opentext™

OpenText™ AppEnhancer

Administration Guide

This document describes OpenText AppEnhancer concepts and provides guidelines on how to manage the OpenText AppEnhancer software.

EAXCORE240200-AGD-EN-1

OpenText™ AppEnhancer
Administration Guide

EAXCORE240200-AGD-EN-1
Rev.: 2024-June-20

This documentation has been created for OpenText™ AppEnhancer CE 24.2.
It is also valid for subsequent software releases unless OpenText has made newer documentation available with the product, on an OpenText website, or by any other means.

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Tel: +1-519-888-7111
Toll Free Canada/USA: 1-800-499-6544 International: +800-4996-5440
Fax: +1-519-888-0677
Support: https://support.opentext.com
For more information, visit https://www.opentext.com

Table of Contents

Preface

This document describes OpenText AppEnhancer concepts and provides guidelines on how to manage the AppEnhancer software. The *OpenText AppEnhancer Release Notes* provide information on hardware and software requirements.

Chapter 1

Introduction

AppEnhancer stores, organizes, and manages documents, files, and other business-critical information, and provides fast, security-controlled access to information from Microsoft™ Windows™ or web-based clients. AppEnhancer integrates document imaging, reports management, workflow, and document management services within an easy-to-use Windows-based system.

You can use AppEnhancer Administrator to perform system administration tasks. Additionally, you can use AppEnhancer Administrator to configure data sources, license server connections, and other general configurations, and to complete the setup of your AppEnhancer system by creating applications and configuring user and group security. AppEnhancer is also used frequently to maintain user and group information, modify applications, or maintain the license server connection for a workstation.

OpenText AppEnhancer Installation Guide provides more information on AppEnhancer concepts.

1.1 Logging in to AppEnhancer Administrator

Ensure that your system meets the requirements. For information about the system requirements, see *OpenText AppEnhancer Release Notes*.

To log in to AppEnhancer Administrator, follow these steps:

1. In the browser, type the URL to launch the AppEnhancer Administrator:

   https://<*ip address*>/AppEnhancerAdmin

2. On the login page, you can select either **Global Administration** or a data source. Select **Global Administration** to log in to all data sources and to view and configure the options in the **Environment** and **Server Management** nodes.

3. Select the role for the login session. Each role manages the scope of what you can do in AppEnhancer Administrator during the login session. There are 8 roles supported: Global Administrator, Server Manager, Data Source Administrator, Data Source Manager, Application Manager, User Manager, Resource Monitor, and Report Reader. For more information about the roles, see "Understanding roles" on page 49.

4. Enter the login credentials.

5. Click **SIGN IN**.

When you log in to AppEnhancer Administrator, you are logging in to all of the data sources in AppEnhancer Administrator simultaneously. The user account that you use to log in to AppEnhancer Administrator must meet the following criteria:

- It must exist on all data sources.
- It must have the same password on all data sources.
- It must have the AppEnhancer Administrator user privilege for each data source. This criterion does not apply to the default administrator account (sysop).

If there are several data sources and the password for the default administrator account (sysop) are different in these data sources, you have an option to reset the password for the default administrator account (sysop) during the login process. You can provide the correct old password to reset the password to the specified new one or skip resetting password.

Note: Even if you cannot log in to all data sources with the user account, all data sources that can be logged in to are visible to that user. However, the **Environment**, **Server Management**, and **Reporting** nodes are not visible.

AppEnhancer Administrator supports mixed security providers. If there is a user who is configured to use CM security or Windows security, irrespective of the security provider the data source is configured, you can use that user to allow to log in to the AppEnhancer Administrator.

When you add a new data source to AppEnhancer Administrator, these criteria do not apply until the next time you log in to AppEnhancer Administrator with the new data source.

To add an existing data source into AppEnhancer Administrator, you must ensure that it has a user account that satisfies the preceding criteria before you can add it. However, if the user account that you want to use to log in to AppEnhancer Administrator has a different password in the data source that you want to add (but otherwise satisfies the criteria), you can change the password in AppEnhancer Administrator.

AppEnhancer Administrator also supports Active Directory Federation Services (ADFS), Central Authentication Service (CAS), OpenText Directory Services (OTDS), and Security Assertion Markup Language (SAML) 2.0 security providers.

1.2 Understanding nodes and options

The following table describes the nodes and options in AppEnhancer Administrator:

Node and Option	Description
Environment	
Data Sources	Enables you to configure data sources.
Desktop Credentials	Enables you to configure the Desktop global authentication accounts.
License Servers	Enables you to configure license servers.

Node and Option	Description
Options	Enables you to configure AppEnhancer options, such as the data encryption type.
OTDS Server	Enables you to configure OpenText Directory servers and user attribute mappings.
Storage Management	Enables you to configure connectivity to storage servers.
Application Management	Enables you to design AppEnhancer applications and configure or manage users and groups.
Server Management	
Administrative Services	Enables you to configure the Archive Service, Migration Service, Index Image Import Service, and AutoIndex KeyRef Service.
Auto Retention Filer	Enables you to configure credentials for the Auto Retention Filer service.
Event Dispatch Broker	Enables you to configure the properties of Event Dispatch Broker.
Indexing Service	Enables you to configure settings for the Indexing Service.
Rendering Server	Enables you to configure settings for the Rendering Server.
REST Services	Enables you to configure REST API services.
Web Access Server	Enables you to configure the Web Access Server.
Web Services	Enables you to configure login, session management, and file path information for web services.
Workflow Integration Module	Enables you to configure settings for the Workflow Integration Module. This component is required for AppWorks.
Roles Management	Enables you to configure the roles for each data source in AppEnhancer Administrator, including the Administrator user role.
Reporting	Enables you to generate reports about audit events, DLS, user permissions, and user roles.
Monitoring	Enables you to monitor activity on AppEnhancer system components such as Indexing Service, Rendering Server, Web Access Server, and so on.

Chapter 2

Security

Security involves both authentication and authorization. Authentication requires all users to enter a valid user name and password to access most modules. AppEnhancer Administrator enables you to configure authentication credentials and select a security provider for each data source. AppEnhancer supports the following security providers:

- CM
- Windows
- ADFS
- CAS
- OTDS
- SAML 2.0
- Auth0

Note: ADFS, CAS, OTDS, and SAML 2.0 are supported only by AppEnhancer Administrator and AppEnhancer Web Access.

2.1 Implementing security

The AppEnhancer system provides a range of security features, enabling your system with flexible, easy-to-administer data protection. AppEnhancer Administrator enables you to specify credentials for various AppEnhancer server authentication accounts and to specify a security provider for each data source.

By using the User and Group Security functions in the **Application Management** node in AppEnhancer Administrator, you can define global or application-level security settings for individual users or for groups of users. These security settings, called *privileges*, govern the ability of a user or group of users to access functions in AppEnhancer. Through the Document Level Security function in the **Application Management** node you can make, you can make particular documents accessible or inaccessible to groups of users based on index values attached to the documents. Annotation groups enable you to control user access to specific annotations.

2.1.1 User security

Security in AppEnhancer can be implemented by user or by group. This section discusses the features available for implementing security for each individual user.

User security is implemented by creating user settings containing privilege settings that enable user access to AppEnhancer functions. You can create global profiles, which grant the same set of privileges for all AppEnhancer applications, and application profiles, which grant a set of privileges only for the selected application, for the individual user.

Users can also gain (or be denied) access to AppEnhancer functions by becoming members of groups that have group security profiles configured. Group security profiles, like user security profiles, can be global or application-specific. The process for configuring a group profile is essentially identical to that for a user settings; the settings for a group profile, however, apply to every user who is a member of the group. If a function is enabled in a group profile for a particular application, and a user setting is created for the same application, you can choose to disable that function in the user settings.

2.1.1.1 Creating a user

If you intend to use the same user and group structure in your AppEnhancer system as in Windows, consider using the Windows user maintenance utility to create users and then import them into **Application Management**. For the instructions, see "Importing user accounts" on page 20.

If the data source uses the Windows security provider, a user that you create in AppEnhancer Administrator is valid only when a user of the same name exists in Windows.

To create a user, follow these steps:

1. Navigate to the **Application Management** > **<***your data source***>** > **Users** node in AppEnhancer Administrator. For more information, see "Logging in to AppEnhancer Administrator" on page 11.
2. To add a new user, on the **Users** page, click **ADD**.

   Note: Click **SEARCH** to view all the existing users. To search for a specific user, type the name of the user in the **Search for Users** field and click **SEARCH**.

3. On the **User** tab, configure the options as described in the following table:

Field	Description
User Name	Unique user name. The user name can be up to 64 characters. If the data source uses the Windows security provider, you must precede the user name with its domain name and a backward slash (\). If the data source uses the CM security provider, the forward slash (/) and the backward slash (\) are invalid characters. The domain name can be up to 64 characters.
Full Name	Full name of the new user. The full name can be up to 132 characters.
Password and Confirm Password	Password if the data source uses the CM security provider. The password can be up to 64 characters. In the **Confirm Password** text box, type the same password in exactly the same format. **Note:** By default, the Password and Confirm Password fields are automatically populated with a randomized password. Click the **Show Password** check box to see the password. You can change this password.
License Group	License group. The license group name can be up to 32 characters. For more information, see "License servers" on page 39.

4. On the **Groups** tab, select a group that needs to be associated with the user. If the group does not exist, create a group. For the instructions to create a group, see "Creating a group" on page 23.

5. On the **Profile** tab, configure the options as described in the following table:

Field/Option	Description
Application	Enables the following choices: • Select **<Global Profile>** to assign the same privileges for all AppEnhancer applications. • Select the application name from the list to define privileges for one application only.

Field/Option	Description
Privileges	Selects the items appropriate for the responsibilities of the user. Enable an option by selecting the check mark in its check box, disable an option by clearing the check box, or, when applicable, accept the default settings.
No Privilege	Disables all privileges for the selected security profile. For more information, see "User and group privileges" on page 27.
Delete Profile	Deletes the selected security profile. For more information, see "User and group privileges" on page 27.
Full Privileges	Provides full privileges for all system functions. For more information, see "User and group privileges" on page 27.

6. On the **Security Mapping** tab, configure the options as described in the following table:

Field	Description
Alternative Security	Overwrites the options. This option enables you to implement security mapping for a user. This is useful if you intend to use the AppEnhancer Migration Wizard to migrate documents and security information from one data source to another. Security mapping enables you to map a user in the source database to a user in the destination database. By default, **Alternative security** is disabled.
Overwrite Options	
Same user name and password	Maps this user with same name and password. The values in the **User Name**, **Full Name**, **Password**, and **Confirm Password** text boxes cannot be edited.
Same user name, but different password	Maps this user with same name, but with a different password. The values in the **User Name**, and **Full Name** text boxes cannot be edited. You can type a new password in the **Password** and **Confirm Password** text boxes.

Field	Description
Different user name and different password	Maps this user with a different user name and password. The values in the **User Name**, **Full Name**, **Password**, and **Confirm Password** text boxes can be edited. The user name can be up to 64 characters. If the destination database uses the Windows security provider, you must precede the user name with its domain name and a backslash. The domain name can be up to 64 characters. The full name can be up to 132 characters. The password can be up to 64 characters.

7. On the **Account State** tab, it displays the current state such as **Active**, **Disabled**, **Suspended**, or **Must Change Password**.

   - Click **ACTIVATE** to change the state to **Active**.
   - Click **DISABLE** to change the state to **Disabled**.
   - If the state is **Active**, select the **Must Change Password** option to change the state to **Must Change Password**.

     Note: If **Must Change Password** is selected, you will be prompted to change the password when you log in to AppEnhancer Web Access. This impacts AppEnhancer Web Access log in only.

After a user has been created, you can change any user setting except the user name.

You can also use the **COPY PRIVILEGES** option to create numerous user accounts with identical privileges.

Note: The remote login of the default administrative account (sysop) user is disabled by default. To enable remote login, run the following command in the `web.config` file of Web Access:

```
<add key="SYSOPRemoteLogin" value="<true>"/>
```

2.1.1.2 Creating a user with write-only permission

You can create a user with write-only permission to allow REST and other web services to log in and create documents without consuming a license.

To set up a user with write-only permissions, activate the Permission Isolation option in AppEnhancer Administrator or the `web.config` file. When set to true, the dependency between modify index and view permissions is ignored.

```
<add key="PermissionIsolation" value="<true>"/>
```

To allow document creation by users with write-only permissions via REST and web services, you must also grant the user with Multi-login, Add-page, and Modify index permissions.

To allow exporting of documents to Output Transformation Server via REST services, you must also grant the user with Multi-login, Batchscan, COLD import, Add-page, and Modify index permissions.

2.1.1.3 Importing user accounts

The Application Management feature offers an import option that makes it easier for system administrators to configure security information for new users. You can import user name lists from the Security Authority of the workstation, such as Microsoft Domain Security Authority. This feature also reduces data entry when you add several new users at the same time. You can also import a list of user names from your network into Application Management.

1. Navigate to the **Application Management > <***your data source***> > Users** node in AppEnhancer Administrator.
2. In the **User List** page, click **IMPORT**.
3. Select a domain from the list box from which you want to import the users.
4. Type a keyword or leave it blank, and then click **SEARCH**.
5. From the list of users, select an user or multiple users.
6. Select the **Import as Native User** option to import as native users.
7. Select the **Import Groups** option to import the groups associated with the selected users.
8. Click **IMPORT**.

The information that AppEnhancer imports depends on the security provider used by the data source :

- If the **Import as Native User** option is selected, then the user will be prompted as CM security and AppEnhancer imports the user name. All user names are imported with blank passwords. The CM security provider cannot decrypt Windows passwords, and therefore cannot import passwords.
- If the **Import as Native User** option is not selected, the user will be prompted as Windows security and AppEnhancer imports the user account. With this security provider, passwords are not managed in AppEnhancer Administrator.

2.1.2 Group security

An AppEnhancer system administrator can create or import a group of users to grant the same security settings to all of the members of the group. Groups can be used to assign global and application-level security settings (by configuring group security profiles) or to protect documents from access at the document level.

Group security, like user security, uses profiles to assign privileges in AppEnhancer, but privileges assigned to a group apply to all members of the group, rather than a single user. The privileges to perform functions in AppEnhancer, such as adding documents, printing, and creating and modifying applications, are assigned in security profiles. By creating group security profiles, you can easily assign the same privileges to all of the members of a group. Group security profiles, like user security profiles, can be used to grant privileges to all applications in the data source, or to assign privileges to a specific application. A global security profile grants group members access to the AppEnhancer functions enabled in the profile in all AppEnhancer applications. An application security profile grants group members access to the functions enabled in the application to which the profile applies.

Groups are also used when assigning Document Level Security (DLS) settings. You associate a group with an index field and then assign values for that field that either grant or deny access to documents.

2.1.2.1 Configuring group security profiles

Administrators can configure security settings for large groups of users by creating a single group profile. If several users will be performing the same functions, you can create a group, configure a security profile that enables access to each needed function, and then add each of the users as a member of the group.

As with user settings, when new group profiles are created, you assign privileges that enable the group members to access AppEnhancer functions. Users are granted privileges to functions in all applications (in a global profile) or in a single application (in an application profile). You can set up a global profile for a group, enabling the members of the group to access a minimal set of default functions in any AppEnhancer application, and then override those settings by creating application-specific profiles for the group, which add additional privileges or remove privileges.

Global profiles give group members common functional privileges for all AppEnhancer applications. These globally defined privileges are automatically granted to group members for all applications in the data source. By creating different application profiles, you can give group members different privileges for each AppEnhancer application. Privileges granted in group security profiles can be overridden in user security profiles created for individual users. If the data source is using the CM security provider, a user security profile, when viewed, displays a check mark next to each function that is enabled by a user's membership in a group.

Users can be members of more than one group simultaneously. When a user belongs to more than one group, the user is granted all privileges enabled in each of the

group profiles. In other words, if the privilege to perform a function is enabled in a profile for one group and disabled in a profile for another group, a user who belongs to both groups will be able to perform that function.

Be careful when you remove users from a group because any security conveyed by the group's security profiles or Document Level Security settings will no longer apply to those users. Whenever a user is removed, check to make sure that any necessary privileges assigned at the group level are not lost to the user. For example, a user might be granted privileges to an application by a group security profile. If the user is removed from the group, you must either add the user to another group with privileges to the application or create a user security profile granting access. Similarly, adding a user to a group causes any security settings for the group to apply to the user. Because Document Level Security settings are assigned by association with groups, by adding a user to a group you might accidentally deny a user access to documents that the user should be able to access. When a user is added to a group, make sure that no settings in the user's user security profile will cause the user to have different privileges other than the ones you intend.

If a global profile does not exist for a group, a blank global profile for the group appears. Similarly, if an application name is selected for which the group does not already have a security profile, a blank profile for the application appears. Privileges must be configured in the blank profile, and the profile saved, for the group members to have access to all AppEnhancer applications (in the case of the global profile) or to the specific application (in the case of an application profile).

2.1.2.2 Understanding guidelines for group profiles

AppEnhancer users can usually be classified as particular user types according to the functions that they perform in AppEnhancer. One set of users might be responsible for scanning documents and adding them to AppEnhancer, for example, while another group primarily uses AppEnhancer to retrieve and process documents. You can set up group accounts for each type of user relevant to your AppEnhancer system, and then add users as members in the appropriate groups.

The following table provides guidelines for assigning privileges to profiles for typical AppEnhancer user types. These profiles are examples that illustrate typical settings; you can add or remove privileges to customize profiles. You can create more than one group of a particular type; for example, two scan groups with different privileges could be created.

Group name	User duties	Privileges
Scan Users	• Scanning and indexing documents or pages online • Batch scanning • Batch indexing	• Add Page • Batch Scan • Batch Index • Scan/Index Online Optionally: • Display • Modify Index • Delete Doc • Delete Page • Enhance Pages • Edit Annotations • Edit Redactions • OCR • Full-Text Index • Full-Text Query
Retrieve Users	• Retrieving, displaying and printing documents	• Display • Print Optionally: • Edit Annotations • Edit Redactions • Full-Text Query • Submit Workflow
Administrative Users	• All user and administrative functions	• Full Privileges

2.1.2.3 Creating a group

If you intend to use the same user and group structure in your AppEnhancer system as in Windows, consider using the Windows user maintenance utility to create groups and then import them into **Application Management**. For more information, see "Importing group accounts" on page 26.

If the data source uses the Windows security provider, a group that you create in **Application Management** is valid only when a group of the same name exists in Windows.

1. Navigate to the **Application Management** > <*your data source*> > **Groups** node in AppEnhancer Administrator.

2. In the **Group List** page, click **ADD**.

Note: Click **SEARCH** to view all the existing groups. To search for a specific group, type the name of the group in the **Search for Groups** field and click **SEARCH**.

3. On the **Group** tab, configure the options as described in the following table:

Field	Description
Group Name	Unique name for the group. The name can be up to 64 characters. If the data source uses the Windows security provider, you must precede the group name with its domain name and a backward slash. The domain name can be up to 64 characters.
Description	Description for the group. The description can be up to 132 characters.

4. On the **Users** tab, select an user or multiple users from the available list of users that you want to associate to the group.

Note: If the group uses the Windows security provider, you must use the Windows user maintenance utility to add or remove users from the group. Users in any security provider can be added as members of a group in CM security provider.

5. On the **Profile** tab, configure the options as described in the following table:

Field/option	Description
Application	Enables the following choices: • Select **<Global Profile>** to assign the same privileges for all AppEnhancer applications. • Select the application name from the list to define privileges for one application only.
Privileges	Selects the items appropriate for the responsibilities of the user. Enable an option by clicking a check mark in its check box, disable an option by clearing its check box, or when applicable accept the default settings.
No Privilege	Disables all privileges for the selected security profile. For more information, see "User and group privileges" on page 27.
Add Profile	Adds the selected security profile. For more information, see "User and group privileges" on page 27.

Field/option	Description
Full Privileges	Provides full privileges for all system functions. For more information, see "User and group privileges" on page 27.

6. On the **Security Mapping** tab, configure the options as described in the following table:

Field/option	Description
Alternative Security	Overwrites the options. This option enables you to implement security mapping for a group. This is useful if you intend to use the AppEnhancer Migration Wizard to migrate documents and security information from one data source to another. Security mapping enables you to map a group in the source database to a group in the destination database. By default, **Alternative security** is disabled.
Overwrite Options	
Same group name	Maps this group with same name and description. The value in the **Group Name** and **Description** text boxes cannot be edited.
Different group name	Maps this group with a different group name and description. The value in the **Group Name** and **Description** text boxes can be edited. The group name can be up to 64 characters. If the destination database uses the Windows security provider, you must precede the group name with its domain name and a backslash. The domain name can be up to 64 characters. The description can be up to 132 characters.

7. Click **SAVE**.

After a group has been created, you can change any group setting except the group name.

2.1.2.4 Importing group accounts

The Application Management feature offers an import option that makes it easier for system administrators to configure security information for new groups. You can import group name lists from the Security Authority of the workstation, such as Microsoft Domain Security Authority. This feature also reduces data entry when you add several new groups at the same time. In addition, you can import a list of group names that is already in your network.

The information that AppEnhancer imports depends on the security provider used by the data source:

- If the **Import as Native Group** option is selected, the group will be imported as CM security provider. AppEnhancer imports the group name and description.
- If the **Import as Native Group** option is not selected, the group will be imported as Windows security provider. AppEnhancer imports the group name and description. In addition, the users who are members of the imported group can immediately log in to AppEnhancer components.

To complete the group account setup process, security profiles must still be configured for the imported groups.

1. Navigate to the **Application Management > <***your data source***> > Groups** node in AppEnhancer Administrator.
2. In the **Group List** page, click **IMPORT**.
3. Select a domain from the list box from which you want to import the groups.
4. Type a keyword and then click **SEARCH**.
5. From the list of groups, select a group or multiple groups.
6. Select the **Import as Native Group** option to import as native group.
7. Select the **Import Users** option to import the users associated with the selected groups.
8. Click **IMPORT**.

For each of the groups that you have imported, you can change the description of the group and profile.

2.1.2.5 Troubleshoot invalid users and groups

To determine the cause of the issue, check each of the following items:

- When the user or group is created, an appropriate domain name and a backslash (\) precedes the user or group name in the **User Name** or **Group Name** text boxes.
- Verify the spelling of the domain name and user or group name. The spelling of the name in **Application Management** must exactly match the spelling of the name in Windows security.

If any of these issues occur, you must delete the user or group from **Application Management** and recreate it. To prevent these issues, consider using the Windows user maintenance utility to create groups and then import them into **Application Management**.

2.1.2.6 User and group privileges

The following table describes each user and group privilege, and indicates whether another privilege is required:

Privilege	Description	Other required privileges
Scan/Index Online	Performs online indexing of scanned documents.	**Add Page** **Note:** If you create a new document, you also need the **Batch Scan** and **Batch Index** privileges. If you scan into an existing document, you do not need these additional privileges.
Batch Scan	Performs batch creation or batch importing.	
Batch Index	Performs batch indexing.	**Add Page**
Modify Index	Modifies the document indexes.	
Display	Displays documents.	
Print	Prints, emails, or exports pages or documents.	
Configure Work Station	The **Configure Work Station** permission is required to customize User Settings for AppEnhancer Web Access.	

Privilege	Description	Other required privileges
Delete Doc	Deletes documents in the application, including those marked as final revisions.	
Delete Page	Deletes pages in the document. The **Delete Page** and **Display** privileges are both required to perform these functions.	
Add Page	Adds pages to documents in the application. The **Add Page** and **Display** privileges are both required to add pages to existing documents.	
Create Application	Creates new applications.	
Modify Application	Modifies existing applications.	
Delete Application	Deletes or purges applications.	
Migrate Application	Performs migration of application.	
COLD Import	Performs Computer Output to Laser Disk (COLD)/ Enterprise Report Management (ERM) extracts.	
COLD Import Maintenance	Maintains COLD/ERM extract definitions.	**COLD Import**
COLD Batch Extract	Enables user to perform COLD/ERM batch extractions.	

Privilege	Description	Other required privileges
Administrator	• Accesses AppEnhancer Administrator. • Changes the license configuration in AppEnhancer Administrator. • Accesses in AppEnhancer any applications with names that begin with an underscore (_), such as **FORMS** or **RSTAMP**. • Delegates responsibility for assigning user privileges for a subset of applications, users, and permissions to one or more lower-level administrators or users. • Resets a batch. • Creates, modifies, or deletes custom data types and custom data formats. • Uses Archive, Migration, and the Full Text Index.	
Multiple Logins	Logs in to AppEnhancer from different workstations simultaneously.	
Doc Level Security Maintenance	Configures the **Document Level Security** tab for an application in **Application Management**.	
Key Reference Maintenance	Configures the **Key Reference File Setup** tab for an application in **Application Management**.	
Auto Index Maintenance	Configures the **Auto Index Import Setup** tab for an application in **Application Management**.	

Privilege	Description	Other required privileges
User Security Maintenance	Maintains user security at either the application level or the global level based on the security profile. Use this setting to delegate responsibility for assigning user privileges for a subset of applications, users, and permissions to one or more lower-level administrators or users. This privilege is required to access the **Users**, **Groups**, and **Annotation Groups** options in **Application Management** and to change the security provider.	
Key Reference Import	Imports Key Reference files.	
Auto Index Import	Imports Auto Index files.	
Index/Image Import	Configures the **Index/Image Import Setup** tab for an application in **Application Management** and imports Index Image files.	
Create Annotations	Adds annotations.	**Display**
Edit Annotations	Edits, deletes, or hides the annotations created by the same user.	**Display**
Create Redactions	Adds redactions.	**Create Annotations** and **Display**
Edit Redactions	Edits, deletes, or hides redactions created by the same user.	**Edit Annotations** and **Display**
Global Annotations	Adds annotations; can edit, delete, or hide annotations created by other users, and enables user to view the text of text annotation icons created by other users. In addition, if **Edit Redactions** is selected, the user can add redactions and can edit, delete, or hide redactions created by other users.	**Edit Annotations** and **Display**

Privilege	Description	Other required privileges
Full Text Index	Submits documents in the application to the AppEnhancer Indexing Service for full-text indexing if the **Allow full-text** option on the **Full-Text** tab is enabled for the workstation. If the **Allow full-text** option is enabled or disabled, the clients must be restarted to implement this change. This privilege is also available in AppEnhancer Web Access.	
Full Text Query	Performs a full-text search for documents in the application if the **Allow full-text** option on the **Full-Text** tab is enabled for the workstation. If the **Allow full-text** option is enabled or disabled, the clients must be restarted for the change to take effect. The **Full-Text Query** and **Display** privileges are both required to view the results of the full-text search.	
OCR	Processes documents in the application with OCR if the **Allow OCR** option on the **OCR** tab is enabled for the workstation. If the **Allow OCR** option is enabled or disabled, the clients must be restarted to implement this change.	
Retention User	Files a document for retention if retention is enabled for the AppEnhancer application. **Note:** A valid Software Retention Management license is required.	**Display**

Privilege	Description	Other required privileges
Retention Administrator	Enable and configure retention for an application. In addition, if retention is enabled for the AppEnhancer application, the user can perform the following retention-enabled tasks: • File a document for retention using any policy defined for the application. • Extend the retention period for a document under retention. • Place and remove a retention hold. • Manage expired documents under retention. **Note:** A valid Software Retention Management license is required.	**Display** and **Delete** (delete expired documents)
Submit Workflow	Submits documents in the application to a workflow.	
Public Access License User	The user can access AppEnhancer documents only in read-only mode by using the AppEnhancer Web Client. A user with the AppEnhancer Web **Public Access License User** privilege cannot log in to any other AppEnhancer component, regardless of the other privileges in the user security profile.	

The following privileges are available only on the **<Global Profile>**:

- **Configure Work Station**
- **Create Application**
- **Multiple Logins**
- **Public Access License User**

You can also copy user permissions by selecting the **COPY PRIVILEGES** option on the **Users** page.

2.1.3 Document level security

With Document level security, administrators can restrict documents to a group of users based on index values attached to the documents. Document level security is implemented at the group level and individual documents can be made accessible or inaccessible to the group of users based on index values.

Security rules on the document level are mutually exclusive; if a user is in two groups and each group has accessible values for two different fields, then the user can only access documents that satisfy both accessible rules.

2.1.3.1 Configuring Document level security

To configure Document level security:

1. Go to the **Application Management**> <*your datasource*> > **Applications** tab.
2. On the **Applications** screen, select the **Application** you want to configure.
3. On the selected Application's properties screen, go to the **Field** tab.
4. For the fields you want to restrict based on its values, select the **Doc Level Security** check box.
5. Go to the **Document Level Security** tab.
6. The **Fields** list displays all fields marked with the **Document Level Security** flag. Before continuing, verify that the field you want to use is in the list.
7. In the **Groups** list, select the group for which you want to edit the security settings.
8. In the **Data Values** section, you must specify the type of security access users in the group will possess:
    - If you want to prevent users from accessing documents with the specified data values for the selected field, then select **Inaccessible**.
    - If you want to allow users to only view documents with the specified data values for the selected field, then select **Accessible**.
9. In the **Data Value** box, you must specify the values for the selected field using the **ADD** button to enter each field value. Alternatively, you can also import field values from files using **IMPORT**.

To demonstrate a sample configuration on the Document Level Security tab, assume there is a group named ABC, a field called A1 set with the Inaccessible security type, and a specified data value of 123. Then based on these settings, all users in the ABC group are prohibited from viewing documents with the A1 field that contain 123 as the value.

Furthermore, the following special use cases may be helpful if your security requirements are similar:

- To allow a group to access documents with field values starting with a particular string character, add the value as:

  `<character>*`

  For example, if you want to allow access to all documents with a field that starts with the letter a, add the Data Value as:

  `a*`

- To allow access only to documents created by the currently logged in user, you must set up the following criteria:

  – Add the **Username** field to the Application.

  – For the **Username** field, set the **Document Level Security** flag.

  – On the **Document Level Security** tab, select the **Username** field and group.

  – In the **Data Values** settings, select **Accessible** and then add `%U` as a value.

2.1.4 Annotation security

You can implement security in AppEnhancer by annotations.

2.1.4.1 Creating an annotation group

To create an annotation group, follow these steps:

1. Navigate to the **Application Management > <***your data source***> > Annotation Groups** node in AppEnhancer Administrator.
2. In the **Annotation Groups** page, click **ADD**.
3. In the **Name** text box, type an unique name for the annotation group. An annotation group name can be up to 64 characters.
4. Click **ADD**.
5. In the **Select Users and Groups** dialog box, select a user, multiple users, group, or multiple groups to be added to the annotation group, and then click **OK**.

   By default, each user or group is configured to follow legacy rules. This means that the ability of each user or group to view or edit annotations or to hide or edit redactions is governed by the privileges assigned to their user or group profile.
6. If you want to change the configuration for a user or group, select that user or group from the list and clear the **Follow Legacy Rules** option. For the selected users or groups, select the options in a sequence as described in the following table:

Option	Description
Annotations	

Option	Description
Annotations > View	View all annotations in the current annotation group.
Annotations > View, Annotations > Create	Create annotations.
Annotations > View, Annotations > Edit	Edit your own annotations in the current annotation group.
Annotations > View, Annotations > Edit, Global Edit	Edit all annotations in the current annotation group.
Redactions	
Redactions > Hide	Hide all redactions in the current annotation group.
Annotations > View, Annotations > Create, Redactions > Hide, Redactions > Create	Create redactions.
Annotations > View, Annotations > Edit, Redactions > Hide, Redactions > Edit	Edit your own redactions in the current annotation group.
Annotations > View, Annotations > Edit, Redactions> Hide, Global Edit	Edit all redactions in the current annotation group.

Note: It is recommended that you assign the same options to all members of each annotation group. For example, one annotation group can contain users and groups who all have the **Annotations > View** option and another group can contain users and groups who all have the **Redactions > Hide** option.

The flexibility of this feature enables you to customize it to your needs. However, this feature might be confusing to your users. For users who can assign annotations to annotation groups, provide guidelines that indicate which annotations they should assign to each annotation group.

7. Click **DELETE** to delete selected users or groups added to the annotation group.
8. Click **SAVE**.

2.1.4.2 Follow legacy rules example

For a user who is a member of an AppEnhancer group within an annotation group, if the group follows legacy rules, then the user follows legacy rules regardless of other configurations for the user within the annotation group. For example, an annotation group ANNOTATORS contains two AppEnhancer groups. For example, ONE and TWO. Within the ANNOTATORS annotation group, ONE follows legacy rules and TWO has one or more of the other options. For users who are members of both groups (ONE and TWO), the **Follow Legacy Rules** option configured in ANNOTATORS for ONE overrides the other options configured for TWO.

2.2 Managing security

If you are using AppEnhancer Web Access or Utility Services, you must restart the website in Internet Information Services (IIS) on each AppEnhancer Web Access or Utility Services server after any changes to the AppEnhancer database, such as the modification of a user or group, to enable the changes to take effect.

Note: The Utility Services is used only when you configure a data source to use directory service security providers. It is deprecated.

