tracking and change management.

1. Make sure you have loaded the PAS Workflows asset model. For more information, see *Loading (Importing) Asset Models* (page 32).
2. Create the workflow definition to use for change tracking. For more information, see *Steps for Workflow Configuration* (page 83).
3. Specify the owner of each monitored system to ensure DOC4000 notifies the appropriate person when the property of a system is changed. For more information, see *Defining the Owner for Each Monitored System* (page 103).
4. Specify the location of each monitored system to ensure DOC4000 correctly sets the location field in the workflow case. For more information, see *Defining the Location for Each Monitored System* (page 105).
5. Configure the change tracking workflow properties to identify the workflow to use for change tracking cases and the time delay to use when reviewing changes for case management. For more information, see *Defining the Change Tracking Workflow and Setting the Time Delay* (page 106).
6. Schedule the import sequence to review identified changes and create workflow cases for changes that meet the defined criteria. For more information, see *Detecting Security Changes and Creating Related Cases* (page 106).

Defining the Owner for Each Monitored System

For each system, you need to identify the system owner so that DOC4000 can notify the appropriate person when a change management, policy management, or patch management workflow case is created. DOC4000 allows you to specify the object type and property to use to

define the system owner for each system. You can use Configuration Manager to modify the following property values for the **CyberIntegrityWorkflows** object in the PAS Workflows asset model:

MonitoredSystemOwnerObjectType

Specifies the object type that DOC4000 uses to identify the name of the system owner. DOC4000 uses the Asset Inventory tree to find the object of the specified type, and then uses the value of the property specified in the **MonitoredSystemOwnerPropertyName** property as the owner's full (first and last) name.

MonitoredSystemOwnerPropertyName

Specifies the property that DOC4000 uses to identify the full (first and last) name of the system owner. DOC4000 uses the **MonitoredSystemOwnerObjectType** and **MonitoredSystemOwnerPropertyName** properties together.

These configuration properties are used for change management, policy management, and patch management workflows. If a property does not exist, use Configuration Manager to add that property.

DOC4000 searches the defined users and groups for the owner's full name, and then uses the email address associated with that account. DOC4000 can use application authentication or Windows authentication. For more information, see *Configuring Users and Groups* (page 22).

To define the owner for each monitored system:

1. Identify an object type and property that you want DOC4000 to use to define the full name of the owner for each system. For example, you can add a property called **SystemOwner** to each DataOwner object, and set the property value to the first and last name of the owner for that asset (data owner). Each value must exactly match a user defined for DOC4000.

   In this example, the system owner defined for a PAS Recon data owner is used for all computers in the collection group associated with that data owner.

2. Open Configuration Manager on the DOC4000 server. To open Configuration Manager, run the following file:

   InstallPath`\DataCollector\ConfigurationManager.exe`

3. In the right pane, check **Asset Model**.
4. In the **Asset** field, select **PAS Workflows**.
5. In the **Object Type** field, select **Setting**.
6. In the **Objects** list on the Object List tab, select **CyberIntegrityWorkflows**. The **Properties** field is populated with the properties for this object.
7. If the MonitoredSystemOwnerObjectType or MonitoredSystemOwnerPropertyName property is not listed in the right pane, complete the following steps for each missing property:
   a. Click in the **Property Name** column at the bottom in the first empty row.
   b. Type the name for the property to add, such as `MonitoredSystemOwnerObjectType` or `MonitoredSystemOwnerPropertyName`.
8. In the **PropertyValue** column, specify values for the following properties:

- **MonitoredSystemOwnerObjectType** - type the object type that you want DOC4000 to use to identify the system owner name, such as `DataOwner`.
- **MonitoredSystemOwnerPropertyName** - type the name of the property that you want DOC4000 to use to identify the full (first and last) name of the system owner, such as `SystemOwner`.

9. Click **Save**.

Defining the Location for Each Monitored System

For each system, you need to identify the location so that DOC4000 can correctly set the location field in the workflow case when a policy, change management, or patch management case is created. For patch management workflow cases, the location is defined by the **PatchAssessmentTestCaseLocation** property. For more information about defining the location for patch management, see *Understanding the Workflow Configuration Settings* (page 113) and *Defining the Patch Management Workflows to Use* (page 115).

For policy and change management workflow cases, DOC4000 allows you to specify the object type and property to use to define the location for each system. You can use Configuration Manager to modify the following property values for the **CyberIntegrityWorkflows** object in the PAS Workflows asset model:

LocationObjectType

Specifies the object type that DOC4000 uses to identify the location of the system. DOC4000 uses the Asset Inventory tree to find the object of the specified type, and then uses the value of the property specified in the **LocationPropertyName** property as the system location.

LocationPropertyName

Specifies the property that DOC4000 uses to identify the location of the system. DOC4000 uses the **LocationObjectType** and **LocationPropertyName** properties together.

If a property does not exist, use Configuration Manager to add that property.

To define the location for each monitored system:

1. Identify an object type and property that you want DOC4000 to use to define the location for each system. For example, you can add a property called **SystemLocation** to each DataOwner object, and set the property value to the location for that asset (data owner).

   In this example, the location defined for a PAS Recon data owner is used for all computers in the collection group associated with that data owner.

2. Open Configuration Manager on the DOC4000 server. To open Configuration Manager, run the following file:

   InstallPath`\DataCollector\ConfigurationManager.exe`

3. In the right pane, check **Asset Model**.
4. In the **Asset** field, select **PAS Workflows**.
5. In the **Object Type** field, select **Setting**.
6. In the **Objects** list on the Object List tab, select **CyberIntegrityWorkflows**. The **Properties** field is populated with the properties for this object.

7. If the **LocationObjectType** or **LocationPropertyName** property is not listed in the right pane, complete the following steps for each missing property:
   a. Click in the **Property Name** column at the bottom in the first empty row.
   b. Type the name for the property to add, such as `LocationObjectType` or `LocationPropertyName`.
8. In the **PropertyValue** column, specify values for the following properties:
   - **LocationObjectType** - type the object type that you want DOC4000 to use to identify the system location, such as `DataOwner`.
   - **LocationPropertyName** - type the name of the property that you want DOC4000 to use to identify the location of the system, such as `SystemLocation`.
9. Click **Save**.

Defining the Change Tracking Workflow and Setting the Time Delay

DOC4000 provides configuration settings to define when DOC4000 creates workflow cases to track the resolution of changes and what workflow definition to use for those cases. You can define a time interval in days since the last import. When the scheduled import sequence runs, which is usually once a day, DOC4000 identifies import changes per asset/data owner that are not reconciled for the defined time interval, and DOC4000 automatically creates workflow cases using the workflow definition you define.

To define the workflow definition to use and the time delay properties:

1. Open Configuration Manager on the DOC4000 server. To open Configuration Manager, run the following file:

   InstallPath`\DataCollector\ConfigurationManager.exe`
2. On the Create and Edit Objects tab in the right pane, check **Asset model**.
3. In the **Asset** field, select **PAS Workflows**.
4. In the **Object Type** field, select **Setting**.
5. In the **Objects** list on the Object List tab, select **CyberIntegrityWorkflows**. The **Properties** field is populated with the properties for this object.
6. In the **PropertyValue** column for the **DelayToCreateSecurityChangeCase** property, type the number of days since the last import you want DOC4000 to wait before creating a workflow case.
7. In the **PropertyValue** column for the **WorkflowDefSecurityChange** property, type the name of the workflow definition you created for DOC4000 to use when creating a workflow case.
8. Click **Save**.

Detecting Security Changes and Creating Related Cases

The PAS Workflows asset model provides the **Create MOC Cases for Security Changes** sequence definition. You schedule this sequence definition through the Admin Utility to run once a day and automatically detect and create cases for the unreconciled changes. Each time this

sequence runs, it checks to see if the last import time of each asset has passed the specified time delay interval. If the specified number of days have passed since the last import time, DOC4000 performs the following tasks:

- Groups the objects of the unreconciled security changes by location
- Creates a workflow case per location and attaches the objects as associated assets.
- Sends an email to the owner of the monitored system to notify that owner of the workflow case created for reconciling the changes.

To schedule the Create MOC Cases for Security Changes sequence:

1. In the Admin Utility, click the **Schedules** link under **Initial Setup**.
2. On the **Schedules** tab, click **Add**.
3. On the **General** tab, type the **Schedule Name**.
4. On the **Sequences** tab, select the **MOC** asset from the **Asset** list.
5. In **Definitions**, click **Create MOC Cases for Security Changes**, and then click the right arrow (**>**) button to add the selected definition to the **Sequence** list.
6. On the **Schedule** tab, configure when and how often to run the sequence, such as once a day.
7. Click **OK** to save.

Configuring Patch Management Workflows

You can configure Cyber DOC4000 to use workflow cases to assign and record the testing, implementation, and mitigation processes of patch management. You can create the checklists and workflow definitions, and then you can configure Cyber DOC4000 to create cases using these workflow definitions when a user clicks the corresponding disposition button in the Cyber DOC4000 web interface.

The following list guides you through the configuration tasks to support using workflows for patch management.

1. Make sure you have loaded and configured the required asset models. To configure and use the Patch Management workflows in Cyber DOC4000, you must load and configure the Cyber Integrity, PAS Workflows, and PAS Recon asset models. You also need to import the PAS Patch Management asset model and configure patch management. For more information, see Steps for Configuring Cyber DOC4000 and Steps for Implementing Patch Management.
2. Create a patch testing checklist. You will incorporate this checklist into the workflow definition you create for the patch testing portion of patch management. For more information, see *Creating the Patch Testing Checklist* (page 108).
3. Create a patch implementation and mitigation checklist. You will incorporate this checklist into the workflow definitions you create for the patch implementation and patch mitigation portions of patch management. For more information, see *Creating the Patch Implementation and Mitigation Checklist* (page 110).
4. Create the patch testing workflow definition to guide the patch testing process of patch management. For more information, see *Creating the Patch Testing Workflow* (page 112).

5. Create the patch implementation workflow definition and the patch mitigation workflow definition to guide these processes. For more information, see *Creating the Patch Implementation and Patch Mitigation Workflows* (page 113).
6. Specify the owner of each monitored system to ensure DOC4000 notifies the appropriate person when patch management workflow case is created. For more information, see *Defining the Owner for Each Monitored System* (page 103).
7. Review the workflow configuration settings available to connect patch management with the workflows you created and several other options. For more information, see *Understanding the Workflow Configuration Settings* (page 113).
8. Configure the patch management workflow properties to identify the workflow definition to use when creating cases for patch management. For more information, see *Defining the Patch Management Workflows to Use* (page 115).

After you create, configure, and save the checklists, workflow definitions, and the **CyberIntegrityWorkflows** properties, users can begin to perform the patch management tasks, such as adding vendors and vendor aliases and creating vendor bulletins.

Creating the Patch Testing Checklist

Before you create the patch management workflow definitions, you need to create the checklists that are used by those workflow definitions. These checklists need to exist before you can incorporate them into the workflows. This section identifies the specific requirements for the patch testing checklist. For more information about checklists, see *Creating Checklists for Workflows* (page 89).

To create the patch testing checklist:

1. In the Admin Utility, click the **Workflows** link.
2. On the Workflows window, click the **Create and Edit Checklists** link in the **Workflow-related Tasks** area.
3. In the Checklist Builder window, click **Add** to create a new checklist.
4. In the **Checklist title** field, type a name for the checklist, such as `Patch Testing`, and *remember this name*. You will use this checklist in the **Patch Testing** workflow definition so name it appropriately.
5. Click **Save**.
6. Create a Documentation and Details section by completing the following steps:
   a. Click the **Sections** tab.
   b. Click **Add**, and then click on the new section in the right pane.
   c. In the **Section title** field, type the name for the section, such as `Documentation and Details`.
7. Add the required fields to this section by completing the following steps:
   a. In the right pane, select the section you want to add items to. The section should be expanded in the right pane.
   b. On the Sections tab, click the arrow button next to the **Text Entry** item to add a text box to the checklist section.

c. In the right pane, click on the new item to open the **Items** tab so you can type values for the following text box options:

Field Name	Value to Specify or Select
Item Name	`[PatchDetails]`
Label Text	`Patch Details`
Text Box Size	**Large (Multi-line)**

NOTE Specify the **Item Name** value exactly as directed, including the square brackets, to make sure that DOC4000 processes the information correctly. DOC4000 uses this large, multi-line text box to display information about the patch, including the object name, vendor, bulletin ID, product name, product version, and Microsoft KB number.

