ramco

RAMCO AVIATION SOLUTION

VERSION 5.8

USER GUIDE

UTILITIES

ramco

©2018 Ramco Systems Limited. All rights reserved.
All trademarks acknowledged.

This document is published by **Ramco Systems Ltd**. without any warranty. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose without the written permission of **Ramco Systems Limited**.

Improvements and changes to this text necessitated by typographical errors, inaccuracies of current information or improvements to software programs and/or equipment, may be made by Ramco Systems Limited, at any time and without notice. Such changes will, however, be incorporated into new editions of this document. Any hard copies of this document are to be regarded as temporary reference copies only.

The documentation has been provided for the entire Aviation solution, although only a part of the entire solution may be deployed at the customer site, in accordance with the license agreement between the customer and Ramco Systems Limited. Therefore, the documentation made available to the customer may refer to features that are not present in the solution purchased / deployed at the customer site.

ABOUT THIS MANUAL

This manual briefly describes the basic processes and functions in Ramco Aviation Solution.

WHO SHOULD READ THIS MANUAL

This manual is intended for users who are managing the Aviation industry processes and are new to Ramco Aviation Solution.

This manual assumes that the user is familiar with the Aviation Industry nomenclatures and systems based software.

HOW TO USE THIS MANUAL

Ramco Aviation Solution provides extensive Online Help that contains detailed instructions on how to use the application. Users are suggested to use this manual for specific references, along with the Online Help. This manual contains enough information to help the users perform the basic tasks and points toward the Online Help for more detailed information.

HOW THIS MANUAL IS ORGANIZED

The User Guide is divided into 5 chapters and an index. Given below is a brief run-through of what each chapter consists of.

Chapter 1 provides an overview of the entire Utilities business process chain. The processes are explained in the remaining chapters.

Chapter 2 focuses on the Objects Attachments process.

Chapter 3 highlights on Smart Card Interface process.

Chapter 4 talks about the Dual Authentication process.

Chapter 5 focuses on Technical Document Interface process.

Chapter 6 offers insight into the LineAnywhere process to be undertaken in the Desktop Ramco Aviation system

The **Index** offers a quick reference to selected words used in the manual.

DOCUMENT CONVENTIONS

- The data entry has been explained taking into account the “Create” business activity. Specific references (if any) to any other business activity such as “Modify” and “View” are given as “Note” at the appropriate places.
- **Boldface** is used to denote commands and user interface labels.
  Example: Enter **Company Code** and click the **Get Details** pushbutton.
- *Italics* used for references.
  Example: *See Figure 1.1.*
- The @ icon is used for Notes, to convey additional information.

REFERENCE DOCUMENTATION

This User Guide is part of the documentation set that comes with Ramco Aviation Solution.

The documentation is generally provided in two forms:

- The Documentation CD in Adobe® Systems’ Portable Document Format (PDF).
- Context-sensitive Online Help information accessible from the application screens.

WHOM TO CONTACT FOR QUERIES

Please locate the nearest office for your geographical area from www.ramco.com for assistance.

content

ramco

INTRODUCTION

The business process chain, Utilities comprises of processes that extend the capabilities of Ramco Aviation Solutions by helping users to;

- Upload/maintain object/files/documents
- Maintain E-signatures
- Manage Dual authentication
- Maintain technical documents
- Interact with third party software/objects
- Maintain customized reports
- Facilitate audit

Chapter 2 of the Utilities user guide elaborates on the **Object Attachments** process, which provides the interface to upload and store objects/documents attached to any business process into a central depository, for future reference.

Chapter 3 of the Utilities user guide explains the **Smart Card Interface** process that enables electronic signature (e-sign) by users.

Chapter 4 of the Utilities user guide elaborates on the management of **Dual Authentication** signoff and Timesheet signoff in the system.

Chapter 5 Utilities user guide explains about **Technical Document Interface (TDI)** that makes external technical document systems (CMS) easily accessible to Ramco Aviation solution users, thereby providing the maintenance personnel with a single point access to refer to the required maintenance documents without having to opt for multiple document for access systems. The TDI allows you to perform the following:

Create Maintenance Change Request

The OEMs communicate the chvange notifications to fleet operators in the form of SBs and ADs. These SBs and ADs are available in SGML format. The TDI allows you to upload the SGML document to automatically create a Maintenance Change Request (MCR) in Ramco Aviation solution

View maintenance documents

Maintenance documents will be available through predefined Technical Document Systems. The TDI allows you to access the technical document systems for viewing the maintenance document details. In addition, links may be provided in the Ramco Aviation Solution screens to directly access the relevant chapters of the Technical Document Systems.