You can perform the following managing tasks:

- Managing Group Security: Modify and delete groups
- Managing User Security: Modify and delete users
- Managing Document Level Security: Modify document-level security settings
- Managing Annotation Groups: Modify and delete annotation groups

Chapter 3

Environments

This chapter provides information about the nodes available in the **Environment** node in AppEnhancer Administrator. For more information about the AppEnhancer concepts, see the *OpenText AppEnhancer Installation Guide*.

3.1 Data sources

1. Navigate to the **Environment > Data Sources** node in AppEnhancer Administrator and click **ADD**.

2. In the **New Data Source** page, configure the options as described in the following table:

Section/Field	Description
Data Source Identification	
Name	Unique name for your data source. Do not use the following characters: backslash (\), slash (/), colon (:), asterisk (*), question mark (?), double quote ("), angle brackets (<>), or pipe (|)
Description	Description to identify your data source.
Data Source Connection String	
Database	Information to connect to the database server.
Schema	Name of the schema if it has been set up in the database. The schema name is used for all database table names created for this data source. The name should be in a valid format for the database. Avoid using spaces or keywords, or beginning the name with a numeral. **Note:** Schema is supported only for SQL Server, PostgreSQL, and Oracle databases.
DB String Type	Type of the database string. By default, **Unicode** is selected. Unicode is used for multibyte languages (for example, Chinese). Select **ASCII** for single-byte languages (for example, English and European languages).

Section/Field	Description
License Server	
License Server	License server to connect to the data source. "License servers" on page 39 provides more information.
License Group	License group.
Security Model	Security provider that you want to use.
System Credentials	
Application Global Supplied	Types of credentials.
AppEnhancer Service Credentials	Identifies the AppEnhancer impersonation account user who will perform actions on behalf of NT services such as Auto Retention Filer.
User Name	AppEnhancer impersonation account user name.
Password and Confirm Password	Password of the user.
Audit Trail DB Connection String	
Database	Information to connect to the database server.
Schema	Name of the schema if it has been set up in the database. The schema name is used for all database table names created for this data source. The name should be in a valid format for the database. Avoid using spaces or keywords, or beginning the name with a numeral. **Note:** Schema is supported only for SQL Server, PostgreSQL, and Oracle databases.

3. Click **SAVE**.

You can also manage, edit, remove data sources, set a data source as default, hide a data source, and validate the configuration.

You can perform a deep analysis of AppEnhancer data source tables and fix any issues that are not consistent with our built-in table schema. In the Environment > Data Sources node in AppEnhancer Administrator, click **Check DB**. The Check DB command performs the following tasks:

- Find and fix missing tables
- Find and fix missing table columns

- Find and fix missing table indexes
- Verify column data types and column size
- Recreate stored procedures

3.2 License servers

AppEnhancer product licenses are defined through one or more license files that you add to the License Server to activate licensed use of the product.

License Server needs to be installed on a Windows server that is available for all AppEnhancer services and clients, such as the SQL Server workstation.

3.2.1 Obtaining a product license

You can obtain licenses for AppEnhancer products through OpenText MySupport. To retrieve product license files, you must first run Fingerprint Generator to produce a key, which is then used to retrive the license.

Note: You must have a fingerprint ready via Fingerprint Generator prior to requesting a license. Any changes made to the License Server machine may invalidate the license and will require a new fingerprint.

Fingerprint Generator

1. Copy FingerprintGenerator.exe to a folder on the License Server machine.
2. Launch a CMD window.
3. Go to the folder in Step 1.
4. Run FingerprintGenerator.exe.

You will see the fingerprint displayed in the command window. This is what you need to request a new license. You can copy it to the clip board or write it into a file using a command like `fingerprintgenerator.exe > .\fingerprint.txt`.

The AppEnhancer product license files you receive from OpenText enable product features and limit maximum concurrent users based on your purchase agreement.

3.2.2 Adding a license to the License Server

AppEnhancer product licenses are provided in the form of license files, depending on which AppEnhancer products that you purchase. A license file, which has a `.dat` or `.lic` file extension, is a text file that contains information on the product features and user limits defined by the license. When AppEnhancer license files are retrieved from the OpenText MySupport site, they must be added to the License Server for the licensing to be recognized by AppEnhancer products.

1. On the machine where the License Server is installed, navigate to the License Server directory (default installation location is `C:\Program Files\XtenderSolutions\Content Management\License Server`).
2. Add the AppEnhancer license files to the License Server directory.
3. From the **Start** menu, select **Program Files > Administrative Tools > Services** and start AppEnhancer License Server *<version number>* (if already running, stop and restart it):
4. The license file has now been added to the AppEnhancer License Server.

If you purchase additional products or features, updated license files should be retrieved from OpenText MySupport and then added to the License Server using the same procedure.

3.2.3 Connecting to License Servers

You can create a connection to the License Server and associate that connection with the data source.

1. Navigate to the **Environment > License Servers** node in AppEnhancer Administrator and click **ADD**.
2. Type the network address for the License Server workstation.
3. Select a license group, if it exists, from the **License Group** list box and click **OK**. it is recommended that you specify a license group for each data source rather than for each License Server connection.
4. Click **OK**.
5. Click **VERIFY** to verify the connection.

Note: Ensure that the license server is running before you add it.

3.2.4 Creating and allocating license groups

Licensing for AppEnhancer Web Access enables you to subdivide a license purchase across groups. A group can represent a department or any select set of users or groups of users. Using license groups, you can allocate purchased licenses to various groups, thereby limiting access and controlling license distribution throughout the enterprise. When users log in to the associated products, they pull their product licenses (and the associated rights or limitations) from the license group to which they are assigned. License groups can consist of only one type or aspect of a product license, multiple aspects of a license, or even multiple product licenses (if the products work in conjunction with one another and both require separate licenses for each logged on user).

1. Navigate to the **Environment > License Servers** node in AppEnhancer Administrator.
2. Click on a license server location for which you want to add a license group.
3. Type a license group name and click **ADD**. The license group name should be descriptive so that you can easily determine the function of the licenses in the group. The name cannot begin with a number, contain spaces, or contain any other non-alphanumeric characters.
4. If you want to allocate the license group you have created, select the license group from the **License Group** list box and click **ALLOCATE**.
5. In the **License Group Allocations** dialog box, select the license type from the **License Type** list box.

   

   Note: If you did not purchase a particular aspect of a product license (for example, AppEnhancer Read-Only), or if you have allocated all available instances of a license type, that type does not appear in the list box.

   - **Total Licenses**: Specifies the total number of licenses for the selected license type.
   - **Unallocated Licenses**: Specifies the total number of licenses unallocated for the selected license type.
6. Type the number of licenses you want to assign to this license group in **Licenses Allocated To This Group** and click **OK**.
7. Click **SAVE**.

You can also delete, edit the license group, clear, and modify allocations.

3.2.5 Configuring a SPS license server

To configure a Software Protection Services (SPS) license server, you must complete the following tasks:

1. "Step 1: Installing an OTDS server" on page 42
2. "Step 2: Configuring an OTDS server for a SPS license" on page 42
3. "Step 3: Adding a SPS license server in AppEnhancer" on page 45

3.2.5.1 Step 1: Installing an OTDS server

Before you can configure the SPS license server, you must install an OTDS server. For complete instructions on installing an OTDS server, refer to *OpenText Directory Services Installation and Administration Guide*. During installation of the OTDS server, ensure your configuration meets the following requirements:

- Minimum JDK version 11.0.8 or later
- Fully configured installation of Apache Tomcat as the application server
- SQL Server database with a JDBC connection

Also, the default **otadmin@otds.admin** Administrator user account is used but you must make note of the administrator password you created during the installation process because it is required in subsequent steps.

3.2.5.2 Step 2: Configuring an OTDS server for a SPS license

To configure the OTDS server for the SPS license, you must complete the following tasks:

- Retrieving a SPS license
- Creating an OTDS resource
- Configuring the license key
- Creating an OTDS Administrator account

Retrieving a SPS license

The SPS fingerprint is a unique token used to identify the OTDS instance on the server and is used to generate a license. License files are only valid for the OTDS instance that has the same SPS fingerprint.

To acquire a SPS license for your OTDS server:

1. In the OTDS web administration client, go to **Info** > **System Status**.
2. Copy the **SPS Fingerprint** value.

3. Go to My Support (https://support.opentext.com/) and use the **Request Catalog** to request a license. You must provide the fingerprint value for a license to be generated for you.
4. When you receive the license, **save** the license file to your local machine. The license is required in subsequent steps.

Creating an OTDS resource

To create an OTDS resource:

1. In the OTDS web administration client, go to **Setup** > **Resources**.
2. Click **Add**.
3. On the **New Resource** page, type a name to identify the resource in the **Resource Name** box.
4. On the **Synchronization** screen, click **Next**.
5. On the **Principal Attribute** screen, click **Next**.
6. Click **Save**.
7. In the **Resource Activation** dialog that appears, click **OK**.

   The **Resources** page reappears with the new resource in the list. You must make note of the **Resource ID** because it is required in subsequent steps.

Configuring the license key

To configure the license key:

1. In the OTDS web administration client, go to **Setup** > **License Keys**.
2. Click **Add**.
3. On the **New License** page, type a name to identify the license key in the **License Key Name** box.
4. In the **Resource ID** box, make sure that the resource ID shown corresponds with the resource you created in the previous step.
5. Click **Next**.
6. On the **License Key** screen, click **Get License File** and select the SPS license file for your OTDS instance. The license file is provided by Customer Support and stored as a LIC file. When you are finished, click **OK** to upload the license.

   After the upload, you can optionally review the license info in the **License Key** box.
7. Click **Save**.

   The **License Keys** page appears.

Creating an OTDS Administrator account

You must create a new user account for the OTDS administrator and then add the new user to the administrator group membership.

To create an OTDS administrator account:

1. In the OTDS web administration client, go to **Setup** > **Partitions**.
2. On the **Partitions** page, two partitions should already exist in the list of partitions. Locate **otds.admin** in the list. In the otds.admin row, click **Action** and in the menu that appears, click **View Members**.
3. On the **otds.admin** page, click **Add** > **New User**.
4. On the **New/Edit User** page, type a unique user name for the administrator in the **User Name** box. When you are finished, click **Next**.
5. On the **Account** screen, in the **Password Options** list choose **Do not require password change on reset**.
6. Select the **Password never expires** check box.
7. In the **Initial Password** area, type the password to use for the administrator's account in the **Password** and **Confirm Password** boxes.
8. Click **Next**.
9. On the **Organization** screen, click **Next**.
10. On the **User Attributes** screen, click **Next**.
11. On the **Custom Attributes** screen, click **Save**.

    The **Partitions** page reappears and your new administrator user appears in the list.
12. On the **Partitions** page, locate the new administrator user account in the list. In the admin user account's row, click **Action** and in the menu that appears, click **Edit Membership**.
13. On the properties page for the new admin user account, click **Add to Group**.
14. On the **Member Selection** page, select the **otdsbusinessadmins@otds.admin** group check box and then click **Add Selected**.

3.2.5.3 Step 3: Adding a SPS license server in AppEnhancer

To add a SPS license server in AppEnhancer:

1. In AppEnhancer Administrator, click **Environment** > **License Servers**.
2. On the **License Servers** page, click **Add**.
3. In the **License Server** dialog, in the **Server Type** list click **SPS**.

   When SPS is selected, more configuration options are displayed.
4. You must complete the following fields with values according to your OTDS server:

Field	Description
Server URL	Complete URL to the OTDS server, including http or https, IP address or domain name, and the port number.
Resource ID	Resource ID for the OTDS server, which was established when the OTDS resource was created
User Name	OTDS administrator user name
Password and Confirm Password	OTDS administrator password

   When you are finished, click **OK**.
5. On the **License Servers** page, click **Save**.

   The new license server appears in the list.

3.3 Desktop credentials

AppEnhancer Desktop global authentication account grants security privileges to AppEnhancer Desktop in instances where an authentication context is required to access a resource and the global credentials option is selected for that resource. You can configure credentials settings in AppEnhancer Administrator to override the use of the global account for authentication. However, any accounts that are used to provide credentials as an authentication context for AppEnhancer Desktop resources must have the rights to access to those resources.

You can configure credentials to enable AppEnhancer Desktop clients to access secure storage paths for an AppEnhancer application. You must use secure paths for applications that are enabled for AppEnhancer Software Retention Management. These credentials are used only when a path is using global credentials.

1. Navigate to the **Environment > Desktop Credentials** node in AppEnhancer Administrator.
2. In the **Desktop Credentials** page, configure the options as described in the following table:

Section/field	Description
Service Credentials	
Domain\User	Full name for the user account that should be used as the global authentication account.
Password and Confirm Password	Password for the user account.

3. Click **SAVE**.

3.4 Storage management

You can configure AppEnhancer to store elements of document pages (such as scanned images, Word files, and OLE objects) on any storage device that can be mapped as a logical volume on the workstation. This provides flexibility when you store document pages on a network file server, local hard drive, WORM and erasable optical media. On the **Storage Management** page in AppEnhancer Administrator, add a storage server and provide the information for the UNC path (including secure paths) and dual write paths and Cerner storage path.

3.4.1 Configuring Microsoft Azure File service

On the Storage Management page in AppEnhancer Administrator, click **Azure Files Service**. Enter the Azure File server name, storage account name, and storage account key, and add the Azure File paths.

Azure File paths are supported only as Application Path and Secure Path Root.

3.5 OpenText Directory Services (OTDS)

OTDS manages the users for single sign on (SSO) to the OpenText Enterprise Information Management products.

3.5.1 Setting up OTDS Server

1. Install OTDS. For more information about installing OTDS, see the *OpenText Directory Services (OTDS) Installation and Administration Guide*.
2. Create a new OTDS partition. You will need to provide the domain IP address and domain administrator account during the configuration process.

   During the partition set up, complete the following:

   1. Add user mapping by mapping the Windows Active Directory user's SID to an OTDS user's attribute.
   2. Click **Test Mappings** to check the mapping results.
3. Create an OTDS resource with the default settings. Enter a sign out URL (for example, http://<*WXServerHost*>/WebAccess/Account/OTDSSingleSignOutHandler).

4. A new access role will be created for the resource automatically. Go to the details of the access role and add the users of the new partition to the access role.
5. Add the AppEnhancer Web Access server URL to the OTDS trusted sites. For example, http://<*WXServerHost*>/.

3.5.2 Setting up OTDS in AppEnhancer Administrator

1. Log in to AppEnhancer Administrator.
2. On the OTDS Server page, enter the OTDS Server URL and Resource ID, and activate the resource.
3. Map the OTDS user attribute to the AppEnhancer user attribute. The SID (Security ID) should be mapped to the OTDS user attribute you specified when you configured the OTDS server.
4. Reset IIS.
5. Log in to AppEnhancer Administrator.
6. On the Users page, click **OTDS Import** to go to the OTDS user import page.
7. Provide query criteria to search for and import the users.
8. Set user permissions for the imported users.

3.5.3 Importing OTDS Groups in AppEnhancer Administrator

1. Log in to AppEnhancer Administrator.
2. On the **OTDS Server** page, enter the OTDS Server URL and Resource ID, and activate the resource.
3. Map the OTDS user attribute to the AppEnhancer user attribute. The SID (Security ID) should be mapped to the OTDS user attribute you specified when you configured the OTDS server.
4. Reset IIS.
5. Go to the **Application Management > <your data source> > Groups** node.
6. On the **Groups** page, click **OTDS Import**.
7. Select an option from the list for each of the following values and click **SEARCH**.
   - Select Partition: Select a group partition.
   - Type Group Name: The groups have names and IDs and these are fixed attributes.

   Note: The privileges are assigned at a group level.

8. Select the group to be imported and click **Import**.

Chapter 4

Roles

This chapter provides information about the roles that can be configured in the Roles Management node in AppEnhancer Administrator.

4.1 Understanding roles

Users who have Administrator permissions and are in the Global Administrator role can configure the roles in AppEnhancer Administrator. The SYSOP user can configure the roles by default. The Global Administrator can configure the user roles by adding or deleting users in the selected role types for each data source.

The Global Administrator and Server Manager roles are global roles. These two role configurations are shared by all the data sources. When the administrator changes the user in one role from one data source, the change can be seen in other data sources. After a user is configured in a global role, the administrator must make sure that the user exists in all the data sources. Otherwise, the user will not be able to log in as the global role. The other roles are data source local roles. They are not shared between data sources.

The following tables show the roles and the settings that each role is able to access in AppEnhancer Administrator.

Notes

- The **Global Administrator** role has access to all the nodes and settings in AppEnhancer Administrator, and is therefore not included in the tables below. The **Roles Management** node is accessible only to the Global Administrator role.
- The following tables show the roles and the settings that each role is able to *view*. Additional permissions may be required to configure and edit the settings.

Node	Roles						
	Applica-tion Manager	User Manager	Server Manager	Report Reader	Re-source Monitor	Data Source Manager	Data Source Admin
Environ-ment			Visible				
Server Manage-ment			Visible				

Node	Roles						
	Application Manager	User Manager	Server Manager	Report Reader	Resource Monitor	Data Source Manager	Data Source Admin
Reporting				Visible	Visible		
Roles Management							

Node	Roles						
	Application Manager	User Manager	Server Manager	Report Reader	Resource Monitor	Data Source Manager	Data Source Admin
Application Management							
Applications	Visible					Visible	Visible
Users		Visible				Visible	Visible
Groups		Visible				Visible	Visible
Annotation Groups		Visible				Visible	Visible
Audit Trail	Visible					Visible	Visible
Data Types	Visible					Visible	Visible
Web Access User Settings		Visible				Visible	Visible
Auto Index Options	Visible					Visible	Visible
Global UDL	Visible					Visible	Visible
Password Policy List		Visible				Visible	Visible

Node	Roles						
	Application Manager	User Manager	Server Manager	Report Reader	Resource Monitor	Data Source Manager	Data Source Admin
Monitoring							
Registered Components			Visible				
Running Components			Visible				
Indexing Service			Visible				
Rendering Server			Visible				
Web Access Server			Visible				
License Pool					Visible		Visible
Locked Documents					Visible		Visible
Checked-out Documents					Visible		Visible
Queues					Visible		Visible
Sessions					Visible		Visible
PID Table					Visible		Visible
System Id Usage					Visible		Visible
Application Usage					Visible		Visible
System Path Entries					Visible		Visible

Node	Roles						
	Applica-tion Manager	User Manager	Server Manager	Report Reader	Re-source Monitor	Data Source Manager	Data Source Admin
Monitoring							
Admin-istrative Services Jobs					Visible		Visible

4.2 Managing roles

To configure roles:

1. In AppEnhancer Administrator, navigate to **Roles Management** > <*your data source*>.
2. In the **Role Type** column, click the role that you want to configure.
3. Do any of the following:
   - To add users to the selected role, in the top-right corner of the screen, click **ADD**. In the **User** dialog window, select a user and click **OK**.
   - To remove users from the selected role, select the user that you want to remove. In the top-right conrner of the screen, click **DELETE**.

Chapter 5

Applications

5.1 Managing applications

To use AppEnhancer to store and manage documents, you must first design and then create applications to store your documents.

Notes

- It is recommended that you back up all databases before you make changes to any application.
- Application changes are allowed only if there are no documents in the application. After documents are added to an application, you can use the Migration Service or the Migration Wizard to move and consolidate index data.

5.1.1 Creating new applications

You can create a new application by using the AppEnhancer Administrator. Each data source can support up to 2048 different applications.

Note: Secure write paths are required for AppEnhancer Software Retention Management applications, including retention-enabled applications (applications that are configured for retention by using the Retention Management Configuration Utility). It is recommended that you use secure paths for all applications. Otherwise, any Windows user who has access to the file share location can delete .BIN files even if the files are under retention. Before you create an application, ensure that the necessary secure paths are defined in AppEnhancer Administrator.

1. Install and configure the storage server.
2. Provide your workstation with read and write privileges to all paths that the AppEnhancer system will use.
3. Navigate to the **Application Management** > <*your data source*> > **Applications** node in AppEnhancer Administrator.
4. In the **Application List** page, click **ADD**.
5. In the **Application Information** page, configure the options for the following tabs:

   Applications tab:

   - **Application Name**: Unique name that can be up to 64 alphanumeric characters.

Notes

- The application name must not start with a number and also must not contain any of the following symbols: double quote ("), single quote ('), space, slash (/), backslash (\), period (.), comma (,), asterisk (*), pipe (|), semicolon (;), colon (:), question mark (?), percent (%), or angle bracket (< >)
- Only system administrators can access applications that begin with an underscore.

- **Application Description**: Identifies the application. The description can be up to 128 alphanumeric characters and must not use the following characters: double quote ("), single quote ('), or percent (%).
- Enable the following options, depending on the requirement:
  - **Multiple indexes referencing single document**: Stores a single document once, but makes it available for indexing many times and saves storage space. However, if you want each document to have a separate index record, do not use this option. If you intend to use the Document Level Security feature for any index field in this application, it is recommended that you do not use this option.
  - **Reason Code**: Prompts users to enter comments and select the functionality that they use whenever they create, display, export, print, or email a document in the current application. This option facilitates compliance with the Health Insurance Portability & Accountability Act of 1996 (HIPAA) by enabling you to capture information about the use of documents within AppEnhancer. If you use this option and do not have the audit trail option enabled, a message appears, indicating that audit trail is disabled and HIPAA messages will not be logged.
  - **Prompt for checkout when open documents**: Prompts users to check out documents from the current application when they open documents for display. This option performs the following functions: enables the check in/check out mode for the application; enables the final revision feature.
  - **Check-out comments required**: Enables users to enter a comment whenever they check a document out of the current application. Each comment is saved to the audit trail database table or log file, depending on the audit trail configuration.
  - **Check-in comments required**: Enables users to enter a comment whenever they check a document into the current application. Each comment is saved to the audit trail database table or log file, depending on the audit trail configuration.
  - **Enable EDB**: Configures the application to dispatch events to the Event Dispatch Broker each time a user adds, modifies, or deletes a document index.
  - **Enable Recycle Bin**: Enables the Recycle Bin feature in the application for deleted documents or document revisions and marks them for

recycling. When this option is enabled and you delete a document or document revision, they are temporarily moved to the Recycle Bin for your review instead of being deleted immediately.

- **Full-text Engine**: Full-text engine for the application. This engine will be used to process documents in this application when they are submitted for full-text indexing.
- **OCR Queue**: The default queue to submit documents for OCR indexing. If no queue is selected, the first queue is used.
- **Full-Text Index Queue**: The default queue to submit documents for full-text indexing. If no queue is selected, the first queue is used.

Retention Enabled: Filters the applications for which you have configured retention.

- **Yes**: To filter applications with retention.
- **No**: To filter applications without retention.

Note: You cannot enable retention and modify an existing application.

Paths tab:

- **Storage Settings**: Enable the options and provide the information depending, on your requirement.
  - **No Retention**: Creates applications without retention.
  - **Enable Software Retention Management**: Creates applications with Software Retention Management.
- **Document Write Path**: Path where you want document page files to be stored. If you opted to use a secure path in **Storage Options**, the **Document Write Path** and **Annotation Write Path** text boxes are populated with the root directory. You can create a subdirectory for document files by appending `\docs` to the end of the root path in this text box. For non-secure paths, you can enter the appropriate path in the text box, or click **SELECT** to search and choose an existing path. After the existing path is selected, you can add subfolders. A document write path must be specified for each application for AppEnhancer to store documents and pages added to the application. Documents are stored as .BIN files. The document write path could be a local hard drive or network file server. If dual write paths have been configured in AppEnhancer Administrator for the data source, the document write path could be a remote or primary path. If you use a network file server as the write path, it is recommended that you create a secure path to prevent Windows users from deleting AppEnhancer files.

  The following table provides some examples. The Example column indicates what you might type in the **Document Write Path** text box, and the Result column indicates the storage path for an application named RECORDS:

Storage location	Example	Result
Local Hard Drive	C:\OPTICAL	C:\OPTICAL\RECORDS
Network File Server (mapped drive)	P:\OPTICAL	P:\OPTICAL\RECORDS
Network File Server (UNC)	\\SERVERNAME\ \OPTICAL	\\SERVERNAME\ OPTICAL\RECORDS

If you use a network file server as the write path, it is recommended that you create a secure path to prevent Windows users from deleting AppEnhancer files.

If you are using cerner specific storage, you can type the path (for example, CerOIF://cerner) directly in the **Document Write Path** text box.

- **Annotation Write Path**: Path where you want annotations to be stored or click **SELECT** to search and choose an existing path. After the existing path is selected, you can add subfolders.

  An annotation write path must be specified so that annotations can be added to AppEnhancer document pages. Annotations are stored as .ANO files. The annotation write path could be a local hard drive or network file server. If dual write paths have been configured in AppEnhancer Administrator for the data source, the annotation write path could be a remote or primary path.

  Note: The **Annotation Write Path** text box is disabled if you have selected **Enable Software Retention Management** in **Storage Options**.

  If a path managed by DX and using file retention is assigned to the annotation write path of application, annotations can no longer be modified after they are created and saved.

- **OCR Write Path**: Path where you want optical character recognition (OCR) output text to be stored (if you want to use OCR) or click **SELECT** to search and choose an existing directory path. After the existing path is selected, you can add subfolders.

  If a path managed by DX and using file retention is assigned to the OCR write path of application, after an image has been processed by using OCR and a text view of the image has been created, a new text view can not be produced through OCR processing.

Fields tab:

- **Field List**: Lists all the fields defined in the application. You can also drag and drop fields to reorder the field list.
- **Field Name**: Name for the index field. The field name can be up to 64 alphanumeric characters. The first character must be a letter of the alphabet; it should not be a number, blank space, or symbol. The following characters must not be used: double quote ("), single quote (‘), backslash (\), or percent (%).

- **Data Type**: Data type that you want to associate with the index field. The following table describes the available data type conversions:

Data type	Available conversions
Currency	Decimal/Numeric, Integer, or Text
Date	Time Stamp or Text
Decimal/Numeric	Integer, Currency, or Text
Integer	Decimal/Numeric, Currency, or Text
SSN	Integer or Text
Telephone	Text
Text	Anything but Boolean Choice or User-defined
Time	Time Stamp or Text
Time Stamp	Date, Text, or Time
Zip Code	Integer or Text

Note: When converting a field with a Date data type to a Text field type, ensure that the field length is ten characters or more. This will prevent the truncation of existing information.

- **Field Length**: Number of characters or digits that you want the index field length to be if you are defining a Currency, Decimal/Numeric, Integer, or Text field. The maximum field length varies, depending on the data type you have chosen. AppEnhancer Administrator automatically populates the length for the following field types: Boolean Choice, Date, SSN, Telephone, Time, Time Stamp, User-defined List, or ZIP Code
- **Field Format**: Format that you want to use for the field. The list box provides options, depending on the selected data type.
- **Flags**: Flags that you want to apply to the field. Flags specify the index field functionality.
  - **Required**: Requires a user to enter data in this field.
  - **Search**: Enables this field for searching.
  - **Read-Only**: Protects this field from being modified.
  - **Doc Level Security**: Enables or disable user access based on the contents of this field.
  - **Part of Unique Key**: Requires unique data in this field for each document.
  - **Dual Data Entry**: Requires a user to enter this data twice as a validation measure.
  - **Key Reference**: Used for key reference file indexing. If you set this field, you must also define at least one **Data Reference** field. If you select this,

a new tab **Key Reference File** appears. After you have created an application with this **Key Reference** flag, you cannot clear it while modifying an application.

– **Data Reference**: Used for key reference file indexing. If you set this field, you must also define a **Key Reference** field. If you select this flag and if there is no **Key Reference File** tab, a new tab **Key Reference File** appears. When an application is created, you cannot clear the **Data Reference** flag while modifying an application.

– **Auto Index**: Populates the index of document from imported data. If you select this, a new tab **Auto Index File** appears.

– **Validation Mask**: Creates and sets a template format for this field. If you enable **Validation Mask** for a text field when defining your index fields, the **Format** text box is enabled so that you can create a mask. AppEnhancer supports input validation and field display masks.

  An input validation mask validates the user input in text index fields, character by character. When adding documents, users are required to match the character pattern that you specify for this index field. This action ensures that data is stored in the database in the designated format.

  A field display mask hides confidential data in text index fields to prevent unauthorized users from viewing the data. You can create full or partial display masks for index fields. You can also define a format for a text index field that uses any combination of input validation and field display mask characters, depending on your business needs.

  You can use the characters as described in the following table to create a template for the data to be contained in the text field by specifying the exact characters that reflect an allowable entry in the **Format** text box.

Input validation mask characters	Field display mask characters	Enables or hides characters
n	d	Numerical character (0–9)
z	y	Numerical character (0–9) or space
a	c	Alphabetic character (A-Z)
x	m	Non-space character
?	p	Any character

Each character in the mask string represents one character in the index field value. For example, to hide a text index value consisting of four alphabetic characters, create a field display mask by using the format `cccc`.

Use the following rules when defining a mask:

- The field length defined for the index field must be at least as long as the mask. After you have entered the mask requirements in the field, other characters can be added, if the overall length of the entry does not exceed the allowable length as defined in index creation.
- Although z is the special mask character representing a number or space, a space is not allowed as the leading entry in an index field.

The following table provides examples of input validation masks:

To enable only this format	Enter this in the field validation mask dialog box
Any two alphabetic characters and four numbers	aannnn
A plus or minus sign, two numbers, a space, and three numbers	xnnznnn
Letter A followed by five numbers	Annnnn
Two numbers, a hyphen and an alphabetic character	nnxa

– **Leading Zeroes**: Preserve leading zero characters in an integer field.

– **Hidden**: Designates a field as hidden. You cannot apply the **Required**, **Doc Level Security**, **Part of Unique Key**, **Dual Data Entry**, **Key Reference**, or **Auto Index** flags to any hidden fields.

Legacy access rules:

- For SYSOP users, all fields are unhidden.
- For non-SYSOP users, regardless of their permissions, the following applies:
  - Users cannot create new hidden field index values when creating new documents or document indexes. To create these values, you must be a SYSOP user.
  - Users cannot view or modify existing hidden field index values in doc index display, doc query result set, match index result set, or auto index result set.

New access rules:

- For users with AEAdmin permissions, all fields are unhidden.
- For users without AEAdmin permissions, the following applies:
  - Users cannot create new hidden field index values when creating new documents or document indexes.
  - Users cannot view or modify existing hidden field index values in doc index display, doc query search criteria, doc query result set, match index result set, or auto index result set.

AppEnhancer will automatically use the new access rules unless there is a need to use the legacy rules. If you need to enable the legacy access rules, complete the following steps:

- For C++ legacy components, define a registry entry to force AppEnhancer Desktop to use legacy access rules. Both AppEnhancer Desktop and AexDB API layer will check this registry to determine which rule should be used. The registry key is a DWORD value named `HiddenFieldLegacyRules` that can be found at one of the following locations, depending on your operating system:

  - 32–bit OS: `HKEY_LOCAL_MACHINE\Software\XtenderSolutions\AppEnhancer\Settings`
  - 64–bit OS: `HKEY_LOCAL_MACHINE\Software\WOW6432Node\XtenderSolutions\AppEnhancer\Settings`

  The value for new access rules is *<0>* (default), and the value for legacy access rules is *<1>*.

- For .NET legacy components, define an application setting in app.config/web.config to force .NET applications to use legacy access rules. Both the AppEnhancer Web Access application and AEEngine API layer will check this setting to determine which rule should be used. The setting is named 'AEHiddenFieldLegacyRules'. The default value to use new access rules is *<false>*. Set this value to *<true>* to enable legacy access rules.

To add your custom fields, provide the information for the field name, data type, and other options and click **ADD**. Also, if the standard data types or their formats do not meet your requirements, you can create custom data types or custom data formats. You can insert or delete fields from the list. You can also drag and drop to reorder the list.

- **USER-DEFINED LIST**: Click the field name to enable **USER-DEFINED LIST**. Click **USER-DEFINED LIST**. Type a name and then click **ADD**. You can add an unlimited number of items to the list, but a large number of items (more than 400) in a user-defined list adversely affects performance. For example, if an application has three user-defined list fields, each of which has 200 items, then the effect is equivalent to having one user-defined list field with 600 items. Each item can contain up to 132 characters.

  You can choose to use a Global UDL or define the UDL on your own. If you want to define the UDL on your own, you can add an unlimited number of items.

  The following are the available options:

  – To import text from a file for use as a list item, click **IMPORT**. In the **File Upload** dialog box, click **Choose File** to browse and select a file for import.

  – To remove an entry from the list, select it and click **DELETE**. You can also modify an entry.

You can also modify, insert, or delete the fields.

You can use the following formatting options to create vmasked text fields.

- **"%USERNAME%"**
- **"%FULLNAME%"**

These formatting options can be read only or non-read only, searchable, required or non-required.

While creating a document, users can add details in the fields. The server updates the user details if no data is added in the fields. If the field is non-read only, the user can provide any value which will not be validated.

A non-read only field can be edited after it is set either by the user or the server.

Read only fields are set by the server and cannot be edited.

If the user creating the document does not have a full name, **%FULLNAME%** will be replaced by the user's username.

Audit trail tab: Lets you enable and configure the Audit Trail feature.

Index Image File tab: You can find two lists, **Specification List** and **Field list**. **Specification List** contains the specification name and the field delimiter. When you select a specification from the **Specification List**, you can edit the field list. Each field has the **Field Name**, **Max Width**, and **Format** attributes.