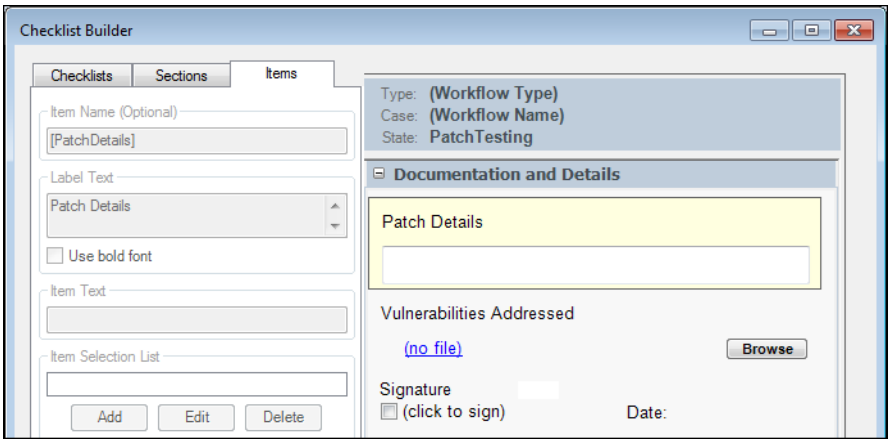
d. On the Sections tab, click the arrow button next to the **Attach File** item to add a file attachments field to the checklist section.

e. In the right pane, click on the new item to open the **Items** tab for this item and type `Vulnerabilities Addressed` in the **Label Text** field.

f. On the Sections tab, click the arrow button next to the **Signature** item to add an approval check box to the checklist section.

g. In the right pane, click on the new item to open the **Items** tab for this item and type `Signature` in the **Label Text** field.

h. Check the **Indicates that the Section is complete** check box.



8. On the **Checklists** tab, click **Save**.
9. Click the **Publish current changes** link to finalize the checklist so that it can be assigned to a state in a workflow definition.
10. Click **Yes** to confirm publication of the checklist.

Creating the Patch Implementation and Mitigation Checklist

Before you create the patch management workflow definitions, you need to create the checklists that are used by those workflow definitions. These checklists need to exist before you can incorporate them into the workflows. This section identifies the specific requirements for the checklist used by both the patch implementation and the patch mitigation workflows. For more information about checklists, see *Creating Checklists for Workflows* (page 89).

To create the patch implementation and mitigation checklist:

1. In the Admin Utility, click the **Workflows** link.
2. On the Workflows window, click the **Create and Edit Checklists** link in the **Workflow-related Tasks** area.
3. In the Checklist Builder window, click **Add** to create a new checklist.
4. In the **Checklist title** field, type a name for the checklist, such as `Patch Implementation and Mitigation`, and *remember this name*. You will use this checklist in the **Patch Implementation** and **Patch Mitigation** workflow definitions so name it appropriately.
5. Click **Save**.
6. Create a Documentation and Details section by completing the following steps:
   a. Click the **Sections** tab.
   b. Click **Add**, and then click on the new section in the right pane.
   c. In the **Section title** field, type the name for the section, such as `Documentation and Details`.
7. Add the required fields to this section by completing the following steps:
   a. In the right pane, select the section you want to add items to. The section should be expanded in the right pane.
   b. On the Sections tab, click the arrow button next to the **Text Entry** item to add a text box to the checklist section.
   c. In the right pane, click on the new item to open the **Items** tab so you can type values for the following text box options:

Field Name	Value to Specify or Select
Item Name	`[PatchDetails]`
Label Text	`Patch Details`
Text Box Size	**Large (Multi-line)**

NOTE Specify the **Item Name** value exactly as directed, including the square brackets, to make sure that DOC4000 processes the information correctly. DOC4000 uses this large, multi-line text box to display information about the patch, including the object name, vendor, bulletin ID, product name, product version, and Microsoft KB number.

d. On the Sections tab, click the arrow button next to the **Text Entry** item to add a text box to the checklist section.

e. In the right pane, click on the new item to open the **Items** tab so you can type values for the following text box options:

Field Name	Value to Specify or Select
Item Name	`[ComputerSystems]`
Label Text	`Computer Systems`
Text Box Size	**Large (Multi-line)**

NOTE Specify the **Item Name** value exactly as directed, including the square brackets, to make sure that DOC4000 processes the information correctly. DOC4000 uses this large, multi-line text box to display information about the computers with the patch implementation or mitigation.

f. On the Sections tab, click the arrow button next to the **Signature** item to add an approval check box to the checklist section.

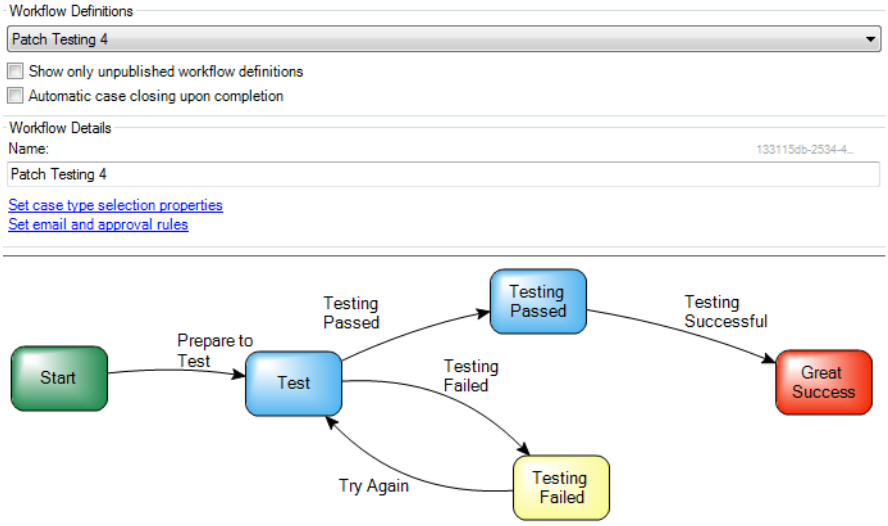
g. In the right pane, click on the new item to open the **Items** tab for this item and type `Signature` in the **Label Text** field.

h. Check the **Indicates that the Section is complete** check box.

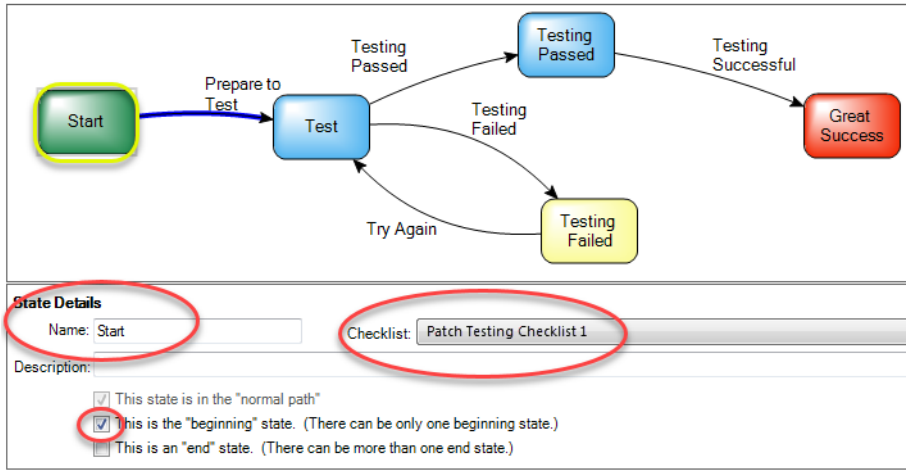
8. On the **Checklists** tab, click **Save**.
9. Click the **Publish current changes** link to finalize the checklist so that it can be assigned to a state in a workflow definition.
10. Click **Yes** to confirm publication of the checklist.

Creating the Patch Testing Workflow

The **Patch Testing** workflow should use the following general flow. You need to define a *normal path* signifying a successfully passed test and a *non-normal path* signifying problems and failed testing as shown in the following figure.



The beginning state of this workflow must contain the **Patch Testing** checklist you created. For more information, see *Creating the Patch Testing Checklist* (page 108).



Save this workflow and remember its name. You need to specify this exact name when you define the patch management workflow to use for the patch testing process. For more information about creating workflow definitions, see *Creating a Workflow Definition* (page 93).

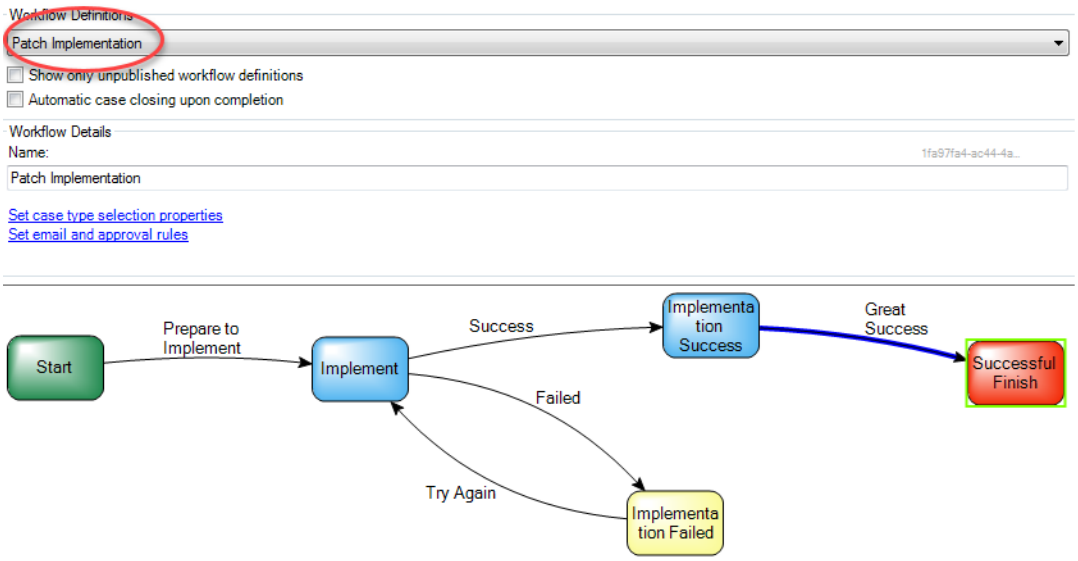
NOTE This workflow definition name must match the value you will specify for the **PatchAssessmentTestCaseWorkflowName** property.

Creating the Patch Implementation and Patch Mitigation Workflows

Now, create a workflow definition for patch implementation and a workflow definition for patch mitigation following the same general steps as the Patch Testing workflow. Remember the naming requirements:

- The name of the **Patch Implementation** workflow definition must match the value you specify for the **PatchAssessment-ImplementationCaseWorkflowName** property.
- The name of the **Patch Mitigation** workflow definition must match the value you specify for the **PatchAssessment-MitigationCaseWorkflowName** property.

The **Patch Implementation** workflow beginning state must contain the **Patch Implementation/Mitigation** checklist you created. For more information, see *Creating the Patch Implementation and Mitigation Checklist* (page 110).



Save the **Patch Implementation** workflow definition and remember its name. You need to specify this exact name when you define the patch management workflow to use for the patch implementation process. For more information about creating workflow definitions, see *Creating a Workflow Definition* (page 93).

Then, create one more workflow definition for **Patch Mitigation**. This workflow should be similar to the **Patch Implementation** workflow, but the states and transitions should be named appropriately for a mitigation plan instead of an implementation. Save the **Patch Mitigation** workflow with an appropriate name and remember its name.

The next step is to define the configuration options that associate a workflow you created with each part of the patch management process. For more information, see *Defining the Patch Management Workflows to Use* (page 115).

Understanding the Workflow Configuration Settings

DOC4000 allows you to adjust a number of workflow-related configuration settings so you can use the workflow definitions you need to manage your cases. You can use Configuration Manager to modify these property values for the **CyberIntegrityWorkflows** object in the PAS Workflows

asset model. If a property does not exist, such as the **PatchAssessment** properties, use Configuration Manager to add that property to the **CyberIntegrityWorkflows** object. For more information, see *Defining the Owner for Each Monitored System* (page 103) and *Defining the Patch Management Workflows to Use* (page 115).

DOC4000 uses the following property values to define the workflows features:

LocationObjectType and LocationPropertyName

Specifies the object type and property that DOC4000 uses to identify the location of an asset. DOC4000 uses the Asset Inventory tree to find the object of the specified object type, and then uses the value of the specified property as the location. These properties are for *change tracking- and policy-related* workflows.

MonitoredSystemOwnerObjectType and MonitoredSystemOwnerPropertyName

Specifies the object type and property that DOC4000 uses to identify the name of the owner of a monitored system. DOC4000 uses the Asset Inventory tree to find the object of the specified object type, and then uses the value of the specified property as the owner's full (first and last) name. These properties are for *change tracking-, policy-, and patch management-related* workflows.