OBJECT ATTACHMENTS

This chapter explains the sub tasks involved in the **Object Attachments** process including setting parameters for uploading files and the procedure for the actual upload of files.

Typically, Aviation business like any other engineering business/industry generates documents such as task cards, agreements, contracts, work orders, engineering orders and diagrams, invoices, etc. during daily tasks/transactions. These documents become crucial means of reference at a later point of time as they hold vital information required for the continuity of the very transactions/business that created them in the past. Sizeable pieces of information held in these documents may be graphical / dynamic / movie / animation in nature. Such information is typically converted into digital format and stored along-with the entity as associated “attachments” for reference. Thus, the management of these crucial documents becomes a critical requirement impacting the effectiveness of the business. The document management process **Object Attachments** enables users to store, maintain, print, retrieve and archive documents associated with any business process in the entire Ramco Aviation application. The Object Attachments process supports documents in a range of formats including pdf, doc, xls, ppt, jpeg, wmv, etc.

These digital objects can be stored in a central repository (typically a file storage device) on upload.

2.1 SETTING PARAMETERS FOR UPLOADING DOCUMENTS

Prior to the actual upload of files, the following tasks must be

- Setting up HTTP server
- Setting up parameters for document upload

Subsequent to the above, you may upload files/documents associated with various business processes/tasks/maintenance objects into the central repository.

You must define the path for the destination folder to which files must be uploaded before the upload process. You can upload files, documents or reference information for various organization units and business components. The maximum file size and the file save option for an organization unit and business component combination must also be defined prior to upload.

1. Select the **Set Options** link under the **Object Attachments** business component. The **Set Options** page appears as shown in *Fig 2.1.*