- **Specification Name**: Unique name for the specification. Do not use the following characters in specification names: double quotation mark ("), single quotation mark (‘), percent (%).
- **Field Delimiter**: Character that the import file uses to separate fields.
- **Field Name**: New field from the list box.
- **Max Width**: Maximum width for the field. The maximum width indicates the maximum number of characters to import from the file.
- **Format**: Format for the field. The format indicates the format of that field in the import file.

Click **ADD**. You can insert or delete fields.

6. Click **SAVE**.

Note: When an Audit Trail setting is changed, IIS (Internet Information Services) must be restarted before the change takes effect.

5.1.1.1 Creating a new retention policy

1. Navigate to the **Application Management > <your data source> > Applications** node in AppEnhancer Administrator.
2. Type **Yes** in the **Retention Enabled** field.
3. Select the required application from the list of retention enabled applications and click **Retention**.
4. Click **NEW** to add a new policy to the application.
5. Type a policy **Name** and provide retention period details.

   For more information on retention period details, see "Retention tab" on page 62.
6. Select the **Type** of retention policy.
7. Click **ADD** and **SAVE**.

Editing a policy

1. Select the policy and click **EDIT**.
2. Make the required changes and click **UPDATE**.

Deleting a policy

1. Select the policy and click **DELETE**.
2. Click **YES** in the deletion confirmation window.

Retention tab

This tab is displayed only for applications with retention.

- **Policies**:
  - **Allow users with "Retention User" privilege to override the default policy setting**: Enable this option to allow users with Retention User privilege to override the default policy and choose from the list of available policies defined for the application when applying retention manually.
  - **Default Policy**: When a manual retention is configured for an application, the first retention policy created is assigned as the default policy for the application. You can switch between policies from the list.

    Note: A default policy cannot be deleted.
  - **Show Policy Types**: Lists the type of policies.
    - **Manual**: The policies that are manually applied to a document.

- **Automatic**: The policies that are automatically picked up and applied to the document.
- **All**: All the configured policies.

- **Policy Configuration**:
  - **Name**: A descriptive name for the retention policy you are defining. The name should not have space or special characters.
  - Specify the retention period for the retention policy by selecting any one of the following options.
    - **Expire at 11:59 PM (GMT) on**: The time and date on which the retention period expires. The default expiration date is one calendar year from the current date.
    - **Expire in years and days**: The number of years or days after which the retention period expires. The default retention period is 30 days.
    - **Use app index date field**: The expiration date for the retention period is based on an application date index field. Select the desired index field from the list and specify the number of years and/or days after the index field date that the policy expires. You can specify a maximum of 999 years and 364 days using this option.
    - **Permanent Retention**: Indicates the retention period never expires for a document.

      Note: A document with permanent retention cannot be deleted.
  - **Type**: You can select **Automatic** or **Manual** as the retention type.
- **Rule Configuration**:
  - **Name**: A descriptive name for the new rule.
- **SAVE**: Saves all the retention updates for an application.
- **RESET**: Allows to modify and update existing retention policies and rules.

5.1.1.2 Creating a new retention rule

1. Select any existing policy and click **ADD** under Rules.
2. Type a rule name under **Rule Configuration**.
3. From the **Type of Comparison** list, select the type of search you want to perform and click **OK**.

   The following are the options available:

   - **Between**: Values from x through y.
   - **Greater Than**: Values greater than x.
   - **Greater Than or Equal**: Values greater than or equal to x.

- **Less Than**: Values lesser than x.
- **Less Than or Equal**: Values lesser than or equal to x.
- **Not Equal To**: Values other than x.

4. Add a **Field Value** and click **OK**.

   You can perform the following actions for the field values:

   - **ADD**: Adds all the values entered into the field value.
   - **REPLACE**: Overwrites the selected value with a corrected value.
   - **DELETE**: Removes values that are not required.
   - **DELETE ALL**: Removes all values from the list.

5. To validate the values you entered, click **Test**.
6. Click **ADD** and **SAVE**.

Assigning a rule to a policy

1. Select the required rule and click **ASSIGN**.
2. Select any policy or type the name of the policy and click **OK**.

Editing a rule

1. Select the rule and click **EDIT**.
2. Make the required changes and click **UPDATE**.

Deleting a rule

1. Select the rule and click **DELETE**.
2. Click **YES** in the deletion confirmation window.

5.1.2 Deleting or purging applications

You can also delete or purge application by using the AppEnhancer Administrator if the data stored in an application is no longer needed. When an application is deleted, the index information related to each stored document is deleted and the index field definitions for the application are deleted. Purging an application deletes all index records, but keeps the application definition in place. If the data stored in an application is no longer needed, but you anticipate using the same application in the future, the data in the application should be purged. If you do not foresee a future need for the application, the application should be deleted. When an application is either purged or deleted, the disk space occupied by the index information is reclaimed for other uses. The .BIN files containing the documents themselves are not deleted. These .BIN files can be deleted by deleting the document files within AppEnhancer before deleting the application.

Navigate to the **Application Management > <***your data source***> > Applications** node in AppEnhancer Administrator. In the **Application List** page, select the application, and depending on the requirement click, **DELETE**, or **PURGE ALL DATA**, or **PURGE AND KEEP KEY REF TABLE DATA**.

Caution

The **PURGE ALL DATA** option purges all index values currently stored in the selected application and recovery of the data is not possible.

5.1.3 Creating and managing import specifications

A specification is a set of rules followed by AppEnhancer when you import data from an import file by using one of the three import wizards. In most cases, you can import the data by using a default import specification provided in AppEnhancer. Whenever data will be imported into all available fields in an application, and the data format and field length of those fields does not need to be altered, rather, you can use a default specification to perform the import. If an existing default specification is not sufficient for an import, you can either modify a default specification or create a new, customized specification for the import.

For a successful import, AppEnhancer must correctly read the data to be imported from the file. Each line of data in the import file must be organized in a specific format. AppEnhancer stores each line of the file as a separate record, or group, of index field values, by using the hard return character as an indicator of the end of a record. Within each record, there must be a value for each field into which data is being imported. These values are separated by a delimiter, such as a comma or a tab. When AppEnhancer parses a line of the import file, it creates a record and stores the data preceding the first delimiter in the first field of the record, the data preceding the second delimiter in the second field, and so on.

A specification provides the following information to AppEnhancer during the import process:

- The fields into which data are imported
- The order in which fields are imported
- The data format and length of each field
- The delimiter that will be used to separate one field value from another in the import file

A default specification automatically imports data into every available field in an application in the order specified in the application, and uses the data format configured when the application was created. The only difference between one default specification and another is the delimiter used to separate data. The default specifications, therefore, are each named for the delimiter used in the specification. The following table describes the default specifications:

Delimiter	Description
none	Fixed length records (no delimiter)
,	Comma
|	Pipe
~	Tilde
\t	Tab

An administrator can modify a default specification by reordering fields. However, to prevent confusion when importing data for the same application in the future, it might be better to create a new specification.

Administrators can remove fields from the field list in the specification. This enables a user to import data into only the fields on the field list, rather than all available fields in the application. If fields have previously been removed from a specification, you can add them again. You can also reorder the fields in the field list, so that AppEnhancer will import index field data from the file in a different order.

You can make changes to data formats to accommodate discrepancies between the format of data in the import file and what AppEnhancer will accept as a valid index field value. AppEnhancer will automatically reformat the data as it is imported so that it conforms to the application index field setting. For example, if the field setting for a date field is mm-dd-yy, and the dates in the file are formatted yy-mm-dd, the data format for the field can be changed in the import specification. When AppEnhancer imports the dates from the file, it will copy the numbers it reads as yy-mm-dd, convert them to the format mm-dd-yy, and store them in the application in the mm-dd-yy format.

5.1.3.1 Import Specification for a new application

You can create a new import specification and customize it to your needs while creating an application. The following procedure assumes that you are familiar with the procedures for creating an application.

1. On the **Fields** page, as you create each field, if you want to configure the field for Auto Index Import or Key Reference Import, apply the appropriate import flag to the field.
2. On the import file setup page, create the new import specification.

If you want to perform Auto Index Import or Key Reference Import, ensure that you have applied the appropriate flag or flags to the fields into which you intend to import data. Consider the following points:

- If you intend to use Auto Index Import Wizard to import data into a field, apply the Auto Index field flag to that field.
- If you intend to use Key Reference Import Wizard to data into an application, apply the Key Reference flag to one field, and apply the Data Reference flag to at least one field.

5.1.3.2 Import Specification For Existing Application

Standard templates are included for import files that are an acceptable format (the files use one of the standard field delimiters and are in the application's index field order). Custom specifications should be added only if the standard templates cannot be used.

You can create a new import specification and customize it to your needs, in an existing application. The following procedure assumes that you are familiar with the procedures for modifying an application.

1. On the **Fields** tab, if you want to configure a field for Auto Index Import or Key Reference Import, apply the appropriate import flag to the field.
2. Click the appropriate File Setup tab (Auto Index, Key Reference, or Index Image).

   Note: The Auto Index and Key Reference File Setup tabs are available only if their field flags are enabled within the application.

3. On the import file setup tab, create the new import specification.

5.1.3.2.1 Applying an Import Flag to an Existing Field

If you want to perform Auto Index Import or Key Reference Import, ensure that you have applied the appropriate flag or flags to the fields into which you intend to import data. Consider the following points:

- If you intend to use Auto Index Import Wizard to import data into a field, apply the Auto Index field flag to that field.
- If you intend to use Key Reference Import Wizard to import key reference data into a field, apply the Key Reference flag to that field.
- If you intend to use Key Reference Import Wizard to import data reference data into a field, apply the Data Reference flag to that field.
- If you intend to use Key Reference Import Wizard to data into an application, apply the Key Reference flag to one field, and apply the Data Reference flag to at least one field.

5.1.3.2.2 Creating New Import Specification For Existing Applications

The File Setup tabs (Auto Index, Key Reference, or Index Image) enable you to configure custom specifications for importing data into AppEnhancer. By default, the Index Image Import File Setup tab always appears. If Key Reference or Auto Index flags were set for any fields, these specifications can also be set now. Standard templates are included for import files that are an acceptable format (the files one of the standard field delimiters and are n the index field order of application). Custom specifications should be added only if the standard templates cannot be used. Custom specifications can be set after applications are created.

Depending on how the index fields of application are configured, you might be presented with multiple File Setup tabs. Repeat the following procedure for each File Setup tab.

1. In the **Specification Name** text box, type a unique name.
2. From the **Field Delimiter** list box, select the character that the import file uses to separate fields.
3. Click **ADD**. The new specification appears in the Specification List along with the standard formats. The **Field Name** text box also becomes available.
4. In the **Field List** box, list the fields in the order in which they are listed in the import file.
5. After all fields have been added, click **SAVE** to save the specifications (delimiter, field formats, field lengths, field order, and so on) for use in importing data. To quit the procedure at any point, click **CANCEL**.

5.1.4 Using the import utilities

5.1.4.1 Creating an index image import job

AppEnhancer users who are assigned to the **Application Manager** role and have Administrator and Index/Image Import permissions can submit index image import jobs.

Note: To import image files to a newly added data source, restart the import service before creating index image import jobs.

1. Navigate to the **Application Management** > <*your data source*> > **Applications** node in AppEnhancer Administrator.
2. Select an application.
3. In the **Import Utilities** drop-down menu, select **Index Image Import**.

   The **Create Import Job** dialog window appears.
4. From the **Application** list box, select the application into which you want to perform an Index Image Import.
5. From the **Specification** list, select an import specification. The specification defines the rules AppEnhancer will follow in importing data (such as date formats, delimiters, and so on).
6. Click **Import From**. In the **Open** dialog box, navigate to and select the file containing the import data and click **Open**.

   Note: File paths that reference a volume label are not supported in this release.

7. If you want to test the Index Image Import setup before performing the import, click **Preview**. For more information about using the Preview, see "Previewing import files" on page 75.

8. Under **Import Options**, select the options as required.

   The following table describes the available options:

Option	Description
Create new indexes and documents	AppEnhancer creates a new index and document for each import item. AppEnhancer does not check for duplicate document indexes.
Merge data with existing documents	AppEnhancer checks the selected application for duplicate document indexes. If AppEnhancer finds an existing document with the same index information as an imported item, AppEnhancer adds the item as a new page to that document. AppEnhancer imports any documents with new index information as new documents.
FT Queue	If full-text queues have been created, you can select one from the **FT Queue** list box. If the selected queue has been properly configured, the documents imported by the Index Image Import service are processed using the selected queue.
Check for unique key	If any of the fields in the application have been flagged as unique keys, and if you want the import service to check the values imported into these fields, enable this option. If the import service discovers multiple documents listed in the import file with the same values in the unique key fields, the import service imports the first such document and rejects all remaining redundant documents. If the import service discovers any documents listed in the import file with values in the unique key fields that duplicate the values for a document already in the application, the import service rejects all redundant documents.

Option	Description
Merge for unique key	If any of the fields in the application have been flagged as unique keys and the import service discovers any files listed in the import file with values in the unique key fields that duplicate the values for a document already in the application, the import service will append all redundant files to that document. This option is enabled when **Check for unique key** is selected.
Allowed # of consecutive errors	Type the highest number of consecutive errors that you want the import service to accept. When the import service has encountered the number of errors specified, the import service stops processing the file and marks the import as partially completed.
Allow document additions while importing	If you want other users to be able to add documents to the application to which you are importing documents during the import, enable this option. **Note:** If you do not enable this option and there is a lock on the application, the import will be marked as failed.
Skip	If you want to omit a record or a group of records from the import at the end of the import file, you must specify the number of lines that you want AppEnhancer to skip when processing the import file. In the **Skip** text box, type the number of lines that you want AppEnhancer to skip.

Option	Description
Then Load	If you want to limit the size of a record or group of records at the end of the import file, you must specify the number of lines that you want AppEnhancer to load when processing the import file. In the **Then Load** text box, type the number of lines that you want AppEnhancer to load. After the import service stops processing the file, the import will be marked as partially completed. **Note:** You can use the Skip and Then Load text boxes simultaneously. For example, if you want AppEnhancer to process only lines 21 through 30, specify 20 in the **Skip** text box and 10 in the **Then Load** text box. AppEnhancer skips the 20 leading lines in the import file, and then processes only the subsequent 10 lines (lines 21 through 30).
Use bulk objects	If you have placed database triggers on the DT and DL tables in your AppEnhancer application, you should disable this option. The option is enabled by default; to disable it, select the check box to clear the check mark and disable use of database bulk objects.
Bulk Size	When Use bulk objects is enable, you can set the size of the bulk object. The default size is 500.
Preserve file time	If you want the imported files to retain their file time after import, enable this option.

Option	Description
Batch Size	During the Index Image Import, database transactions commit document records to the database. Type the number of records that each database transaction should commit to the database. The default batch size is 100 records, but you can enter any integer from 1-10,000. **Note:** If you enable Allow document additions while importing, the Batch Size is set to 1 and this option is dimmed. When you enable document additions while importing, the import service commits each record from the import as a separate database transaction rather than committing multiple document records to the database at a time.
Inspect PDF File	Performs a scan of the PDF file to check for any errors. If errors are found, the import process will fail.
Decrypt PDF File	When importing PDF files, all encrypted files are automatically decrypted and saved as a regular PDF.
PDF Portfolio	Sets the PDF Portfolio file settings. You can choose from No Detect, As Foreign File, or Extract Embedded Files. No Detect indicates that no attempts are made to identify PDF Portfolio files. As Foreign File indicates that portfolio files are maintained as foreign files and to view a file, users must first download it before opening it in a PDF viewer. Extract Embedded Files indicates that all embedded files are extracted from the portfolio file and imported as separate pages before the original PDF portfolio file is deleted.

9. When you are finished, click **OK**.

5.1.4.2 Creating an auto index import job

AppEnhancer users who are assigned the **Application Manager** role and have both Administrator and Auto Index Import permissions can submit auto index import jobs.

Note: To import auto index data to a newly added data source, you must restart the AutoIndex KeyRef Service before creating the auto index import jobs.

1. Navigate to the **Application Management** > *<your data source>* > **Applications** node in AppEnhancer Administrator.
2. Select an application.
3. In the **Import Utilities** list, select **Auto Index Import**.
4. In the **Create Auto Index Import Job** dialog box, select the application that you want to import the auto index to from the **Applications** list.
5. In the **Specification** list, select an import specification. The specifications define the rules that AppEnhancer must adhere to when importing data (for instance, date formats or delimiters).
6. Click **Import From**.
7. In the **Open** dialog box, navigate to and select the file containing the import data and then click **Open**.
8. If you want to test the Auto Index Import setup before performing the import, click **Preview**. For more information about using the Preview, see "Previewing import files" on page 75.
9. Under **Import Options**, select the options as required.

   The following table describes the available options:

Option	Description
Append data	AppEnhancer appends, or adds, the imported records to the Auto Index table for the selected application. Existing data is not affected.
Replace existing data	AppEnhancer replaces all existing data in the Auto Index table with the imported records.
Skip	If you want to omit a record or a group of records from the import at the end of the import file, you must specify the number of lines that you want AppEnhancer to skip when processing the import file. In the **Skip** text box, type the number of lines that you want AppEnhancer to skip.

Option	Description
Then Load	If you want to limit the size of a record or group of records at the end of the import file, you must specify the number of lines that you want AppEnhancer to load when processing the import file. In the **Then Load** text box, type the number of lines that you want AppEnhancer to load. After the import service stops processing the file, the import will be marked as partially completed. **Note:** You can use the Skip and Then Load text boxes simultaneously. For example, if you want AppEnhancer to process only lines 21 through 30, specify 20 in the **Skip** text box and 10 in the **Then Load** text box. AppEnhancer skips the 20 leading lines in the import file, and then processes only the subsequent 10 lines (lines 21 through 30).

10. When you are finished, click **OK**.

5.1.4.3 Creating a key reference import job

AppEnhancer users who are assigned the **Application Manager** role and have both Administrator and Key Reference Import permissions can submit key reference import jobs.

Note: To import key reference data to a newly added data source, you must restart the AutoIndex KeyRef Service before creating the key reference import jobs.

1. Navigate to the **Application Management** > <*your data source*> > **Applications** node in AppEnhancer Administrator.
2. Select an application.
3. In the **Import Utilities** list, select **Key Reference Import**.
4. In the **Create Key Reference Import Job** dialog box, select the application that you want to import the Key Reference to from the **Applications** list.
5. In the **Specification** list, select an import specification. The specifications define the rules that AppEnhancer must adhere to when importing data (for instance, date formats or delimiters).
6. Click **Import From**.
7. In the **Open** dialog box, navigate to and select the file containing the import data and then click **Open**.

8. If you want to test the Key Reference Import setup before performing the import, click **Preview**. For more information about using the Preview, see "Previewing import files" on page 75.

9. Under **Import Options**, select the options as required.

10. When you are finished, click **OK**.

5.1.4.4 Previewing import files

The preview dialog box enables you to test the import setup against each line of the import file before performing the import.

The following table describes each element of the preview dialog box:

Dialog box element	Description
Line Number: #	Contains the specified line (record) of data from the import file, and displays it as it appears in the file.
Line Status	Indicates the status of the specified line (record) of data.
Recognized Fields	Contains the specified line (record) of data from the import file, and displays it as it will appear after being parsed according to the option selected under Format Specifications. If one of the fields fails during the attempt to preview the line, no other fields are displayed after that field.
Next Line	Displays the next line in the import file.

1. Note the status indicated in the **Line Status** text box and examine the text under **Recognized Fields**.

2. If the status is not OK, or the text under **Recognized Fields** does not appear as you expect, try each of the following troubleshooting tips until the problem is resolved. Ensure that:

   - The import file uses the proper syntax. Ensure that the line of the import file that you are previewing uses the same syntax as the rest of the import file.
   - You have selected the correct specification.
   - You have selected the correct import file. Click **Close**, specify a different file name, and click **Preview** again.
   - You have selected the correct application. Click **Close**, specify a different application, and click **Preview** again.
   - The specification setup meets your needs. Close the preview dialog box. Configure the specification again or create a new one, then click **Preview** again.

3. When the status is OK and the text under **Recognized Fields** appears as you expect, click **Next Line**.

4. Click **Close**. The preview dialog box closes and any changes you have made are saved.

5.2 Managing users

You can add, delete, import user accounts, and copy privileges from one user to another user. "User security" on page 16 provides more information.

5.3 Managing groups

You can add, delete, and import groups. "Group security" on page 21 provides more information.

5.4 Managing annotation groups

You can add and delete annotation groups. "Annotation security" on page 34 provides more information.

5.5 Managing the audit trail

You can configure audit trail options to track the creation, deletion, and modification of applications, users, and groups.

The Audit Trail feature enables you to track user activities on a global or per-application basis. Audit events, such as the creation, use, or deletion of documents, document pages, batches, queries, and various AppEnhancer tools, can be tracked for each AppEnhancer application. In addition, activity related to the creation and deletion of users, groups, and applications can be tracked on a system-wide basis. Use of queues and import tools can also be tracked. The Audit Trail feature also supports compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Each option on the **Audit Trail** page represents one audit event. When a user activity triggers an audit event, details of the audit event are recorded in the database. AppEnhancer Audit Trail encodes the time column `tsstamp` in the audit table in Greenwich Mean Time (GMT) format. This enables the audit table entries to maintain consistency when workstations are located in multiple time zones. You can calculate your local time by applying your time zone offset.

Navigate to the **Application Management > <***your data source***> > Audit Trail** node in AppEnhancer Administrator and configure audit trail options to track the creation, deletion, and modification of applications, users, and groups. In addition to tracking system-wide changes, you can configure default audit settings for user activities within AppEnhancer applications. When you set options for user activities within applications, you set audit defaults for all applications.

When creating or editing applications, you can choose to either use the default settings for user activities within applications or you can configure specific audit settings for user activities within each application.

Note: When an Audit Trail setting is changed, IIS (internet Information Services) must be restarted before the change takes effect.

The following table describes the information that can be tracked:

Option	Description
Enable Audit Trail	Tracks enabling and disabling of audit trails and changes in audit trail settings.
Application > Create/Delete/Modify	Tracks all creation, deletion, and modification of applications.
Application > Document > Add	Tracks addition of documents.
Application > Document > Delete	Tracks deletion of a document or revision. When a user has the Recycle Bin Delete permission enabled, deleted documents are moved to the Recycle Bin.
Application > Document > Index > Create	Tracks creation of a document index.
Application > Document > Index > Delete	Tracks deletion of a document index.
Application > Document > Index > Modify	Tracks modification of a document index.
Application > Document > Page > Add	Tracks addition of a page to a document.
Application > Document > Page > Delete	Tracks deletion of a page from a document.
Application > Document > Page > View/ Print/Export/Mail	Tracks when a document page or document page text view is displayed; a document page, document (all pages), or list of document pages are printed; a document page or document page's OCR text is exported; and a document page, document reference, or document (all pages) is mailed.
Application > Document > Page > Version > Add	Tracks addition of a page version.
Application > Document > Page > Version > Delete	Tracks deletion of a page version.
Application > Document > Page > Version > Annotate	Tracks additions and modifications of annotations.
Application > Document > Page > Version > OCR/Text-view	Tracks the changes to OCR/Text view of a page version.

Option	Description
Application > Recycled Document > Permanently Delete Document	Tracks permanent deletion of recycled documents or revisions. User must have the Recycle Bin Delete permission enabled to perform this task.
Application > Recycled Document > Restore	Tracks the restoration of a document or revision to its original location from the Recycle Bin. User must have the Recycle Bin Delete permission enabled to perform this task.
Application > Batch > Create	Tracks creation of a batch.
Application > Batch > Delete	Tracks deletion of a batch. Depending on the event, logs account data of user, delete event, batch name, file status and index data, batch name, batch ID, and module.
Application > Batch > Batch import/scan	Tracks batch import/scan of batch open and close.
Application > Batch > Batch Index	Tracks indexing of a batch.
Application > Batch > Batch Page > Add	Tracks addition of a batch page.
Application > Batch > Batch Page > Delete	Tracks deletion of a batch page.
Application > Batch > Batch Page > Attach to a document	Tracks saving a batch page in a document.
Application > Query > Save	Tracks saving of a query.
Application > Query > Delete	Tracks deletion of a query.
Application > Query > Execute	Tracks execution of a query.
Application > Query > Modify	Tracks modification of a query.
Application > ODMA operations	Tracks execution of ODMA operations.
Application > Tools > Import utilities	Tracks import operations for the Index Image Import, Auto Index Import, and Key Reference Import services.
Application > Tools > Migration Wizard	Tracks when a document is migrated to a destination database or when a source document is deleted from the source database (Delete source document option is selected).
User > Login/Logout	Tracks user login/logout activity.
User > Create/Delete/Modify	Tracks when a new user is created, a user is deleted, or settings of user are changed.
Group > Create/Delete/Modify	Tracks when a new group is created, a group is deleted, and group settings are changed in a group profile.

Option	Description
Queue > Create/Delete	Tracks creation, deletion, and modification of a queue.
Generic Import Tools	Tracks generic bulk-load operation.
License Server	Tracks all changes to the License Server settings.
Create/Delete/Modify Annotation Groups	Tracks the creation, deletion, and modification of annotation groups.
Audit Trail Table	Enables the user to select the audit trail table for the data source.
New Audit Trail Table Name	A name for the audit trail table.

5.6 Managing data types

AppEnhancer enables you to choose from a variety of data types and formats for each field. The Custom data type and format is discussed here and information about other data types and formats can be found in *OpenText AppEnhancer Installation Guide*.

5.6.1 Creating a custom data type and format

If you create a custom data type, you must create at least one data format before you can use the new data type to describe index fields.

You can also create custom data formats for existing data types if the predefined formats are not adequate for your organization needs.

Note: You can also modify or delete custom data formats. Ensure that you do not modify or delete data formats that are being used in a live application. You should create, test, and finalize your new data types and formats using a test application before deploying them within a live application.

The following rules pertain to each of the custom formats:

- Boolean Data Type:
  - Do not use the Validation Expression and Data Conversion Expression text boxes; they should remain blank.
  - The Formatting 1 box is used for the True value.
  - The Formatting 2 box is used for the False value.
- Currency Data Type:
  - Do not use the Validation Expression and Data Conversion Expression text boxes; they should remain blank.
  - The Formatting 1 box is optionally used to specify the currency symbol.

  - The Formatting 2 box is used for the format string. For example, " (n,nnn.nn)" would use the thousand separator and display negative values using the parentheses.

- Other Data Types: Custom formats for data types Date, Time, ZIP, SSN, TELEPHONE, NUMERIC, and INTEGER work like custom data types except the DB type is determined by data type.

  - Where Date, Time, ZIP, SSN, TELEPHONE are DB Type = STRING
  - Where NUMERIC is DB Type = NUMBER
  - Where INTEGER is DB Type = I4

1. Navigate to the **Application Management > <***YOUR DATA SOURCE***> > Data Types** node in AppEnhancer Administrator.
2. On the **Data Types** page, click **ADD**.
3. On the **New Data Type** page, configure the options as described in the following table:

Section/Field	Description
Type Name	Name for the custom data type.
Database Type	Database type for the data type that you want to create. The database type for the data type determines the set of characters allowed for that data type. You have the following choices: • If the index values has alphabetical characters, symbols, or formatted numbers (ANSI or ASCII characters, like the SSN, Telephone, and ZIP Code data types), select **DBTYPE_STR**. • If the index values has alphabetical characters (Text data types only), select **DBTYPE_WSTR**. • If the index values has numeric characters without a decimal point (whole numbers, like the Integer data type), select **DBTYPE_I4**. • If the index values has numeric characters with a decimal point (numbers that may have a fractional component, like the Decimal/Numeric data type), select **DBTYPE_NUMERIC**. **Note:** User-defined lists cannot be created using the custom data type functionality.

Section/Field	Description
Variant Size	Variant size for the data type. Specify the minimum size and maximum size for the data type, in number of characters. For example, the Currency data type has a minimum size of 1 and a maximum size of 38. When calculating how many characters to allow, if the index value is stored to the database with formatting marks, remember to count the formatting marks. For example, xxx-xx-xxxx is 11 characters, not 9. You can also choose not to enable this option.
Available Attributes	
Required, Part of Unique Key, Auto Index, Doc Level Security, Data Reference, Date Stamp, Key Reference, Leading Zeroes, Validation Mask, Read-Only, Search, Dual Data Entry	Flags for the custom data type. For example, the Time Stamp data type has only the **Doc Level Security**, **Search**, and **Part of Unique Key** flags available.
Default Attributes	
Required, Part of Unique Key, Auto Index, Doc Level Security, Data Reference, Date Stamp, Key Reference, Leading Zeroes, Validation Mask, Read-Only, Search, Dual Data Entry	Default flags for the custom data type. For example, the Text data type has the **Required** and **Search** flags enabled by default.

4. Click **SAVE**.
5. In the **Formats** section, click **ADD**.
6. On the **New Data Format** page, configure the options as described in the following table:

Field	Description
Format Name	Name for the custom data format.
Scale	Number of digits after the decimal point for the custom format. For example, the Decimal/Numeric data type has a n,nnn.nnn format which has a scale of 3. This text box is enabled only if the data type for which you are creating a custom format is **DBTYPE_NUMERIC**.
DB Width	Width of the index value stored in the database. For example, if you are creating a simple date format of YYYY-MM-DD, type 8, as you do not want to save the dashes (-) in your database.

Field	Description
Format Width	Width of the index value in AppEnhancer, including all formatting characters. For example, if you are creating a simple date format of YYYY-MM-DD, type 10.
Validation Expression	Regular expression syntax to define the format in AppEnhancer. For example, to create a format that appears as YYYY-MM-DD, type `(\d{4})-?(\d{2})-?(\d{2})`. For more information, see "Using regular expression syntax to define custom data format" on page 84.
Date Conversion Expression	Regular expression syntax to define the information that should be included in the database if the format that is stored in the database is different than the format displayed in AppEnhancer. For example, to store the YYYY-MM-DD format in the database, type `$1$2$3` where `$1`, `$2`, and `$3` represent the subexpressions `(\d{4})`, `(\d{2})`, `(\d{2})` in the expression provided in **Validation Expression**. For more information, see"Using regular expression syntax to define custom data format" on page 84.

Field	Description
Formatting 1 and Formatting 2	Format depending on the type of format you have added: • If you are creating a simple string expression (like the one in our example), type the format you want AppEnhancer to use to display the expression. For example, type `$1-$2-$3` in the **Formatting 1** text box, where `$1`, `$2`, and `$3` match our sample expression's subexpressions, to display text that is typed into an AppEnhancer document index as 20020626 as 2002-06-26 after the index is saved. • If you are creating a Boolean format (for example, an expression like `^\bPublic$|^\bPrivate$`, where users can only type one or two values, type the first string (in this case, Public) in the **Formatting 1** text box, and the second (Private) in the **Formatting 2** text box. These choices appear in the **Boolean Choice** list box. • If you are using a numeric or integer format that can contain negative values, type the positive format in the **Formatting 1** text box (for example, `$1`), and the negative format in the **Formatting 2** text box (for example, `-$1`).
Default Value	Default value for the format.  **Note:** Each index field using a custom data format with a default value should also be set as Read-Only. In this case, the index field is automatically populated with the default value.
Locale	Locale that you want to use as default. This enables AppEnhancer to display currency symbols specific to the locale you have chosen.

7. Click **SAVE**.

5.6.1.1 Using regular expression syntax to define custom data format

To create a valid data format, you must use regular expressions to populate the **Validation Expression**, **Data Extraction Expression**, and **Format** text boxes.

In the **Validation Expression** text box, you can define a full expression that describes the data format you want to create. In the **Data Extraction** and **Format** text boxes, you can use a reduced set of regular expression syntax to extract information from the **Validation Expression** to instruct the AppEnhancer Administrator how to save the index information in the database, and how to display it in AppEnhancer.

A backslash (\) acts as the escape character. Characters that are used as operators in regular expressions must be preceded by a backslash if you want to use them literally. For example, to display a period or dollar sign, you must use \ and \$ to display them. The following characters must be preceded by a backslash to signify their literal representation: ., *, (,), ?, ^, $, {, }, \, [,]

Here are some examples of regular expression:

- A period (.) matches any character. For example: (ab.) will match abc, abd, ab3, ab5, and so on.
- An asterisk (*) matches zero or more occurrences of a character or expression. For example: (abc)* matches null, abc, abcabcabc, and so on. abc* matches abc, abcc, and so on.
- A plus sign (+) matches one or more occurrences of a character or expression. For example: (abc)+ matches abc, abcabc, and so on.
- A question mark (?) matches zero or one occurrence of a character or expression. For example: (abc)? matches null or abc only.
- A pipe (|) matches one of the listed choices. For example: (a|b|c) would match a, b, or c.
- A caret (^) is used to mark the beginning of a line, and the dollar sign ($) is used to mark the end of a line. You need only to use this in AppEnhancer Administrator when you have two options in a single expression (as is used in Boolean Choice). For example: ^Choice1$|^Choice2$
- When the caret is used within square brackets ([ ]), it excludes values. It is same as the example used for square brackets ([ ]). Parentheses () are used to group items together in a subexpression, which can then be called using $1, where 1 represents the number of the subexpression within a sequence. For example: In the expression (a|b|c)(a*), $1 would represent (a|b|c) in the **Data Extraction** and **Formatting** text boxes within AppEnhancer Administrator, and $2 would represent (a*).
- A question mark and colon within parentheses (?:*<n>*) indicate a grouping that will not be considered a subexpression. For example: In the expression (a|b|c)(?:\$)(a*), $1 would represent (a|b|c) in the **Data Extraction** and **Formatting** text boxes within AppEnhancer Administrator, and $2 would represent (a*). (?:\$) would not be represented for extraction at all.