WorkflowDefTest

Specifies the name of the Test workflow definition that validates the required change in a test environment before the actual implementation. This property is for using *policy-related* workflows.

WorkflowDefImplementation

Specifies the name of the Implementation workflow definition that applies the tested change to the production environment. This property is for using *policy-related* workflows.

WorkflowDefSecurityChange

Specifies the name of the workflow definition you created for DOC4000 to used when creating a workflow case for changes categorized as **Security** changes. These cases are used to reconcile the security changes. For more information, see *Configuring Change Tracking Workflows* (page 103).

TransitionToCreateImplementationCase

Specifies the name of the transition in a Test case that upon completion creates the Implementation case. This property is related to the **WorkflowDefTest** and **WorkflowDefImplementation** properties for *policy-related* workflows.

TransitionToMoveMonitoredSystems

Specifies the name of the transition in an Implementation case that upon completion moves the monitored systems from the previous version to the current version of a policy. This property is related to the **WorkflowDefTest** and **WorkflowDefImplementation** properties for *policy-related* workflows.

DelayToCreateSecurityChangeCase

Specifies the number of days since the last import that DOC4000 waits before creating a workflow case for changes categorized as **Security** changes. For more information, see *Configuring*

Change Tracking Workflows (page 103). The Create MOC Cases for Security Changes sequence definition identifies unreconciled **Security** changes, and then creates a case if the specified time period has passed.

PatchAssessmentTestCaseWorkflowName

Specifies the name of the workflow definition Cyber DOC4000 uses when a user clicks the **Start New Test Case** button in the Cyber DOC4000 web interface for patch management.

PatchAssessmentTestCaseLocation

Specifies the value set for the **Location** common field in a new patch testing case.

PatchAssessmentImplementationCaseWorkflowName

Specifies the name of the workflow definition Cyber DOC4000 uses when a user clicks the **Start New Implementation Case** button in the Cyber DOC4000 web interface for patch management.

PatchAssessmentMitigationCaseWorkflowName

Specifies the name of the workflow definition Cyber DOC4000 uses when a user clicks the **Start New Mitigation Case** button in the Cyber DOC4000 web interface for patch management.

Defining the Patch Management Workflows to Use

Cyber DOC4000 requires several configuration settings for the patch management workflow features. You can use Configuration Manager to set these property values for the **CyberIntegrityWorkflows** object. If a property does not exist, use Configuration Manager to add that property, and then to set its value. For more information about these properties, see *Understanding the Workflow Configuration Settings* (page 113).

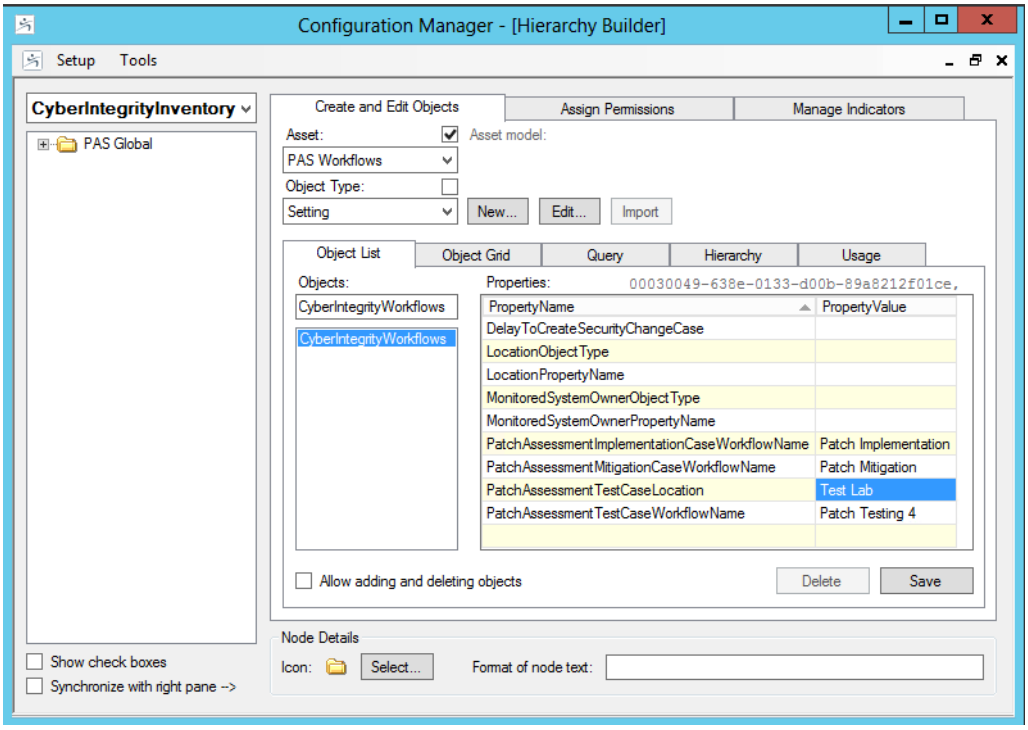
To define which workflows the patch management features use:

1. Open Configuration Manager on the DOC4000 server. To open Configuration Manager, run the following file:

   InstallPath`\DataCollector\ConfigurationManager.exe`

2. In the right pane, check **Asset Model**.
3. In the **Asset** field, select **PAS Workflows**.
4. In the **Object Type** field, select **Setting**.
5. In the **Objects** list on the Object List tab, select **CyberIntegrityWorkflows**. The **Properties** field is populated with the properties for this object.
6. If one or more of the PatchAssessment properties are not listed in the right pane, complete the following steps for each missing property:
   a. Click in the **Property Name** column at the bottom in the first empty row.
   b. Type the name for the property to add, such as PatchAssessmentTestCaseWorkflowName. For more information about these properties, see *Understanding the Workflow Configuration Settings* (page 113).
7. In the **PropertyValue** column, specify values for the following properties:

- **PatchAssessmentTestCaseLocation** - type the value for DOC4000 to use for the **Location** field when creating a patch testing case.
- **PatchAssessmentTestCaseWorkflowName**- type the name of the workflow definition you created for DOC4000 to use when creating a patch testing case.
- **PatchAssessmentImplementationCaseWorkflowName**- type the name of the workflow definition you created for DOC4000 to use when creating a patch implementation case.
- **PatchAssessmentMitigationCaseWorkflowName**- type the name of the workflow definition you created for DOC4000 to use when creating a patch mitigation case.



8. Click **Save**.

Configuring a Vulnerability Management Workflow

To configure and use a vulnerability management workflow in Cyber DOC4000, you need to complete the following configuration requirements:

- Have a license for the Cyber Integrity, PAS Workflows, PAS Vulnerability Management, and PAS Recon asset models.
- Load and configure the Cyber Integrity, PAS Workflows, and PAS Recon asset models. For more information, see Steps for Configuring Cyber DOC4000.
- Load the PAS Vulnerability Management asset model and configure vulnerability management. For more information, see *Loading (Importing) Asset Models* (page 32) and Steps for Implementing Vulnerability Management.

To use workflows, you also need to create and define a Location common field. For more information, see *Defining the Location Common Field for Workflows* (page 87).

Once you have completed the previously listed configuration requirements, you need to create the workflow definition to use for vulnerability management cases, and then specify the name of that workflow definition, so DOC4000 can use it when the user selects a vulnerability and clicks the **Investigate** button. For more information, see the following topics:

- *Creating the Vulnerability Management Workflow* (page 117)
- *Defining the Vulnerability Management Workflow to Use* (page 117)

Creating the Vulnerability Management Workflow

For Vulnerability Management, you need to create one workflow definition. DOC4000 uses this workflow when the user selects a vulnerability and clicks the **Investigate** button. The workflow should address all aspects of the investigation process, including whether you decide to remediate the issue, mitigate it in some way, or ignore it.

As the workflow case progresses from state to state, DOC4000 sets the disposition of the vulnerability matches for that case to the name of the workflow state. When the workflow case is closed, DOC4000 sets the disposition of the vulnerability matches to **Closed,** *workflow-completion-status*, such as **Closed, Remediated**.

NOTE Do not include the word **Closed** in any state of your vulnerability management workflow. Cyber DOC4000 uses this word in the disposition value to determine which vulnerability matched objects to display.

You can create the workflow in the Admin Utility through the **Workflow** link. For more information about workflows, see *Creating and Configuring Workflow Definitions* (page 80).

Defining the Vulnerability Management Workflow to Use

Once you create the workflow with any checklists required to support your vulnerability management processes, you need to specify the name of the workflow to use for vulnerability management.

To specify which workflow to use for vulnerability management cases:

1. Open Configuration Manager on the DOC4000 server. To open Configuration Manager, run the following file:

   InstallPath`\DataCollector\ConfigurationManager.exe`

2. In the right pane, check **Asset Model**.
3. In the **Asset** field, select **PAS Workflows**.
4. In the **Object Type** field, select **Setting**.
5. In the **Objects** list on the Object List tab, select **CyberIntegrityWorkflows**. The **Properties** field is populated with the properties for this object.
6. In the **PropertyValue** column for the **WorkflowDefVulnerabilityInvestigate** property, type the name of the workflow definition you created for DOC4000 to use when creating a vulnerability management case.
7. Click **Save**.

Configuring Baseline Workflows

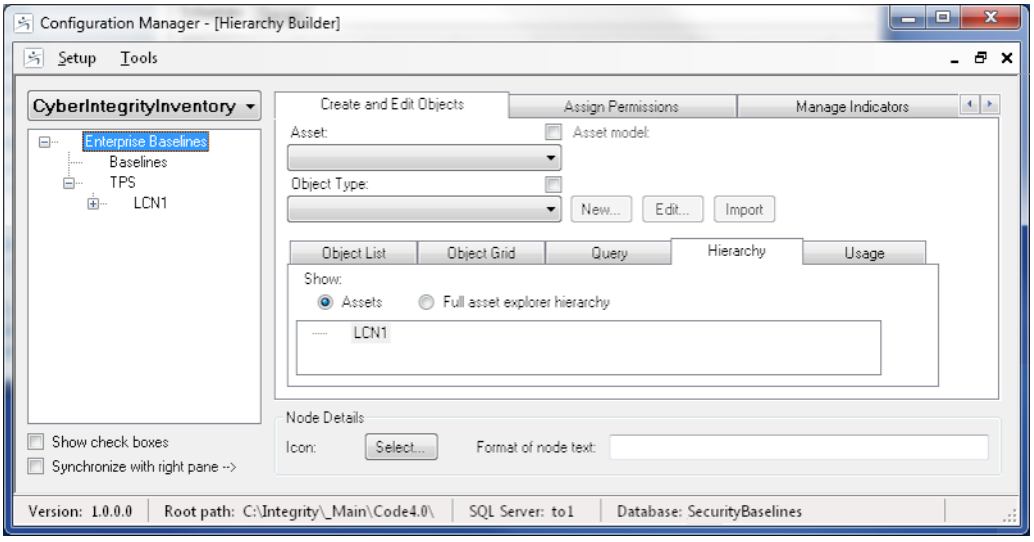
To configure and use a baseline workflow in Cyber DOC4000, you need to complete the following configuration requirements:

- Have a license for the Cyber Integrity, PAS Workflows, and PAS Baselines asset models.
- Load and configure the Cyber Integrity, PAS Workflows, and PAS Baselines asset models. For more information, see Steps for Configuring Cyber DOC4000.
- Load the system-specific asset models you need, such as Honeywell TPS, and configure the assets for those models. For more information, see the *Implementation Guide* for each system asset model.

To use workflows, you also need to create and define a Location common field. For more information, see *Defining the Location Common Field for Workflows* (page 87).

To configure workflows for baselines:

1. Use Configuration Manager to build the asset hierarchy:
   a. Build the hierarchy. For more information, see Understanding and Defining Your Asset Hierarchy.
   b. Assign the assets from the Hierarchy tab to locations in the hierarchy.



2. Use the Asset Model Development Kit (AMDK) to create baseline assets from pre-configured baseline filters:
   a. Open the Asset Model Development Kit (AMDK) on the DOC4000 server. To open the ADMK, run the following file:

      InstallPath`\DataCollector\ADMK.exe`

   b. In the **Asset Model** field, select **PAS Baselines**.
   c. Click **Baselines > Baseline Management**.
   d. Select the **Add** (**+**) button to add a baseline.

e. Select baseline type.

f. Type baseline name.

g. Add source assets from the list on the left to the list on the right.

h. Select a location in the hierarchy.

i. Click **Save**.

3. Create workflow definitions for the **Deviation Dispositions** of **Accept**, **Investigate**, and **Reject**. For more information, see *Creating and Configuring Workflow Definitions* (page 80).

