

Security and LDAP

Administration and Set-up Guide v1.0

© SYSCON JUSTICE SYSTEMS

Last Updated: March 20, 2024

Revision History

Name	Date	Reason for Changes
Joel Basart	March 14, 2014	Start Guide content.
Joel Basart	June 24, 2014	Add content.
Joel Basart	Oct 25, 2014	Updated content.
Joel Basart	May 2, 2015	WF 1.0 Release content updated and added.

About this Guide

This guide describes the security requirements for Workflow™ using Role Based Access Control (RBAC) to control user access to inmate records and restrict what system operations a user performs on inmate data.

Typographical Conventions

The following typographical conventions are used:

Convention	Purpose
Bold	Executable names, including titles of items you must select. For example: • Click a **button** on the screen with the mouse. • Press a **key.** • Type **information** in a field. • Select a **function** from a pull-down menu.
Italics	Important notes
Title Case	Proper names Names of Workflow features, for example, 'Toolbar,' 'Header' block, 'Schedule Inquiry' button.
Other	Symbols are utilized to illustrate a procedure or other relevant information.

CONTENTS

ABOUT THIS GUIDE 3

Typographical Conventions 3

OVERVIEW 6

Regular User 6

Administrative User 6

Role-Based Access Control (RBAC) 7

Lightweight Directory Access Protocol (LDAP) 7

USER AUTHENTICATION 8

Logging into Workflow 8

Updating Your Password 9

RESOURCE AUTHORIZATION 10

Business Processes 11

Reports 11

Reference Domain/Reference Codes 11

Task Management 11

Global Business Processes 12

Global Activities 12

Global Reports 12

WORKFLOW ADMIN CONSOLE (WAC) 13

Create/Maintain User Accounts/Roles and Facility Sets 13

User Roles 14

Facility Sets 14

Components 14

Create/Maintain Facilities 14

Set Up User Accounts 14

Attributes 14

Associations: 15

Set Up Reference Domains/Codes 15

Set Up Custom Fields 15
Create/Maintain Business Rules 15
Set Up System Profiles 15
RETRIEVAL OPTIONS 16
Selection of a Facility Set 16
Retrieval Options Use Cases 16
GLOSSARY 18

Overview

Workflow uses **Role Based Access Control** (RBAC) to control user access to inmate records and restrict what system operations a user performs on inmate data.

The Authentication of user data is based on a **User Name** and **Password**.

RBAC (**Role Based Access Control**) uses authorization of a role assigned to a **User Account**, against a **Facility Set**. The RBAC module governs the access to the following components, based on the type of **User Role**:

Regular User

- Business practices
- Activities
- Tasks in the Task Pool, operations on tasks such as Clear or Assign.
- Navigation menu for processes, activities, reports, and dashboards.
- Facility sets in the agency.
- Global business processes/activities
- Reference codes.

Administrative User

- System profiles
- Reference domains/codes
- CCFs
- Business rules
- Ad-hoc reports
- Menu navigation
- User accounts
- Maintain organization, facilities, facility internal location, and user accounts.

There are two primary objectives for this security model:

1. To control what inmate records are accessed by a user.
2. To control what system operations are performed.

Both are determined by job responsibilities at one or more facilities on a need-to-know basis. They are configured for each individual staff member in the user account to reflect responsibilities at any time. The general purpose of the system is to make information widely available to any user requiring it at any time, system access is necessary and users are cleared in advance as part of their job assignment.

If you are a correctional officer at a facility, you need access to all inmates now held at that facility. Your specific job influences what you can view in those records, and most officers are able to see more than they are able to update.

For example, Housing Officers make housing assignments and may also need to know an inmate's Trust Account balance without being able to update it. A Cashier can update the Trust Account, and can see an inmate's current housing but cannot update it.

Access to inmate records is controlled by a Facility Set, a pre-defined group of one or more named facilities. If your Facility Set includes access to Facilities A, B, and C, then you have access to inmates in those facilities.

Access to system functions is controlled by User Roles pre-defined to include all functions required to perform an assigned duty. Typical Roles can include: Intake Officer, Property Officer, or Watch Commander. **Administrative Roles** are also used by a few staff to grant access to the whole system.

Role-Based Access Control (RBAC)

RBAC is a security system used to restrict system access to only authorized users. All access is authorized using roles.