- Braces ({}) indicate bounds (in other words, values within the braces indicate the number of characters to match). For example: Within an expression, {5} would match any combination of five characters.
- Sets ([ ]) indicate a range of values that can be selected. For example: Within an expression, [123] would match 1, 2, or 3. [^123] would match any character that is not 1, 2, or 3. [0-9] would match any number from 0 to 9. [^0-9] will match any character that is not a numeral.
- Shortcuts can be used in place of sets: \w matches any alphanumeric character, including underscore. \d matches any digit. \l signifies lowercase, \u signifies uppercase, \s signifies space. For a more detailed list of these operators, consult a regular expression syntax reference. For example: \d{4} would match any series of 4 digits (1234, 9845, and so on). \w{2} would match any series of 2 alphanumeric characters (ab, df, 1g, and so on).

Here are some examples of data formats:

- Long Series of Numbers: In an example of a data format that accommodates a long series of numbers, n-nn-nnn-nnnnnnn, might be used for international phone numbers. Only the numbers (no dashes) will be saved to the database. It will be formatted as n-nn-nnn-nnnnnnn.
- Date, Month, and Year in YYYY-MM-DD: In an example of a data format that accommodates a date in the YYYY-MM-DD format require that only the years 1999, 2001, and 2002 be accepted, and you could change the **Validation Expression** to `(1999|2001|2002)-?(\d{2})-?(\d{2})`.
- Boolean format: In an example of a data format where users can choose either Print Version or Online Version when indexing a document with this format, if Print Version is chosen, Print will be stored in the database. If Online Version is chosen, Online will be stored in the database.

5.7 Managing Web Access user settings

You can customize Web Access user settings on a per-user basis, and also edit the default user settings for all AppEnhancer Web Access users. "Web Access User Settings" on page 91 provides more information.

5.8 Managing auto index options

1. Navigate to the **Application Management** > <*your data source*> > **Auto Index Options** node in AppEnhancer Administrator.
2. In the **Auto Index Options** page, configure the options as described in the following table:

Field	Description
Disable Auto Index <Delete> Option	Disables **Delete** on the **Auto Index Result** dialog box.

Field	Description
Disable Auto Index <Delete All> Option	Disables **Delete All** on the **Auto Index Result** dialog box.
Disable Auto Index <Select> Option	Disables **Select** on the **Auto Index Result** dialog box.
Preserve Auto Index Records	Preserves Auto Index records. By default, when an index record in the Auto Index table is used to index a new document, the record is deleted from the Auto Index table. You can configure the data source so that records are preserved in the Auto Index table even after they have been used.
Auto Index Values are Read-Only during Document Indexing	Maintains the Read-Only state in Read-Only index fields when using Auto Index during Document Indexing. By default, when a record from the Auto index table is used to index a document, the index values can be changed (until the document is saved) even if the index fields are flagged as Read-Only. You can configure the data source so that index values in Read-Only fields cannot be changed after the field is populated with the Auto Index value.

3. Click **SAVE**.

5.9 Managing Global UDL

You can create a global user-defined (UDL) that can be shared between AppEnhancer applications within a data source. Each global UDL has a unique name.

1. Navigate to the **Application Management > <***your data source***> > Global UDL** node in AppEnhancer Administrator.
2. Click **ADD**.
3. In the **Global UDL** page, provide a unique name, description, and the number of user-defined list items. "Creating new applications" on page 53 contains more information.
4. Click **OK**.

5.10 Managing password policies

During password policy loading and initialization, the built-in password policy plug-in is installed. The built-in password policy is shared by all data sources.

Any changes made in AppEnhancer Administrator take effect immediately. To take effect in Web Access and Rest components, you must restart the IIS.

1. Navigate to the **Application Management** > **<***your data source***>** > **Password Policy List** node in AppEnhancer Administrator.
2. Click a policy from the list.
3. On the policy page, enter the minimum password length.
4. Select the **Enable this policy** check box to enable the policy.
5. Click **Save**.

5.11 Managing Queues

To use full-text search and the OCR features, Queues for full-text and OCR are controlled from **Queues** under each DataSource. You can locate this node in AppEnhancer Administrator by navigating to **Application Management** > **<***your data source***>** > **Queues**.

You can create/modify and delete queues from the **Available Queues** list. The queues are then moved to **Processing Queues** to be picked jobs for Indexing Service.

A queue is unique for each data source and a queue can have the same name in different data source.

Any changes made in **Queues** within AppEnhancer Administrator take effect immediately. Before changes will be applied in Indexing Service, you must start or restart the **AppEnhancer Indexing Service** from Windows Service.

5.11.1 Adding a New Queue

Adding a new queue adds a new entry for the queue in the **AE_QUEUE** table in the database for storing full-text database information for documents. You can choose whether a queue will be a full-text queue (for documents that are already in text format or for images that have been processed using OCR) or an OCR queue (for documents that must be processed to extract text from an image). These options are only available for Available Queues.

To add a new queue:

1. In AppEnhancer Administrator, click **Application Management** > **<***your data source***>** > **Queues**.
2. Click **New**.

3. In the **Create New Queue** dialog box, type a name in the **Name** box.
4. In the **Type** list, select a queue type. You can choose from **OCR** or **FULLTEXT**. OCR queues can be used by users submitting documents for OCR and FULLTEXT queues can be selected when a user submits a document for full-text indexing.
5. In the **Description** box, you can enter an optional description that will appear in the Available Queues list with the queue name.
6. Click **OK**.

   The new queue is listed in the **Available Queues** list.
7. For each additional queue you want to create, repeat Step 3 to Step 6.
8. When you are finished, click **CANCEL** to close the **Create New Queue** dialog box.

5.11.2 Modifying a Queue

Users can only modify a queue's description in Available queues.

To modify a queue description:

1. Select a queue from the **Available Queues** list.
2. Click **Modify**.
3. In the **Modify Queue Description** dialog box that appears, update the description.
4. When you are finished, click **OK**.

   The updated description appears in the Available Queues list.
5. When you are finished, click **CANCEL** to close the **Modify Queue Description** dialog box.

5.11.3 Deleting a Queue

If a queue is no longer required, you can delete the queue from the Available queues list. When deleting a queue, you must ensure that it is not assigned to any applications.

To delete a queue:

1. Select a queue from the **Available Queues** list.
2. Click **Delete**.
3. In the **Confirmation** dialog box that appears, confirm the deletion by clicking **OK**.

   The selected queue is deleted from the Available queues list.

4. When you are finished, click **CANCEL** to close the Confirmation dialog box.

5.11.4 Moving Queues between Available Queues and Processing Queues lists

The Available Queues list displays the existing queues in your database and the Processing Queues list displays queues you can currently use in a job. Users can move queues between the **Available Queues** to **Processing Queues** lists.

Note: Following any changes with moving queues between the lists, you must restart Indexing Service to apply the changes.

To move a queue from the Available Queues list to the Processing Queues list:

1. In the **Available Queues** list, select a queue.
2. Click the right arrow button.

   The selected queue is moved from the Available Queue list to the Processing Queues list.
3. Click **Save** to save the move.

To move a queue from the Processing Queues list to the Available Queues list:

1. In the **Processing Queues** list, select a queue.
2. Click the left arrow button.

   The selected queue is moved from the Processing Queues list to the Available Queue list.
3. Click **Save** to save the move.

Chapter 6

Web Access User Settings

A user setting is a set of default properties assigned to an AppEnhancer Web Access user by the administrator. The user setting is created when a user logs in to AppEnhancer Web Access for the first time.

Note: If the current data source is using the Windows security provider, user settings are not created for users until they have logged in to Windows.

You can edit user settings through **Web Access User Settings** in AppEnhancer Administrator. You can customize profiles on a per-user basis, and also edit the default user settings for all AppEnhancer Web Access users. If users are not given the **Configure Work Station** privilege, they cannot alter the settings that you have configured in their user settings. This enables you to uniformly configure functionality across clients, if needed. You can make changes to user setting values and save the changes to the database. Also, you can export settings to a file and import settings from a file. You can also undo changes that you have made, copy one setting to specific users and groups, or restore default values to reinitialize the database values to their original defaults.

Caution

Changes made to the user settings can accidentally disable AppEnhancer Web Access functionality. Settings should be changed only if necessary. If your AppEnhancer Web Access does not function correctly after you make a change, reset the settings to the default values.

1. Navigate to the **Application Management** > <*your data source*> > **Web Access User Settings** node in AppEnhancer Administrator.
2. Select a user or group. You can also select multiple users and groups.
3. On the **Data Source** tab, configure the options as described in the following table:

Section or field	Description
Search/Result Set	
Enable Preview Thumbnails for Each Document in Query Results	Allows user to specify whether to preview thumbnails for each document in query results.
Page Index of Preview Thumbnail	Sets which page will be used in thumbnail preview.

Section or field	Description
Display Document in Separate Popup Window	Opens each document in a separate browser window. **Note:** This setting applies only when you open documents from the **Query Results** page. It does not affect document display during batch import or document indexing.
Show Document ID	Includes AppEnhancer document IDs in the query results.
Enable search by Document ID	Allows user to search for a document with the document ID. You can allow the user to search documents through group permission.
Show Previous Document Version	Displays the previous document revisions in the query results.
Document ID Sort Order	Sets the sort order (the order in which a result set is sorted and displayed, based on the document ID) for documents in the query results.
Query Results Page Size Limit	Limits the number of results per page in the query result. Type any number from 1 to 500.
Enable Document Properties Search	Configures the search criteria page to include document properties as well as document index values.
Document Index Export Format	Sets the format for exporting document index values.
Enable Preview Thumbnails for Each Document in Query Results	Enables you to specify whether to preview thumbnails for each document in query results.
Page Index of Preview Thumbnail	Sets which page will be used in thumbnail preview.
Document View	
Prompt for Checkout	Prompts you to check out the document when you open it from the **Query Results** page.
Show Page Thumbnails	Displays page thumbnails for an open document.
Enable Inline Rendering of Foreign Files	Enables HTML export of foreign files on the server side.

Section or field	Description
Use Browser to Display PDF Files	Provides a link to view the PDF files in a new browser tab or window if the browser can display PDF files in their native format. You can also install Adobe Acrobat Reader to view PDF files.
Use Browser to Display Secured PDF Files	Provides a link to view the secured PDF files in a new browser tab or window if the browser can display PDF files in their native format. You can also install Adobe Acrobat Reader to view PDF files.
Enable Inline Viewing of PDF Files	Enable inline viewing of PDF files inline in Viewer instead of a PDF file link while using a browser to display PDF files or secured PDF files.
View Native Images	Display Bitmap, GIF, JPEG, PNG images in Viewer in native format without Render Server capability.
The Number of Pages to Pre-render	Set the number of pages to pre-render after current page is loaded. Its valid value is from 0 to 5 and its default value is 3. Sets 0 means turns off pre-render function.
Thumbnail Number Limit	Limits the number of thumbnails for a document to help improve rendering performance.
Open Office Documents with Office Online Server	Enables viewing and editing Microsoft Office Documents using Office Online Server (OOS).
Display DPI of PDF/Image file in viewer	Sets the display DPI of PDF and Image files in the viewer. The value range is 72-999. The default value (-1) is the original DPI. This option can be configured by the administrator only.
Automatic Displaying DPI	Renders images using dynamic DPI scaling to improve rendering server performance. When this option is enabled, the DPI value set in **Display DPI for PDF/ Image file in viewer** is ignore. **Note:** If you do not encounter performance issues while rendering, this option should be disabled.
Index	
Show Index View	Enables you to specify whether to display index fields for an open document.

Section or field	Description
Check for Matching Index	When you index a new document, checks for duplicate index entries for documents in the current application and provides an error message if a matching index is found.
Enable Dual Data Entry	Enables you to set dual data entry as the required method for entering document indexes. Selected by default.
Ignore Date Stamp	Ignores the date stamp field for the matching index check.
Index Results Page Size Limit	Limits the number of indexes displayed on a page.
Import	
Display Batch in Separate Popup Window	Opens the batch in a separate window.
Enable Scanning	Scan feature can create a new document or batch. It can also scan documents into an existing document or batch.
Scan File Type	Sets the scanned file format to AutoDetect, TIFF, JPEG, PDF, or PNG.
Scan Feed Mode	Sets the scan feed mode to Auto or Single.
Import Email Attachment as New Page	If set to true, imports email (.msg) body as one page and attachment as another page (If attachment contains attachment, adds more pages).
Start New Document from a temporary Batch	Create a document from batch (legacy way by default) or new document directly.
Inspect PDF File	Inspects PDF files when they are imported.
Decrypt PDF File	Decrypts secured PDF files when they are imported.
PDF Portfolio Import Options	Sets the import settings for PDF Portfolio files. You can choose from No Detect, As Foreign File, or Extract Embedded Files. No Detect indicates that no attempts are made to identify PDF Portfolio files. As Foreign File indicates that portfolio files are maintained as foreign files and to view a file, users must first download it before opening it in a PDF viewer. Extract Embedded Files indicates that all embedded files are extracted from the portfolio file and imported as separate pages before the original PDF portfolio file is deleted.

Section or field	Description
Export	
Use PDF Format if Possible	Exports documents in the PDF format, if applicable. **Note:** If you select this option, you cannot set the image format for black and white, 4-bit and 8-bit color, and true-color images.
PDF	Sets the PDF file export format for PDF or image.
Black and White Images	Sets the image format for black and white images. Available values are: Windows BMP, TIFF, and Compressed TIFF.
4-bit or 8-bit Color Images	Sets the image format for 4-bit or 8-bit color images. Available values are: Windows BMP, Compressed Windows BMP, GIF, TIFF, and Compressed TIFF.
True-Color Images	Sets the image format for true-color images. Available values are: Windows BMP, GIF, JPEG, TIFF, and Compressed TIFF.
JPEG Quality Factor	Sets the quality factor when you select JPEG as the **True Color Image** format. Type any number from 1 to 100.
Text	Specifies whether you want to export textual data as text or as an image.
Use Multipage Files	Enables the export of multipage documents.
Export in Archived Format	Enables the export of documents in the archived format.
COLD Form Overlay for Export	Sets the type of COLD overlay you want to use when you export documents. Available values are: Text, Image, None.
Merge Selected Documents into One	Combines the selected documents from a query results list into single document.
COLD	
Default View COLD Form Overlay	Specifies the type of COLD overlay to use when you open documents. Available values are: None, Text, and Image.
Show Color Bars	Turns on the color view.
Color Bar Lines (1-6)	Sets the width of color bar bands. Use a number from 1 to 6. The default is 3.

Section or field	Description
Color Bar Color	Sets the color that is used for the color bar bands. When you view documents in AppEnhancer Web Access Document Viewer, the background is composed of alternating bars of a selected color and white.
Text Font Name	Sets the name of the font to use for text data.
Text Font Size	Sets the point size to use for the selected font. This is a required field. Type a font size from 6 points to 24 points.
Text Font Bold	Displays text in *bold* typeface.
Text Font Italic	Displays text in *italic* typeface.
Print	
COLD Form Overlay for Print	Sets the type of COLD overlay you want to use when you print documents. Available values are: Text, Image, None.
Endorse Printed Pages	Configures printing so that printed documents are endorsed.
Endorsement Position	Sets the endorsement position, if you select **Endorse Printed Pages**. Available values are: LeftTop, LeftBottom, RightTop, and RightBottom.
Endorsement Text (Maximum of 70 characters)	Specifies the text to appear in an endorsement, if you select **Endorse Printed Pages**. This field also supports predefined macros. You can type up to 70 characters, including spaces.
Page Fetch Retry Enabled	If an error occurs, sets the application to continue its attempts to retrieve a page as many times as you specify in the **Page Fetch Retry Count** field. Selected by default.
Page Fetch Retry Count (1-10)	Sets the number of attempts that the application makes to retrieve a page if an error occurs. Applicable only if you select **Page Fetch Retry Enabled**.
Show Print Log	Displays the log when the print operation ends.
Email	
Use PDF Format if Possible	Sets the format for email attachments to PDF.

Section or field	Description
PDF	Sets the PDF file export format for PDF or image.
Use XPS Format if Possible	Sets the format for email attachments to XPS. **Note:** You can choose either the PDF or XPS format. If you select these options, you cannot set the image format for black and white, 4-bit and 8-bit color, and true-color images.
Black and White Images	Sets the image format for black and white images. Available values are: TIFF, Windows BMP, and Compressed TIFF.
4-bit or 8-bit Color Images	Sets the image format for 4-bit or 8-bit color images. Available values are: Windows BMP, Compressed Windows BMP, GIF, TIFF, and Compressed TIFF.
True-Color Images	Sets the image format for true color images. Available values are: Windows BMP, GIF, JPEG, TIFF, and Compressed TIFF.
JPEG Quality Factor	Sets the quality factor when you select JPEG as the **True Color Image** format.
COLD Form Overlay for Email	Sets the type of COLD overlay you want to use when you email documents. Available values are: Text, Image, None.
Display Text as	Indicates the display of textual data as text or image. **Image** is selected by default.
Use Archive File Format	Enables you to use the archive file format for email messages.
Use Multipage Files	Enables you to email multipage documents. Selected by default.
Send Attachments as Hyperlinks	Enables you to use hyperlinks for email attachments. Selected by default.
Send Documents as Email Attachments	Enables you to choose if you want to include documents as hyperlinks or attachments in an email. When this option is set to False, you can sent documents as hypelinks only. This option can be configured by the administrator only.
Merge Selected Documents into One	Combines the selected documents from a query results list into a single document.

Section or field	Description
Mail Message Format	Specifies the format for email messages. HTML is selected by default.
Client Email Format	Specifies the format for email messages that are saved to the desktop client. **MSG** is selected by default.
Registered Mail Address	Specifies the default mail address of a user. This option can be configured by the administrator only.
Full-text	
Enable Full-Text Search	Configures the search criteria page for full-text search. The option is selected by default. Select **Request Full-Text Search Support** on the login page when you log in to a data source to enable this feature. **Note:** Disabling this option does not release the full-text license that was assigned to you when you logged in to AppEnhancer Web Access.
OCR Language	Sets the default language to submit documents for OCR indexing.
Prompt Submitting Full-Text Index/OCR Dialog	If selected, each time you submit documents for full-text or OCR indexing, a dialog box appears to enable you to select an OCR language from a list box. If not selected, no dialog box appears. The value set in the **OCR Language** field is the default.
Others	
Show Checked Out Documents in Home Page	Allows user to specify whether to show currently checked out documents in home page.
Only Show Recently Created Documents by Current User	Shows only the recently created documents by the current logged in user in the application page.
Job Manager (only in Administrator)	Maximum Count of Backend Print/Export/Email Job – When enabled, changes long-running print/export/email jobs to the backend from the WebAccess UI. It improves user experience by allowing other WebAccess operations simultaneously. This item defines the maximum job count of a user.

4. On the **Application** tab, select an application and configure the options as described in the following table:

Section/field	Description
Search/Result Set	
Result Set Sort Column	Column sorting of the result set. This option is used to configure which column the query results are sorted by (it requires an index of the column as opposed to the column name). This option can be configured by the administrator only.
Result Set Sort Order	Sort order of the result set. This option can be configured by the administrator only.
Result Set Display Columns	Number of columns to be displayed in the result set. This option can be configured by the administrator only.
Result Set Column Order	Order of columns of the result set. This option can be configured by the administrator only.
Index	
Sort by Index Field Name	Sort order of index.
Result Set Sort Order	Sort order of the result set.
Others	
Document Title Field	Title for the document. The list of index fields populates according to the application you select. The value assigned to the selected field appears as the title of all documents that belong to the selected application.
Batch	
Batch Sort Column	Default column sorting of the batch list. This option can be configured by the administrator only.
Batch Sort Order	Default sort order of the batch list. This option can be configured by the administrator only.
Allow Public Owner	Enable batch public owner. This option can be configured by the administrator only.
Allow Private Owner	Enable batch private owner. This option can be configured by the administrator only.

Section/field	Description
Allow Group Owner	Enable batch group owner. This option can be configured by the administrator only.

5. Click **SAVE**.

You can also configure additional settings by using the following options:

- **SET DEFAULT**: Initialize selected user settings to default values.
- **COPY TO**: Copy user settings from one user or default profile to other users and groups.
- **IMPORT**: Import existing user settings or merge with current profile.

  Note: If the merge file does not contain a value for a particular setting, the existing setting does not change.

- **EXPORT**: Export the user settings to a file (XML).

Chapter 7

Servers

You must configure AppEnhancer server settings in AppEnhancer Administrator.

7.1 Configuring Auto Retention Filer service

1. Navigate to the **Server Management > Auto Retention Filer** node in AppEnhancer Administrator.
2. For **Service Credentials**, provide the following:
   - **Domain\User**: The impersonation account used by the Auto Retention Filer Service to access the resources.
   - **Password** and **Confirm Password**: Password for the account.
3. Go to the **Data Sources > AppEnhancer Service Credentials** tab and provide the user credentials for the impersonation account in the **User Name**, **Password**, and **Confirm Password**.
4. Click **SAVE**.

7.2 Configuring Event Dispatch Broker

1. Navigate to the **Server Management > Event Dispatch Broker** node in AppEnhancer Administrator.
2. For **Properties**, provide the following:
   - **Enabled**: Enables the Event Dispatch Broker.
   - **Event Dispatch Broker URL**: URL of the workstation where integration components of Event Dispatch Broker is installed.
3. Click **SAVE**.

7.3 Configuring Rendering Server

1. Navigate to the **Server Management > Rendering Server** node in AppEnhancer Administrator.
2. On the **Rendering Server** page, configure the options as described in the following table:

Section/field	Description
Service Credentials	
Domain\User	The impersonation account used by the Rendering Server to access the resources. This account must have at least Read and Write access to any resources the AppEnhancer Rendering Server needs to access, to fulfill rendering requests.
Password and Confirm Password	Password of the user.
Cache	
Location	Location where rendered files are cached for repeated access. **Note:** If the AppEnhancer Web Access Server and Rendering Server are on the same workstation, the AppEnhancer Rendering Server cache location can either be a UNC path or local drive letter path. If the AppEnhancer Web Server and Rendering Server are not on the same workstation, the AppEnhancer Rendering Server cache location must be a UNC path, because the cache location must be available to AppEnhancer Web Access Server and Rendering Server.
Database	Database information containing tables used to manage the rendering queue. **Note:** If your database is MySQL, you must use `RenderServer` as the ODBC name.
Schema	Database schema, if needed. **Note:** Schema is supported only for SQL Server, PostgreSQL, and Oracle databases.
Generation	

Section/field	Description
Max number of concurrent conversions	Limits the total number of image conversions or foreign file HTML rendering conversions at any particular time. All converted files except the rendering results in the mainframe of the client viewer are affected by these options, including thumbnails, rendering of documents for email, rendering of documents for export, and rendering for documents for print. If you want to allow more conversions to occur simultaneously (to support more users simultaneously requesting documents), calculate the maximum number of concurrent connections: Multiply the number of CPU cores on the Rendering Server by 5. Type the resulting number in this field.
Image type to generate	Image type (GIF or JPEG files) to be created when it converts AppEnhancer web images, COLD/ERM documents with image form overlay, and thumbnails.
Max wait time for an image conversion to complete (sec)	Delay interval (in seconds) between image conversion attempt retries. Real time rendering is not affected by this option.
Render foreign files as HTML	Renders foreign files as HTML files.
Max wait time for a HTML conversion to complete (sec)	Delay interval (in seconds) between foreign file conversion attempt retries. Real time rendering is not affected by this option.
COLD Form Overlay Font	Custom font for AppEnhancer image form overlay. Various font types, font styles, and font sizes can be configured for form overlays. It is recommended that you use only fixed width fonts for Form Overlay.
Cleanup	
Check the cache every (min)	Delay (in minutes) between each garbage collection attempt.
Maximum Files Limit	Maximum number of files allowed in cache before garbage collection takes place.
Maximum Space Used Limited (MB)	Maximum megabytes allowed for all files in cache. This number should be larger than the largest possible file to be retrieved from AppEnhancer or the file might not be rendered.

Section/field	Description
When limit is reached, decrease by (%)	Percentage of used space that must be reclaimed through garbage collection before a garbage collection attempt stops, after it has started.

Note: The real time rendering is not affected by the options of **Cleanup** because it has its own cache mechanism.

3. Click **SAVE**.

Note: Ensure that the Rendering Server and Web Access Server use the same data source.

7.3.1 Render server performance tuning tips

Configure the Web Access Convertor properties

1. Open Windows Component Services from the Start menu
2. Double-click **Console Root** > **Component Services** > **Computers** > **My Computer** > **Running Processes**.
3. Ensure that the process **Web Access Image Convertor** is *not* running.
4. Double-click **COM+ applications** and select **Web Access Image Convertor**.
5. Right-click and select **Properties**.
6. In the dialog which appears, select the **Pooling & Recycling** tab and set the Pool Size to 5* the number of CPU cores.

7.4 Configuring REST services

1. Navigate to the **Server Management > REST Services** node in AppEnhancer Administrator.
2. For **Service Credentials**, provide the following:
   - **Domain\User**: The impersonation account used by the REST Services to access the resources.
   - **Password** and **Confirm Password**: Password for the account.
3. Click **SAVE**.

7.5 Configuring utility services

1. Navigate to the **Server Management > Utility Services** node in AppEnhancer Administrator.
2. On the **Utility Services** page, configure the options as described in the following table:

Section/Field	Description
Service Credentials	
Domain\User	The impersonation account used by the Utility Services to access the resources.
Password and Confirm Password	Password of the impersonation account.
Authentication and Authorization	
Permissions Cache Timeout (min)	Time taken for permission of users to be cached before they are refreshed. The value can range from 0 to 1440 (0 means refresh As Soon As Possible). Increasing this setting improves performance. Decreasing this setting speeds up the implementation of permission changes.
Principal Timeout (min)	Time, in minutes, before timeout of an authenticated credentials of user. The value can range from 1 to 1440. When a user successfully logs in, a principal object is created as proof of user authentication. This setting controls the length of time the AppEnhancer Authentication Web Service keeps this object. Increasing this setting improves security. Decreasing this setting speeds implementation of authentication changes.

3. Click **SAVE**.

7.6 Configuring Web Access Server

This section describes the configuration of AppEnhancer Web Access Server by using AppEnhancer Administrator and also discusses about the security settings for AppEnhancer Web Access.

7.6.1 Configuring Web Access Server using AppEnhancer Administrator

1. Navigate to the **Server Management > Web Access Server** node in AppEnhancer Administrator.
2. On the **Web Access Server** page, configure the options as described in the following table:

Section/field	Description
Service Credentials	
Domain\User	This account grants security privileges to AppEnhancer Web Access where an authentication context is required to access a resource and the global credentials option is selected for that resource.
Password and Confirm Password	Password for the account.
File Type Map	
Extension	Extension for the type of file that you want to map.
File Types	File type that you want to associate with the extension. For example, **Image Format**, which enables you to import files into AppEnhancer Web Access. AppEnhancer Web Access natively supports many file types such as TIFF, Windows bitmaps, TGA, RTF, JPEG, GIF, PCX, and DCX. By default, files that are not natively supported are imported as foreign files.
Email Setup	
Save Mail to Client	Saves document in email formats (.msg or .eml) or sends email via SMTP server.
Email Address	Configures the email address list. Adding, removing, editing, importing, and exporting can be used to configure the Email Users list. You can also import an address book in comma-delimited or tab-delimited Outlook CSV format and also export the listed email addresses to a file for use with other email clients.

3. Click **SAVE**.

7.6.2 Configuring IIS authentication type

On installation of AppEnhancer Web Access, only **Anonymous Authentication** is enabled for AppEnhancer Web Access. You can change the authentication type by using IIS. When the data source is using a Windows security provider, you can enable Windows Authentication and disable Anonymous Authentication in IIS. Then, the client can automatically log in to AppEnhancer Web Access by using Windows Credentials.

1. Open IIS Manager.
2. Navigate to the AppEnhancer Web Access web application. By default, it is <\ *Default Web Site**AppEnhancer*>.
3. Double-click **Authentication**.

   In the **Authentication** page, if you enable both **Anonymous Authentication** and **Windows Authentication**, anonymous authentication takes precedence over Windows authentication.

   If you want to automatically log in to AppEnhancer Web Access as a Windows user, disable **Anonymous Authentication**.

Note: AppEnhancer Web Access provides various application settings for different business or deployment requirement. To configure the settings, open `web.config`, navigate to the `appSettings` element, and make the required changes.

7.6.3 Configuring ADFS for AppEnhancer Web Access

1. In `web.config` in the Web Access installation folder, from the subnode `<modules>` in the `<system.webServer>` node, uncomment the configuration of `WSFederationAuthenticationModule` and `SessionAuthenticationModule` modules.
2. Uncomment the `<system.identityModel>` node and change the configuration of the `<audienceUris>` node (Web Access URL should be changed in this node) and `<trustedIssuers>` (ADFS server issuers should be changed in this node).
3. Uncomment the `<system.identityModel.services>` node and change the configuration of `<wsFederation>` node (in this node, issuer is the URL of the ADFS server issuer, realm and reply are the Web Access URL).
4. Add the following in `web.config`:

```
<externalAuth>
<providers>
<provider name="adfs"
enabledToAllDataSources="true"aeAuthenticationChain="ProviderId, AD">
</provider>
</providers>
</externalAuth>
<adfsClientConfig
serverName="https://ZJDev2K8R2.aeqa.com"
attributeMap_Usrnam="http://schemas.xmlsoap.org/
ws/2005/05/identity/claims/name"
```

```
attributeMap_Securid="http://schemas.microsoft.com/
ws/2008/06/identity/claims/primarysid"/>
```

The following table describes the attributes:

Attribute	Description
serverName	The server name that hosts the web application.
attributeMap_Usrnam	The value of this attribute is used to create a mapping to the column `Usrnam` in the ae_login table of the AppEnhancer database.
attributeMap_Securid	The value of this attribute is used to create a mapping to the column `Securid` in the ae_login table of the AppEnhancer database.

Notes

- If a provider is not enabled to all the data sources, it should have a `datasources` element. In this element, all of the data sources that support this provider should be listed.
- The value of `aeAuthenticationChain` is the authentication methods that are used to locate the SSO user in the ae_login table. Three methods are supported: `ProviderId`, `AD` and `Any` (case insensitive). `ProviderId` means searching for the user in theae_login table that matches the specific SSO provider ID. `AD` means searching the ae_login table for matching AD user. `Any` means any user that matches the SSO user will be used.

5. Change the Web Access server address in the `FederationMetadata\2007-06\FederationMetadata.xml` file in the Web Access installation folder.
6. In the ADFS server, create a new Relying Party Trusts for Web Access. In the Relying Party Trusts, add new Issued Claims for user's Name and user's Primary SID.
7. Import the users. If you have many users, you can create an .xml file and import it from AppEnhancer Administrator. If Windows Active Directory is used, you can import the users from the **User List** page and change the `providerid` of each user after the import.

   Note: This step is optional.

8. Launch the AppEnhancer Web Access login page and click the **ADFS LOGIN** button. The browser redirects you to the ADFS server or prompts you to provide the login credentials (depends on the settings of ADFS server). After you provide the login credentials, the browser redirects you to AppEnhancer Web Access.

Note: ADFS is also supported for AppEnhancer Administrator. To configure ADFS for AppEnhancer Administrator, follow the procedure provided for

AppEnhancer Web Access server and make the necessary changes for the AppEnhancer Administrator server.

7.6.4 Configuring CAS for AppEnhancer Web Access

1. Add the following in `web.config`:

```
<externalAuth>
<providers>
<provider name="cas"
enabledToAllDataSources="true"aeAuthenticationChain="ProviderId">
</provider>
</providers>
</externalAuth>
<casClientConfig
casServerLoginUrl="http://AECAS-JASIG.aeqa.com:8080/
cas-server-webapp-3.4.12.1/login"
casServerUrlPrefix="http://AECAS-JASIG.aeqa.com:8080/
cas-server-webapp-3.4.12.1/"
serverName="http://ZJDev2K8R2.aeqa.com"
ticketValidatorName="Saml11"
attributeMap_Usrnam="uid"
attributeMap_Securid="udcid"
serviceTicketTimeout="60"/>
```

The following table describes the attributes:

Attribute	Description
casServerLoginUrl	CAS server login URL.
casServerUrlPrefix	URL to the root of CAS server application. This URL is used to validate a service ticket.
serverName	Server name that hosts AppEnhancer Web Access.
ticketValidatorName	Name of validating ticket that validates CAS tickets using a particular protocol. For example, Saml11, Cas20.
attributeMap_Usrnam	Value of this attribute that is used to create a mapping to the column `Usrnam` in the ae_login table of the AppEnhancer database.
attributeMap_Securid	Value of this attribute that is used to create a mapping to the column `Securid` in the ae_login table of the AppEnhancer database.
serviceTicketTimeout	Period of time after a service ticket has been validated.