4. Use Configuration Manager to associate each workflow definition with the appropriate disposition:

   a. Open Configuration Manager on the DOC4000 server. To open Configuration Manager, run the following file:

      InstallPath`\DataCollector\ConfigurationManager.exe`

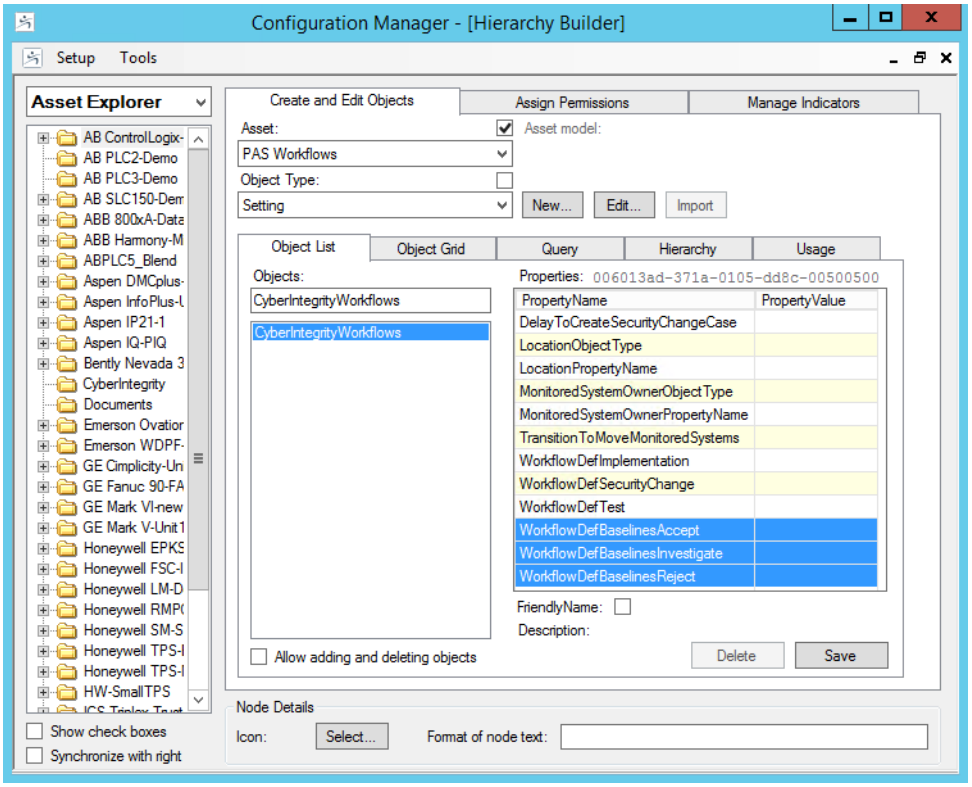
   b. In the right pane, check the **Asset Model** check box on the Create and Edit Objects tab.

   c. In the **Asset** field, select **PAS Workflows**.

   d. In the **Object Type** field, select **Setting**.

   e. On the Object List tab, select **CyberIntegrityWorkflows** in the list of objects.

   f. In the **PropertyName** column, add the **WorkflowDefBaselinesAccept**, **WorkflowDefBaselinesInvestigate**, and **WorkflowDefBaselinesReject** property names if they do not exist.



g. In the **PropertyValue** column, type the name of the corresponding workflow definition you created for the **WorkflowDefBaselinesAccept**, **WorkflowDefBaselinesInvestigate**, and **WorkflowDefBaselinesReject** properties.

5. Use the Asset Model Builder to configure how the workflows obtain locations. You may have already performed this task for other DOC4000 features, such as outlined in *Defining the Location Common Field for Workflows* (page 87):

   a. Open the Asset Model Builder on the DOC4000 server. To open the Asset Model Builder, run the following file:

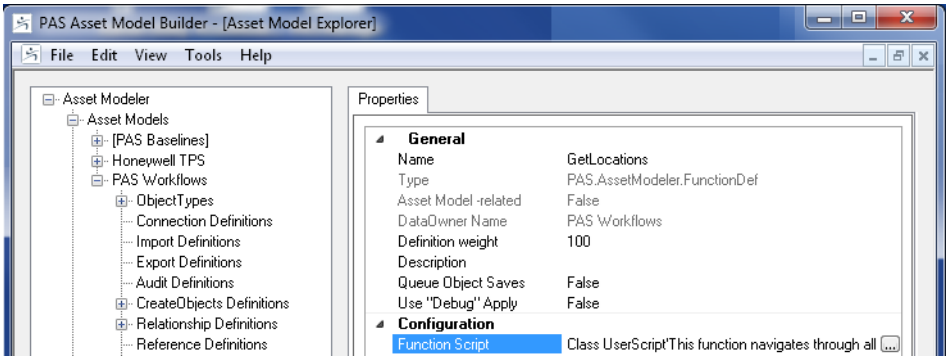
      InstallPath`\DataCollector\AssetModelBuilder.exe`

   b. Click **Edit** > **Asset Model Explorer**.

   c. In the left pane, click the plus sign next to the following nodes to expand these nodes: **Asset Models**, **PAS Workflows**, and **Function Definitions**.

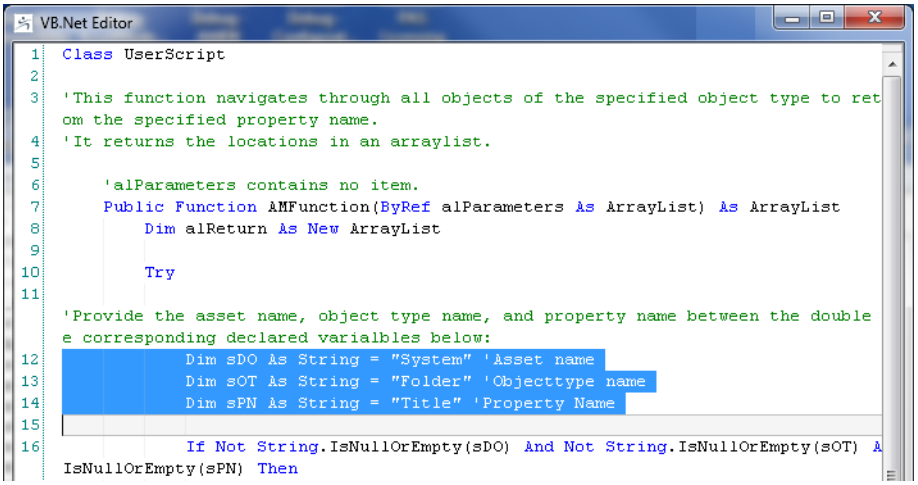
   d. In the left pane, click **GetLocations**. The right pane displays the properties.

   e. In the right pane, click **Function Script**.



   f. Click the ellipses button (**...**) to edit the script. The VB.Net Editor window is displayed.

   g. Specify the appropriate values between the double quotes on lines 12-14 of the script. For example, the following figure shows how to set the location values from the system folders in your asset hierarchy.



   h. Click **Save** on the script editor window.

i. Click **Save** on the Properties tab of the Asset Model Explorer window.

j. Close Asset Model Builder.

SECTION 5

Managing Additional Modules

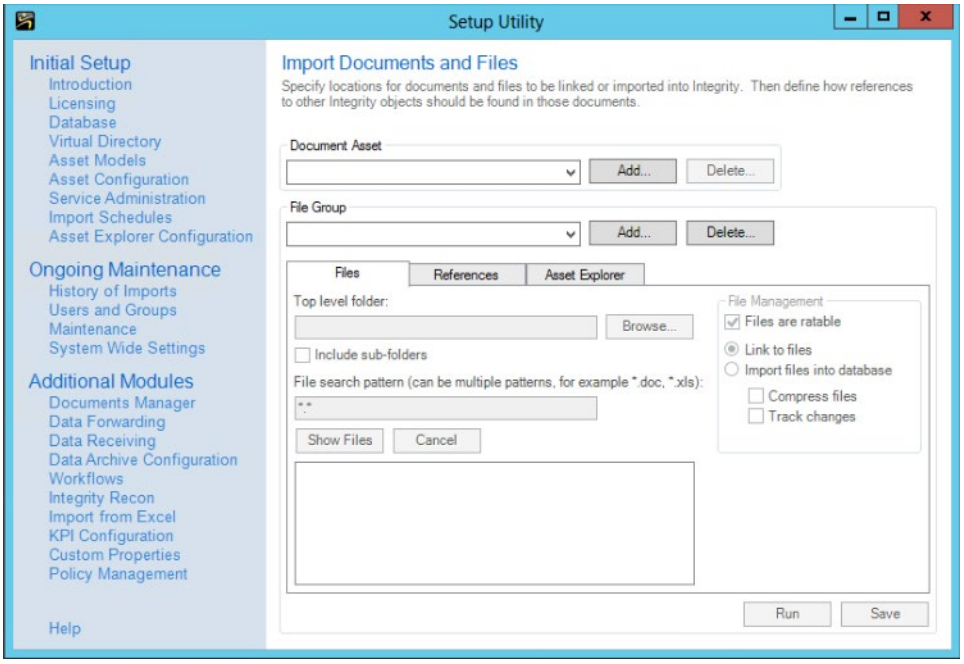
DOC4000 provides a number of additional modules to help you collect and view the information you need. These modules also help you manage the data and define workflows to match your business processes:

- Document Manager allows you to import or link to external documents so you can then create references between these documents and other DOC4000 objects. For more information, see *Using Document Manager* (page 122).
- Custom properties allow you to expand object definitions in DOC4000 so you can track and manage the information you need. This flexibility helps you have all your information in one place. For more information, see *Configuring Custom Properties* (on page 128) and *Importing Custom Property Values from a Microsoft Excel File* (on page 132).
- Key performance indicators can capture and track information about data imports. You can then display this information on the Home tab of the DOC4000 web interface. For more information, see *Configuring KPIs* (on page 134).
- Windows system information and event logs can be collected using the PAS Recon asset model. You can then view this information and event analytics in DOC4000 web interface. For more information, see *Recon Configuration for Windows Systems* (page 135) and *Configuring Event Log Collection and Analytics* (on page 135).
- Inventory items for computers, network devices, and industrial control systems help you identify and analyze both OT and IT assets. You can view summary widgets, browse your environment, and identify the various components that make up a specific endpoint. For more information, see *Configuring Inventory Items* (on page 137).

Using Document Manager

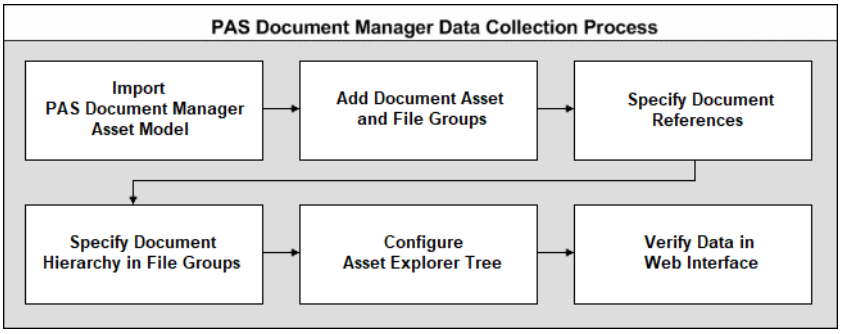
The PAS Document Manager asset model allows you to import or link to external documents, which creates objects for each file in DOC4000. Then, you can create references between these documents and other objects. DOC4000 can search text-based documents, such as Microsoft Word files, Excel files, and many other types of files, to establish references between the documents and existing DOC4000 objects. For example, if a set of documents you import are for management of change, the documents might reference tags that were modified for a specific asset. The references created in DOC4000 can tie the document information to the associated tags.

The **Documents Manager** link in the Admin Utility opens the Import Documents and Files window. This window allows you to configure how documents are imported or linked, define file groups, establish references between the documents and other objects, and define the file structure within asset explorer. Once you complete the configuration, users can work with the documents in the same way as other objects in DOC4000.



To use Document Manager, you need to import the PAS Document Manager asset model. Once the model is imported, the **Documents Manager** link is available in the **Additional Modules** section of the Admin Utility. For more information, see *Steps for Implementing Document Manager* (page 123).

The following figure illustrates the data collection process and how it fits with other configuration tasks.



Steps for Implementing Document Manager

The following list provides guidance for the various tasks involved in planning for and configuring Document Manager. This checklist guides you through the remaining topics in this section.

1. Import the PAS Document Manager asset model. For more information, see *Loading (Importing) Asset Models* (page 32).

2. Create one or more document manager data owners. For more information, see *Adding a Document Manager Data Owner (Asset)* (on page 124).
3. Create one or more file groups in each document manager asset. For more information, see *Adding a File Group* (on page 124).
4. Identify and create references between files in a file group and a defined set of objects. For more information, see *Establishing Document References* (on page 126).
5. Review documents and their viewers in the DOC4000 web interface. For more information, see *Verifying Document Manager Asset Imports* (on page 127).