A role is a collection of permissions, and all users receive permissions only through the roles to which they are assigned, or through roles they inherit through the role hierarchy. Roles stay relatively stable, while users and permissions are numerous and change rapidly.

There are three main rules defined for RBAC:

1. **Role assignment:** Users can exercise a permission only if they have been assigned a role.
2. **Role authorization:** A user's active role must be authorized. With rule 1 above, this rule ensures that users can only take on roles for which they are authorized.
3. **Permission authorization:** A user can exercise a permission only if the permission is authorized for their active role. With rules 1 and 2, this rule ensures that users can only exercise permissions for which they are authorized.

RBAC is also referred to as role-based security.

Lightweight Directory Access Protocol (LDAP)

Authentication is managed using Lightweight Directory Access Protocol and against our database.

The Lightweight Directory Access Protocol is a set of protocols for accessing information directories.

It accesses and maintains distributed directory information services over an Internet Protocol network.

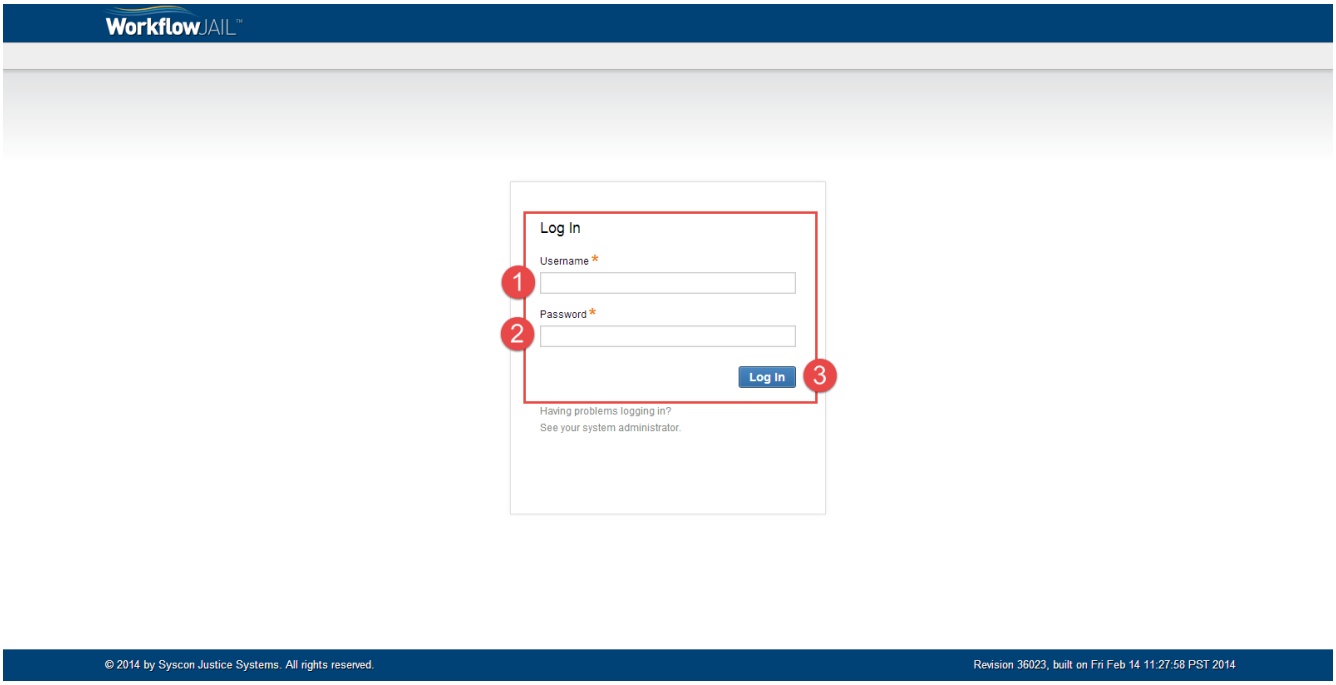
It is used to provide a "single sign-on" where one password for a user is shared between many services. In this case to apply a login code so that staff log in only once, and then are automatically logged into the application.

User Authentication

Logging into Workflow

A staff member must have an active user account to access or configure Workflow.