The attributes casServerLoginUrl, casServerUrlPrefix, serverName should be changed. The attributes attributeMap_Usrnam and attributeMap_Securid also need to be changed, based on the CAS server configuration.

2. Configure CAS server to return LDAP attribute values. For example:

```
<property name="resultAttributeMapping">
<map>
<!--Mapping beetween LDAP entry attributes (key)
and Principal's (value)-->
<entry key="uid" value="uid"/>
<entry key="sn" value="udcid"/>
</map>
```

3. Import the users. If you have many users, you can create an `.xml` file and import it from AppEnhancer Administrator.
4. Launch the AppEnhancer Web Access login page and click the **CAS LOGIN** button. The browser redirects you to the CAS server. When prompted, provide the login credentials (depends on the settings of CAS server). After you provide the login credentials, the browser redirects you to AppEnhancer Web Access.

Note: CAS is also supported for AppEnhancer Administrator. To configure CAS for AppEnhancer Administrator, follow the procedure provided for AppEnhancer Web Access server and make the necessary changes for the AppEnhancer Administrator server.

7.6.5 Configuring Auth0 for AppEnhancer Web Access

Creating an Auth0 Administrator account

1. Go to the **Application Management** > <*your data source*> > **Applications** node in AppEnhancer Administrator.
2. On the **Application List** page, click **ADD**.
3. Select **Regular Web Applications** and click **Create**.
4. Record the domain, Client ID, and secret for entry in the AppEnhancer `web.config` settings.
5. Enter a name for your application login URL and allowed CallBack URLs.
6. Click **Save**.
7. Configure the other Auth0 options as per your requirements.

Note: The **Advance Settings** and **Grant Types** tabs contain information on the selection of grants allowed. You can select implicit, authorization code, client credentials, and password, if required.

The configuration of an admin `web.config` for OAUTH is optional and does not need to be completed if you do not want to allow OAUTH users to log into AppEnhancer Administrator.

It is highly recommended you create a backup of the configuration files before editing.

Add the following sections to your `web.config` file:

```
<configSections>
     <section name="oauthClientConfig1"
type="XtenderSolutions.Authentication.OAUTH.Configuration.OAUTHClientConfiguration"/>
     <section name="oauthClientConfig2"
type="XtenderSolutions.Authentication.OAUTH.Configuration.OAUTHClientConfiguration"/>
</configSections>
```

You can configure the name of the provider that appears on the login page.

Set *enabledToAllDataSources* to `True` to enable a provider to all data sources.

```
<externalAuth>
   <providers>
     <provider name="AUTHO" enabledToAllDataSources="true"
axAuthenticationChain="ProviderId" sectionConfigName="oauthClientConfig1"
assemblyName="XtenderSolutions.ExtAuthOAUTHProvider"
typeName="XtenderSolutions.Authentication.OAUTH.ExternalAuthenticationOAUTHProvider">
     </provider>
     <provider name="AZURE" enabledToAllDataSources="true"
axAuthenticationChain="ProviderId" sectionConfigName="oauthClientConfig2"
assemblyName="XtenderSolutions.ExtAuthOAUTHProvider"
typeName="XtenderSolutions.Authentication.OAUTH.ExternalAuthenticationOAUTHProvider">
     </provider>
   </providers>
</externalAuth>
```

When *enabledToAllDataSources* is set to `False`, the provider is enabled to the data sources listed in the internal datasources element.

```
<externalAuth>
  <providers>
     <provider name="AUTHO" enabledToAllDataSources="false"
axAuthenticationChain="ProviderId" sectionConfigName="oauthClientConfig1"
assemblyName="XtenderSolutions.ExtAuthOAUTHProvider"
typeName="XtenderSolutions.Authentication.OAUTH.ExternalAuthenticationOAUTHProvider">
       <datasources>
          <datasource name="AppXtenderDEMO"/>
      </datasources>
    </provider>
    <provider name="AZURE" enabledToAllDataSources="false"
axAuthenticationChain="ProviderId" sectionConfigName="oauthClientConfig2"
assemblyName="XtenderSolutions.ExtAuthOAUTHProvider"
typeName="XtenderSolutions.Authentication.OAUTH.ExternalAuthenticationOAUTHProvider">
      <datasources>
          <datasource name="AppXtenderDEMO"/>
      </datasources>
    </provider>
  </providers>
</externalAuth>
```

Each OAUTH configuration section named oauthClientConfig1 to oauthClientConfig9 must have the corresponding providerId assignment of "AA31ACD6-FF95-4FF2-B17F-000000000001" to "AA31ACD6-FF95-4FF2-B17F-000000000009".

```
<oauthClientConfig1
  providerId="AA31ACD6-FF95-4FF2-B17F-000000000001"
  openIdCfg="https://yourname.us.auth0.com/.well-known/openid-configuration"
  serverName="https://WXServer.ax.com"
  attributeMap_Usrnam=""
  attributeMap_Securid="email"
  serviceTicketTimeout="900"
  clientId="G9ozasdfjsad89f7y23kalsdfh87"
  clientSecret="yourclientsecret"
```

```
  scope="openid email profile"
  ignoreGroups="true"/>
```

```
<oauthClientConfig2
 providerId="AA31ACD6-FF95-4FF2-B17F-000000000002"
 openIdCfg="https://login.microsoftonline.com/common/.well-known/openid-configuration"
 serverName="https://WXServer.ax.com"
 attributeMap_Usrnam=""
 attributeMap_Securid="unique_name"
 serviceTicketTimeout="900"
 clientId="12345678-1234-1234-1234-123456789012"
 clientSecret="yourclientsecret"
 scope="openid email profile"
 ignoreGroups="false"
 />
```

To test the OAUTH configuration, you must create and configure users in AppEnhancer Administrator. You can import a user list with the username, optional full name, security ID and the provider ID.

The following table describes the attributes:

Attribute	Description
providerId	GUID for the OAuth provider. Starting provider id is "AA31ACD6-FF95-4FF2-B17F-000000000001". Each configuration requires a unique provider Id with a suffix of 1–9.
openIdCfg	URL for the OAuth.
serverName	Server name that hosts AppEnhancer Web Access.
attributeMap_Usrnam	Value of this attribute is used to create a mapping to the column `Usrnam` in the ae_login table of the AppEnhancer database.
attributeMap_Securid	Value of this attribute is used to create a mapping to the column `Securid` in the ae_login table of the AppEnhancer database.
serviceTicketTimeout	Length of time after a service ticket has been validated.
clientId	OAuth client ID.
clientSecret	OAuth client secret.
Scope	OAuth client scope.
ignoreGroups	Ignore Group is set to true to prevent the loading of the user's data group list.

AppEnhancer web addresses for the IdP

The following is a list of AppEnhancer web addresses for the IdP:

- https://server.com/AppEnhancer/Account/OAuthSingleSignOnHandler

- https://server.com/AppEnhancer/Account/OAuthSingleSignOutHandler
- https://server.com/AppEnhancerAdmin/Account/OAuthSingleSignOnHandler
- https://server.com/AppEnhancerAdmin/Account/OAuthSingleSignOutHandler

The AppEnhancer web address is also the IdP Single Sign On web address. If you want to use SSO with an Admin user, then you must list both web addresses for the IdP Redirect URIs. For the Application ID URI, you can use https://WXServer.ax.com, which is the AX Server name.

The logout web address is:

- https://server.ax.com/AppEnhancer/Account/OAuthSingleSignOutHandler

If you are using a provider id other than AA31ACD6-FF95-4FF2-B17F-000000000001, you must append the provider ID or appropriate GUID to your logout web address. Append the provider ID or GUID in the following format:

```
“?ProviderId= AA31ACD6-FF95-4FF2-B17F-000000000002”
```

OAuth log settings in web.config file

The `web.config` file contains entries for verbose logging of OAuth operations.

To enable logging:

1. In the `web.config` file, locate the switches node and then add a new switch named **OAUTHSwitch**. The valid logging levels are **Off**, **Error**, **Warning**, **Information**, or **Verbose**. The command for the new switch is similar to the following:

   ```
   <add name="OAUTHSwitch" value="<log_Level_value>"/>
   ```

   where

   <log_Level_value> is the log level you want to use.

   Note: The Verbose log level is valuable when debugging the OAuth integration.

2. Next, you must add the new switch to the **sources** node. The code appears similar to the following:

   ```
   <source name="OAUTHTrace"
         switchName="OAUTHSwitch"
         switchType="System.Diagnostics.SourceSwitch">
     <listeners>
       <add name="axEventLogListener"/>
       <!--<add name="axFileListener1"/>-->
     </listeners>
   </source>
   ```

7.6.6 Configuring OTDS for AppEnhancer Web Access

Add the following in `web.config`:

```
<externalAuth>
  <providers>
    <provider name="otds"
enabledToAllDataSources="true"aeAuthenticationChain="ProviderId, AD">
    </provider>
  </providers>
</externalAuth>
<otdsClientConfig
        serverName="http://<WXServerHost>"
        attributeMap_Usrnam="oTExternalID1"
        attributeMap_Securid="oTUserID1"
        serviceTicketTimeout="0"
        useOAuth="true"
        clientId="<WXClientId>"
        clientSecret="<WXClientSecret>" />
```

Note: *<attributeMap_Usrnam>* should be same as the value of *<User Name>*

<attributeMap_Securid> should be same as the value of *<Security Id>*.

`useOAuth` should be set to **true** if OAuth protocol is used. The default value is **false**.

`clientId` is the OAuth client id that is registered at the OTDS server.

`clientSecret` is the client secret that is generated by the OTDS server. It should be empty if the OAuth client registered at the OTDS server does not support 'Confidential'.

For more information, refer to **Administrator** > **OTDS Server** > **User Attribute Mapping**.

7.6.7 Configuring SAML 2.0 for AppEnhancer Web Access

SAML 2.0 is an XML-based framework that allows identity information to be shared across multiple applications. SAML makes single sign-on (SSO) technology possible by providing a way to authenticate a user once and then communicate that authentication to multiple applications.

The configuration of an admin `web.config` for SAML2 is optional and does not need to be completed if you do not want to allow SAML2 users to log into AppEnhancer Administrator.

You can use `Self-signed certificates` or `Free trusted certificates` to configure AppEnhancer to use HTTPS.

SAML requests are signed using a PKI, a certificate with both public and private keys. The PKI must be stored in the local machine and identified in the configuration by its thumbprint.

Add the following in `web.config`:

```
<saml2ClientConfig
        serverName="https://<WXServerHost>"
        attributeMap_Usrnam="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"

attributeMap_Securid="http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"
        issuer="https://<WXServerHost>/WebAccess"
        saml2Server="https://<ae_ADFS_Server>/adfs/ls/"
        saml2ServerSloEndpoint=""
        nameIDPolicy="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
        certificateValidator="None"
        clientCertificateThumbprint="065c4b6a86b952f4ef00ebf18d8a19632db882d8"
        signingAlgorithmUrl="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
        isCasServer="false"
        />
```

where

<WXServerHost> is the Web Access server address.

<ae_ADFS_Server> is the ADFS server address for AppEnhancer.

You can install the ID provider's certificate to the AppEnhancer web servers local machine certificate store to validate the responses. It is highly recommended you create a backup of the configuration files before editing.

Set *enabledToAllDataSources* to `True` to enable a provider to all data sources.

```
<externalAuth>
  <providers>
    <provider name="saml2"
enabledToAllDataSources="true"axAuthenticationChain="ProviderId,AD">
    </provider>
  </providers>
</externalAuth>
```

When *enabledToAllDataSources* is set to `False`, the provider is enabled to the data sources listed in the internal datasources element.

```
<externalAuth>
  <providers>
    <provider name="SAML2"
enabledToAllDataSources="false"axAuthenticationChain="ProviderId,AD">
    <datasources>
         <datasource name="AppXtenderDEMO"/>
      </datasources>
      </provider>
  </providers>
</externalAuth>
```

To test the SAML2 configuration, you must create and configure users in AppEnhancer Administrator. You can import a user list with the username, optional full name, security ID and the provider ID.

The following table describes the attributes:

Attribute	Description
providerId	GUID for the SAML provider.
serverName	Server name that hosts AppEnhancer Administrator.

Attribute	Description
attributeMap_Usrnam	Value of this attribute is used to extract the value from a security token and create a mapping to the column `Usrnam` in the ae_login table of the AppEnhancer database.
attributeMap_Securid	Value of this attribute is used to extract the value from a security token and create a mapping to the column `Securid` in the ae_login table of the AppEnhancer database.
issuer	The ID string representing the service provider. This is enforced for single logout.
saml2Server	The SAML server hosting the web address of the ID provider.
assertionConsumerServiceIndex	The default value is –1, which sets the AssertionConsumerServiceURL upon Authentication request. If 0 or greater is used, then the AssertionConsumerServiceIndex attribute is set to the value supplied.
saml2ServerSloEndpoint	SAML server single logout endpoint URL.
nameIDPolicy	The name ID policy that the SAML server uses to create the name ID. An example is: `"urn:oasis:names:tc:SAML:2.0:nameid-format:transient"` For more information about name ID policies, consult your IdP documentation.
certificateValidator	Indicates the certificate to validate the SAML assertion. The following options are available: • None • PeerTrust • ChainTrust • PeerOrChainTrust If using Peer Trust, you must store your ID providers certificate with the local machine's Trusted Root Certification Authorities certificates.

Attribute	Description
clientCertificateThumbprint	The thumbprint of the certificate used to sign the SAML Requests. This certificate has public and private keys. The Impersonation account needs access to the private key. This certificate is stored in the local machine's Personal certificates and the public key certificate is uploaded to the ID provider.
isCasServer	The flag used to indicate if the SAML server is a CAS server.
ignoreGroups	Specifies that a group is to be ignored. You must set this to `false` if you do not want to look for groups in the SAML response metadata.
AddRequestDestination	Adds the `Destination` attribute set to the `saml2Server` value during a SAML request. The default setting is `false`.
serviceTicketTimeout	Specifies the timeout, in minutes, for the SSO session. The default is 900.
signingAlgorithmUrl	Indicates the web address for the signing algorithm. The default is: http://www.w3.org/2000/09/xmldsig#rsa-sha1 Other valid signing algorithm web addresses are: • http://www.w3.org/2001/04/xmldsig-more#rsa-sha256 • http://www.w3.org/2001/04/xmldsig-more#rsa-sha384 • http://www.w3.org/2001/04/xmldsig-more#rsa-sha512

7.6.8 Configuring session timeout interval by using IIS

1. Open IIS Manager.
2. Navigate to the AppEnhancer Web Access web application. By default, it is <\ *Default Web Site**AppEnhancer*>.
3. In **Features View**, double click **Session State**.
4. In the **Idle Time-out (minutes)** field, type a number in minutes.
5. In the **Actions** pane, click **Apply**.

7.6.9 Modifying maximum upload size

The default maximum upload size is 10 M for AppEnhancer Web Access. You can change the value as follows:

1. Open the `web.config` file.
2. Find the following section:

```
<system.web>
<compilation debug="true" targetFramework="4.5"/>
<httpRuntime targetFramework="4.5" executionTimeout="600"
maxRequestLength="10240" requestValidationMode="2.0" />
```

3. Change the value of `maxRequestLength`. The unit is 1 K. For example, if you want to change the maximum size to 30 M, the value should be `maxRequestLength="30720"`.

7.6.10 Configuring application settings for Web Access

AppEnhancer Web Access provides various application settings for different business or deployment requirement. To configure the settings, open `web.config`, navigate to the `appSettings` element, and make the required changes.

The following table lists some of the important settings:

Setting name	Description	Default value
AutoLogoutOnClose	Automatically log out from Web Access when you close the browser. Set the value to <*true*> to automatically log out when you close the browser window or tab.	<*false*>
RequestFTLicForAutoLogin	Request for Full-Text License when you automatically log in with Windows Authentication. Set the value to <*true*> to request Full-Text Search Support.	<*false*>
ImportPDFAsSinglePage	Import PDF (non-image-based) as multipage document or single page document. Set the value to <*false*> to import multipage PDF documents as multipage documents or set the value to <*true*> to import multipage PDF documents as a single page document.	<*false*>

Setting name	Description	Default value
SYSOPRemoteLogin	Allow SYSOP user log in to Web Access remotely. Set the value to <*true*> to allow SYSOP user to log in to Web Access remotely.	<*false*>
MaxQueryResults	Maximum number of query results retrieved per query.	<*1000*>
MaxDocIndexes	Maximum number of document indexes retrieved per document.	<*1000*>
AutoFTIndexNewDoc	Automatically submit new document for full-text indexing.	<*true*>
SameSiteSupportForOldBrowsers	If using an older browser that does not support the SameSite attribute, set the value to <*true*> to automatically remove the `sameSite=None` attribute from cookies when an older browser is detected.	<*true*>
UnmaskDocIndexNativeValueForModifyIndex	Unmask Document Index Native Values if user has Modify Index permission.	<*true*>
WinNTUserLoadGroups	If the value is set to <*false*>, Active Directory user logins do not load Active Directory groups for the user, and only CM group membership is used.	<*false*>

7.6.11 Configuring license pool and session parameters

The license pool feature of AppEnhancer Web Access enables you to reserve more licenses in the memory of the AppEnhancer Web Access process so that the communication between the AppEnhancer Web Access server and license server is reduced. By default, the license pool is enabled in AppEnhancer Web Access. The AppEnhancer Web Access administrator can change the configuration of the license pool in the `web.config` file.

When an AppEnhancer Web Access session is active, it will update its information in the database and check if there are any requests to terminate the session periodically.

The configuration of license pool and session parameters are commented in the `web.config` file. The administrator can remove the comments and change the values of these parameters. The following is a sample of the license pool and session parameters in the `web.config` file:

```
<!--
<add key="LicensePoolEnabled" value="false"/>
<add key="SessionUpdatePidInterval" value="60"/>
<add key="SessionCheckTerminationInterval" value="90"/>
<add key="LicensePoolLicCheckInterval" value="60"/>
<add key="LicensePoolDBCheckInterval" value="10"/>
<add key="LicensePoolNewReserveExpireInterval" value="2"/>
<add key="LicensePoolMaxNum" value="10"/>
<add key="LicensePoolMinReserveNum" value="2"/>
-->
```

License pool parameters:

Name	Description
LicensePoolEnabled	Whether license pool is enabled (it is enabled by default)
LicensePoolMaxNum	The maximum number of license pool (10 by default)
LicensePoolMinReserveNum	The minimum reserve number of the license pool (2 by default)
LicensePoolNewReserveExpireInterval	The interval to keep the new license reservation alive (2 minutes by default)
LicensePoolLicCheckInterval	The interval for checking the license pool to release the idle licenses (60 seconds by default). If a new reserved license expires and the current reserved license number is greater than the minimum reserve number of the license pool, the idle license is released after the check.

Note: If the license pool is enabled, after a user logs out from AppEnhancer Web Access, the license is released to the license pool and not to the License Server. When the license becomes idle and if there is no active license usage from the license pool, or the reserved license number is greater than the minimum reserve number in the license pool, the idle license is released to the License Server. Therefore, the maximum interval that the license is released from AppEnhancer Web Access session and then released to the License Server is determined by the value of `LicensePoolLicCheckInterval` plus the value of `LicensePoolNewReserveExpireInterval`. If license pool is disabled, after a user logs out from AppEnhancer Web Access, the license is released to the License Server directly.

Session parameters:

Name	Description
SessionUpdatePidInterval	The interval for updating the latest time stamp (60 seconds by default). This interval is used by each active session to update the information in the database, periodically.

Name	Description
SessionCheckTerminationInterval	The interval for checking the session status change (90 seconds by default). This interval is used by a background thread that checks the database periodically for the request from the Administrator to terminate an active session.

7.6.12 Configuring Office Online Server for AppEnhancer Web Access

To install Office Online Server (OOS) visit https://docs.microsoft.com/en-us/officeonlineserver/deploy-office-online-server.

Note: OOS can be installed only on a Windows Server operating system. The target host machine should be added in the domain.

1. After you install OOS, run the following command in Windows PowerShell to configure a new instance of OOS:

   ```
   New-OfficeWebAppsFarm -<InternalURL> "http://<servername>" -AllowHttp
   –EditingEnabled
   ```

   The following table describes the attributes:

Name	Description
InternalURL	An address through which OOS exports its service. It should be the full computer name or IP address of the OOS host.
AllowHttp	This option enables the service to be hosted without HTTPS.
EditingEnabled	This option specifies the OOS support edit function.

   If Office Online Server is already configured and you wish to change these options, run the following command:

   ```
   Set-OfficeWebAppsFarm -EditingEnabled:$true
   ```

2. In `web.config`, add the following line in appSettings:

   ```
   <add key="OOSUrl" value="<http://oos_server>" />
   ```

   Note: Replace <*http://oos_server*> with the IP address or FQDN (Fully Qualified Domain Name) of your Office Online Server.

7.7 Configuring Web Services

1. Navigate to the **Server Management > Web Services** node in AppEnhancer Administrator.
2. On the **Web Services** page, configure the options as described in the following table:

Section/Field	Description
Service Credentials	
Domain\User	The impersonation account used by the Web Services to access the resources.
Password and Confirm Password	Password for the impersonation account.
Session Management	
Session Timeout (min)	Duration of session idle time that AppEnhancer Web Services enables to elapse before closing inactive user sessions.
Session Cache Path	Stores user session data for active sessions. Session data includes authorization and authentication data for user sessions and user session context for operations a user is engaged in. The session cache path can be a local drive letter path or a UNC path (recommended).
Security	
Users may access the server using NTLM Authentication	Users may access the server using NTLM Authentication.
Automatic Login	Valid when the NTLM Authentication option is selected.
Request Full-Text License	Request full-text license on automatic login when the **Automatic Login** option is selected.
Users may access the server via Anonymous user account	Users may access the server via Anonymous user account.
User Path	
File Path	Path of the storage content.

3. Click **SAVE**.

7.8 Configuring Workflow Integration Module

The Workflow Integration Module (WIM) is an optional component to integrate workflow solutions with AppEnhancer. The WIM hosts the interfaces which facilitate communication between AppEnhancer and workflow solutions.

1. Navigate to the **Server Management** > **Workflow Integration Module** node in AppEnhancer Administrator.
2. On the **Workflow Integration Module** page, configure the options as described in the following table, and click **SAVE**:

Section/Field	Description
Enabled	Enables the Workflow Integration Module.
WIM Host	Workstation name or IP address of the server hosting the Workflow Integration Module.

7.9 Configuring administrative services

1. Navigate to the **Server Management** > **Administrative Services** node in AppEnhancer Administrator.
2. Configure the options as described in the following table, and click **SAVE**:

Section/Field	Description
Service Credentials	
Domain\User	The impersonation account used by the Administrative Services to access the resources.
Password and Confirm Password	Password for the impersonation account.
Job Folder	
Job Location	The UNC path configured on the Storage Management page. It is the folder where all the Administrative Services jobs, logs, and other files are stored.
Job Files Retention Days	The number of days that job files are kept in the Job Location folder after the job is completed.
Enable Job Files Backup (Optional)	Set this option to **True** to back up all the job files. If this option is not turned on, job files in the Job Location folder will be permanently removed when the number of days specified in **Job Files Retention Days** is reached.

Section/Field	Description
Job Files Backup Folder	When the number of days specified in Job Files Retention Days is reached, the job files are copied to the backup folder. This configuration works only when the **Enable Job Files Backup** option is set to **True**.

7.10 Configuring the Indexing Service

To configure the Indexing Service, you must complete tasks on three separate pages:

- **Service Credentials** and **Settings** tabs under the Indexing Service options in the Server Management node
- **Queues** menu for each data source in the Application Management node

To manage the full-text database, you must go to the **Full-Text Database management** tab under the Indexing Service options in the Server Management node.

7.10.1 Service Credentials tab

Navigate to **Server Management** > **Indexing Service** and on the **Service Credentials** tab, specify the user name and password for the **AppEnhancer** and **Impersonation** accounts.

7.10.2 Settings tab

On the **Server Management** > **Indexing Service** page, switch to the **Settings** tab and configure the following fields for your indexing service:

Configuration Option	Note
Indexing Service Role	You can choose the appropriate role from the list: • **Full-text & OCR Both** • **Full-text Only** • **OCR Only**
OCR Processor number	User can add a value between 0-8. The default value is 0, which indicates that the indexing service can set this setting automatically.
Remove job from queue when finished	Users can indicate whether to remove the job from the queue when it is finished running using a True or False setting. By default, this is set to False.

Connection Timeout	User can add a value between 0-10 minutes to specify the amount of time before the connection times out. The default value is 2.
Max Retry time	User can add a value between 0-15 to indicate the maximum time between retries. The default value is 2.
Retry Interval	User can add a value between 5-300 seconds to indicate the retry interval. The default value is 10.

7.10.3 Queues

As part of configuring the Indexing Service, you must set up queues. To access the **Queues** menu, you must select a data source under **Application Management**.

Note: A queue setting is unique for each data source and a queue can have the same name in different data sources.

For more information about queues, see "Managing Queues" on page 87.

7.10.4 Full-text Database Management tab

To manage the full-text databases, go to the **Server Management** > **Indexing Service** page and switch to the **Full-Text Database management** tab.

To see the full-text database list, which contains database names and full-text indexed pages, enter the **Full-Text Server URL** and click **SEARCH**.

To add a new full-text database, enter the **Full-Text Database Name** and click **ADD**.

To delete a full-text database from the list, click the database's respective **Delete**, , button.

7.11 Configuring AppWorks in AppEnhancer Administrator

Before proceeding, you must already have AppWorks installed and OTDS properly configured. For more information on installing AppWorks and configuring OTDS, see *OpenText AppWorks Platform Installation Guide for Windows*

1. In AppEnhancer Administrator, navigate to **Server Management** > **AppWorks Server**.
2. On the **AppWorks Server** screen, in the **AppWorks Platform Server URL** box, enter your full AppWorks server address. For example, `http://<server_address>:<port>/home/system` while replacing the variables with your server details.
3. Add your **AppWorks OTDS Resource ID**.

4. In OTDS, create a new user and assign both Administrator and Sysadmin permissions for AppWorks to the user. Make note of the user name and password used.
5. Returning to the **AppWorks Server** page, in the **User Name** box, type the user name of the new user you created in the previous step.
6. In the **Password** and **Confirm Password** boxes, type the password used for the previously created user.
7. Click **SAVE**.

7.12 Configuring TestLaunch in AppEnhancer Web Access

The TestLaunch tool simplifies the process of generating and testing URLs for integrating third-party applications with AppEnhancer.

The TestLaunch parameter is configured in the Administrator `web.config` file. The administrator can remove the comments and change the value of the parameter. The following is a sample of the TestLaunch parameter in the `web.config` file:

```
<!--
 <add key="TestLaunchEnabled" value="false"/>
<!--
```

Note: The default value is false. Set the value to true to enable TestLaunch and save it in administrator mode.

Using TestLaunch

You can perform a query by configuring the following fields required by the interface.

1. Select any option from the **Target Interface** list.
   - **ISubmitQuery**: Runs, searches and submits queries for an application.

     For more information, see “ISubmitQuery”.
   - **IDocument**: Manages viewing of documents and supports different functionalities of document viewing.

     For more information, see “IDocument”.
   - **IDocImport**: Facilitates the import of documents into AppEnhancer.

     For more information, see “IDocImport”.
2. The **Target Site** is populated by default, displaying an URL for web access.
3. Select **Auto logout on close** to enable auto logout when you close the application.
4. Select **Block Navigation** to allow viewing the document without the ability to browse through the document.

5. Select an option from the **Display Mode** list. You can select any of the following options to view or hide the documents in the application.

   - **Not Set**: This is the default value.
   - **Hide Application List**: To hide the list of applications.
   - **Hide Logout Button**: To hide the logout button.
   - **DocumentView Page: Hide Document/Page Menus**: To hide the document and page menus.
   - **Document View Page: Hide Document Operations**: To hide the document operations.
   - **Hide Logout, Application List and Document Operations**: To hide the logout button, list of applications and the document operations.

6. Provide **Custom Error Page** details.
7. Select**Error Pass Thru** to enable the errors to pass through.
8. Provide your details in the **User** and **Password** fields and click **GENERATE** to generate your **Credentials**.

   - **Domain**: The domain for the user account.
   - **User**: The user name used to log in to AppEnhancer web access.
   - **Password**: The password to log in to the user account.

9. Provide **Data Source** details. The data source will act as the domain for web access user account.
10. Add an **Application Name**.

    Note: If you do not provide an application name, all the available applications are displayed.

11. Click **Compile**.

    The **Path** is auto populated in the **Target URL**.

    Tip: You must generate the credentials and then compile and launch the path every time you make any changes in the configuration.

12. Select **Encrypt Parameters** to allow encryption of the parameters you configure.
13. Click **Launch** to generate encrypted URLs with the specified configurations.

    After configuring and generating the URLs, you can test them directly from TestLaunch to ensure they work as expected.

ISubmitQuery

Parameter	Description

Query Type	Select any one of the options from the list: • **Saved Query**: To display the name of the saved queries. • **Normal Query**: To display all the queries.
Saved Query	Name of the saved query. This field is applicable only if you select **Saved Query** as the query type.
Save and Run	To save and run a query multiple times.
View Mode	Select any one of the options from the list: • **Not Set**: To not display any results or criteria for a query. • **Query Criteria**: To display details on the query criteria. You can make modifications to the query. • **ResultSet**: To display the query results.
Search All Revisions	Searches and displays all the revision results of the query.
Public Query	Select this option to enable public query display.
Update Fields	Select any one of the options from the list: • **Available Fields Only**: Only the available fields are displayed. The hidden fields will not be displayed. • **All Fields**: This is the default value. All the hidden and enabled fields are displayed.
Fulltext Query	Provide a name to enable fulltext query.
Fulltext Query Type	Select any one of the options from the list: • **AND** • **OR** • **EXACT** • **EXPRESSION**
Fulltext Operation	Select any one of the options from the list: • **AND** • **OR**
Field Value Criteria	**Field Name**: Name of the field. • **ADD**: To add new field names with values. • **DELETE ALL**: To delete all the existing field names with their values. **Field Value**: Value for the field name.

IDocument

Parameter	Description
Document ID	The identifier of a document in an application.
Page Number	A specific page number of the document.

IDocImport

Parameter	Description
Allow Editing Index	To allow editing of the index.
Field Name	Name of the field. • **ADD**: To add new field names with values. • **DELETE ALL**: To delete all the existing field names with their values.
Field Value	A value for the field name.

7.13 Configuring Core Signature in AppEnhancer Administrator

To set the Core Signature properties, go to **Server Management** > **Core Signature** > <*CoreSignatureServiceName*>. On the **Configuration** page, the following Core Signature properties are shown:

- **Subscription Name** indicates the name of your Core Signature subscription, which is retrieved from your OT2 Core Signature subscription. To change the subscription used, you must sign in to the OT2 AdminCenter and select the Core Signature subscription.
- **Login URL** specifies the address of the OT2 sign in page. The default location is:

  https://sign.core.opentext.com/#/?auth_provider=opentext_ot2
- **Authentication URL** specifies the address of the OTDS website. Construct the URL of the OTDS web interface, using the **Tenant ID** that is displayed on the **Tenant details** screen, as follows:

  https://otdsauth.ot2.opentext.com/otdstenant/<*tenantId*>/oauth2/token
- **Client ID** and **Client Secret** are required for the API service. Use the **API service credentials** page to create the client ID and secret pair. Furthermore, in AppEnhancer AdminCenter, you must set the **Grant Type** for the client ID and secret to password.
- **Event URL** indicates the external AppEnhancer website to use if you want to save signed documents as AppEnhancer Batch or Append to Document or create a revision of the document. This field is optional.
- **AE User Name** and **Password** credentials are used when events are received. The designated account is audited as the creator of Batches or the user that created a document revision.

- **Core Signature User Name** and **Password** credentials allow AppEnhancer users to share a single Core Signature for the Template source and document signing account. AppEnhancer users can override this account in the **Web User Profile** settings at any time.

7.14 Complete Port list

Consult the following table for a complete list of the default Port numbers used by the product.

Component	Default Port
AppEnhancer Web Access	80/443
AppEnhancer Web Administrator	80/443
AppEnhancer Web Service	80/443
AppEnhancer REST Services	80/443
AppEnhancer License Server	9251 for current users and 27000 for EMC ELM/AX License server 2010
AppEnhancer Render Server	8527
AX Render Server / WxRenderService	8523
AX AppWorks	8855
AX full-text Server	9300
WIM (Workflow Integration Module)	9275/9285
EDB (Event Dispatch Broker)	9276
Microsoft SQL Server	1433
MySQL	3306
Oracle	1521
ADFS	1505
PixTools for Web (HTTP)	49732, 49733, and 49734
PixTools for Web (HTTPS)	49735, 49736, and 49737
File storage	Dependent on storage device

Note: All ports must be opened from the client side.

Chapter 8

Reporting

8.1 Audit Report

You can use AppEnhancer audit information to generate reports that provide detailed information about event types. To specify criteria and generate an audit report, perform the following:

1. Ensure that the audit trail in the data source is enabled.
2. Navigate to the **Reporting** > **<***your data source***>** > **Audit Report** node in AppEnhancer Administrator.
3. Select an active data source from the **Data Source** list box.
4. Type the query criteria and then click **GENERATE REPORT**. The query result appears.
5. Click **EXPORT REPORT** to export a report in CSV format.