Documents in a file group can be organized in asset explorer as a set of files at the same level or they can use the hierarchy from the file system. This configuration option is available for each file group. For more information, see *Specifying the Document Hierarchy within File Groups* (page 127).

Adding a Document Manager Data Owner (Asset)

After you have imported the PAS Document Manager asset model, you can add one or more data owners (assets). Unlike other types of data owners you add in DOC4000, PAS Document Manager data owners are not added using the **Asset Configuration** link in the Admin Utility. All PAS Document Manager configuration, including data owners, is done using the **Documents Manager** link in the Admin Utility.

To add a Document Manager data owner:

1. In the Admin Utility, click the **Documents Manager** link.
2. Click **Add** in the **Document Asset** section.
3. Type a new data owner name (the asset to contain the documents), and then click **OK**. Asset (data owner) names can have a maximum of 50 characters.

Next, you need to create file groups and establish the references between the files in those groups and selected object types. Each Document Manager data owner must have at least one file group. For more information about configuring Document Manager, see *Steps for Implementing Document Manager* (page 123).

Adding a File Group

After you have imported the PAS Document Manager asset model and added a data owner, you can then add file groups to the data owner. For more information about configuring Document Manager, see *Steps for Implementing Document Manager* (page 123).

A file group identifies a set of similar files. File groups are the equivalent of object types in DOC4000 and you can use them to organize groups of similar documents. For example, you can create a file group for your Honeywell EPKS documentation files, and then search for references to EPKS systems in those files. Each Document Manager data owner must have at least one file group, but a data owner will often have many file groups.

To add a file group to a data owner:

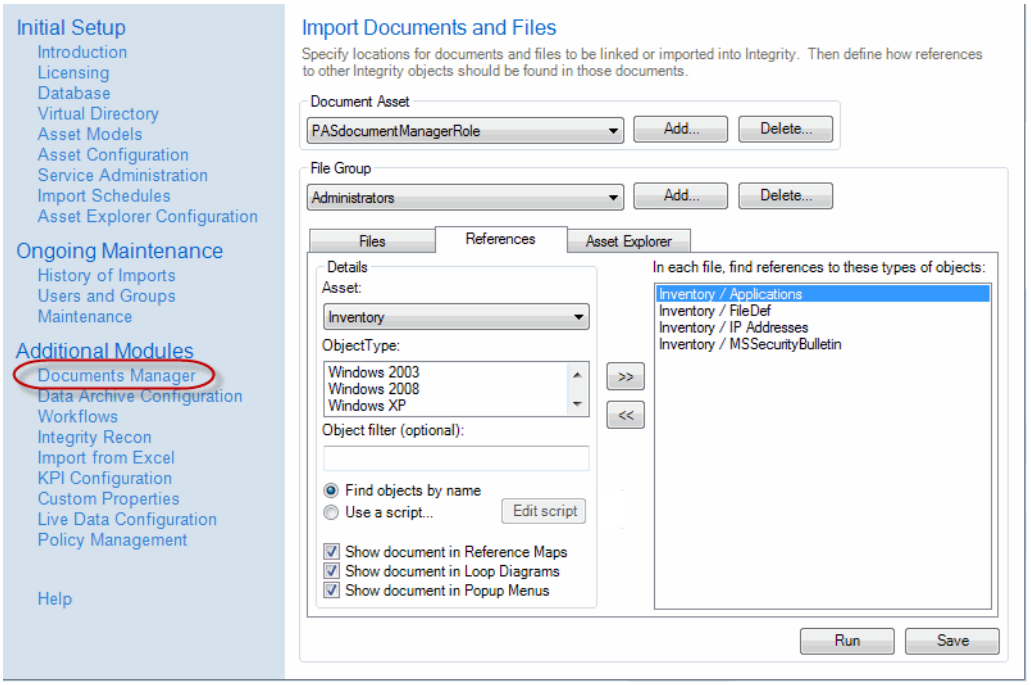
1. In the Admin Utility, click the **Documents Manager** link.
2. In **Document Asset**, select the data owner to add a file group to.

3. Click **Add** in the **File Group** section.
4. Type a name for the new file group, and then click **OK**. The bottom section of the Import Documents and Files window provides several tabs to define the file group and how those files are referenced and organized.
5. Click the **Files** tab to identify the folder where the files are located, which files to include in the file group, whether to import or link to the files, and other file management options.
6. In **Top level folder**, type the folder location where the files are stored. You can also browse to the folder where the documents are located.
7. If you want to also include files in the subfolders, check **Include sub-folders**.
8. In the **File search pattern** field, type a wildcard value that matches one or more files to include, such as `*.doc`. To include multiple types of files, separate each file value with a comma, such as `*.doc,*.xls,*.pdf`.
9. Click **Show Files**. The files in the selected location that match the specified file search pattern are displayed. Review the list to make sure you have identified the set of files you want.
10. If you want users to be able to assign ratings to these files, check **Files are ratable**. When users search, higher-rated files are listed first and take precedence.
11. If you want to link to the files rather than import them, click **Link to Files**. A connection is established to access the files. If the files are moved or deleted from this location, they can no longer be accessed from DOC4000. If you link to files, you cannot select to compress files or track changes for those files.
12. If you want to compress the imported files, check **Compress files**. This compression stores the files in zip format, which can reduce the database size.
13. If you want to track changes for the imported files, check **Track changes**. Each time a file is imported, DOC4000 can compare it with the file by the same name that was previously imported. If the files are different, DOC4000 archives the old file and adds a change tracking record to indicate that the file has changed.
14. Click the **Asset Explorer** tab to specify how the files are organized in asset explorer. By default, a node is added for the data owner. Each file group is then added as a node under the data owner. Then, you can specify whether all files within a file group are listed at the same level or in the structure from the file system.
15. If you want to create a hierarchy within asset explorer that matches the file system structure, click **Maintain file system folder structure**. Imported files create the same folder hierarchy in asset explorer as the structure from where they came.
16. If you want to list all imported files at the same level under the file group node, click **Place all files at the same level**.
17. Click **Save**.
18. Click **Run**.

Repeat this task for each file group and set of files to add. After you have created your file groups and indicated which files to include, you can establish references between objects and files. For more information, see *Establishing Document References* (on page 126).

Establishing Document References

After you have created your file groups and indicated which files to include in each group, you can specify whether to create references between the documents in a file group and existing objects in DOC4000. You can limit the objects to check for each file group. For example, you can create a file group for your EPKS documentation files and limit the search for those files only for references to a single item, such as the EPKS system name.



To establish document-to-object references:

1. In the Admin Utility, click the **Documents Manager** link.
2. In **Document Asset**, select the data owner.
3. In **File Group**, select the file group that identifies the set of files to search.
4. Click the **References** tab.
5. For each set of objects you want to use for establishing references, complete the following steps:
   a. In the **Details** section, select the desired **Asset** and **ObjectType**.
   b. If you want to narrow the list of objects by name, click **Find objects by name** and specify the name to include in the **Object filter (optional)** field. For example, if you want to search the file for references to only a single item, type the name of the item in this field. The name must match exactly.
   c. If you want to narrow the list of objects using a script, contact Technical Support. While working with Technical Support, you can click **Use a script**, and then click **Edit script**. Then, modify and save the script as needed.

d. If you want to show the document information in additional viewers, check the appropriate **Show document in...** check boxes.

e. Click the **>>** button to add the object type and its specified options to the list of objects to search for references.

6. Click **Save**.
7. Click **Run**. Each document in the file group is searched for the specified item. A reference is created for each matching object found.

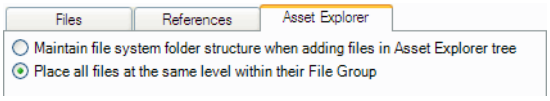
Specifying the Document Hierarchy within File Groups

You can organize documents in a file group in asset explorer as a set of files at the same level or they can use the hierarchy from the file system. This option is available for each file group.

If you select **Include sub-folders** when you create a file group, all documents are placed at the same level within the file group in the asset hierarchy by default. Instead of placing all files at the same level under their file group, you can select **Maintain file system folder structure** on the Asset Explorer tab to create the same folder hierarchy in the asset explorer tree as the structure from where the files came.

To indicate whether documents should be placed in corresponding subfolders under the file group:

1. In the Admin Utility, click the **Documents Manager** link.
2. In **Document Asset**, select the data owner.
3. In **File Group**, select the file group that you want to define the hierarchy for.
4. Click the **Asset Explorer** tab.
5. Click either **Maintain file system folder structure** or **Place all files at the same level**.



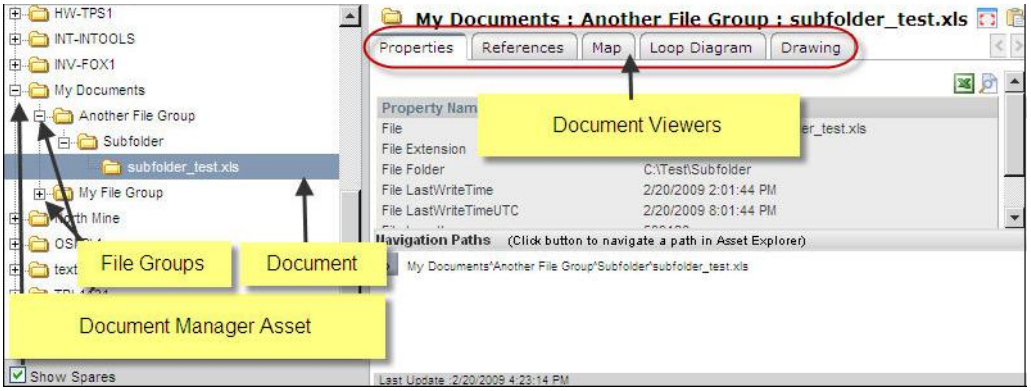
6. Click **Save**.
7. Click **Run**.

Verifying Document Manager Asset Imports

Once you have added documents to DOC4000 through Document Manager, document information is displayed in DOC4000 using various viewers:

- By default, all document objects have the Properties viewer. This viewer shows various information about the document, such as the name, extension, and folder.
- The References, Map, Loop Diagram, and Drawing viewers are added to document objects based on selections you make when configuring Document Manager.

The following example illustrates how DOC4000 displays Document Manager objects in the Asset Explorer view. If DOC4000 does not display the processed files in a manner similar to the following examples, errors might have occurred during the processing.



Configuring Custom Properties

DOC4000 allows you to create sets of custom properties that can extend existing objects. You can also create new object types with these custom properties. You can then populate these properties either by importing the values from a Microsoft Excel spreadsheet or by creating a template for a viewer that allows you to specify the values. For more information, see *Importing Custom Property Values from a Microsoft Excel File* (on page 132).

The **Custom Properties** link in the Admin Utility opens the Configure Custom Properties window. This window provides options to add new properties, select an appropriate editing control such as a text box or check box for each property, group the properties, create a template for a viewer with a set of property groups, and then attach the template to an existing or new object type. Alternatively, you can use the Asset Model Development Kit (AMDK) to configure custom properties. For more information, see the AMDK Help in the `DataCollector` folder for your DOC4000 installation.

After you complete the configuration, the template is displayed as a new tab when users view the details of an object of that type. This new tab allows users to edit the values for the properties on that tab. These properties can then be searched or queried, and the changes can be tracked as other data elements are within DOC4000.

To use custom properties, perform the following tasks:

1. Create the custom properties you need. For more information, see *Creating a Custom Property* (on page 129).
2. Create groups of the custom properties you created. For more information, see *Creating a Custom Property Group* (on page 130).
3. Create a viewer template for each set of custom properties you want to associate with an object type. For more information, see *Creating a Custom Property Template* (on page 131).
4. Specify the values for the custom properties as needed. You can display the new viewer tab for an object and set the values on that tab. If you want to set the property values for many objects, you can import them from a Microsoft Excel file. For more information, see *Importing Custom Property Values from a Microsoft Excel File* (on page 132).