The system prompts you for your **Username** and **Password** either internally or externally. External logon is accomplished using LDAP.



The system checks the **Username** and **Password** according to password policies:

1. If the password is expired, the system prompts you to enter an updated password.
    a. The system then checks it against the **Password Complexity** rules.
2. If the **Username** or **Password** is incorrect, the system prompts you to re-enter them.
3. If you reach the maximum number of allowed attempts, the system warns you and locks the account.

Password Expiration: Duration after which the user account password expires and you are forced to change the password.

Password Complexity: The password length, special and required characters making up the password.

Historical Password Usage: Rule ensuring the new password is not the same as a configured number of historical old passwords.

Number of Incorrect Logins: The number of incorrect logins before an account is locked.

Updating Your Password

If you access Workflow and your password has expired, then the system prompts you to enter a new password.

You select the "Forgot Password" option and you are then asked to confirm your identity using a token-driven confirmation email.

A form is displayed to update your password then enter your new password and confirm it. The system checks this new password against any Password Complexity rules and if it does not conform to these rules you are asked to re-try.

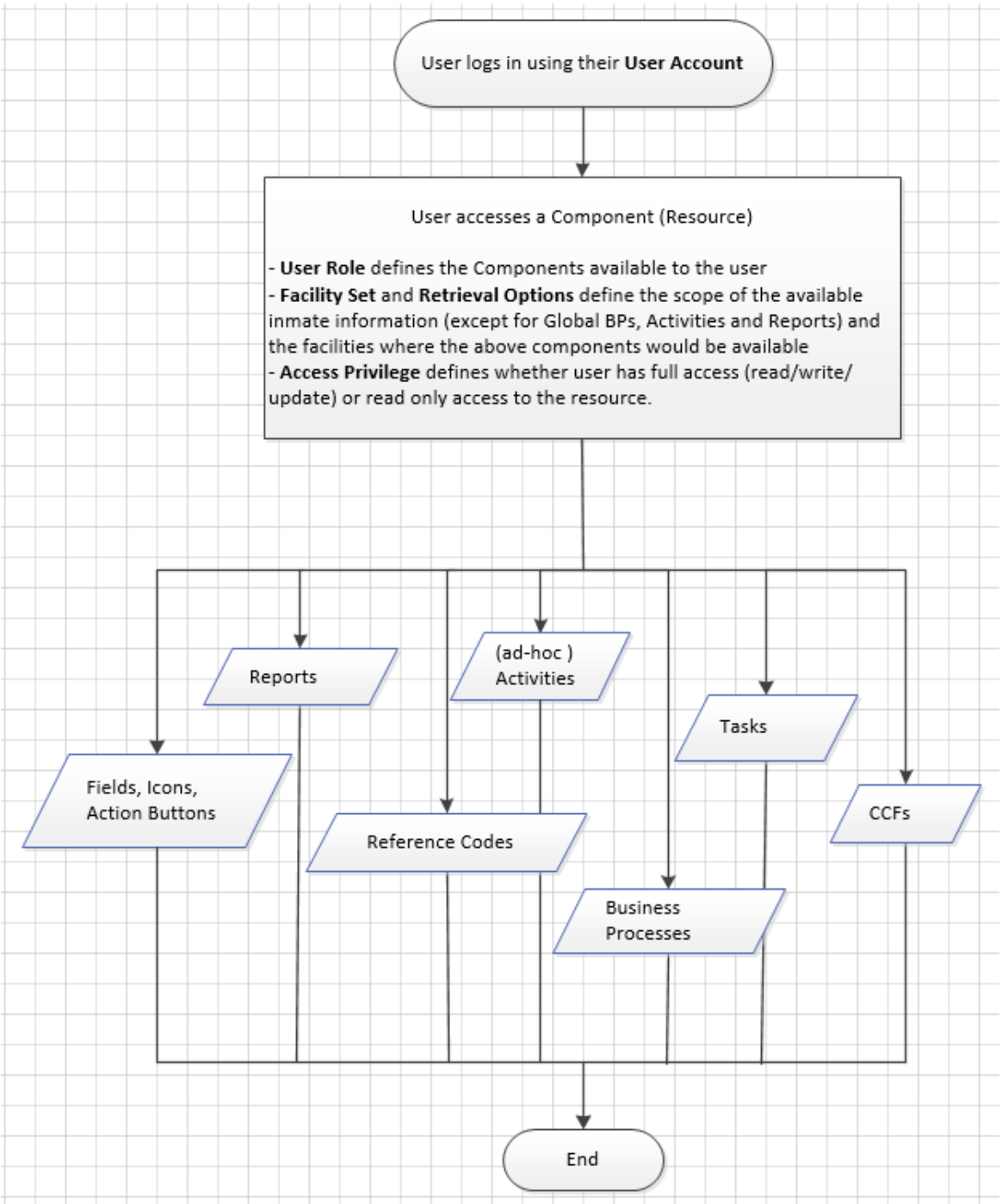
Your new password is stored once successful and the system informs you of the update.