8.2 User Effective Permission Report

The effective permission report shows the user permissions that are compiled from user profiles and group membership profiles. To generate a user effective permission report, perform the following steps:

1. Navigate to the **Reporting** > **<***your data source***>** > **User Effective Permission Report** node in AppEnhancer Administrator.
2. Perform either of the following:
   - To view all the existing users, click **SEARCH**.
   - To search for a specific user, type the name of the user in the **Search for Users** field and click **SEARCH**. Click the user name. A report that shows the selected user's effective permissions appears.
3. Click **EXPORT REPORT** to export this report in CSV format.

8.3 User Configured Permission Report

The user configured permission report shows the configured permissions for each user. To generate a user configured permission report, perform the following steps:

1. Navigate to the **Reporting** > **<***your data source***>** > **User Configured Permission Report** node in AppEnhancer Administrator.
2. Perform either of the following:
   - To view all the existing users, click **SEARCH**.
   - To search for a specific user, type the name of the user in the **Search for Users** field and click **SEARCH**. Click the user name. A report that shows the selected user's configured permissions appears.
3. Click **EXPORT REPORT** to export this report in CSV format.

8.4 User's Group Report

The user's group report shows information about the user's group membership. To generate a user's group report, perform the following steps:

1. Navigate to the **Reporting** > **<***your data source***>** > **User's Group Report** node in AppEnhancer Administrator.
2. Perform either of the following:
   - To view all the existing users, click **SEARCH**.
   - To search for a specific user, type the name of the user in the **Search for Users** field and click **SEARCH**. Click the user name. A report that shows the selected user's group membership appears.
3. Click **EXPORT REPORT** to export this report in CSV format.

8.5 Group Configured Permission Report

The group configured permission report shows the configured permissions for each group. To generate a group configured permission report, perform the following steps:

1. Navigate to the **Reporting** > **<***your data source***>** > **Group Configured Permission Report** node in AppEnhancer Administrator.
2. Perform either of the following:
   - To view all the existing groups, click **SEARCH**.
   - To search for a specific group, type the name of the group in the search field and click **SEARCH**. Click the group name. A report that shows the selected group's permissions appears.

3. Click **EXPORT REPORT** to export this report in CSV format.

8.6 Group's User Report

The group's user report shows the list of users in a group. To generate a group's user report, perform the following steps:

1. Navigate to the **Reporting** > **<***your data source***>** > **Group's User Report** node in AppEnhancer Administrator.
2. Perform either of the following:
   - To view all the existing groups, click **SEARCH**.
   - To search for a specific group, type the name of the group in the search field and click **SEARCH**.
3. Click **EXPORT REPORT** to export this report in CSV format.

8.7 DLS Report

Navigate to the **Reporting** > **<***your data source***>** > **DLS Report** node in AppEnhancer Administrator. Click the type of DLS report that you would like to generate for the data source. You will be prompted to download the report as a .csv file.

8.8 Roles Report

The Roles Report provides data about the users in each role for each data source.

Navigate to the **Reporting** > **<***your data source***>** > **Roles Report** node in AppEnhancer Administrator. To export the report, click **Export Report**.

Chapter 9

Monitoring

You can use a variety of utilities, such as AppEnhancer Administrator and Windows Management Instrumentation (WMI), to monitor AppEnhancer Servers. WMI is a component of the Microsoft Windows operating system. Additional utilities are available for monitoring the AppEnhancer Web Access Server and AppEnhancer Indexing Service.

You can use AppEnhancer Administrator to check that AppEnhancer content management components have been correctly registered for the data group being managed through that AppEnhancer Administrator installation. You can also monitor performance on the servers (AppEnhancer Rendering Server, Web Access Server, and Indexing Service) through AppEnhancer Administrator.

You can use Windows Management Instrumentation (WMI) to monitor performance on the servers. For example, if you have a large number of rendering sessions to monitor, you might find it more practical to access this log data through WMI. By using a custom application or script, you can use this data to automate your restart, recovery, and maintenance tasks. WMI is a component of the Microsoft Windows operating system.

Also, you can configure **Audit Trail** to track system-wide activities.

Note: You must allow the WMI-related Windows firewall exception to monitor server activities on remote servers:

1. Open the Local Group Policy Editor.
2. Navigate to **Computer Configuration > Administrative Templates > Network > Network Connections > Windows Firewall**.
3. Open the Domain Profile if servers that need to be monitored are in the same domain (otherwise Standard Profile).
4. Enable **Windows Firewall: Allow inbound remote administration exception**.

9.1 Viewing registered components

Navigate to the **Monitoring > Registered Components** node in AppEnhancer Administrator to view detailed information about running components.

Note: To display Indexing Service details in the **Registered Components** page, perform the following:

- Navigate to the **Monitoring** > **Indexing Service** node in AppEnhancer Administrator, in **Select component**, type the workstation name or IP address of the Indexing Service server and click **REFRESH**.

If necessary, you can unregister a selected component. If you unregister a component, the data source group no longer uses that component, even if it is still installed and running. To register a component that has been unregistered, you must run the Component Registration Wizard for that component again on the workstation where the component is installed.

9.2 Viewing running components

Navigate to the **Monitoring** > **Running Components** node in AppEnhancer Administrator to view detailed information about running components.

9.3 Viewing Indexing Service activities

To view detailed information related to the operation of an Indexing Service, navigate to the **Monitoring** > **Indexing Service** node and select the component.

The following table describes the options available on the page:

Field	Description
Indexing Service	Name of the AppEnhancer Indexing Service.
DocsIndexed	Number of documents successfully indexed.
DocsIndexFailed	Number of document indexing attempts that failed.
DocsOCRed	Number of documents successfully OCR processed.
DocsOCRFailed	Number of document OCR attempts that failed.
DocsResumitted	Number of resubmitted documents successfully indexed.
LocalConfig	Whether Indexing Service uses a local configuration

9.4 Managing Rendering Server activities

Navigate to the **Monitoring > Rendering Server** node in AppEnhancer Administrator and select a component to view the current activity on the AppEnhancer Rendering Server.

Configure the options as described in the following table and click **SAVE**:

Field	Description
WxRS: <Workstation Name>	
ConfigurationTimestamp	Time of last configuration.
CurrentConversions	Number of current file conversions. Real time rendering is not included.
DiskFullPercent	Full percentage of cache disk.
LastGCCount	Count of last garbage collection. Real time rendering is not included.
LastGCSizeMB	Size of last garbage collection in megabytes. Real time rendering is not included.
LastGCTime	Time of last garbage collection. Real time rendering is not included.
ServerStatus	Current status of AppEnhancer Rendering Server (for example, running, suspended, stopped)
StartTime	Time AppEnhancer Rendering Server was last started.
StopTime	Time AppEnhancer Rendering Server was last stopped.
TotalEntries	Total number of rendered items. Real time rendering is not included.
TotalForeignFiles	Total number of rendered foreign files. Real time rendering is not included.
TotalImageFiles	Total number of rendered images. Real time rendering is not included.
TotalJobs	Total number of rendered jobs.
TotalPDFFiles	Total number of rendered PDF files. Real time rendering is not included.
TotalSize	Total size in megabytes. Real time rendering is not included.
TotalThumbnails	Total number of rendered thumbnails.
TotalXPSFiles	Total number of rendered XPS files.
UpdateTime	Time of last update.

Field	Description
WorkstationName	Name of workstation.
WxRSC: <Workstation Name>	
ClearCacheRequest	When set to 1, the cache clears.
GarbageCollectionEnabled	When set to 1, garbage collection will run.
GarbageCollectionFileSetSize	Current file size set for garbage collection.
GarbageCollectionFrequency	Frequency of garbage collection in seconds.
GarbageCollectionReductionPercent	Current garbage collection reduction percentage.
LoggingEnabled	When set to 1, the AppEnhancer Rendering Server logs data to disk.
MaximumCacheEntries	Maximum number of cache entries.
MaximumCacheKilobytes	Maximum cache size in kilobytes.
QueuePollingInterval	Interval for polling queues in milliseconds.
WorkstationName	Name of workstation.

You can also start, stop, or refresh the AppEnhancer Rendering Server service.

9.5 Managing Web Access Server activities

Navigate to the **Monitoring > Web Access Server** node in AppEnhancer Administrator and select the component to view information related to the operation of an AppEnhancer Web Access Server.

The following table describes the options:

Field	Description
Anonymous Requests	Number of requests utilizing anonymous authentication.
Anonymous Requests/Sec	Number of requests per second utilizing anonymous authentication.
Cache Total Entries	Total number of entries within the cache (both internal and user added).
Cache Total Turnover Rate	Number of additions to and removals from the total cache per second.
Cache Total Hits	Total number of hits from the cache.
Cache Total Misses	Total number of cache misses.
Cache Total Hit Ratio	Ratio of hits from all cache calls.
Cache Total Hit Ratio Base	Cache Total Hit Ratio Base.

Field	Description
Cache API Entries	Total number of entries within the cache added by the user.
Cache API Turnover Rate	Number of additions and removals to the API cache per second.
Cache API Hits	Number of hits from user code.
Cache API Misses	Number of cache misses called from user code.
Cache API Hit Ratio	Ratio of hits called from user code.
Cache API Hit Ratio Base	Cache API Hit Ratio Base.
Output Cache Entries	Current number of entries in the output cache.
Output Cache Turnover Rate	Number of additions to and removals from the output cache per second.
Output Cache Hits	Total number of output cacheable requests served from the output cache.
Output Cache Misses	Total number of output cacheable requests not served from the output cache.
Output Cache Hit Ratio	Ratio of hits to requests for output cacheable requests.
Output Cache Hit Ratio Base	Output Cache Hit Ratio Base.
Compilations Total	Number of .asax, .ascx, .ashx, .asmx, or .aspx source files dynamically compiled.
Debugging Requests	Number of debugging requests processed.
Errors During Preprocessing	Number of errors that have occurred during parsing and configuration.
Errors During Compilation	Number of errors that have occurred during compilation.
Errors During Execution	Number of errors that have occurred during the processing of a request.
Errors Unhandled During Execution	Number of errors not handled by user code, but by the default error handler.
Errors Unhandled During Execution/Sec	Rate of unhandled errors.
Errors Total	Total number of errors that occurred.
Errors Total/Sec	Rate of error occurrence.
Pipeline Instance Count	Number of active pipeline instances.
Request Bytes In Total	Total size, in bytes, of all requests.

Field	Description
Request Bytes Out Total	Total size, in bytes, of responses sent to a client. This does not include standard HTTP response headers.
Requests Executing	Number of requests currently executing.
Requests Failed	Total number of failed requests.
Requests Not Found	Number of requests for resources that were not found.
Requests Not Authorized	Number of requests failed due to unauthorized access.
Requests In Application Queue	Number of request in the application request queue.
Requests Timed Out	Number of requests that timed out.
Requests Succeeded	Number of requests that executed successfully.
Requests Total	Total number of requests since the application was started.
Requests/Sec	Number of requests executed per second.
Sessions Active	Number of sessions currently active.
Sessions Abandoned	Number of sessions that have been explicitly abandoned.
Sessions Timed Out	Number of sessions timed out.
Sessions Total	Total number of sessions since the application was started.
Transactions Aborted	Number of transactions aborted.
Transactions Committed	Number of transactions committed.
Transactions Pending	Number of transactions in progress.
Transactions Total	Total number of transactions since the application was started.
Transactions/Sec	Transactions started per second.
Session State Server connections total	Total number of connections to the State Server used by session state.
Session SQL Server connections total	Number of connections to the SQL Server used by session state.
Events Raised	Number of events raised.
Events Raised/sec	Number of events raised per second.
Application Lifetime events	Application Lifetime events.
Application Lifetime events/Sec	Application Lifetime events per second.

Field	Description
Error Events Raised	Number of error events raised.
Error Events Raised/Sec	Number of error events raised per second.
Request Error Events Raised	Number of requests for error events raised.
Request Error Events Raised/Sec	Number of requests for error events raised per second.
Infrastructure Error Events Raised	Infrastructure error events raised.
Infrastructure Error Events Raised/Sec	Infrastructure error events raised per second.
Request Events Raised	Number of request for events raised.
Request Events Raised/Sec	Number of request for events raised per second.
Audit Success Events Raised	Audit success events raised.
Audit Failure Events Raised	Audit failure events raised.
Membership Authentication Success	Membership authentication success.
Membership Authentication Failure	Membership authentication failure.
Forms Authentication Success	Forms authentication success.
Forms Authentication Failure	Forms authentication failure.
Viewstate MAC Validation Failure	Viewstate MAC validation failure.
Request Execution Time	Request execution time.
Requests Disconnected	Number of requests that were disconnected.
Requests Rejected	Number of requests that were rejected.
Request Wait Time	Request wait time.
Cache % Machine Memory Limit Used	Cache percentage machine memory limit used.
Cache % Machine Memory Limit Used Base	Cache percentage machine memory limit used base.
Cache % Process Memory Limit Used	Cache percentage process memory limit used.
Cache % Process Memory Limit Used Base	Cache percentage process memory limit used base.
Cache Total Trims	Cache total trims.
Cache API Trims	Cache API trims.
Output Cache Trims	Output cache trims.
% Managed Processor Time (estimated)	Percentage of managed processor time (estimated).
% Managed Processor Time Base (estimated)	Percentage of managed processor time base (estimated).

Field	Description
Managed Memory Used (estimated)	Managed memory used (estimated).
Request Bytes In Total (WebSockets)	Number of request bytes in total (WebSockets).
Request Bytes Out Total (WebSockets)	Number of request bytes out total (WebSockets).
Requests Executing (WebSockets)	Number of requests executed (WebSockets).
Requests Failed (WebSockets)	Number of requests failed (WebSockets).
Requests Succeeded (WebSockets)	Number of requests succeeded (WebSockets).
Requests Total (WebSockets)	Number of total requests (WebSockets).

9.6 Viewing license pool

Navigate to the **Monitoring > License Pool** node in AppEnhancer Administrator.

You can manage and view detailed information about the license pool. You can also release an idle license and export the license information.

9.7 Managing locked documents

Navigate to the **Monitoring > Locked Documents** node in AppEnhancer Administrator. In the **Locked Document** page, select an active data source from the **Data Source** list box. The **Locked Document** page enables you to manage and to view detailed information about all locked documents.

If necessary, you can release selected locked documents or all locked documents to unlock them.

9.8 Managing locked applications

Navigate to the **Monitoring** > **Locked Applications** node in AppEnhancer Administrator. Select the application that you want to unlock and click **UNLOCK**.

9.9 Managing checked out documents

Navigate to the **Monitoring > Checked Out Documents** node in AppEnhancer Administrator. In the **Checked Out Document** page, select an active data source from the **Data Source** list box. The **Checked Out Document** page enables you to manage and to view detailed information about all checked out documents.

If necessary, you can select the checked out document(s) and perform the cancel check out operation.

9.10 Managing queues

Navigate to the **Monitoring > Queues** node in AppEnhancer Administrator. In the **Queues** page, select an active data source from the **Data Source** list box and a job queue from the **Select Queue** list box. The **Queues** page enables you to manage and to view detailed information about AppEnhancer Web Access full-text and OCR jobs.

Double-click the job to view the information about the elements.

If necessary, you can resubmit or delete selected jobs or all jobs.

9.11 Managing sessions

Navigate to the **Monitoring > Sessions** node in AppEnhancer Administrator. In the **Sessions** page, select an active data source from the **Data Source** list box. The **Sessions** page enables you to manage and to view detailed information about the current AppEnhancer Web Access sessions.

If necessary, you can terminate selected user sessions or all user sessions.

9.12 Managing PID Table

The AE_PID table in the AppEnhancer database stores information that relates to the currently active login sessions on the AppEnhancer system and their states.

Navigate to the **Monitoring > PID Table** node in AppEnhancer Administrator to view the PID table. In the **PID Table** page, select an active data source from the **Data Source** list box. The **PID Table** page enables you to manage and to view detailed information that relates to the currently active login sessions.

If necessary, you can delete selected user login sessions from the PID table.

9.13 Viewing system ID usage

To view system id usage information, navigate to the **Monitoring** > **System Id Usage** node in AppEnhancer Administrator. In the **Data Source** drop-down menu, select the data source that you would like to monitor.

9.14 Viewing application usage

To view application usage information, navigate to the **Monitoring** > **Application Usage** node in AppEnhancer Administrator. In the **Data Source** drop-down menu, select the data source that you would like to monitor.

You can also export the application usage data by clicking the **Export Usage** button. The data is exported as a .tsv file.

9.15 Viewing system path entries

To view system path entries information, navigate to the **Monitoring** > **System Path Entries** node in AppEnhancer Administrator. In the **Data Source** drop-down menu, select the data source that you would like to monitor.

9.16 Managing administrative services jobs

The Archive Service, AutoIndex KeyRef Service, Migration Service, Index Image Import Service, and Indexing Service are subcomponents of Administrative Services.

To manage any of the Administrative Services jobs, navigate to the **Monitoring** > **Administrative Services Jobs** node. You can filter the jobs by service using the **Select Service Type** list. To view a job's details, double-click a job.

The following table describes the available options:

Option	Description
Cancel	To cancel a job, select a running or pending job and click **Cancel**.
Re-Submit	To restart a partially-completed or cancelled job, or a job that failed to complete, select the job and click **Re-Submit**. The job status is changed to Pending.
Download Log File	To view log files, select a completed or cancelled job and click **Download Log File**.

Note: Management of the Indexing Service can only be performed on the **Monitoring** > **Queues Jobs** node.

Chapter 10

Tools

This chapter describes AppEnhancer Import Utility.

10.1 AppEnhancer Import Utility

This section contains information about the AppEnhancer Import Utility.

10.1.1 Overview of AppEnhancer Import Utility

Storing and indexing documents individually in AppEnhancer is quick and efficient when you need to add only a few documents at a time. However, when you are storing and indexing hundreds or thousands of documents, typing index information for each document is not an efficient means of data entry. For this reason, AppEnhancer provides an import utility to enable users to add documents more efficiently.

The import features offered by AppEnhancer enable entering and updating data. Two of these features, the AppEnhancer Auto Index Import and the AppEnhancer Key Reference Import, enable you to build a data entry table by importing index information from a text file. After the table has been built, users can index documents by accessing index records from the table. The third feature, AppEnhancer Index Image Import, enables users to import index data and document files in a single step.

To use the AppEnhancer Import Utility, follow these steps:

1. Familiarize yourself with the three import features.
2. Create an import file.
3. If you will be importing data for all fields in an application, in the order and format that they occur in the application, you can use one of the default import specifications. However, you must create or configure a custom import specification if you want to do any of the following:

   - Include a subset of the fields
   - Change the field order
   - Change any of the field formats

   For instructions about creating and managing custom import specifications, see "Creating and managing import specifications" on page 65.
4. Run AppEnhancer Import Utility. For instructions about using the AppEnhancer Import Utility, see "Using AppEnhancer Import Utility" on page 152.

The following table briefly describes each import feature:

Import feature	Brief description
Auto Index Import	Auto Index Import enables you to import index values from a text file, so users adding documents can automatically populate indexes by using the imported data. Auto Index is ideal for the import of index records that are applicable to only one document. In an Auto Index Import table, after a record (or a group of index values) has been used to index a document, the record is deleted (by default).
Key Reference Import	Key Reference Import enables you to use the [TAB] key to import index values from a text file. Key Reference is most effective in situations where each imported record may be used to describe several documents. Key Reference Import maintains the index records in the Key Reference table even after records have been used to index documents. Any change made to a record in the Key Reference table is reflected in the indexes of all documents described by that record.
Index Image Import	Index Image Import enables you to import index data and document files in a single step. A text file is created, which contains a line of text for each document to be imported, with a value for each index field and a reference to the location of the file to be imported. You can import all index information and documents by using AppEnhancer Import Utility. No manual document indexing is required.

The system administrator can import index data (or index data and documents) by using these features through AppEnhancer Import Utility. In most cases, the information in the import file matches the index field order and data format of the AppEnhancer application. In those cases, a default specification can be used to import the data. If you can use a default specification, you do not need to create a custom import specification.

There are certain circumstances, however, where changing the rules used to import data can either make an otherwise impossible import possible or remove the need to reformat import files. Customizing an import specification enables you to perform the following tasks (which cannot be performed by using the default specification):

- Import data for fields in a different order than the order of fields in the AppEnhancer application (while importing the correct data into the correct field).
- Import information into selected fields only in an application.

- Reformat data that is of the correct data type but in a different data format from what the application requires. For example, dates can be formatted mm-dd-yy in the import file, but imported into an AppEnhancer date field formatted dd-mm-yy because the customized rules enables AppEnhancer to reformat the dates to fit the field format during the import.

10.1.1.1 Auto Index Import

The first step in performing an AppEnhancer Auto Index Import is to import a file that contains index data into an Auto Index table (AE_AI#) in AppEnhancer. To import data into a field by using AppEnhancer Import Utility, the Auto Index field flag must be enabled for that field. Field flags can be enabled during application creation, or later by modifying an application.

After an Auto Index table has been created, the user can enter data into any one of Auto Index enabled fields of document during indexing and press [F7]. If the data is unique, AppEnhancer extracts the matching record from the Auto Index table and populates the rest of the index of document with the values in the record. If more than one record matches the contents of the Auto Index field, AppEnhancer displays a result set. When the user chooses an entry from the result set, the fields in the index are automatically populated with the appropriate data. After an index is used, by default, it is deleted from the Auto Index table and cannot be reused. This prevents use of the same index information for two different documents, and enables the user to track unindexed records.

Notes

- The Auto Index or Key Reference status of a field can be changed to enabled or disabled, but the entire application must then be rebuilt. This can be very time-consuming on large databases. Also, if the Auto Index or Key Reference status of a field is disabled, any corresponding import tables are permanently removed from AppEnhancer.
- If an Auto Index table is used to enter a value into an index field, even if that field is flagged for dual data entry, the user is not prompted to enter data for the second time.

To complete the import successfully, the import file must be formatted correctly. The data for insertion in index fields must be formatted and ordered to correspond exactly to the fields as defined and ordered in the AppEnhancer application. For example, one line that references an image file, could read as follows:

```
123121234,JOHN DOE,092964
```

In this example, the social security number, name, and birth date make up the record in the import file. During import, each record listed in the import file is added to the Auto Index table.

10.1.1.2 Key Reference Import

The first step in performing an AppEnhancer Key Reference Import is to import a file containing index data into a Key Reference table (AE_RF#) in AppEnhancer. The data in the table is used to automatically populate AppEnhancer index fields. When a user performs Key Reference Import, the first step is to import a file containing index data into a Key Reference table in AppEnhancer.

To import data into a set of fields by using the AppEnhancer Import Utility, the Key Reference field flag must be enabled for one of those fields and the Data Reference field flag must be enabled for the remaining fields. Field flags can be enabled during application creation, or later, by modifying the application. When configuring an index of application for AppEnhancer Key Reference Import, mark one field as a Key Reference field and other fields as Data Reference fields.

After a Key Reference table has been created, the user can enter data into the key field of an index of document during document creation and press **Tab**. AppEnhancer automatically fills in the fields marked as data fields with the values from the record in the Key Reference table with that key field value. The data fields are populated based on the value entered in the key field. AppEnhancer uses the key field value to find the appropriate data values. After a record in the Key Reference table is used to describe a document, the record is maintained in that table (unlike Auto Index, where the record is deleted). The same record can be used to fill in all or part of the index information for several documents. Whenever index information for a data field that is stored in the Key Reference table is modified, the index information is modified for all documents with that key field. When the information in a key field is modified, AppEnhancer changes the information for only that document.

The Key Reference Import is useful when the same information must be entered for several documents, if that information is the same for all of the documents. For example, a corporation sets up an application where several documents are stored that relate to each of the employees at the corporation. The key field for the application is the social security number of the employee (which is unlikely to change), and the name of employee is specified as a data field. If the name of employee changes, the modification to the name field can be done only for one document, and that change will be reflected in the index record for every document that relates to that employee.

To perform the import successfully, the import file must be formatted correctly. The data for insertion in index fields must be formatted and ordered to correspond exactly to the fields as defined and ordered in the AppEnhancer application. For example, one line that references an image file could read as follows:

```
123121234,JOHN DOE,092964
```

In this example, the social security number, name, and birth date make up the record in the import file. During import, each record listed in the import file is added to the Key Reference table.

10.1.1.3 Index Image Import

The Index Image Import feature functions as a conversion tool. If images are located in another system, you can easily import them into AppEnhancer, along with the corresponding index data. When a user uses the Auto Index Import and Key Reference Import features, the user still adds each document manually, and then accesses imported data to help populate the index of document. In Index Image Import, however, the import feature performs the document addition automatically. The user sets up a file where lines contain the information for the document index and a reference to the storage location of the file to be added as a document. AppEnhancer then imports each document and attaches the associated index information to it in a process that is transparent to the user who is performing the import.

After the data is formatted correctly in the import file, the AppEnhancer Import Utility can be used to import the records into the designated AppEnhancer application. All of the index information for each document is populated during the import; no data entry is required.

Notes

- You can use double quotes (") in the import file to denote a literal string in cases where special characters would interfere with the import of the index value and image. The AppEnhancer Import Utility removes the quotes when it saves the index value. For example, "H44555@1" in the import file is saved as index value H44555@1. If you want the double quotes to be saved as part of the index value (for example, "H44555@1"), enclose the value in two sets of double quotes (for example, ""H44555@1"").
- When Index Image Import is processed in an application with Key Reference enabled fields, the index information in the Key Reference table is also updated.

To perform the import successfully, the import file must be formatted correctly. One or two @ symbols must immediately precede a file name and path. The following table lists the file types that can be preceded by one @ symbol and the file types that must be preceded by two @@ symbols:

Can use one @ symbol	Must use two @@ symbols
• AppEnhancer single-page image types • PDF • Basic Windows RTF • HTM	• Foreign files • Multipage image files • Text files (require a file type mapping)

Note: If you import a multipage PDF file, the result in AppEnhancer is a single page with multiple subpages. If necessary, you can convert these subpages to pages.

When AppEnhancer processes an import file with file names preceded by two @@ symbols, AppEnhancer identifies the file type mappings and image storage format

settings for those file names. The following table explains the trade-off between using one @ symbol or two @@ symbols:

For this scenario	Do this	Result
All of the files listed in the import file are of a format that is natively supported by AppEnhancer.	Precede each file name and path with only one @ symbol.	AppEnhancer imports the file without checking the file type. Each file must be a natively supported file format.
Some of the files listed in the import file are of a format that is natively supported by AppEnhancer and some are not, and you do not have time to edit the import file.	Precede each file name and path with two @@ symbols.	AppEnhancer checks the file type and treats the file as the detected type (such as image, text, or foreign file format). The number of files that AppEnhancer must check increases the import time.
Some of the files listed in the import file are of a format that is natively supported by AppEnhancer and some are not, and you do have time to edit the import file.	For each supported file, precede the file name and path with only one @ symbol. For each unsupported file, precede the file name and path with two @@ symbols.	If one @ precedes the file name and path, AppEnhancer imports the file without checking the file type. If two @@ signs precede the file name and path, AppEnhancer checks the file type and treats the file as the detected type.
None of the files listed in the import file is of a format that is natively supported by AppEnhancer.	Precede each file name and path with two @@ symbols.	AppEnhancer checks the file type and treats the file as the detected type (in this case, foreign file format).

The file name should appear immediately after the index fields. The data for insertion in index fields must be formatted and ordered to correspond exactly to the fields as defined and ordered in the AppEnhancer application. For example, one line that references an image file could read as follows:

```
123121234,JOHN DOE,092964@c:\windows\cars.bmp
```

The social security number, name, and birth date make up the first part of the record in the import file, and the `CARS.BMP` image is attached to that record. Both the index data and the image are imported as a document in AppEnhancer. The following is an example of a line that references a text file:

```
123121234,JOHN DOE,092964@@c:\windows\cars.txt
```

In this example, again the social security number, name, and birth date on the record are taken from the first three entries in the line, but here, the `CARS.TXT` text file is attached to the index. The same format is used to import a file of foreign file format.

10.1.1.3.1 Format for import referencing a volume label

A volume label can be used as the root of the file path in place of a drive letter, to enable batch index input from multiple pieces of media. If, for example, the images to be stored in AppEnhancer are located on several different optical disks, each of those disks can be referenced in the import file by the volume label on the disk. As references to different volume labels are found during the import, you will be instructed to insert the correct media. Volume labels can be referenced by placing the name of the volume with a dollar sign in front, where the drive letter would usually be:`$<VOLUME_NAME>` . The following is an example of a line that includes the volume label VOLUME_01:

```
123121234,JOHN DOE,092964@$VOLUME_01\images\castle.bmp
```

10.1.1.3.2 Format for import of multiple page documents

To import multiple page documents, add a new line after the index record for every page to import. It is not necessary to repeat the index field names. Subsequent lines must contain the @ symbol and the image name and location:

```
123121234,JOHN DOE,092964@c:\windows\cars.bmp
@@c:\windows\squares.txt
@$VOLUME_01\images\castle.bmp
```

The following format is also acceptable:

```
123121234,JOHN DOE,092964
@c:\windows\cars.bmp
@@c:\windows\squares.txt
@$VOLUME_01\images\castle.bmp
```

10.1.1.3.3 Importing multiple pages with a single command

You can use the asterisk (*) wildcard character to import several files from a single location. Rather than entering a line in the import file for each file in the directory, you can reference files with similar names with one command. Use the asterisk to replace some or all of the letters, and AppEnhancer will import all of the files in the referenced directory whose names contain the remaining pattern of letters. If, for example, the filenames for all of the financial reports in the directory "C:\FINANCE \" begin with the word "REPORT," placing the line "`C:\FINANCE\REPORT*.*`" in the import file will import all of those files. All files in a particular directory can be imported with one command by entering "`*.*`" in place of the filename. The following are examples of the use of the wildcard character in an Index Image Import file:

```
123121234,JOHN DOE,092964
@c:\windows\cars.bmp
@@c:\windows\squares.txt
@$VOLUME_01\images\castle*.bmp
@c:\images\*.bmp
@c:\images\new\*.*
```

The first two lines each import a single page. The third line imports all bitmap files with the prefix "castle" in the images directory on the disk labeled Volume_01 as pages. The fourth line imports all bitmap files in the C:\IMAGES directory. The fifth line imports all files in the C:\IMAGES\NEW directory.

10.1.1.3.4 Entering the @ Symbol on a French keyboard

The at (@) symbol is a crucial component of an index image import file, but this symbol can be difficult to find on a French keyboard.

To type the at (@) symbol using a French keyboard, type <Ctrl>+<Alt>+0 (the number zero key).

10.1.2 Using AppEnhancer Import Utility

AppEnhancer Import Utility can only be used at the command line. A command line import can be performed from a DOS prompt or batch file.

Using AppEnhancer Import Utility, you can import Auto Index, Key Reference and Index Image. Following each run of the utility, a job ID is provided that can be used to verify the job status from AppEnhancer Administrator.

Before you can run AppEnhancer Import Utility, you must:

- Update the configuration file. For more information, see "Updating the configuration file" on page 152.
- Create an import file and, if necessary, configure an import specification.

To run an import command, at the DOS command prompt, type the import command and click **OK**.

Updating the configuration file

The configuration file is stored in the folder where AppEnhancer Import Utility is installed. Be default, it is the `c:\Program Files\XtenderSolutions\AppEnhancerImportUtility` folder.