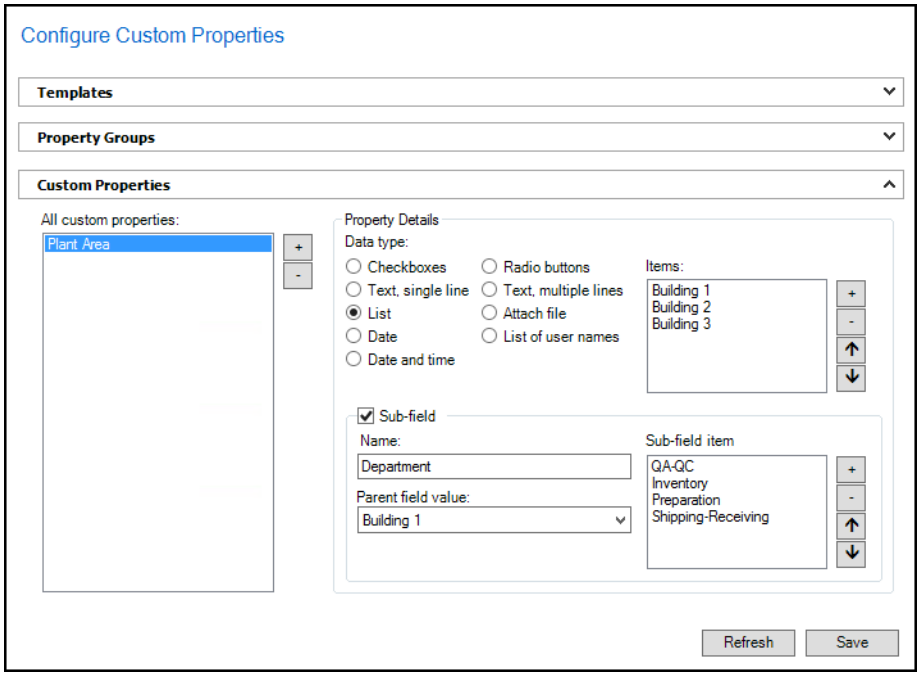
Creating a Custom Property

You can create one or more custom properties to extend the information stored in DOC4000 about various objects, such as adding the department or location within the plant. When you create a custom property, you name the property, specify the type of property, and for some types you specify the supported values. Review the following considerations when creating custom properties:

- The name for each custom property needs to be unique.
- The name for each property, including custom and standard properties, should be unique. If you create a custom property and store it in an existing object type, the custom property value can overwrite a standard property with the same name.
- If you create a custom property and store it in custom object types, the conflicts with standard property names can be avoided. You specify which object types when you attach a template to one or more object types. For more information, see *Creating a Custom Property Template* (on page 131).

To create a custom property:

1. In the Admin Utility, click the **Custom Properties** link. Alternatively, you can use the Asset Model Development Kit (AMDK) to configure custom properties. For more information, see the AMDK Help in the `DataCollector` folder for your DOC4000 installation.
2. If the Custom Properties section is collapsed, click the **Custom Properties** heading to expand the section and display the fields in that section.



3. Click the add (**+**) button next to the **All custom properties** list.
4. On the Add Custom Property window, type a name for the property, and click **OK**.

5. In the **Property Details** area, select an option to specify the type of field that is displayed for the property.
6. If you select **Checkboxes**, **Radio buttons**, or **List**, click the add (**+**) button next to the **Items** list to specify the available values for this property.
7. Use the up and down arrow buttons to order the values in the **Items** list as you want them to be displayed.
8. Click **Save**.

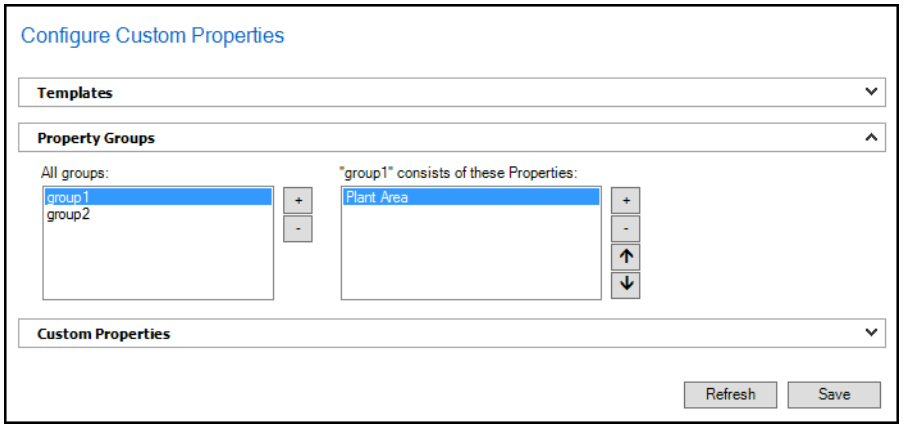
Creating a Custom Property Group

You can create one or more custom property groups, and add one or more custom properties to each group. A custom property can be in more than one property group. Then, you include one or more property groups in a custom property template and attach the template to one or more object types. This process allows you to use the same custom property for multiple object types and arrange the properties as you need.

When you create a custom property group, use a unique name to identify the group.

To create a property group:

1. In the Admin Utility, click the **Custom Properties** link. Alternatively, you can use the Asset Model Development Kit (AMDK) to configure custom properties. For more information, see the AMDK Help in the `DataCollector` folder for your DOC4000 installation.
2. If the Property Groups section is collapsed, click the **Property Groups** heading to expand the section and display the fields in that section.



3. Click the add (**+**) button next to the **All groups** list.
4. On the Add Groups window, type a name for the group, and then click **OK**.
5. Add one or more properties to this property group by completing the following steps for each property you want to add:
   a. In the **Custom Properties** section, select the property in the **All custom properties** list you want to add to the property group.
   b. In the **Property Groups** section, click the add (**+**) button to the right of the **consists of these Properties** list.

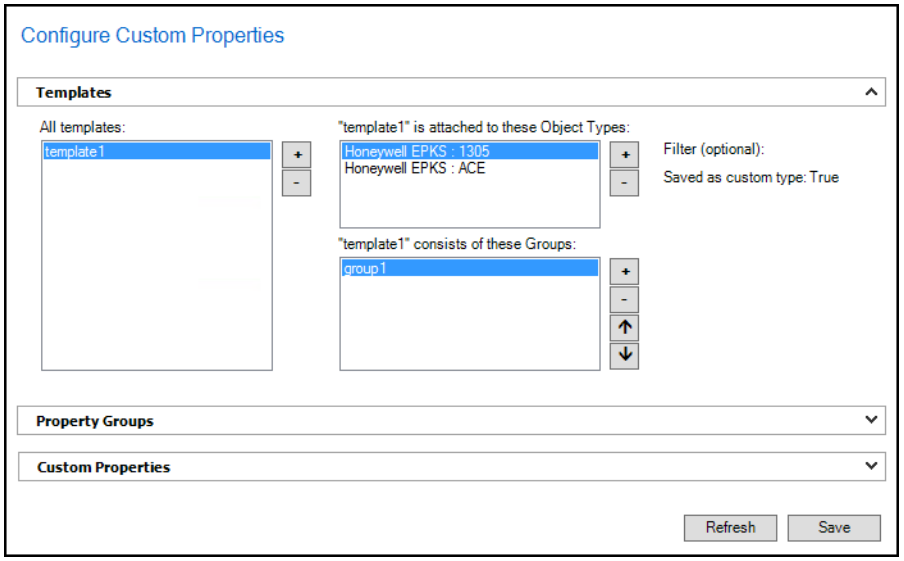
6. Use the up and down arrow buttons to order the properties in the **consists of these Properties** list as you want them to be displayed in the group.
7. Click **Save**.

Creating a Custom Property Template

When you create a custom property template, you specify the custom property groups to include in the template. You also specify the object types to attach the template to. When you specify the object types, you indicate whether to create a custom object type or to add the properties to an existing object type. If you check the **Save as Custom Type** check box, DOC4000 uses the selected object type name and creates a new object type called `User.`*typename*, where *typename* is the name of the selected object type. This new object type extends the selected object type and is used for related functions going forward.

To create a template:

1. In the Admin Utility, click the **Custom Properties** link. Alternatively, you can use the Asset Model Development Kit (AMDK) to configure custom properties. For more information, see the AMDK Help in the `DataCollector` folder for your DOC4000 installation.
2. If the Templates section is collapsed, click the **Templates** heading to expand the section and display the fields in that section.



3. Click the add (**+**) button next to the **All templates** list.
4. On the Add Template window, type a name for the template, and click **OK**.
5. Click the add (**+**) button next to the **is attached to these Object Types** list. The Select Object Types window is displayed.
6. In **Assets**, select the asset with the object type you want to set the custom property values for.
7. In **Types**, select the object type you want to set the custom property values for. You can also type the name of a new object type.
8. If you want to apply the template only to objects that meet specific criteria, type a filter in the **Filter** field.

9. If you want to save the custom properties as additional properties in the selected object type, clear the **Save as Custom Type** check box. Leaving this check box checked creates a custom object type with the custom properties.
10. Click **OK**.
11. Add one or more property groups to this template by completing the following steps for each property group you want to add:
    a. In the **Property Groups** section, select the property group in the **All groups** list you want to add to the template.
    b. In the **Templates** section, click the add (**+**) button to the right of the **consists of these Groups** list.
12. Use the up and down arrow buttons to order the property groups in the **consists of these Groups** list as you want them to be displayed in the viewer tab.
13. Click **Save**.

Deleting a Custom Property, Property Group, or Template

When you delete a custom property, the existing values and properties are not deleted from the DOC4000 database. The custom property is removed only from its custom property groups.

When you delete a custom property group, the group is removed from its templates, but the custom properties within that group remain defined and are in any other property groups that include them.

When you delete a template, that viewer tab is no longer available. In each of these cases, the existing values for the custom properties are still displayed on default Properties tab for the associated object types.

To delete a template, property group, or custom property:

1. In the Admin Utility, click the **Custom Properties** link. Alternatively, you can use the Asset Model Development Kit (AMDK) to configure custom properties. For more information, see the AMDK Help in the `DataCollector` folder for your DOC4000 installation.
2. If the appropriate section is collapsed, click the heading for that section to expand the section and display the fields in that section.
3. Click the item, such as a template, group, or property, that you want to delete.
4. Click the delete (**-**) button.
5. Click **Yes** on the confirmation message window.
6. Click **Save**.

Importing Custom Property Values from a Microsoft Excel File

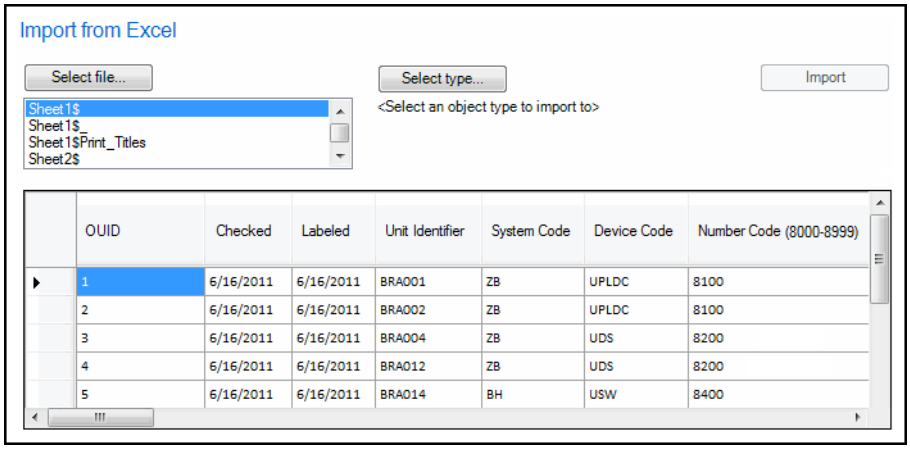
Once you create a custom property template and attach it to one or more object types, you can select an object and then use the tab defined by the template to populate the custom properties for the associated object. Rather than setting these property values one object at a time, you can import the property values for many objects from a Microsoft Excel file.

The **Import from Excel** link in the Admin Utility displays the Import from Excel window, which allows you to import custom property values for objects. Each row in the spreadsheet represents an object and each column is a property for the object. The Microsoft Excel file must be formatted as follows:

- The first row provides the name of the property for each column, such as OUID, Checked, Labeled, and others.
- The first column defines the OUID of the object and it must be unique. If multiple rows have the same value in the first column, the same object will be modified multiple times and the last row of values will overwrite previous row values.
- Each column, starting with the second column, provides a value for a custom property. Make sure you have already defined each custom property and its name exactly matches the property name specified in the first row of the column.

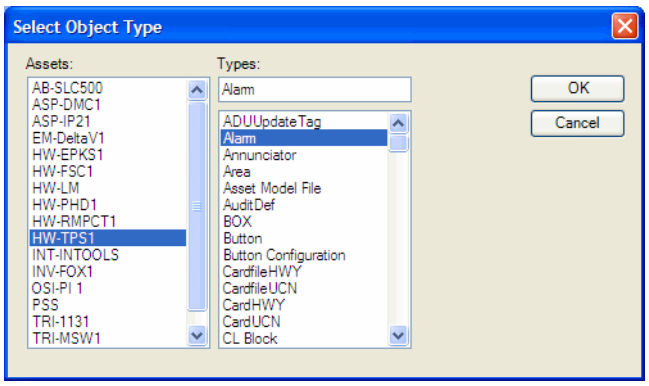
To import custom property values from an Excel spreadsheet:

1. In the Admin Utility, click the **Import from Excel** link.
2. Click **Select file**.
3. Navigate to the location of the Microsoft Excel file, select it, and then click **Open**.