Resource Authorization

Staff are given one or more user accounts that define what they can do (their actions), and who they are able to work with (access).

Actions: What you are able to do within the system, for example, access to resources (components).

Access: Who you can work with, for example, inmate records you are able to work with within different facilities.



Once you log in using your User Account the system checks your User Role to define the Resources that you have access to, including:

- Business Processes
- Reports
- Activities
- Reference Codes
- Task Pool, My Tasks, Manage Tasks
- Global Business Processes
- Global Activities
- Custom Fields (Admin User)
- User Accounts (Admin User)
- System Profiles (Admin User)

The system checks the Facility Set assigned to the User Account that defines the facilities where the user can access those resources, and the access type (for example, Read Only, or Read/Write/Update).

Business Processes

A user's role defines the business processes and tasks that they have access to and defines the availability of the links on menu navigation.

The Facility Set defines the facilities where users can run these business processes and tasks and provides an overall scope for inmate-based inquiry and process related searches.

Reports

A user's role defines the reports that they have access to, and the allowed reports define the availability of the links on menu navigation.

The Facility Set defines the facilities where users can run these reports, and provides an overall scope for available inmate information on reports.

Reference Domain/Reference Codes

A user's role defines the Reference Domain/Reference Codes that they have access to, and the drop-down list of reference codes only includes codes available to the user.

Note: Most Reference Codes are available to all users; the security model only defines reference domains controlled by security controls, such as Cautions.

Task Management

A user's role defines the access to **Cancel/Archive**, **Assign**, **Override Due Date**, and **Send** tasks from the Task Pool.

The Facility Set defines the facilities where users can access Manage Tasks. It provides an overall scope for available tasks in the Task Pool and Manage Tasks.

Global Business Processes

Global business processes are available to all facilities and include any business related process tasks.

Global Activities

Global activities are available to all facilities and are defined as non-business process tasks.

Global Reports

Global reports are available to all facilities and are a specific set of reports that anyone can use.

Workflow Admin Console (WAC)

The Workflow Admin Console allows you to configure operating information so that the system behavior reflects current operating conditions in a facility.

The console is used mainly by three types of users:

1. **IT System Admin:** Technical staff assigned to maintain global application settings.
   Frequency – Once or twice during initial implementation, rarely or never during operation. Can also include additional follow-ups.
   - Set up System Profiles
2. **Agency Business System Admin:** Non-technical users (typically at a head office) assigned to maintain global setup applicable to all facilities in the agency.
   Frequency – Multiple times per day during initial implementation, rarely during operation.
   - Set up reference domains/codes.
   - Customizable fields
   - Business rules
   - Ad-hoc reports
   - Menu navigation
   - User security roles and ACLs.
3. **Facility Business System Admin:** Non-technical users with manager or supervisor duties, assigned to manage a business unit for a named facility.
   Frequency – Multiple times per day, per facility.
   - Create/Maintain Organization
   - Create/Maintain Facilities
   - Create/Maintain Staff/User Accounts.
   - Create/Maintain Facility internal locations and their attributes.

The WAC covers modules such as **Classification**, **Discipline**, **Event Logs**, **Legals**, **Notifications**, **User Security**, or **Visitation** configuration.

Create/Maintain User Accounts/Roles and Facility Sets

Only an **Administrative** user (Account Type = Admin) is able to create or maintain User Accounts.

The same **Administrative** user has to be able to update the **Username** and **Password** of User Accounts, define the **Password Complexity**, the **Maximum Number of Incorrect Login Attempts**, and the **Password Expiry Policies**.