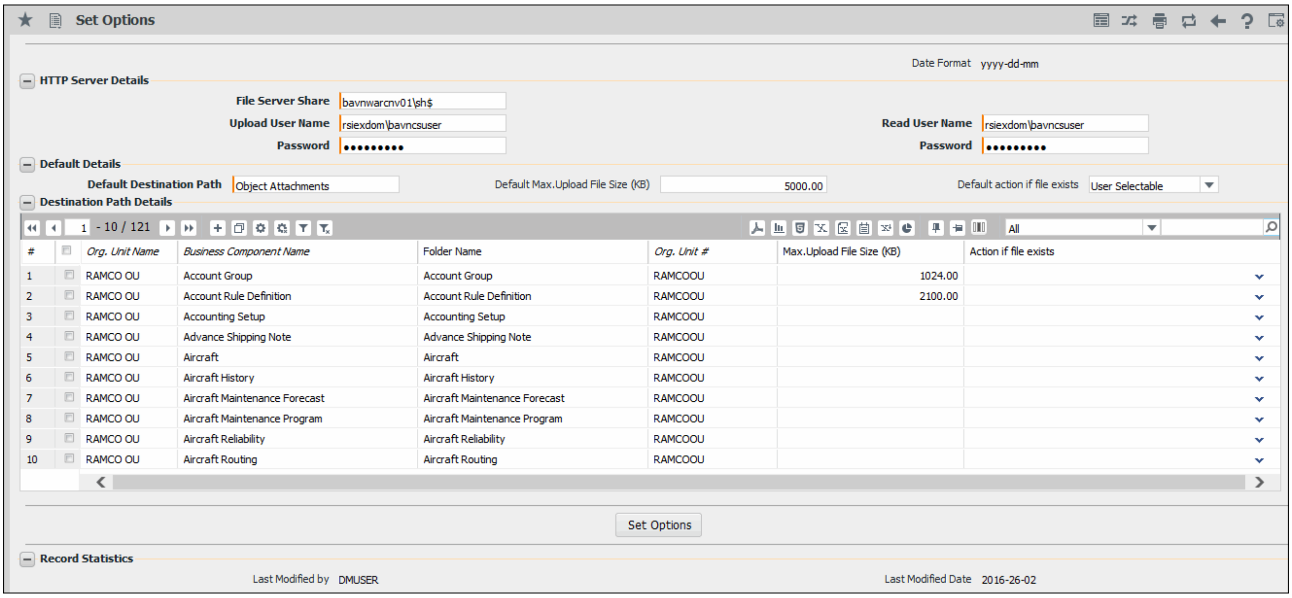


Figure 2. 1 Setting parameters for file upload

2. In the **HTTP Sever Details** group box, in the **File Server Share** field, specify the Hypertext Transfer Protocol (HTTP) server into which you want to upload files.
3. Specify **Upload User Name** and **Password** for access to the FTP server to upload files.
4. Specify **Read User Name** and **Password** for access to the FTP server to view files.
5. In the **Default Details** group box, specify the **Default Destination Path** for uploaded files. The system uploads the document or reference information in this path, if the destination path for any organization unit and business component combination is not specified by users.
6. Specify the maximum file size limit for any file that you want to upload in the **Default Max. Upload File Size (KB)** field. The system limits the size of any file for upload for any organization unit and business component combination to the size you specify here.
7. Use the **Default Action If File Exists** drop-down list box to set the default action to be performed, if a file already exists in the destination path. The system displays the following options:

   Replace – The uploaded file replaces the duplicate file in the destination folder.

- Save as New – The uploaded file is saved in a new name in the destination path.
- Warn & Abort – The uploaded file is ignored and a warning message is displayed.
- User Selectable – The system provides all the above options at the time of file upload.

The system sets the default action for file upload for any organization unit and business component combination to the action that you specify here.

In the **Destination Path Details** multiline, specify the following for organization unit and business component combination.

8. Specify the **Folder Name** where the document or reference information must be stored.
9. The maximum upload size of a file in kilobytes in the **Max. Upload File Size (KB)** field.
10. Use the **Action If File Exists** drop-down list box to set the action to be performed, if a file already exists in the destination path. The system lists the options "Replace", "Save as New", "Warn & Abort" and "User Selectable".
11. Check the box in the multiline for the records you want to save.
12. Click the **Set Options** pushbutton, to update the destination path details.

2.2 UPLOADING DOCUMENTS

You can upload documents/files attached to a maintenance object/task such as component work order, hangar work order, repair order, aircraft or component. The files/documents are uploaded into a pre-defined folder in the FTP server.

You may upload a single file or multiple files at a time. The files for upload may be sourced from a folder in the local disk or the Intranet.

1. Select the **Upload Documents** link under the **Object Attachments** business component. The **Upload Documents** page appears. *See Figure 2.2.*

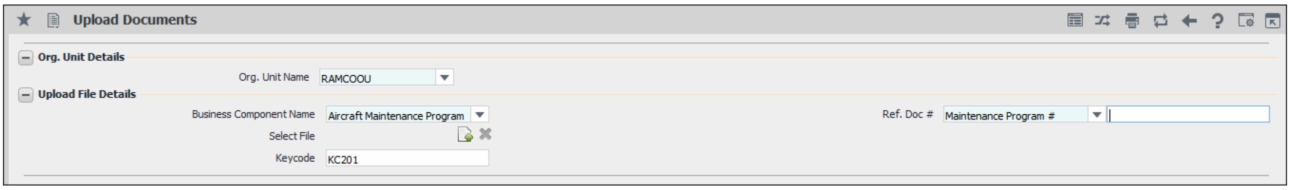


Figure 2. 2 Uploading documents

2. In the **Org. Unit Details** group box, specify the **Org. Unit Name** for which you want to upload files or reference documents.
3. In the **Upload File Details** group box, use the **Business Component Name** drop-down list box to select the business component for which you want to upload files/reference documents.
4. Use the **Ref. Doc #** drop-down list box to select the type of the reference document. The drop-down list box displays document types, such as Component Work order, Aircraft Maintenance Exe. Ref #, Eng. Doc, Goods Receipt, Maintenance Change Request, Repair Receipt, Purchase Order, Part Data Change, Repair Order, Supplier Order Based Invoice, Short Term Esc. Ref #, Engineering Service Request, Engineering Advice Note, Cycle Count Sheet #, Cycle Count Plan #, Journey Log #, Fuel/Oil Log #, etc. based on the Business Component selected. Specify the identification number of the reference document in the field alongside.
5. The system displays the **Select File** field indicating the name of the source document in the local folder or shared network.
6. Click the icon ' ' alongside the **Select File** field, to view the pop-up screen **Upload File**. *See Figure 2.3.*