4. The list below the **Select file** button displays the names of worksheets and name ranges from the Microsoft Excel file. The first item is selected and a preview of the first 100 rows is displayed in the grid. Click on a different worksheet or range to view information for the selected item. You can select only one item at a time.

5. Click **Select type**. The Select Object Type window is displayed.

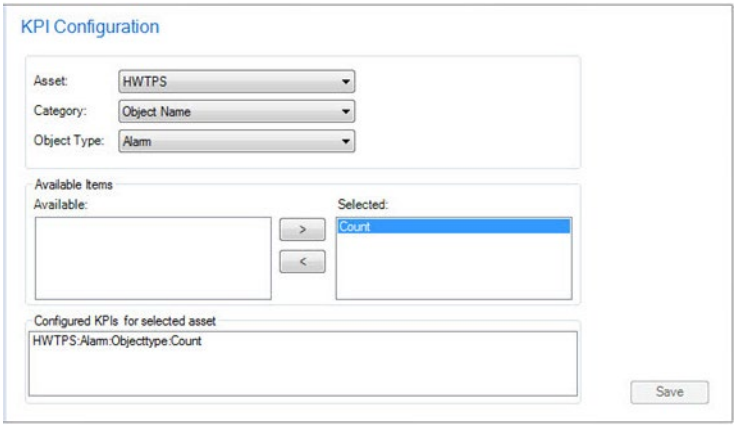


6. In **Assets**, select the asset with the object type you want to set the custom property values for.
7. In **Types**, select the object type you want to set the custom property values for. You can also type the name of a new object type.
8. If you want to save the custom properties as additional properties in the selected object type, clear the **Save as Custom Type** check box. Leaving this check box checked creates a custom object type with the custom properties.
9. Click **OK**.
10. Click **Import** to import the Excel file and set the property values.

Configuring KPIs

A key performance indicator (KPI) can help you measure, track, and evaluate performance over time. DOC4000 allows you to define key performance indicators that users can then display on the Home tab of the Automation web interface.

The **KPI Configuration** link in the Admin Utility allows you to specify the key performance indicators to record for every data import. By default, DOC4000 does not capture KPIs during data imports. You need to configure the KPIs you want to capture for each asset, such as the number of file changes or import data issues.



To configure a KPI to make it available for an asset:

1. In the Admin Utility, click the **KPI Configuration** link.
2. In **Asset**, select the asset you want to capture the KPI for.
3. In **Category**, select the type of indicator you want to capture. These categories are defined as follows:
   - **Object Name** - allows you to count the number of items, such as alarms.
   - **Notes** - allows you to identify notes for the selected object type.
   - **Modification** - allows you to identify the additions, deletions, or modifications for the selected object type.
   - **References** - allows you to identify references for the selected object type.
   - **Issues** - allows you to identify issues with import data, such as missing files.
4. In **Object Type**, select the type of objects you want to include in the KPI.
5. In **Available**, select one or more KPIs, and then click the **>** button to add it to the **Selected** list.
6. Click **Save**.

Recon Configuration for Windows Systems

The PAS Recon asset model (Recon) provides a plant-wide solution for monitoring Windows computer assets. This asset model allows DOC4000 to gather and display the software, services, hardware, system performance, and other essential information for the servers, workstations, and desktop computers on the Process Control Network (PCN). This feature provides the automation organization with a mechanism to manage nodes on the PCN, while also allowing IT to view the control layer without directly accessing the control systems.

With the PAS Recon asset model, DOC4000 identifies firmware revisions and references across the system, facilitating a common operating environment. DOC4000 also provides system health reporting and includes both reactive monitors such as hard drive capacity, plus proactive alerts about incompatible or missing updates.

The PAS Recon asset model is a separately licensed module. If your license includes this model, you can load the PAS Recon asset model into DOC4000. Then, the **Recon** link in the Admin Utility is available and allows you to configure aspects of the asset model.

The PAS Recon asset model can be updated separately from DOC4000. In this case, changes to the configuration instructions may be made between DOC4000 releases. For more information about this asset model and the latest configuration instructions, see the *PAS Recon Implementation Guide*, which describes several important configuration tasks, from data collection to import.

Configuring Event Log Collection and Analytics

DOC4000 can collect Windows event log data from your PAS Recon assets. The fields on the Configure Windows Event Log Collection window in the Admin Utility allow you to configure this event log collection.

The PAS Recon asset model writes collected Windows event log files to a folder on the DOC4000 server or data collector. DOC4000 then processes those files and stores the Windows event log data in a database. This topic describes the DOC4000 configuration parameters for Windows

event log collection. For more information about loading and configuring the PAS Recon asset model, see the *PAS Recon Implementation Guide*.

NOTE DOC4000 caches Windows event log data to provide better performance. This cached data is refreshed each hour. Therefore, it can take up to an hour for newly processed Windows event log data to be displayed in DOC4000.

To configure event log collection:

1. Follow the instructions in the *PAS Recon Implementation Guide*.
2. In the Admin Utility, click the **Windows Event Log** link.
3. If you have not created the database to store the collected Windows event log data, select the **Estimated # of Computers** to collect data from, and then click **Create Database**.

   NOTE The **Create Database** button is disabled if a database with the reserved name exists.
4. Complete the following fields, and then click **Save Collection**.
   - **Parent Path**: Specify the folder where the Windows event log data files and folders should be stored. DOC4000 processes the files and folders stored in this location. If there are multiple levels of folders in the specified location, DOC4000 uses the folder structure to identify the assets and their associated event log data. If you choose to archive files, DOC4000 creates an `Archive` subfolder in this location and stores archived data in that folder.
   - **Text Escape Characters**: Specify the characters used to enclose values in the Windows event log files. The default is the double quote (). These characters can enclose values that include commas or line breaks.
   - **Process Security Event Details: Specify whether to extract security information from the Windows event log. Select this option for computers configured for non-English language regions.**
   - **Groom Files On Success**: Specify whether to delete a file once the Windows event data is successfully written to the database.
   - **Groom Data From Database**: Specify whether to remove data from the database to limit database size. If you check this check box, you need to specify the number of months of data to keep.
   - **Keep *X* months of data**: Specifies the number of months of data to keep in the database. This field is available only if you checked the **Groom Data From Database** check box. For example, if it is March 9th and this field is set to **1**, DOC4000 keeps the Windows event log data since March 1. If this field is set to **3**, DOC4000 keeps the Windows event log data since January 1.
5. If you want to archive event log data, complete the following steps:
   a. Check the **Enable Daily Archive** check box. DOC4000 creates an `Archive` subfolder in the **Parent Path** location. Each day, DOC4000 uses the specified **Filter Criteria** to select data to save as a CSV file. In the `Archive` folder, each data owner has its own folder and in its folder is a set of monthly `.zip` files. Each `.zip` file has the CSV files for that data owner and month.

   b. If you want to filter the type of events included in the archived data, specify the criteria in the **Filter Criteria** field. By default, all events are included in the archive. The format of the

Filter Criteria field is a T-SQL WHERE clause. For more information about this field and example criteria, click the **Filter Criteria Help** link.

c. Click **Save Archive**.

6. Manually start the pasWindowsEventLog service on each DOC4000 server and data collector and where Windows event logs are processed. For more information, see *Defining Your Service Accounts* (page 19).

NOTE You should also configure this service to start automatically on these computers.

Configuring Inventory Items

Within DOC4000, you can look at assets by physical location, and drill-down to a particular area or asset. With inventory items, you can also identify and evaluate systems and their individual components.

An inventory item is an asset or component of an asset, such as an installed software product or a hardware component. The PAS Inventory Items asset model uses information from the other asset models and assets to build a set of inventory items in Cyber DOC4000.

To configure inventory items in Cyber DOC4000:

1. After your initial installation and setup of DOC4000, import and configure the latest versions of the following asset models:
   - PAS Cyber Integrity Asset Model
   - Asset models for your environment
   - PAS Recon asset model
   - PAS Network Devices asset model
   - PAS Inventory Items asset model

   NOTE For more information, see the *Implementation Guide* for each asset model.

1. If you have upgraded DOC4000, complete the following steps:
   a. Re-import the latest versions of existing asset models for DOC4000 to see new data in **Inventory**.
   b. Recalculate widgets shown on the Inventory Summary window.

      NOTE If you re-import asset models at any time, you must recalculate widgets shown on the Inventory Summary window.

2. Run sequence definitions for the PAS Inventory Items asset model for the assets in your environment. For more information, see *Scheduling and Running Data Imports with the Admin Utility* (page 36).
3. Complete the following steps for the Cyber Integrity asset model. For more information, see Scheduling and Running Data Imports with the Admin Utility in the *Administration Guide*.
   a. Create a new schedule to run the new **Update Inventory Items** sequence definition to ensure that the **Update Inventory Items** sequence definition runs whenever the model is imported. This is the last schedule to run after all other asset models.

b. Run this new schedule for the Cyber DOC4000 asset model. This step ensures that your inventory items display in **Inventory Summary** and **Inventory Browse** windows.

4. Install the latest PAS Dashboard, connect with the DOC4000 database, and import the Cyber DOC4000 standard asset model for Dashboard. For more information, see the *PAS Dashboard User Guide*.
5. Navigate to the Cyber DOC4000 web application and click **Inventory** to validate your configuration.

For more information about using Inventory Items, see the *User Guide*.

SECTION 6

Troubleshooting DOC4000

This section provides several troubleshooting tasks to help you resolve potential installation and configuration issues. If you have any issues, please contact Technical Support.

Viewing the Test Page

A test page is available to view information regarding the DOC4000 installation and configuration. This test page ensures the DOC4000 web interface is available.

To launch the test page:

1. Start a supported browser.
2. In the **Address** URL field, type the following URL, and click **Go**:

   `http://`*ServerName*`/`*VDirName*`/DOC4000Test.aspx`

   ServerName is the name of the web server where DOC4000 is hosted and *VDirName* is the name of the virtual directory for the web application, such as DOC4000.

Server Application Unavailable Error

When you have multiple applications on a single Microsoft IIS server and the applications use different versions of the .NET Framework, you must configure the applications to use separate application pools. Without separate application pools, the **Server Application Unavailable** message may be displayed when you run DOC4000.

Use the Microsoft IIS management tool to create a new application pool and assign applications so that each pool contains only the applications that use the same .NET Framework version.

To create a new application pool and configure DOC4000 to use that pool:

1. On the DOC4000 server, click Windows **Start** > **Run**.
2. Type `inetmgr`, and then click **OK** to start Internet Information Services (IIS) Manager.
3. In the left pane, expand the local computer.
4. Right-click on **Application Pools** and click **Add Application Pool**.
5. Type a new **Application Pool Name**, select the **.NET CLR version** for the pool to use, and then click **OK**.

6. Configure DOC4000 to use the new application pool by completing the following steps:
    a. In the left pane of the Internet Information Services (IIS) Manager window, expand the **Sites** folder under the local computer.
    b. Expand the **Default Web Site** folder.
    c. Right-click on the DOC4000 folder, and then click **Manage Application > Advanced Settings**.
    d. Change the **Application Pool** field to the new application pool you created.
    e. Click **OK**.

Missing Graphics in the DOC4000 Web Interface

DOC4000 allows you to use custom images in the DOC4000 web interface. In previous versions, these images were stored in the *InstallPath*`/Images` folder and the `ig_common` virtual directory was defined for this folder location. These images are now stored in the *InstallPath*`/Images/old_common` folder and the virtual directory is no longer defined or used.

If you have missing images after you upgrade DOC4000, copy your image files from the *InstallPath*`/Images` folder to the *InstallPath*`/Images/old_common` folder.

Missing Graphics and Control Maps Due to Directory Permissions

When viewing graphics and control maps, DOC4000 temporarily copies files to a `Temp` folder before displaying them. This `Temp` folder is in the location where you installed DOC4000, `C:\Program Files (x86)\PAS\Integrity` by default. Although the permissions for the folder are set automatically, if you experience problems displaying graphics or control maps, make sure the `Temp` folder has permissions for users to read and execute files in the folder.

If the proper access is not given to this folder, you might see the following types of problems:

- Control maps are not displayed in the DOC4000 web interface.
- Graphic images are not displayed in some viewer tabs.
- Graphic images are not displayed in hardware overviews.

Although the permission is set automatically, if any of these problems occur, verify that users have permissions to read and execute files in the `Temp` folder.