Only an **Administrative** user (Account Type = Admin) is able to create or maintain User Roles and Facility Sets, including:

- Assign/Remove Facilities to/from Facility Sets.
- Assign/Remove Resources to/from a User Role.
- Assign/Remove Retrieval Options to/from User Roles.

Regular Users can update their password according to the Password Complexity Rules.

User Roles

- **Role Name (Configurable):** The name of the role.
- **Role Type:** Defines if a user is **Regular** or **Administrative.**
- **Component:** The components (resources) the User Role has access to, for example, **Business Processes, Reports, Reference Codes**, etc.

Administrative System User
RBAC also provides extended functionality for administrative users to enable the setup and configuration of the system. They include the following roles and responsibilities:

Facility Sets

Name (Configurable): Unique name for the Facility Set.

Type (Configurable): The Facility Set type:

- Global – Set of all facilities within the agency.
- Non-Global – Any specific set of facilities within the agency.

Facility: The facilities included in the Facility Set.

Components

- **Component ID (Configurable):** The unique ID for the component.
- **Component Name (Configurable):** The descriptive name of the component.
- **Component Type (Configurable):** The component type.

Create/Maintain Facilities

Only an **Administrative** user (Account Type = Admin) is able to create or maintain Facilities.

The same **Administrative** user has to be able to maintain **Facility Internal Locations** and their attributes.

Set Up User Accounts

Only an **Administrative** user (Account Type = Admin) is able to assign a Facility Set and one or more User Roles to a User Account.

The same **Administrative** user has to be able to maintain the **User Account Assignments**.

Attributes

- **Username (Configurable):** The unique user name for a user account.
- **Password (Configurable):** The password for a given user account.
- **Locked:** A **Yes** or **No** flag denoting if the user account is locked or not.
- **Locked Date:** If the Locked flag above is Yes, then this is the date that it was locked.
- **Password Expired:** A **Yes** or **No** flag denoting if the password has expired.

Associations:

- **Person (Staff):** The staff member this user account has been created for.
- **User Role:** The roles that the user account is associated with.
- **Facility Set:** The facility set which the user account grants access to.

Set Up Reference Domains/Codes

Only an **Administrative** user (Account Type = Admin) is able to create or maintain Reference Domains and Codes used in the application.

Set Up Custom Fields

Only an **Administrative** user (Account Type = Admin) is able to create or maintain various Custom Fields.

Create/Maintain Business Rules

Only an **Administrative** user (Account Type = Admin) is able to create or maintain business rules to be applied to various modules within the application.

Set Up System Profiles

Only an **Administrative** user (Account Type = Admin) is able to update or maintain the default System Profiles.

Retrieval Options

Selection of a Facility Set

Once you have logged into Workflow before you can access the system you need to select a Facility Set first.

Note: If there is only one Facility Set available, then that is selected automatically.

If a default Facility Set is selected for this User Account (for example, in the Workflow Admin Console) it is highlighted during the login process.

When selecting a Facility Set:

- Only one Facility Set can be selected at a time.
- You can select the Facility Set any time during your session as long as you are not in the middle of performing another action (as long as another Facility Set is available).

There are two types of Facility Sets:

1. User selected type that is a set of facilities within the agency.
2. Global Facility Set that includes all facilities within the agency. Users are not able to select this Facility Set and it is only assigned to a User Role during their Account configuration.

The system then updates all available data throughout Workflow according to the selected Facility Set and the Retrieval Options associated with the User Role.

Retrieval Options determine the inmates retrieved for an activity/task within a business process. The available Retrieval Options for a Facility Set include:

Active Inmates: Inmates currently active in that Facility Set.

Inactive Inmates: All inactive inmates once part of that Facility Set.

All Inmates: Both the Active and Inactive inmates who were once part of that Facility Set, that includes:

- Current Active inmates in the Facility Set.
- Active inmates now in another Facility not in the Facility Set, but who were active in the Facility Set at some point.
- Inactive inmates who were once active in the Facility Set.