Open `AEImportUtility.dll.config` for editing. The file is similar to the following:

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
<appSettings>
     <!--AppEnhancer Administrator URL - eg: http://localhost/AppEnhancerAdmin-->
     <add key="AdminURL" value="<AdminURL>" />
     <!--AppEnhancer Default Datasource.eg:AppEnhancerDEMO-->
     <add key="DefaultDS" value="<DefaultDS>" />
</appSettings>
</configuration>
```

You must update these values:

- *<AdminURL>* is the AppEnhancer Administrator URL
- *<DefaultDS>* is the Datasource name so that users do not need to provide this with command line parameters. You can also import into a different Datasource by using optional import parameters.

10.1.2.1 Index Image Import command

Use the following syntax when performing an Index Image Import:

```
"c:\Program Files\XtenderSolutions\AppEnhancerImportUtility\AEImportUtility.exe /RT
INDEXIMAGE" <switches>
```

In the preceding command, `C:\Program Files\XtenderSolutions\AppEnhancerImportUtility\` is the directory in which AppEnhancer Import Utility has been installed and *<switches>* are a series of command line switches.

10.1.2.1.1 Required Index Image Import switches

The following table describes the required command line switches:

Option	Description
`/U` *<UserName>*	Specifies the user name.
`/W` *<Password>*	Specifies the password.
`/A` *<ApplicationName>*	Specifies the application name.
`/S "`*<SpecificationName>*`"`	Specifies the specification name. The specification name must be enclosed in double quotes. By default, the available specification names are **Fixed Length Records**, **Comma delimited**, **Pipe delimited**, **Tilde delimited**, and **Tab delimited**. Users with permission to create applications can also create custom specification names for use in the application.
`/F` *<PathAndFileName>*	Specifies the path and file name of the import file.

10.1.2.1.2 Optional Index Image Import switches

The following table describes the optional command line switches:

Scenario	Use this switch	Description
If you want to specify a data source other than the default	`/N` *<DataSource>*	AppEnhancer imports documents into the specified data source.
If you want the imported items to be created as new indexes and documents	`/C`	AppEnhancer creates a new index and document for each import item. AppEnhancer does not check for duplicate document indexes.

Scenario	Use this switch	Description
If you want the imported items to be merged with existing documents	`/M`	AppEnhancer checks the specified application for duplicate document indexes. If AppEnhancer finds an existing document with the same index information as an imported item, AppEnhancer adds the item as a new page to that document. AppEnhancer imports any documents with new index information as new documents.
If any of the fields in the application have been flagged as unique keys, and if you want the import wizard to check the values imported into these fields	`/Q`	If you use this switch and the import wizard discovers multiple documents listed in the import file with the same values in the unique key fields, the import wizard imports the first document and rejects all remaining redundant documents.
If you want the import wizard to stop processing after a certain number of consecutive errors	`/E <MaxErrors>`	Specify the highest number of consecutive errors that you want the import wizard to accept.
If you want to omit from the import a record or a group of records at the beginning of the import file	`/K <SkipNumber>`	Specify the number of lines that you want AppEnhancer to skip when processing the import file.
If you want to omit from the import a record or a group of records at the end of the import file	`/L <LoadNumber>`	Specify the number of lines that you want AppEnhancer to load when processing the import file.

Scenario	Use this switch	Description
If you want to specify the number of records that each database transaction should commit to the database	`/B <BatchSize>`	During the Index Image Import, database transactions commit document records to the database. Specify the number of records that each database transaction should commit to the database. The default value is 100, but you can specify any integer from 1-10,000. **Note:** Do not use /B and /I in the same command. If you use the /I switch, the Batch Size will be set to 1, which means that the import wizard commits each record from the import as a separate database transaction rather than committing multiple document records to the database at the same time.
If you want other users to be able to add documents to the application to which you are importing documents during the import	`/I`	AppEnhancer enables other users to add documents to the application to which you are importing documents during the import. **Note:** If you do not use the /I switch, a wait message appears when you run the import and AppEnhancer waits until it can place a lock on the application before beginning the import.
If you have placed database triggers on the DT and DL tables in your AppEnhancer application	`/J`	AppEnhancer disables the use of database bulk objects.
If you want the imported files to retain their file time after import	`/T`	AppEnhancer retains the file time for imported files.

Scenario	Use this switch	Description
If you want to specify a queue for full-text processing	/Y *<QueueName>*	If the selected queue has been properly configured, the documents imported by the Index Image Import Wizard are processed using the selected queue.
If you want to specify description to the import job	/D "*<Description>*"	Specifies job description. The description must be enclosed in double quotes.
If you want to append files to an already existing document for application that has been flagged as unique Keys	/MQ	If any of the fields in the application have been flagged as unique keys and the import service discovers any files listed in the import file with values in the unique key fields that duplicate the values for a document already in the application, the import service will append all redundant files to that document.
If 'Use bulk objects' is enabled, then you can set the size of the bulk object	/JS *<BulkSize>*	Set the size of the bulk object. The default size is 500.
If the import document is PDF, enable 'Inspect PDF File' to check for any errors. If errors are found, the import process will fail.	/IP	Inspect PDF File - Performs a scan of the PDF file to check for any errors. If errors are found, the import process will fail.
If the import document is PDF enable 'Decrypt PDF File' to automatically decrypt all encrypted files and save as regular PDF	/DP	Decrypt PDF File - When importing PDF files, all encrypted files are automatically decrypted and saved as a regular PDF.
If you want to set PDF Portfolio file settings. By default, it is “No Detect”. The PDF Portfolio must be enclosed in double quotes.	/PP *<PDF Portfolio>*	Set PDF Portfolio file settings. You can choose from **No Detect**, **As Foreign File**, or **Extract Embedded Files**. By default it is **No Detect**. The PDF Portfolio must be enclosed in double quotes.
If you are uncertain about Index Image Import command line usage	/?	A message appears that briefly describes the Index Image Import command-line usage.

10.1.2.1.3 Viewing Index Image import job status

Go to the **Monitoring > Administrative Services Jobs** node in AppEnhancer Administrator. On the **Administrative Service Jobs** page, select **Datasource** and then filter the jobs by service using the **Select Service Type** list as **Import Service**. To view a job's details, double-click a job.

To view log files, select a job and then click **Download Log File**.

10.1.2.2 Key Reference Import command

Use the following syntax when performing a Key Reference Import:

```
"c:\Program Files\XtenderSolutions\AppEnhancerImportUtility\AEImportUtility.exe /RT
KEYREFERENCE" <switches>
```

In the preceding command, `c:\Program Files\XtenderSolutions\AppEnhancerImportUtility\` is the directory in which AppEnhancer Import Utility has been installed and *<switches>* are a series of command line switches.

10.1.2.2.1 Required Key Reference Import switches

The following tables describes the required command line switches:

Option	Description
/U *<UserName>*	Specifies the user name.
/W *<Password>*	Specifies the password.
/A *<ApplicationName>*	Specifies the application name.
/S "*<SpecificationName>*"	Specifies the specification name. The specification name must be enclosed in double quotes. By default, the available specification names are **Fixed Length Records**, **Comma delimited**, **Pipe delimited**, **Tilde delimited**, and **Tab delimited**. Users with permission to create applications can also create custom specification names for use in the application.
/F *<PathAndFileName>*	Specifies the path and file name of the import file.

10.1.2.2.2 Optional Key Reference Import switches

The following table describes the optional command line switches:

Scenario	Use this switch	Description
If you want to specify a data source other than the default	/N *<DataSource>*	AppEnhancer imports records into the specified data source.
If you want the imported records to append to the records in the existing Key Reference table, and you want to keep existing data unchanged	/P	AppEnhancer appends, or adds, the imported records to the Key Reference table for the specified application. Existing data is not affected.
If you want the imported records to merge with the records in the existing Key Reference table	/M	AppEnhancer compares the key field values of the imported records with the key field values of records already in the Key Reference table. If an imported record and an existing record have the same value in the key field, the values in the data fields for the imported record overwrite the values in the data fields for the existing record. All other records are added as new records in the table.
If you want the imported records to replace all of the records in the existing Key Reference table	/R	AppEnhancer replaces all existing data in the Key Reference table with the imported records.
If you want to omit from the import a record or a group of records at the beginning of the import file	/K *<SkipNumber>*	Specify the number of lines that you want AppEnhancer to skip when processing the import file.
If you want to omit from the import a record or a group of records at the end of the import file	/L *<LoadNumber>*	Specify the number of lines that you want AppEnhancer to load when processing the import file.
If you want to specify description to the import job	/D "*<Description>*"	Specifies job description. The description must be enclosed in double quotes.
If you are uncertain about Key Reference Import command line usage	/?	A message appears that briefly describes the Key Reference Import command line usage.

10.1.2.2.3 Viewing Key Reference import job status

Go to the **Monitoring > Administrative Services Jobs** node in AppEnhancer Administrator. On the **Administrative Service Jobs** page, select **Datasource** and then filter the jobs by service using the **Select Service Type** list as **AutoIndex KeyRef Service**. To view a job's details, double-click a job.

To view log files, select a job and then click **Download Log File**.

10.1.2.3 Auto Index Import command

Use the following syntax when performing an Auto Index Import:

```
"c:\Program Files\XtenderSolutions\AppEnhancerImportUtility\AEImportUtility.exe /RT
AUTOINDEX <switches>
```

In the preceding command, `c:\Program Files\XtenderSolutions\AppEnhancerImportUtility\` is the directory in which AppEnhancer Import Utility has been installed and *<switches>* are a series of command line switches.

10.1.2.3.1 Required Auto Index Import switches

The following table describes the required command line switches:

Option	Description
`/U <UserName>`	Specifies the user name.
`/W <Password>`	Specifies the password.
`/A <ApplicationName>`	Specifies the application name.
`/S "<SpecificationName>"`	Specifies the specification name. The specification name must be enclosed in double quotes. By default, the available specification names are **Fixed Length Records**, **Comma delimited**, **Pipe delimited**, **Tilde delimited**, and **Tab delimited**. Users with permission to create applications can also create custom specification names for use in the application.
`/F <PathAndFileName>`	Specifies the path and file name of the import file.

10.1.2.3.2 Optional Auto Index Import switches

The following table describes the optional command line switches:

Scenario	Use this switch	Description
If you want to specify a data source other than the default	/N *<DataSource>*	AppEnhancer imports records into the specified data source.
If you want the imported records to append to the records in the existing Auto Index table, and you want to keep existing data unchanged	/P	AppEnhancer appends, or adds, the imported records to the Auto Index table for the specified application. Existing data is not affected.
If you want the imported records to replace all of the records in the existing Auto Index table	/R	AppEnhancer replaces all existing data in the Auto Index table with the imported records.
If you want to omit from the import a record or a group of records at the beginning of the import file	/K *<SkipNumber>*	Specify the number of lines that you want AppEnhancer to skip when processing the import file.
If you want to omit from the import a record or a group of records at the end of the import file	/L *<LoadNumber>*	Specify the number of lines that you want AppEnhancer to load when processing the import file.
If you want to specify description to the import job	/D "*<Description>*"	Specifies job description. The description must be enclosed in double quotes.
If you are uncertain about Auto Index Import command line usage	/?	A message appears that briefly describes the Auto Index Import command line usage.

10.1.2.3.3 Viewing Auto Index import job status

Go to the **Monitoring > Administrative Services Jobs** node in AppEnhancer Administrator. On the **Administrative Service Jobs** page, select **Datasource** and then filter the jobs by service using the **Select Service Type** list as **AutoIndex KeyRef Service**. To view a job's details, double-click a job.

To view log files, select a job and then click **Download Log File**.

10.2 Migration Wizard

The Migration Wizard enables you to migrate applications from one data source to another by using a simple wizard interface that guides you through the migration process. Migration Wizard can migrate all or some of the documents in an application. The wizard can also migrate applications within the same database. All index information, annotations, and the document file itself are migrated automatically, but the migration can be expanded to include security settings.

Custom data types and formats are migrated, but only the ones being used by the source application, and only if they do not already exist in the destination application. In some cases, you can limit the migration to index information only, excluding the actual documents.

If the application does not exist on the destination database, the Migration Wizard creates a new application. The wizard provides options that let you create a new Software Retention Management application. If you leave these options blank, the wizard creates a new application that is identical to the source application. If the application already exists on the destination database, you can choose to merge the documents into the destination application, or to overwrite all existing documents in the destination application with the source application.

The Migration Wizard enables you to perform several migrations without exiting to change the database, because source and destination databases are specified within the wizard. In instances where the same application needs to be migrated periodically, the Migration Wizard also works efficiently. Settings from a migration can be saved and reused, making the migration process almost automatic for subsequent migrations. Command-line options are also available, enabling quick and efficient migrations.

Notes

- Although you can create a new Software Retention Management application by using the Migration Wizard, it is not considered a retention-enabled application until the Retention Administrator configures retention for the application using the RM Configuration Utility.
- Only system administrators can perform migrations. In addition, the Migrate Application privilege must be enabled for the user's security profile or the group’s application security profile for the applications to be viewed in the Migration Wizard and subsequently migrated.
- During a migration, users can continue to retrieve and view documents in the source and destination applications, but cannot add new documents, edit existing documents, or delete documents in the source or destination application, until the migration process is complete.

10.2.1 Migrating document rules

The following rules pertain to migrating documents when you use the Migration Wizard:

- Migrating from a non-Unicode database to a Unicode database is supported. However, migrating from a Unicode database to a non-Unicode database is not supported, to prevent the possibility of data loss.
- Index-only migrations are permitted only when the migration involves like applications. Any existing retention configuration information (that is, retention policies and/or classes defined for the source application as well as retention periods for documents) is exported to the new application.
- The index field structure of the new application must be identical to the old application.
- The following items are not migrated:
  - If an application is migrated with batches waiting to be indexed, the non-indexed batches are not migrated. Batches should be indexed before an application is migrated.
  - Full-text and OCR information from the full-text database is not migrated. If you enable the **Migrate Indexes Only** option and if the destination application is created before the migration, full-text engine settings are migrated. Otherwise, full-text engine settings are not migrated.
  - If you are copying documents from a source application that is retention-enabled, retention configuration options are discarded. The Migration Wizard displays a warning message indicating that retention information will be lost. Retention Administrators can configure the destination application for retention, if they want, by using the RM Configuration Utility.

10.2.2 Migrating applications

The Migration Wizard provides a step-by-step wizard interface for application migration between databases. When migrating an application by using the Migration Wizard, you can select the documents to be migrated by specifying search criteria that describe which documents will be included in the migration. You can choose to:

- Migrate an application to a database that does not already contain the application
- Merge the application with an existing application in the destination database
- Write the application over an existing application in the destination database
- Append the application to an existing application in the destination database
- Migrate an application within the same database
- Migrate index information only
- Migrate security information

- Migrate previous revisions
- Migrate annotation groups

Document annotations in the application are migrated automatically.

Note: You can save the settings for a migration and reload them to save time on later migrations. Command line switches can also be used to preconfigure a migration.

1. Click **AppEnhancer Desktop > Migration Wizard**.
2. In the **Select Source Database** page, in the **Data Source Name** list, select the name of the data source where the application to be migrated resides.

   Notes

   - If saved settings exist from previous migrations, you can load those settings using **Load Settings**.
   - You can also select a data source that is using a previous version of AppEnhancer.

3. For **AppEnhancer Login**, in the **User Name** text box, type a valid user name for the selected data source.

   Note: Your login procedure might vary depending on the security provider in use for the current data source.

4. In the **Password** text box, type a valid password for the selected user name and database and click **Next**.

   Note: If the **User Name** and **Password** text boxes are not filled in correctly prior to clicking **Next**, a login dialog box appears. Type the correct account information, and then click **Login** to proceed to the next page.

5. In the **Select Destination Database** page, in the **Data Source Name** list box, select the name of the database to which you want the application to be migrated.
6. For **AppEnhancer Login**, in the **User Name** text box, type a valid user name for the selected data source.
7. In the **Password** text box, type a valid password for the selected user name and database and click **Next**.
8. In the **Source** list box, select the name of the application that you want to migrate.

   Note: When migrating an application that uses a form overlay, the _FORMS application must be migrated separately. Migration Wizard does not automatically migrate forms data when an application using forms is migrated.

When you have chosen a source application name, the **Destination** list box is populated with the matching application name from the destination database.

9. To change the default destination application, select the application from the **Destination** list box.

10. Select the option depending on the requirement:

Option	Description	More information
Replace Destination	Overwrites an existing application on the destination database.	When this option is enabled, the **Merge** option is disabled automatically and the **Allow duplicate indexes** option is disabled.  **Caution** Selecting this option will permanently delete the existing documents in the destination application. Recovery of the data is not possible through AppEnhancer.
Delete Source Documents	Deletes migrated documents from the source application.	All index information and referenced image or report files will also be deleted.  **Caution** Selecting this option will permanently delete the migrated documents and the index information referencing the documents from the source database. Recovery of the data is not possible through AppEnhancer.

Option	Description	More information
Migrate Indexes Only	Migrates index information only and exclude the actual documents	The actual object files referenced by the index information are not migrated to the destination database. This feature can be useful, for instance, when converting to Microsoft SQL Server from a runtime database. The storage location for the actual document files need not change. **Notes** • This option is available only when the migration involves like applications. In addition, the destination application must have the same name and index field structure as the source application. • If the source application is retention-enabled, retention configuration settings specified using the RM Configuration Utility (that is, retention policies and classes defined for the application) are maintained in the target application. • If you enable this option and if the destination application is created before the migration, full-text engine settings are migrated. Otherwise, full-text

Option	Description	More information
		engine settings are not migrated. • When this option is enabled, the **Delete Source Documents** option is disabled automatically.
Merge	Merges the source application with the destination application.	When this option is enabled, the **Allow Duplicate Indexes** option is disabled automatically. If the source application has the **Multiple indexes referencing a single document** option enabled, the **Merge** option will not be available.
Allow Duplicate Indexes	enables duplicate indexes in the destination application.	This option is enabled by default. This option cannot be enabled if **Merge** is enabled, because Merge overwrites destination documents with source documents that have matching index terms.  **Note:** This option is not enabled if the destination application is being created or replaced. If **Replace Destination** is enabled, the **Allow Duplicate Indexes** option becomes enabled and cannot be altered. If the destination application does not exist, it does not matter if **Allow Duplicate Indexes** is enabled or disabled.

Option	Description	More information
Migrate Security	Migrates security settings with the application, including Document Level Security.	Each user and group that has privileges in the source application will be migrated. Document Level Security is also migrated during a security migration. **Note:** Security is migrated only if **Replace Destination** is enabled or if the destination application does not already exist.
Migrate Previous Revisions	Migrates all revisions of all documents in the application.	This option migrates previous revisions and current revisions from the source database to the target database. If this option is disabled, only the current revision of each document is migrated.
Migrate annotation groups	Migrates all annotation groups in the source data source (and the user and group accounts associated with those annotation groups).	The configuration for each user and group within the annotation group is migrated, but user settings and privileges are not migrated with the user accounts (unless you have chosen to migrate security as well). After migration, you must use AppEnhancer Administrator to assign privileges to each user that was migrated as part of an annotation group migration (unless the user was migrated as part of a security migration).

Option	Description	More information
Use alternative security	Maps users and groups in the source database to users and groups in the destination database.	When the migration is performed and if this option is enabled, only the users and groups with alternative security information configured in AppEnhancer Administrator are migrated. **Note:** You must configure security mapping in AppEnhancer Administrator prior to running the migration if you want to use this option. **Caution** If you do not enable this option during the migration, all users and groups will be migrated, even if you have configured specific users or groups for security mapping.
Migrate document signatures	Migrates all existing signatures with the migrated documents.	None.

11. Click **Next**. The page that appears next depends on the **Migrate By** options you chose.

    - If you enable the **AppEnhancer document search** option, the **Document Search Criteria** page appears.

12. Depending on the options you have selected, perform the following actions:

    - "Selecting documents by specifying criteria" on page 170
    - "Selecting reports by specifying criteria" on page 171
    - "Specifying write paths for destination application" on page 171

13. In the **Summary** page, examine the information listed on this page to ensure that all of the selections are as you intended. If you need to make changes, click

Back until the page in which you want to make changes appears again. After you have made the changes, click **Next** until the **Summary** page.

In the event that you anticipate a subsequent migration of the same application, the **Save Settings** feature can be used prior to migration to save migration settings for reuse.

14. Click **Finish** to begin the application migration process.

    After the migration is completed, a message appears indicating the completion. Click **OK**.

    Note: The message states that the operation was completed, but it does not guarantee that all documents were migrated. You can view the log file to ensure that all designated documents were migrated. For example, if some of the documents searched for were not found, a successful completion message still appears.

15. Choose one of the following:

    - To exit the program, click **Exit**.
    - To migrate another application, click **Back** until the page in which you want to make changes appears again.
    - To migrate all the other applications in the data source using the same settings you used for the initial application, click **Create batch to migrate all applications**. Skip to step 17.

      Note: Using this setting produces a migration options file and a batch file that eliminate the need to migrate each application individually by using the Migration Wizard user interface. However, it is important to note that the same migration settings and write paths will be used for all applications in the data source. These settings cannot be modified when you migrate all applications in batch mode.

16. If you opted to exit the program, click **Exit**.

17. Click **Yes**.

18. In the **Save As** dialog box, type a storage path and file name with a suffix of MIG (for example, `C:\AEX\INVOICES.MIG`) for the migration profile, then click **Save**.

19. In the **Save As** dialog box that appears again, type the storage path you specified in step 18, and file name with a suffix of BAT (for example, `C:\AEX\INVOICES.BAT`) for the migration batch file, then click **Save**.

20. Navigate to the location where you created the migration profile and batch file, then double-click the batch file to execute it.

    The batch file migrates all the remaining applications in the data source using the settings from the initial application you migrated.

The Migration Wizard maintains a log file that contains the details of all migrations, including the errors. By default, it is saved as **C:\AEMigration.log**. If **C:\AEMigration.log** cannot be written to (locked or read-only), the log file is saved within your current directory, which is typically the program directory (by default, `C:\Program Files (x86)\XtenderSolutions\Content Management\`) of the Migration Wizard. However, if you are running a batch file from a different location, the log file is saved to the directory in which the batch file resides. If all of these attempts fail, no log file is written.

You can specify the location and filename of the Migration Wizard log file with the /L command line option. For example:

```
"C:\Program Files (x86)\XtenderSolutions\Content
Management\MigrateWiz32.exe" "C:\App1.mig"
/L C:\Temp\MyLog.log
```

10.2.2.1 Selecting documents by specifying criteria

The **Document Search Criteria** page enables you to select the documents that you want to migrate by specifying search criteria.

1. Type the criteria that match the documents you want to migrate.

   Note: To select all documents in an application, do not type any text into the search fields on this page.

2. If the source application is retention-enabled, the **Document Search Criteria** page displays a **Search** list box. Select an option in the list to specify which documents you want to migrate.

3. If you want to determine how many documents would be migrated based on the document search criteria you have entered, click **Run Query**. A message appears indicating how many documents match the criteria. Click **OK**.

4. If you want to include all reports that are associated with the selected documents, enable the **Include associated reports** option.

5. Click **Next**. The page that appears next depends on these factors:

   - If the destination application does not already exist in the destination data source, the **Application Path Configuration** page appears.
   - If the destination application does already exist in the destination data source, the **Summary** page appears. Continue with the migration process from step 13.

10.2.2.2 Selecting reports by specifying criteria

The **Report Search Criteria** page enables you to select the reports that you want to migrate by specifying search criteria.

1. Type the criteria that match the reports you want to migrate.

   Note: To select all reports in an application, do not type any text into the search fields on this page.

2. If you want to determine how many reports would be migrated based on the report search criteria you have entered, click **Run Query**. A message appears indicating how many reports match the criteria. Click **OK**.

3. If you want to include all documents that are associated with the selected reports, enable the **Include associated documents** option.

4. Click **Next**. The page that appears next depends on the destination application:

   - If the destination application does not already exist in the destination data source, the **Application Path Configuration** page appears.
   - If the destination application does already exist in the destination data source, the **Summary** page appears. Continue with the migration process from step 13.

10.2.2.3 Specifying write paths for destination application

The **Application Path Configuration** page appears if the destination application does not already exist in the destination data source. This page enables you to specify write paths for the new application. You must use secure write paths for AppEnhancer Software Retention Management applications, including retention-enabled applications (applications that are configured for retention using the RM Configuration Utility). In addition, it is recommended that you use secure write paths for all applications. Although secure paths are required only for documents and their associated annotations, you can also specify a secure path for OCR.

Secure paths must be defined on the **Paths** page in AppEnhancer Administrator. In addition, you must configure credentials for the impersonation account that AppEnhancer Desktop clients use when accessing the path.

1. Select **Use secure path** and specify a secure path root directory to enable the AppEnhancer Software Retention Management licensed feature for the destination application. The Migration Wizard automatically populates both the **Document Write Path** and the **Annotation Write Path** with the root path you specify.

2. Click **Enable Software Retention Management**.

3. Type a storage path for the destination database application in the **Document Write Path** text box. You can also select the options from the list box.

If you selected **Use secure path**, only secure paths appear in the list. In addition, the **Document Write Path** text box contains the root path you specified by default. You can append a document subdirectory to the root path.

Note: The document write path for the destination database application must be different from the document write path for the source database application.

4. Type an OCR write path, and for non-retention applications, an annotation write path for the destination database application in the corresponding text boxes. You can also select the options from the list box.
5. Click **Next**. The **Summary** page appears. Continue with the migration process from step 13.

10.2.2.4 Migrating security

Follow therse rules when you perform a security migration:

- When an application is migrated with migrate security selected, copy source security to the destination database for all users and groups that have access to the migrated application.
- When group security is migrated, migrate all users that belong to the group to the destination database.
- For both user and group profiles, copy the source global profile to the destination application if it does not already exist. If a global profile already exists on the destination database, it is not overwritten.

Note: For both user and group profiles, the application-specific profile located in the source database always overrides the application-specific profile in the destination database.

For user settings, permissions are verified for all individual users, and if the destination permissions are not the same as the source (possibly due to membership in multiple groups), the application-specific profile is created or altered to match the user permissions in the source database. If the source data source is using a different security provider than the destination data source, ensure that required actions are taken and conditions are met, as described in the following table:

Question	To database using CM security provider	To database using windows
What is migrated?	• All users and groups that have privileges in the source application	• All users and groups that have privileges in the source application • All users who are members of those groups
What needs to be done after migration?	• Assign passwords to each migrated user account	

Question	To database using CM security provider	To database using windows
Which migrated user accounts can be used after migration?	• All migrated user accounts	Only valid user accounts: • For the Windows security provider, the user accounts that have domain name in the user account name

10.2.2.5 Migrating annotation groups

If the source data source is using a different security provider than the destination data source, ensure that required actions are taken and conditions are met, as described in the following table:

Question	To database using CM security provider	To database using windows
What is migrated?	• All annotation groups in the data source • All users and groups that have been added to those annotation groups	• All annotation groups in the data source • All users and groups that have been added to those annotation groups • All users who are members of those groups
What needs to be done after migration?	• Assign privileges to each migrated user account • Assign passwords to each user account that has been migrated as a result of the annotation group migration	• Assign privileges to each migrated user account
Which migrated user accounts can be used after migration?	• All user accounts	Only valid user accounts: • For the Windows security provider, the user accounts that have domain name in the user account name

10.2.3 Automating migration process

You can use AppEnhancer Migration built-in automation features to script some or all of the archive process for users who perform the same archives on a routine basis. You can save settings files to load for future use. Use the command-line options of AppEnhancer Migration, or use both for a quick and accurate archive. You can also migrate all remaining applications for a data source following the initial migration of an application by using the **Create batch to migrate all applications** option on the Migration Wizard. This option creates a migration options file and a batch file that you can use to automate migration.

Saving and loading migration settings

You can use the **Save Settings** and **Load Settings** to save migration settings from the current migration process and to load saved settings from previous migration processes. Settings from the current migration, including source and destination database, source and destination application, and migration options, can be saved for use for subsequent migrations. You can also load previously saved migration settings so that you can skip some configuration steps.

Command line options

You can use the command-line options (or switches) when executing the Migration Wizard to speed up the migration process. A switch is available for each configurable migration option, and archive settings files can be specified as well. Command-line syntax can be run using a command line, a Windows shortcut, or a batch file. In the **Run** window, type the following syntax:

```
"C:\Program Files (x86)\XtenderSolutions\Content Management\
MigrateWiz32.exe" <optional-settings-file switches>
```

In this command, `"C:\Program Files (x86)\XtenderSolutions\Content Management"` is the directory to which AppEnhancer Desktop has been installed, *`<optional-settings-file>`* is the location and filename of the settings file you want to use, and *`<switches>`* are a series of command-line switches.

Specifying a migration settings file

You can load a previously created migration settings file using command-line options. In the **Run** window, type the following syntax:

```
"C:\Program Files (x86)\XtenderSolutions\Content Management\
MigrateWiz32.exe" C:\AppEnhancer\AEG.MIG <switches>
```

`C:\Program Files (x86)\XtenderSolutions\Content Management\` is the directory AppEnhancer Desktop has been installed, `C:\AppEnhancer\AEG.MIG` is the path and filename of the migration settings file you want to use, and *`<switches>`* are any optional switches you would like to use.

Note: When using a migration settings file and command-line switches together, the Migration Wizard uses information from the migration settings file for information not included as a command line switch. If a parameter

included in the migration settings file has also been specified by using a command-line switch, the command-line switch parameters override settings used in the migration file.

Command-line switches with arguments

Command-line switches with arguments are used to specify parameters that Migration Wizard should use for the migration. Command-line switches can be used alone or in conjunction with migration settings files. The following table provides a list of command-line switches that require arguments:

Option	Description
/SD *<DataSourceName>*	Specifies the name of the data source to be used as the source database.
/SU *<UserName>*	Specifies the user name for logging in to the data source to be used as the source database.
/SP *<Password>*	Specifies the password for the user name specified with the /SU switch.
/SA *<ApplicationName>*	Specifies the source application name.
/DD *<DataSourceName>*	Specifies the name of the data source to be used as the destination database.
/DU *<Username>*	Specifies the user name for logging in to the data source to be used as the destination database.
/DP *<Password>*	Specifies the password for the user name specified with the /DU switch.
/DA *<ApplicationName>*	Specifies the destination application name.
/S "n^z~a%b%c"	Specifies document search criteria. Search criteria contain tilde-separated (~) search fields. Fields can contain single values, multiple values, or a range of values. A percent sign (%) is used to separate multiple values. A caret (^) is used to separate range limits. The entire search string must be surrounded by double quotation marks.
/L *<LogFile>*	Specifies a directory and filename to override the default log file location.
/PD *<DocumentPath>*	Specifies a document write path for the destination application, if it does not already exist.
/PA *<AnnotationPath>*	Specifies an annotation write path for the destination application, if it does not already exist.

Option	Description
/PO *<OcrPath>*	Specifies an OCR write path for the destination application, if it does not already exist.
/PF *<FullTextPath>*	Specifies a full-text write path for the destination application, if it does not already exist.

Example 10-1: Command line argument

Consider a command line argument: `"C:\Program Files (x86)\XtenderSolutions\Content Management\MigrateWiz32.exe" /SD DEMO /SU SYSOP /SP PW1 /SA IMAGEAPP /DD NEWDEMO /DU SYSOP /DP PW1 /DA NEWIMAGES /S "1^9~Smith%Jones~~Invoice"`

In this example, documents in the application IMAGEAPP whose first index fields contain values between 1 and 9, second index fields match either "Smith" or "Jones", and fourth index fields match "Invoice" are migrated from the DEMO data source to the NEWIMAGES application within the NEWDEMO database. The user name and password used to access both databases are SYSOP and PW1, as specified by the /SU, /SP, /DU, and /DP switches.

Command-line switches without arguments

Command-line switches without parameters can also be used to configure your migration process. The following table provides a list of command-line switches that do not require parameters:

Option	Description
/IO	Migrates indexes only
/NOIO	Migrates indexes and images (default)
/MV	Deletes source documents
/NOMV	Retains source documents (default)
/OV	Overrides the destination application
/NOOV	Appends source documents to the destination application (default)
/MS	Migrates security
/NOMS	Does not migrate security (default)
/MRG	Merges documents with matching indexes
/NOMRG	Always creates new documents (default)
/DI	enables duplicate indexes to be created (default)

Option	Description
/NODI	Does not allow duplicate indexes to be created
/DR	Migrates previous document revisions
/NODR	Does not migrate previous document revisions (default)
/AGS	Migrates annotation group security
/NOAGS	Does not migrate annotation group security (default)
/MDS	Migrates by AppEnhancer document search (default)
/NOMDS	Does not migrate by AppEnhancer document search
/IAR	Includes associated reports in the migration
/NOIAR	Does not include associated reports in the migration (default)
/IAD	Includes associated documents in the migration
/NOIAD	Does not include associated documents in the migration (default)
/?	Displays Migration Wizard Command Line Help

10.3 Resubmitting Documents to the AppEnhancer Index Server

If you have changed the full-text engine for an application, keep in mind that full-text searching does not return any documents in this application until you submit them to the AppEnhancer Index Server, even if they have already been full-text indexed by the previous engine.

The AppEnhancer Full-Text Index Wizard is available to assist with submitting documents to the AppEnhancer Index Server for full-text indexing.

To use the AppEnhancer Full-Text Index Wizard:

1. From the Windows Start menu, select **Programs** > **AppEnhancer Desktop** > **AppEnhancer Full-Text Index Wizard**. The wizard appears, starting with the Data Source Selection page.
2. Select the data source in which you want to process documents. In the User Name and Password text boxes, enter your user name and password. (This user

account must have the Administrator privilege.) Click Next. The Application Selection page appears.

3. Select the application in which you want to process documents. Click Next. The Queue Selection and Other Options page appears. This page lists the queues that are available for processing.
4. If you want to add another queue, click Add. The Create New Full-text Queue dialog box appears.
5. In the Queue Name text box, enter a name for the new full-text queue. You can also enter a description in the Description text box. Click OK. The Queue Selection and Other Options page reappears.
6. Under Queue Selection, select the queue in which you want to process documents.
7. If the selected application contains documents that have already been processed by ProIndex, the Only documents already full-text indexed in ProIndex check box is available. Use this check box to specify whether you want to process only those documents. You have the following choices:

   - If you want to process only the documents that have already been processed by ProIndex, enable the check box.
   - If you do not want to exclude documents based on whether they have already been processed by ProIndex, clear the check box.

   Keep in mind that processing takes longer if this check box is enabled, because of the time it takes to determine which documents have already been processed.
8. Click Next. The Query Documents page appears.
9. Enter criteria to match the documents that you want to process. (To select all documents in the application, leave all search fields blank.) Click Next. The Status page appears and the selected documents are submitted to the specified queue. When the documents have been submitted, the Status page indicates the number of documents successfully submitted and the name of the queue to which they were submitted.
10. Click Finish.

10.4 Unindexed .BIN file search

During a rare outage, whether a network failure or a server failure, it is possible that the metadata might not get synchronized with files stored in the AppEnhancer repository. AppEnhancer provides a utility, `FindUnindexedBins.exe`, that searches for .BIN files without metadata and provides a report. The FindUnindexedBins utility also works with applications enabled with Software Retention Management.

The utility performs two separate audits of the selected application, looking at the following tables in the database, as described in the data dictionary:

- ae_dl<#>: The ae_dl<#> table contains the page pointers to images for each page in an application.
- ae_dt<#>: The ae_dt<#> table contains the index data for images in a particular application.
- ae_seq: The ae_seq table stores the next available sequencing numbers for an application. These include the next available document ID, page/object ID, and batch ID.
- ae_bsdat: The ae_bsdat table contains page pointers for batch scan jobs.

Note: The <#> represents the application ID recorded in the ae_apps table. There is no table called ae_dl# or ae_dt#. Instead, there are multiples of dl and dt tables with the <#> replaced by an actual number, for example, ae_dt1, ae_dt2, and so on.

The two audits are:

- Search for unindexed page records

  During this pass, the system identifies DL records without DT records. This is not common but can occur with selective restore of tables where the DT and DL are not kept in synchronization. To test this particular stage of the audit, create a new test document, and then delete the DT record only. The scan should pick it up.

- Search current write path for unindexed BIN files

  During this pass, the system performs a three-way comparison of the objectid values in the ae_seq and ae_dl<#> tables, and also looks at the names of the actual bin files in the write path. To test this particular stage of the audit, add an extraneous .BIN file to the write path. For example, if the highest .BIN file in the write path is 99.bin, then add a new file and name it 100.bin.

1. Navigate to the directory where the utility is stored (for example, `C:\Program Files (x86)\XtenderSolutions\Content Management`).
2. Double-click the **FindUnindexedBins.exe** file and click **OK** until the **Login** dialog box.
3. In the **Login** dialog box, provide the following:

- **Data Source**: Select a data source.
- **User Name** and **Password**: User name and password for the data source.

Click **Login**.

4. Select an application.
5. Select the **Create Batch** option if you want the utility to create batches for any unindexed pages or bins. AppEnhancer Web Access users can then launch AppEnhancer to execute the batches and index the questionable documents.
6. Click **Find**. The following occurs:
   - If the **Create Batch** option is disabled, the utility only reports any problems it detects.
   - If the **Create Batch** option is enabled, the utility creates batches for any unindexed pages or unindexed bins. The batches use the following naming convention:
     – Unindexed page records identified in the first audit are placed in a batch named:
     ```
     RECSYYYY-MM-DD HH:MM:SS
     ```
     – Unindexed bin files identified in the second audit are placed in a batch named:
     ```
     FBINYYYY-MM-DD HH:MM:SS
     ```

Chapter 11

Backup and Recovery

This chapter describes how to export and import system-wide configurations in AppEnhancer Administrator. Constant and reliable access to your data is one of the most critical aspects of your system. It is recommended that you have a comprehensive disaster recovery plan in place in the event of system issues or even an entire system shutdown. AppEnhancer Administrator has a configuration-data export/import feature, which can help you restore the configuration information, even when the problem is minor.

11.1 Importing and exporting configurations

You can import and export system-wide configurations. In the **Environment** node in AppEnhancer Administrator, use **IMPORT CONFIGURATION** and **EXPORT CONFIGURATION**

11.2 Importing and exporting configuration XML data

You can import and export configuration XML data. In the **Application Management** > **<***your data source***>** node in AppEnhancer Administrator, use **IMPORT** and **EXPORT**.

11.2.1 Importing configuration XML data

This section describes additional information about importing XML data. You can import data about applications and security from an XML file to **Application Management > <***your data source***>** node in AppEnhancer Administrator. The XML file should be an exported file by Exporting XML Data, or match the following schema.

11.2.1.1 XML file schema

The XML file that you import must match the following schema:

```
<xs:element name="DsDescriptor">
<xs:complexType>
<xs:sequence>
<xs:element name="CMDataTypes" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="CMDataType" type="CMDataType"
minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Applications" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="Application" minOccurs="0"
maxOccurs="unbounded" type="Application"/>
```

```
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Users" minOccurs="0" >
<xs:complexType>
<xs:sequence>
<xs:element name="User" minOccurs="0"
maxOccurs="unbounded" type="User"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Groups" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="Group" minOccurs="0"
maxOccurs="unbounded" type="Group"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="AnnoGroups" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="AnnoGroup" minOccurs="0"
maxOccurs="unbounded" type="AnnoGroup"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
```

Note: XML file with legacy format can be imported in to AppEnhancer.

11.2.1.1.1 Schema for data type descriptions

The description for each custom data type in the XML file that you import must match the following schema:

```
<xs:complexType name="CMDataType">
<xs:sequence>
<xs:element name="CMDataFormats" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="CMDataFormat" type="CMDataFormat"
minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="defaultAttributes" type="xs:long" use="required"/>
<xs:attribute name="defaultAttributes" type="xs:long" use="required/>
<xs:attribute name="maxsize" type="xs:int" use="required"/>
<xs:attribute name="minsize" type="xs:int" use="required"/>
<xs:attribute name="dbtype" type="xs:int" use="required"/>
<xs:attribute name="name" type="xs:string" use="required"/>
</xs:complexType>
```

11.2.1.1.2 Schema for data format descriptions

The description for each custom data type in the XML file that you import must match the following schema:

```
<xs:complexType name="CMDataFormat"/>
<xs:sequence>
<xs:element name="EditPic" type="xs:string"/>
<xs:element name="ValidateExpr" type="xs:string"/>
<xs:element name="RawExpr" type="xs:string"/>
<xs:element name="FormatExpr1" type="xs:string"/>
<xs:element name="FormatExpr2" type="xs:string"/>
<xs:element name="DefaultValue" type="xs:string"/>
</xs:sequence>
<xs:attribute name="formatWidth" type="xs:int" use="required"/>
<xs:attribute name="dbWidth" type="xs:int" use="required"/>
<xs:attribute name="scale" type="xs:int" use="required"/>
<xs:attribute name="LCID" type="xs:int" use="required"/>
<xs:attribute name="name" type="xs:string" use="required"/>
</xs:complexType>
```

11.2.1.1.3 Schema for application descriptions

The description for each application in the XML file that you import must match the following schema:

```
<xs:complexType name="Application">
<xs:sequence>
<xs:element name="Attributes" type="AppAttributes"
minOccurs="1"/>
<xs:element name="CenteraDeviceName" type="xs:string"
minOccurs="0" maxOccurs="1"/>
<xs:element name="Paths" type="AppPaths" minOccurs="1"/>
<xs:element name="FullText" type="FullText"
minOccurs="0" maxOccurs="1"/>
<xs:element name="Fields" minOccurs="1">
<xs:complexType>
<xs:sequence>
<xs:element name="Field" type="AppField"
minOccurs="1" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="description"
use="optional" type="xs:string"/>
<xs:attribute name="name" use="required"
type="xs:string"/>
</xs:complexType>
```

11.2.1.1.4 Schema for field descriptions

The description for each field in the XML file that you import must match the following schema:

```
<xs:complexType name="AppField">
<xs:sequence>
<xs:element name="Attributes" type="FieldAttributes"
minOccurs="1"/>
<xs:element name="UDLList" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="ListItem" type="xs:string"
minOccurs="1" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
```

```
<xs:attribute name="name" type="xs:string"/>
</xs:element>
</xs:sequence>
<xs:attribute name="valueMask" type="xs:string"/>
<xs:attribute name="length" type="xs:int" use="required"/>
<xs:attribute name="format" type="xs:string"/>
<xs:attribute name="dataType" type="xs:string" use="required"/>
<xs:attribute name="name" type="xs:string" use="required"/>
</xs:complexType>
```

Note: In the `UDLList` element, if the `xs:string type "name"` is set, it is a Global UDL.

11.2.1.1.4.1 Data types in XML

The following table lists the keywords and ID numbers that should be used for each data type in the XML file:

Data type	Keyword	ID number
Boolean Choice	`BooleanField`	10
Currency	`CurrencyField`	9
Date	`DateField`	3
Decimal/Numeric	`DecimalField`	2
Integer	`IntegerField`	1
SSN	`SSNField`	6
Telephone	`PhoneField`	7
Text	`TextField`	0
Time	`TimeField`	4
Time Stamp	`TimeStampField`	5
User-defined List	`UDLField`	11
ZIP Code	`ZipField`	8

11.2.1.1.4.2 Field flags in XML

The field flag in the XML file that you import must match the following schema:

```
<xs:complexType name="FieldAttributes">
<xs:attribute name="Searchable"
type="xs:boolean" use="required"/>
<xs:attribute name="DLSEnabled"

type="xs:boolean" use="required"/>
<xs:attribute name="AutoIndex"
type="xs:boolean" use="required"/>
<xs:attribute name="UniqueKey"
type="xs:boolean" use="required"/>
<xs:attribute name="Required"
type="xs:boolean" use="required"/>
<xs:attribute name="Readonly"
type="xs:boolean" use="required"/>
<xs:attribute name="ReferenceKey"
type="xs:boolean" use="required"/>
```

```
<xs:attribute name="ReferenceData"
type="xs:boolean" use="required"/>
<xs:attribute name="DualDataEntry"
type="xs:boolean" use="required"/>
<xs:attribute name="ValueMask"
type="xs:boolean" use="required"/>
<xs:attribute name="LeadingZero"
type="xs:boolean" use="required"/>
<xs:attribute name="IndexedBy"
type="xs:boolean" use="required"/>
<xs:attribute name="TimeStamp"
type="xs:boolean" use="required"/>
<xs:attribute name="Hidden"
type="xs:boolean" use="required"/>
</xs:complexType>
```

11.2.1.1.4.3 Field formats in XML

The following table lists the field formats that should be used for each data type in the XML file:

Data type	Formats
Boolean Choice	Yes/No True/FalseOn/Off In/Out Male/FemaleExempt/Non-exempt Asset/Liability Income/Expense Receivable/Payable

Currency	$ nnnn.nn
	$ n,nnn.nn$ nnnn
	$ n,nnn
	$ (nnnn.nn)$ (n,nnn.nn)
	$ (nnnn)
	$ (n,nnn)

Data type	Formats
Date	dd-mm-yy dd-mmm-yydd-mm-yyyy dd-mmm-yyyy dd-yy-mmdd-yy-mmm dd-yyyy-mm dd-yyyy-mmm dd/mm/yy dd/mmm/yy dd/mm/yyyy dd/mmm/yyyy dd/yy/mm dd/yy/mmm dd/yyyy/mm dd/yyyy/mmm dd mmmm, yyyy mm-dd-yy mm-yy-ddmm-dd-yyyy mm-yyyy-dd mmm-dd-yymmm-yy-dd mmm-dd-yyyy mmm-yyyy-dd mm/dd/yy mm/yy/dd mm/dd/yyyy mm/yyyy/dd mmm/dd/yy mmm/yy/dd mmm/dd/yyyy mmm/yyyy/dd mmmm dd, yyyy yy-mm-dd yy-dd-mmyy-mmm-dd yy-dd-mmm yyyy-mm-ddyyyy-dd-mm yyyy-mmm-dd yyyy-dd-mmm yy/mm/dd yy/dd/mm yy/mmm/dd yy/dd/mmm yyyy/mm/dd yyyy/dd/mm yyyy/mmm/dd yyyy/dd/mmm

Data type	Formats
Decimal/Numeric	nnnn nnnn.n nnnn.nn nnnn.nnn nnnn.nnnn nnnn.nnnnn n,nnn n,nnn.n n,nnn.nnn,nnn.nnn n,nnn.nnnn n,nnn.nnnnn (nnnn) (nnnn.n) (nnnn.nn) (nnnn.nnn) (nnnn.nnnn) (nnnn.nnnnn) (n,nnn) (n,nnn.n) (n,nnn.nn) (n,nnn.nnn) (n,nnn.nnnn) (n,nnn.nnnnn)
Integer	nnnn n,nnn(nnnn) (n,nnn)
SSN	nnn-nn-nnnn nnnnnnnnn ddd-dd-nnnn dddddnnnn
Telephone	nnn-nnnn nnn-nnn-nnnn (nnn)nnn-nnnn (nnn) nnn-nnnnnnn-ddd-dddd (nnn)ddd-dddd (nnn) ddd-dddd
Text	A field format is not required for the Text data type. However, a validation mask can be specified.
Time	Do not specify a format for the Time data type. Only one format (hh:mm:ss) is valid.
Time Stamp	Do not specify a format for the Time Stamp data type. Only one format (yyyy-mm-dd hh:mm:ss) is valid.

Data type	Formats
User-defined List	Specify a list of values in the following syntax: <UDLField fieldTypeId="11" name="*<FieldName>*" *<FieldFlags>*> <ListItem value="*<FirstValue>*" /> <ListItem value="*<NthValue>*" /> </UDLField>
ZIP Code	nnnnn nnnnn-nnnn

11.2.1.1.5 Schema for user descriptions

The description for security provider type is as follows:

```
<xs:simpleType name="SecurityProviderType">
<xs:restriction base="xs:string"/>
<xs:enumeration value="NATIVE"/>
<xs:enumeration value="WINNT"/>
<xs:enumeration value=THIRDPARTY"/>
</xs:restriction>
</xs:simpleType>
```

The description for each user in the XML file that you import must match the following schema:

```
<xs:complexType name="User">
<xs:sequence>
<xs:element name="GlobalPermission"
minOccurs="0" type="GlobalPermission"/>
<xs:element name="AppPermissions">
<xs:complexType>
<xs:sequence>
<xs:element name="AppPermission" minOccurs="0"
maxOccurs="unbounded" type="AppPermission"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="name" use="required"
type="xs:string"/>
<xs:attribute name="description"
use="optional" type="xs:string"/>
<xs:attribute name="securityProvider"
use="required" type="SecurityProviderType"/>
<xs:attribute name="providerGuid"
use="required" type="xs:string"/>
<xs:attribute name="secureId"
use="optional" type="xs:string"/>
<xs:attribute name="password"
use="optional" type="xs:string"/>
<xs:attribute name="licenseGroup"
use="optional" type="xs:string"/>
<xs:attribute name="alternativeName"
use="optional" type="xs:string"/>
<xs:attribute name="alternativeFullName"
use="optional" type="xs:string"/>
<xs:attribute name="alternativePassword"
use="optional" type="xs:string"/>
```

11.2.1.1.6 Schema for group descriptions

The description for each group in the XML file that you import must match the following schema:

```
<xs:complexType name="MemberUser">
<xs:attribute name="name" use="required"
type="xs:string"/>
<xs:attribute name="securityProvider" use="required"
type="SecurityProviderType"/>
<xs:attribute name="providerGuid" use="required"
type="xs:string"/>
</xs:complexType>
<xs:complexType name="Group">
<xs:sequence>
<xs:element name="GlobalPermission"
minOccurs="0" type="GlobalPermission"/>
<xs:element name="AppPermissions">
<xs:complexType>
<xs:sequence>
<xs:element name="AppPermission" minOccurs="0"
maxOccurs="unbounded" type="AppPermission"/>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="MemberUsers" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="MemberUser" minOccurs="0"
maxOccurs="unbounded" type="MemberUser"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="name"
use="required" type="xs:string"/>
<xs:attribute name="description"
use="required" type="xs:string"/>
<xs:attribute name="securityProvider"
use="required" type="xs:string"/>
<xs:attribute name="providerGuid" use="required"
type="xs:string"/>
</xs:complexType>
```

Note: The description for security provider type is defined in "Schema for user descriptions" on page 188.

11.2.1.1.7 Schema for user or group profile descriptions

The description for each user or group profile in the XML file that you import must match the following schema:

```
<xs:complexType name="AppPermission">
<xs:attribute name="appName"
use="required" type="xs:string"/>
<xs:attribute name="SubmitWorkflow"
use="required" type="PermissionState"
<xs:attribute name="RetentionAdmin"
use="required" type="PermissionState"/>
<xs:attribute name="RetentionUser"
use="required" type="PermissionState"/>
<xs:attribute name="CreateRedact"
use="required" type="PermissionState"/>
<xs:attribute name="CreateAnno"
use="required" type="PermissionState"/>
<xs:attribute name="ReportView"
use="required" type="PermissionState"/>
```

```
<xs:attribute name="OCR"
use="required" type="PermissionState"/>
<xs:attribute name="FullTextQuery"
use="required" type="PermissionState"/>
<xs:attribute name="FullTextIndex"
use="required" type="PermissionState"/>
<xs:attribute name="GlobalAnno"
use="required" type="PermissionState"/>
<xs:attribute name="EditRedact"
use="required" type="PermissionState"/>
<xs:attribute name="EditAnno"
use="required" type="PermissionState"/>
<xs:attribute name="IndexImageImport"
use="required" type="PermissionState"/>
<xs:attribute name="AutoIndexImport"
use="required" type="PermissionState"/>
<xs:attribute name="KeyRefImport"
use="required" type="PermissionState"/>
<xs:attribute name="UserSecurityMaint"
use="required" type="PermissionState"/>
<xs:attribute name="AutoIndexMaint"
use="required" type="PermissionState"/>
<xs:attribute name="KeyRefMaint"
use="required" type="PermissionState"/>
<xs:attribute name="DLSMaint"
use="required" type="PermissionState"/>
<xs:attribute name="COLDBatchExtract"
use="required" type="PermissionState"/>
<xs:attribute name="COLDImportMaint"
use="required" type="PermissionState"/>
<xs:attribute name="COLDImport"
use="required" type="PermissionState"/>
<xs:attribute name="MigrateApp"
use="required" type="PermissionState"/>
<xs:attribute name="DeleteApp"
use="required" type="PermissionState"/>
<xs:attribute name="ModifyApp"
use="required" type="PermissionState"/>
<xs:attribute name="AddPage"
use="required" type="PermissionState"/>
<xs:attribute name="DeletePage"
use="required" type="PermissionState"/>
<xs:attribute name="DeleteDoc"
use="required" type="PermissionState"/>
<xs:attribute name="Print"
use="required" type="PermissionState"/>
<xs:attribute name="Display"
use="required" type="PermissionState"/>
<xs:attribute name="ModifyIndex"
use="required" type="PermissionState"/>
<xs:attribute name="BatchIndex"
use="required" type="PermissionState"/>
<xs:attribute name="BatchScan"
use="required" type="PermissionState"/>
<xs:attribute name="EnhancePages"
use="required" type="PermissionState"/>
<xs:attribute name="Scan"
use="required" type="PermissionState"/>
</xs:complexType>
<xs:complexType name="GlobalPermission">
<xs:attribute name="SubmitWorkflow"
use="required" type="PermissionState"
<xs:attribute name="RetentionAdmin"
use="required" type="PermissionState"/>
<xs:attribute name="RetentionUser"
use="required" type="PermissionState"/>
<xs:attribute name="CreateRedact"
use="required" type="PermissionState"/>
<xs:attribute name="CreateAnno"
use="required" type="PermissionState"/>
<xs:attribute name="ReportView"
```

```
use="required" type="PermissionState"/>
<xs:attribute name="WXPAL"
use="required" type="PermissionState"/>
<xs:attribute name="OCR"
use="required" type="PermissionState"/>
<xs:attribute name="FullTextQuery"
use="required" type="PermissionState"/>
<xs:attribute name="FullTextIndex"
use="required" type="PermissionState"/>
<xs:attribute name="GlobalAnno"
use="required" type="PermissionState"/>
<xs:attribute name="EditRedact"
use="required" type="PermissionState"/>
<xs:attribute name="EditAnno"
use="required" type="PermissionState"/>
<xs:attribute name="IndexImageImport"
use="required" type="PermissionState"/>
<xs:attribute name="AutoIndexImport"
use="required" type="PermissionState"/>
<xs:attribute name="KeyRefImport"
use="required" type="PermissionState"/>
<xs:attribute name="UserSecurityMaint"
use="required" type="PermissionState"/>
<xs:attribute name="AutoIndexMaint"
use="required" type="PermissionState"/>
<xs:attribute name="KeyRefMaint"
use="required" type="PermissionState"/>
<xs:attribute name="DLSMaint"
use="required" type="PermissionState"/>
<xs:attribute name="MultiLogin"
use="required" type="PermissionState"/>
<xs:attribute name="Admin"
use="required" type="PermissionState"/>
<xs:attribute name="COLDBatchExtract"
use="required" type="PermissionState"/>
<xs:attribute name="COLDImportMaint"
use="required" type="PermissionState"/>
<xs:attribute name="COLDImport"
use="required" type="PermissionState"/>
<xs:attribute name="MigrateApp"
use="required" type="PermissionState"/>
<xs:attribute name="DeleteApp"
use="required" type="PermissionState"/>
<xs:attribute name="ModifyApp"
use="required" type="PermissionState"/>
<xs:attribute name="CreateApp"
use="required" type="PermissionState"/>
<xs:attribute name="AddPage"
use="required" type="PermissionState"/>
<xs:attribute name="DeletePage"
use="required" type="PermissionState"/>
<xs:attribute name="DeleteDoc"
use="required" type="PermissionState"/>
<xs:attribute name="ConfigWS"
use="required" type="PermissionState"/>
<xs:attribute name="Print"
use="required" type="PermissionState"/>
<xs:attribute name="Display"
use="required" type="PermissionState"/>
<xs:attribute name="ModifyIndex"
use="required" type="PermissionState"/>
<xs:attribute name="BatchIndex"
use="required" type="PermissionState"/>
<xs:attribute name="BatchScan"
use="required" type="PermissionState"/>
<xs:attribute name="EnhancePages"
use="required" type="PermissionState"/>
<xs:attribute name="Scan"
use="required" type="PermissionState"/>
</xs:complexType>
```

11.2.1.1.8 Schema for annotation group descriptions

The description for each annotation group in the XML file that you import must match the following schema:

```
<xs:simpleType name="AnnoGroupPermType">
<xs:restriction base="xs:string">
<xs:enumeration value="user"/>
<xs:enumeration value="group"/>
</xs:restriction>
</xs:simpleType>
<xs:complexType name="AnnoGroupPerm">
<xs:attribute name="type"
type="AnnoGroupPermType" use="required"/>
<xs:attribute name="FollowLegacy"
type="xs:boolean" use="required"/>
<xs:attribute name="ViewAnno"
type="xs:boolean" use="required"/>
<xs:attribute name="CreateAnno"
type="xs:boolean" use="required"/>
<xs:attribute name="EditAnno"
type="xs:boolean" use="required"/>
<xs:attribute name="HideRedact"
type="xs:boolean" use="required"/>
<xs:attribute name="CreateRedact"
type="xs:boolean" use="required"/>
<xs:attribute name="EditRedact"
type="xs:boolean" use="required"/>
<xs:attribute name="GlobalEdit"
type="xs:boolean" use="required"/>
<xs:attribute name="name"
type="xs:string" use="required"/>
</xs:complexType>
<xs:complexType name="AnnoGroup">
<xs:sequence>
<xs:element name="AnnoGroupPerms" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="AnnoGroupPerm" type="AnnoGroupPerm"
minOccurs="0" maxOccurs="unbounded"/>
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
<xs:attribute name="name"
type="xs:string" use="required"/>
</xs:complexType>
```

11.2.1.2 Managing a duplicate user or group

If you find a duplicate user or group when you import users or groups from an XML file, the resulting changes to the profiles of the user or the group depend on the options you chose.

Similarly, if you find a duplicate group when you import groups from an XML file, the resulting changes to the membership list of the group depends on the options you chose.

11.2.1.2.1 Changes in user or group profiles

If you find a duplicate user when you import users from an XML file, the changes that occur in the profiles of the user depend on whether you enabled or disabled the **Over-write existing user if a duplicate user name is encountered** option. Similarly, if you find a duplicate group when you import groups from an XML file, the changes that occur in the profiles of the user or group depend on whether you enabled or disabled the **Over-write existing group if a duplicate group name is encountered** option.

- If the option is enabled, the profiles for a particular user in the XML file overwrite all of the profiles for that user in AppEnhancer Administrator.
- If the option is disabled, the profiles of user or group are compared. New profiles in the XML file are appended. Profiles in the XML file for the same application overwrite the original profile in AppEnhancer Administrator. Profiles that exist in AppEnhancer Administrator but not in the XML file are maintained.

For example, AppEnhancer Administrator has a user RUDY with profiles for applications A and B. An XML file has a user RUDY with profiles for applications B and C. The B profile in the XML file is different than the B profile in AppEnhancer Administrator. The following table lists resulting profiles of RUDY, depending on the overwrite option:

Profiles of RUDY in AppEnhancer Administrator	Profiles of RUDY in XML file	Resulting profiles of RUDY with overwrite enabled	Resulting profiles of RUDY with overwrite disabled
A			A
B with Display privilege only	B with full privileges	B with full privileges	B with full privileges
	C	C	C

11.2.1.2.2 Changes in a group membership list

When you import groups from an XML file, if you find a duplicate group, the changes that occur in the group's membership list depends on whether you enabled or disabled the **Over-write existing group if a duplicate group name is encountered** option.

- If the option is enabled, the membership list for a particular group in the XML file overwrites the membership list for that group in AppEnhancer Administrator.
- If the option is disabled, the group accumulates users as members.

For example, AppEnhancer Administrator has a group QA with two users as members. An XML file also has a group QA with two users as members, but only one user is the same. The following table lists the membership list of group, depending on the overwrite option.

Members of QA in AppEnhancer Administrator	Members of QA in XML file	Resulting members of QA with overwrite enabled	Resulting members of QA with overwrite disabled
RON			RON
SHIBLY	SHIBLY	SHIBLY	SHIBLY
	JUDD	JUDD	JUDD

11.2.2 Exporting configuration XML data

This section describes additional information about exporting configuration XML data. You can export data about applications and security from the **Application Management > <***your data source***>** node in AppEnhancer Administrator to an XML file. This data is limited to the following:

- Custom data types and formats
- Application name, description, setting for Multiple indexes referencing a single document, and full-text engine settings
- Write paths (document, annotation, OCR, and full-text)
- Field name, data type, length, format (including user-defined lists), and flags
- Security provider setting
- User names, full names, profiles, and privileges
- Group names, descriptions, member lists, profiles, and privileges

Note: Only Global UDL in use will be exported to XML.

Chapter 12

Best Practices

The freedom to create applications provides organizations with flexibility when designing an AppEnhancer system. To use this flexibility most efficiently, it is important to develop and follow an overall approach for the organization. The AppEnhancer system administrator is usually in the best position to implement and support AppEnhancer within the organization. As such, the administrator takes responsibility for surveying users and determining the needs of the company. If possible, the administrator should be enabled to make the final decisions on all application design issues.

There are several aspects to the role of AppEnhancer system administrator. Along with creating applications and managing user security, you can configure workstations, set up license groups, supervise system backups, review documentation updates, and perform many other tasks. These activities can all be performed by one person or distributed among several individuals, but each person involved must have a comprehensive knowledge of the AppEnhancer system.

12.1 Application development and maintenance

A primary function of the AppEnhancer system administrator is to develop and maintain all AppEnhancer applications. You must be well acquainted with the daily operations of the users so that their needs can be addressed in the newly designed application. A system analysis, prior to the design stage, always refines the development of a new application. Any modifications to the system should be approached in the same way—by analyzing the necessity and potential impacts of the change.

Through careful design of each application the AppEnhancer system administrator can control many aspects of document creation and retrieval. You can make document creation easier and more accurate by designing the application to use import and data validation features. You can make document retrieval easier by creating saved queries, so that users can access preconfigured groups of documents.

12.2 System security

AppEnhancer Administrator provides methods of protecting and controlling vital information. AppEnhancer enables installation and use of two prepackaged security providers: CM or Windows. Decide on which security provider you will use before implementing AppEnhancer.

Caution

If you change the security provider after you have already started using AppEnhancer, you will lose all current security information. You must then recreate all users, groups, and permissions.

In addition, the system itself contains various levels of security. You can manage user and group security profiles; issue new user names, passwords, and privileges; remove inactive users; manage group membership; and change passwords, as needed.

In addition, if you are using AppEnhancer Web Access to deliver documents over the Internet or through intranets, AppEnhancer Web Access to AppEnhancer system resources must be correctly configured. You can use global settings to provide credentials for all resources that AppEnhancer Web Access accesses when responding to user requests. You can also configure your system to use different credentials when accessing different resources, but you must ensure that all users who must have access to documents and other resources have that access.

When a user requests a document from an AppEnhancer server, the server needs to access several resources, such as the path to the AppEnhancer documents, to respond to that request. To do so, the server must provide appropriate credentials for each resource. You can configure separate credentials for each resource, if needed. You can choose to pass the credentials from the AppEnhancer component login (Application), the credentials specified as global credentials under the AppEnhancer Web Access or **Desktop Credentials** node in AppEnhancer Administrator (Global), or a specific set of credentials (Supplied).

Global credentials or specific credentials for a resource are controlled by the system administrator through AppEnhancer Administrator. Application credentials originate from the user logging in to the AppEnhancer component. If the default data source is using the Windows security provider, the application credentials are forwarded directly and transparently from the user's browser. To ensure necessary access to resources and at the same time maintain specific control over which credentials have access to particular resources, it is recommended that you use global credentials for all resources. You need to make sure, whenever you assign credentials for a resource, that all credentials that are supplied under that resource authentication method can access the resource in question.

12.3 License groups maintenance

License Groups enable you to control which licenses are allocated to specific users, workstations, or databases. If any license groups have been created in the License Server, you can specify their use for individual users or individual AppEnhancer databases.

12.4 System backups

Regular system backups are crucial for comprehensive data protection. Set up a schedule for backing up the data in the document write paths for your applications. As the final authority on AppEnhancer, the AppEnhancer system administrator is ultimately responsible for the security of the data and is therefore responsible for backing up the system. This task can be automated or delegated, but follow up to be certain of data integrity and accuracy. Depending on the configuration of the website, also set up a schedule for backing up the storage server .

12.5 Database maintenance

You must perform the following maintenance procedures on a regular basis:

- Database backups, which must be included in the regular system backup schedule.
- Periodic checks to ensure that there is sufficient available hard drive space on the database server.
- To optimize database performance, you must periodically rebuild indexes and check for database corruption, using the tools provided for your database, such as the Microsoft SQL Server database consistency checker (DBCC).

The documentation provided with your database software provides more information about the maintenance required for your database.

12.6 Hardware maintenance

Along with the standard workstations and printers, a variety of other hardware can be used with AppEnhancer, including scanners, fax equipment, optical drives and libraries. You should be familiar with any hardware used in conjunction with the system because these components significantly influence AppEnhancer performance. Maintenance contracts from hardware vendors are strongly suggested. Ensure that all your systems meet the system requirements. Also, when you are upgrading from one version of a product to the next, ensure that your existing system still meets the system requirements.

To improve performance of your AppEnhancer system, it is recommended that you select hardware platforms that exceed the minimum requirements and are sufficient to process the number of expected requests on each system.

12.7 Software maintenance

The AppEnhancer system administrator upgrades the AppEnhancer system as needed. This can include installing service releases to products or upgrading when a new product comes out.

The administrator also monitors the need for additional functionality. Ensure that all your systems meet the system requirements. Also, when you are upgrading from one version of a product to the next, ensure that your existing system still meets the system requirements.

12.8 User assistance

The AppEnhancer system administrator is the first point of contact for all questions pertaining to the AppEnhancer system. Be prepared to troubleshoot and provide instructions about how to operate the system.

12.9 Data storage server maintenance

If AppEnhancer documents are stored on a data storage server, you should periodically check the space (storage media space) available on the server and add media to the server when necessary. Media copies can help to ensure complete system integrity. Update copies on a scheduled basis and store them off-site or in a fire-resistant area.

12.10 Acceptance testing

The AppEnhancer system has many interacting modules. AppEnhancer products also provide great flexibility thorough extensive configuration settings. The extent of configuration flexibility could lead to situations in which users might be accidentally denied access to documents or particular system functionality. For this reason, whenever you make a major change to your system, it is recommended that you set up your entire system in a test environment prior to deploying it in your production environment. Use this test environment to verify that a sampling of users can access it and perform basic tasks. Examples of major changes include rolling out a new version of the AppEnhancer system, major adjustments to the applications or security in your system, or adding a new AppEnhancer product to your system.

To perform an effective acceptance test, be sure to define acceptance parameters prior to testing. Acceptance parameters should include a list of basic tasks necessary for the system to function. Acceptance parameters can also include new features and functionality available in the products. To capture an effective set of parameters, check with a sampling of system users to make sure that the interests of all stakeholders are taken into account. To save time with acceptance testing efforts on future upgrades, keep the list of parameters so that it can be reused the next time you need to test rollout of the system.

12.11 Web Access user settings

When a new user is created, that user inherits a set of default AppEnhancer Web Access user settings. You can configure the settings in AppEnhancer Administrator. If you grant users the **Configure Work Station** privilege through AppEnhancer Administrator, users can modify user settings in the AppEnhancer Web Access user interface. However, if you would prefer to control user settings from a centralized location, you can decide not to grant this privilege to users and instead control the user settings only through AppEnhancer Administrator.