To view and modify folder permissions:

1. In Windows File Explorer, navigate to the location where you installed DOC4000, `C:\Program Files (x86)\PAS\Integrity` by default.
2. Right-click on the `Temp` subfolder, and then click **Properties**.
3. Click the **Security** tab.
4. Click **Edit**.
5. Click on the designated group or user.

6. Check **Allow** for the **Read & Execute** option.
7. Click **Apply**.
8. Click **OK**.

Microsoft IIS Is Timing Out

In some cases, DOC4000 logs off a user when it does not recognize activity for more than 20 minutes. Changing the session time-out value in Internet Services Manager or other web server utilities does not change the DOC4000 session time-out definition. The ASPX scripts in DOC4000 run as an ASP.NET application. Therefore, the session time-out value is controlled by the .NET Framework instead of Internet Information Services (IIS).

To change the DOC4000 session time-out value, set the new value in the `web.config` file located where you installed DOC4000, `C:\Program Files (x86)\PAS\Integrity` by default. If you increase the session timeout to a value greater than 20 minutes, you also need to increase the idle time-out **for the Default**AppPool application pool.

To change the DOC4000 session time-out value:

1. On the DOC4000 server, use a text editor to open the *InstallPath*`\web.config` file.
2. Change the value of the `timeout` attribute for the `sessionState` element to the designated number of minutes. For example, to change the session time-out to one hour, change the `timeout` attribute value to `60` as illustrated in the following example, which does not show all the attributes:

   ```
   <sessionState mode="InProc" ... timeout="60" />
   ```

   NOTE Entries in the `web.config` file are case sensitive and take effect immediately. You must use sessionState, and you *cannot* use sessionstate.
3. Save the *InstallPath*`\web.config` file.
4. If you increased the session timeout attribute to a value greater than 20, increase the idle time-out for the **DefaultAppPool** application pool by completing the following steps:
   a. On the DOC4000 server, click Windows **Start** > **Run**.
   b. Type `inetmgr`, and then click **OK** to start Internet Information Services (IIS) Manager.
   c. In the left pane, expand the local computer.
   d. Select the **Application Pools** node to display **DefaultAppPool** in the right pane.
   e. Right-click on **DefaultAppPool**, and then click **Advanced Settings**.
   f. In the **Process Model** section of the Advanced Settings window, change the value for the **Idle Time-out (minutes)** field to a number that is greater than or equal to the session timeout value you defined in the `web.config` file.
   g. Click **OK**.

Reports Longer Than One Page Do Not Run

In some cases, reports consisting of more than one page do not print because of permissions issues with creating temporary files. If this problem occurs, the account that runs the IIS service must be granted full permissions on the `C:\Documents and Settings` folder. The account is typically ASPNET or Network Service, but it might be set up differently by your network administrator.

To view and modify directory permissions for temporary report files:

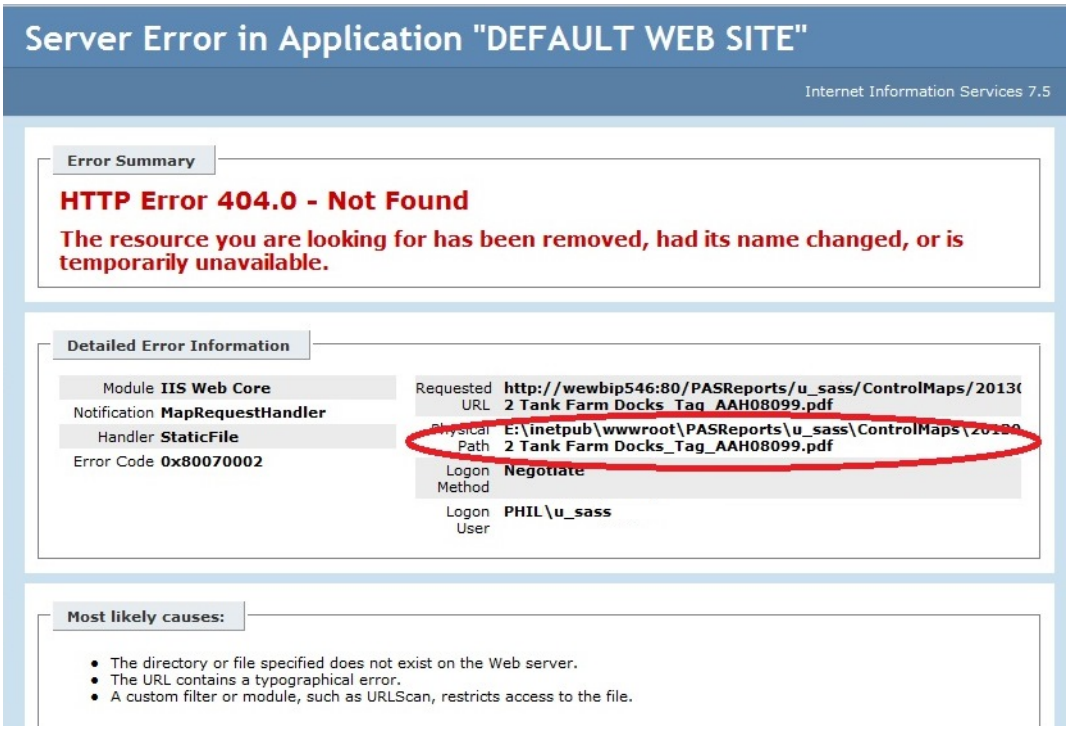
1. In Windows File Explorer, navigate to `C:\`.
2. Right-click on the `Documents and Settings` folder, and then click **Properties**.
3. Click the **Security** tab.
4. Click **Edit**.
5. Click the designated group or the user account that runs the IIS service.
6. Select **Allow** for each option in the **Permissions** area.
7. Click **Apply**.
8. Click **OK**.

Setting the Admin Utility to Run as an Administrator

The DOC4000 Admin Utility needs to run as an administrator. If you do not set it up to run as an administrator, when you click on an area, such as setting the Virtual Directory, the Admin Utility displays an error message.

Unable to Open Control Map Reports

When DOC4000 generates reports, DOC4000 stores the reports in a `Reports` folder it creates at the same level as the folder where you installed DOC4000, such as `E:\PAS\Reports`. In some cases, when you open the report URL, an error message is displayed similar to the following figure:



This error message indicates that the system is using the wrong path. In this case, the error message shows the location is `E:\inetpub\wwwroot\PASReports`.

To fix this incorrect path issue:

1. On the DOC4000 server, click Windows **Start > Run**.
2. Type `inetmgr`, and then click **OK** to start Internet Information Services (IIS) Manager.
3. In the left pane, expand the local computer.
4. Expand the **Sites** folder under the local computer.
5. Right-click **Default Web Site** (or whichever node the virtual path for the DOC4000 website is created under), and then click **Add Application**.
6. In **Alias**, type the name of the folder identified in the circled area of the error message that follows `wwwroot\`, such as `PASReports`.
7. Change the application pool by completing the following steps:
   a. Click **Select**.
   b. In **Application pool**, select DOC4000**AppPool**.

c. Click **OK** to close the Select Application Pool window.

8. In **Physical Path**, specify the location where the reports are generated, such as `E:\PAS\Reports`.
9. Click **OK** to close the Add Application window.
10. Restart DOC4000, and then close the Internet Information Services Manager window.

NOTE If there are still issues, check that `.pdf` and `.vsd` are allowed in **Request Filtering** and **MIME Types** on the IIS Main Directory.

Runtime Web Error in DOC4000

If a **Runtime Error** message is displayed, an application error occurred on the DOC4000 server. The current custom settings for the application prevent the details of the application error from being viewed remotely for security reasons. You can view the details by using a browser running directly on the DOC4000 server.

If you want to allow the details of the error message to be viewable on remote machines, create a `<customErrors>` tag in the `web.config` file located in the root folder of the DOC4000 web application. Set the `mode` attribute in this `<customErrors>` tag to `Off`.

```
<!-- Web.Config Configuration File -->
<configuration>
   <system.web>
      <customErrors mode="Off" />
   </system.web>
</configuration>
```

You can replace the displayed error page with a custom error page by modifying the `defaultRedirect` attribute of the `<customErrors>` configuration tag in the `web.config` file to point to a custom error page URL.

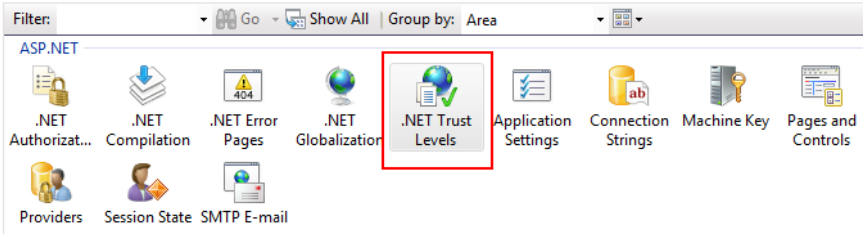
```
<!-- Web.Config Configuration File -->
<configuration>
   <system.web>
      <customErrors mode="RemoteOnly" defaultRedirect="mypage.htm" />
   </system.web>
</configuration>
```

You can also set **.NET Trust Levels** to **Full Internal** in IIS.

To set the .NET Trust Levels for DOC4000:

1. On the DOC4000 server, click Windows **Start > Run**.
2. Type `inetmgr`, and then click **OK** to start Internet Information Services (IIS) Manager.
3. In the left pane, expand the local computer.
4. Expand the **Sites** folder under the local computer.
5. Expand **Default Web Site** (or whichever node the virtual path for the DOC4000 website is created under).
6. Click DOC4000.

7. In the middle pane, double-click the **.NET Trust Levels** icon.



8. In **Trust level**, select **Full (internal)**.
9. Under **Actions** in the right pane, click **Apply**.

Compilation Error in the DOC4000 Web Interface

If a **Compilation Error** message is displayed, an error occurred during the compilation of a resource required to service this request. Review the following specific error details and modify the source code appropriately.

Compiler Error Message:

```
CS0016: Could not write to output file
'C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET
Files\DOC4000\272ed8d5\f97ae7a\App_GlobalResources.apwe5sr7.dll' --
'Access is denied.'
```

Source Error:

```
[No relevant source lines]
```

Source File: Line: 0

```
C:\Windows\SysWOW64\inetsrv> "C:\Windows\Microsoft.NET\Framework\v2.0.50727\csc.exe" /t:library /utf8output /R:"C:\Windows\assembly\GAC_MSIL
\00255922_8267ce01\ActiveReports3.DLL" /R:"C:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files\doc4000\272ed8d5\f97ae7a\as


Microsoft (R) Visual C# 2005 Compiler version 8.00.50727.4927
for Microsoft (R) Windows (R) 2005 Framework version 2.0.50727
Copyright (C) Microsoft Corporation 2001-2005. All rights reserved.

error CS0016: Could not write to output file 'c:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files\doc4000\272ed8d5\f97ae7a
```

To solve this problem:

1. Grant full access to **Network Service** and **IIS_IUSRS** to `C:\Windows\temp`.
2. Restart IIS.

For more information about this issue, see the following Microsoft article:

http://blogs.msdn.com/b/viag/archive/2007/02/09/compiler-error-message-cs0016-could-not-write-to-output-file-c-windows-microsoft-net-framework-v1-1-4322-temporary-asp-net-files-myapp-fadda49e-bbdb0b87-eqdatzch-dll-access-is-denied.aspx
http://blogs.msdn.com/b/viag/archive/2007/02/09/compiler-error-message-cs0016-could-not-write-to-output-file-c-windows-microsoft-net-framework-v1-1-4322-temporary-asp-net-files-myapp-fadda49e-bbdb0b87-eqdatzch-dll-access-is-denied.aspx

Issues with Report Generation for PDF or Visio

If the folders do not exist, create the `Desktop` folder in those locations. Also make sure that the NETWORK SERVICE Windows account has full permission to the `Desktop` folders. You might need to modify COM security to explicitly set the permission for the NETWORK SERVICE Windows account:

To set the appropriate COM security permission:

1. In Windows Run, enter `dcomcnfg`.
2. Expand **Component Services** and **Computers**, and then right click **My computer** and click **Properties**.
3. Click the **COM Security** tab, and under **Launch and Activation Permissions** click **Edit Default**.
4. Add the NETWORK SERVICE account if needed, and then grant NETWORK SERVICE **Local Launch** and **Local Activation** permissions.

To ensure compatibility between Visio and DOC4000, open any Visio file (`*.vsd`), and ensure that the file opens and is displayed correctly. When Visio launches the first time, it may display several windows requesting initial display settings and licenses. After you make sure that Visio opens files correctly, close Visio.

Copyright

Trademarks

Customer Support and Technical User Forum