Retrieval Options Use Cases

1. Community Officer has to be able to add Case Notes for any inmate.
    a. **Role:** Community Officer
    b. **Component:** Case Note
    c. **Retrieval Option:** All Inmates

2. Trust Account personnel are required to manage the accounts for Active/Inactive inmates, even after release.
    a. **Role:** Trust Account Staff
    b. **Component:** Maintain Accounts
    c. **Retrieval Option:** All Inmates

3. Creating internal movements for inmates.
    a. **Role:** Officer
    b. **Component:** Schedule internal movements and perform internal movements.
    c. **Retrieval Option:** Active

Glossary

Term	Definition
Custom Fields (CCFs)	**Client Customizable Fields** are data elements that users can define during configuration. They can be classified as Primary or Secondary. Primary fields are viewable in a data grid, while Secondary fields are informational only.
Component	The components or resources the User Role has access to, for example, **Business Processes, Reports, Reference Codes**, etc.
Facility Set	A set of Facilities associated with a User Account.
LDAP	The Lightweight Directory Access Protocol is a set of protocols for accessing information directories.
RBAC	A role based security authorization system defined for each user logged into the system.
Reference Domains/Codes	**Reference Domains** are the name of the set and each of the values in the set are represented by reference codes. Reference domains are pre-defined as one of three types: Configurable, Non-configurable, and Partially configurable. **Reference Codes** define the data fields that call a List of Values (LOV). Usually the data displayed in these LOVs are defined by reference domains and codes.
Resources	The components or resources the User Role has access to, for example, **Business Processes, Reports, Reference Codes**, etc.
Retrieval Option	Retrieval Options determine the inmates retrieved for an activity/task within a business process.
Task Pool	The pool of tasks not yet assigned to a specific user, along with the attributes of each task.
My Tasks	The pool of tasks assigned to a specific user, along with the attributes of each task.
User Account	The unique account dedicated to a staff member granting access to Facility Sets and User Roles.
User Role	The User Roles associated with a User Account defining what Resources a user has access to.

PRE-PUBLISHING CHECKLISTS:

Generic Proofing (self-check and peer check):

You may want to keep a printout of your document template handy so that you can double check the document against the formatting in the template.

Even the most carefully written guide will have a few typos, pages that break in awkward locations, or a table of contents with incorrect page numbers.

Catching these issues and fixing them requires a trained eye. You need to know what to look for. In such times, it helps to have a checklist of issues to watch for during your proofing pass.

Here is a list of items to watch for when taking a pre-publish look at your work or that of your peers.

- *Flip through review copies and make sure all comments from reviewers were incorporated*
- *Spell check*
- *Regenerate the Table of Contents, or at least spot check the headings and page numbers*
- *Verify that the headers and footers alternate correctly*
- *Verify that the headers match the chapter titles*
- *Verify that the pages are sequentially numbered*
- *Check the copyright date to insure that it includes the current year*
- *Look for images that extend beyond the margins and adjust them, if necessary*
- *Look for images lacking clarity and reshoot or resize them*
- *Check a printout for images that don't show up due to printer errors*
- *Scan a printout for any strange characters or font-substitution issues*
- *Scan for numbered lists and ensure that they are sequentially numbered*
- *Search for any notes to the writer that haven't been removed or hidden*
- *Look for pages that break in awkward places*
- *Verify that trademark symbols are used appropriately for your products and others*
- *Verify that the appropriate cover pages or end pages have been attached, if necessary*
- *Check for images that do not match information described in the text*
- *Regenerate any cross-references to ensure they are up to date*
- *Regenerate the Index [TOC], or at least make sure page numbers are up to date*
- *Check the formatting of headers and footers on special pages, such as the cover, copyright, and first pages of chapters and verify that they match your template / conventions*
- *Check for recent convention decisions that may have been made after the document was written*

- *Look for long tables that break across pages and verify that the column headings are repeated on each page*

This list obviously isn't comprehensive; every document is different and presents unique proofing issues.

PUBLISHING CHECKLIST

- *Ensure proofing and all corrections are completed*
- *Create a PDF file*
- *Working with the PDF file, where a section contains an odd number of pages, insert a blank PDF page; this ensures an even number of pages for each section; this ensures an even number of pages in the entre PDF file; this also ensures the PDF is published for double-sided printing*
- *for guidance on placement of blank pages, see this example:*
- *http://info.syscon.net/download/attachments/230014/ILT_Property.pdf?version=1*