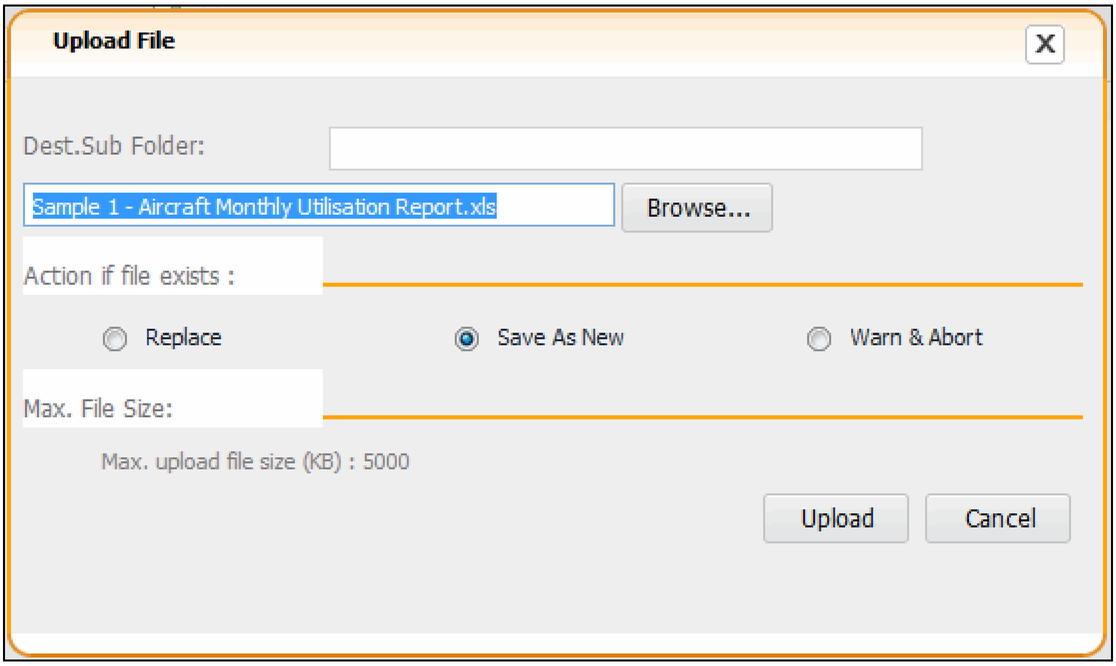


Figure 2.3 Selecting file for upload

7. Click the icon ' ' to delete the selected file.

8. Enter the **Keycode** for the document you want to upload. The system automatically generates the keycode for a document. However, you may specify your own keycode, which will overwrite the keycode allotted to the document by the system.

Uploading Files

9. In the **Upload File** pop-up screen, enter the **Dest. Sub Folder** in which the file is to be uploaded.

10. Select the **Browse** pushbutton to choose the required file from a local folder or Intranet. The file you select is displayed with the path in the "Select a File" field.

11. In the **Action if file exists** field, **s**elect one of the following radio buttons "Replace", "Save as New", "Warn & Abort", to select the action to be performed, if a file already exists in the destination path. The system displays **Max. upload file size (KB)** specified for the business component and organization unit combination.

13. Select the **Upload** pushbutton to save the selected file in the destination path.

14. Click the **Cancel** button to cancel the file upload process.

2.3 DELETING / VIEWING DOCUMENTS

You can search and retrieve specific documents/files attached to an entity from a specific business component, such as Component Work Order, Repair Order, AME or Loan & Rental Order and proceed to delete the file or view the contents. You may delete multiple files at one go though you can view only a single. File at a time.

1. Click the **Delete/View Associated Doc. Attachments** link under the **Object Attachments** business component. The **Delete/View Associated Doc. Attachments** page appears. *See Figure 2.4.*

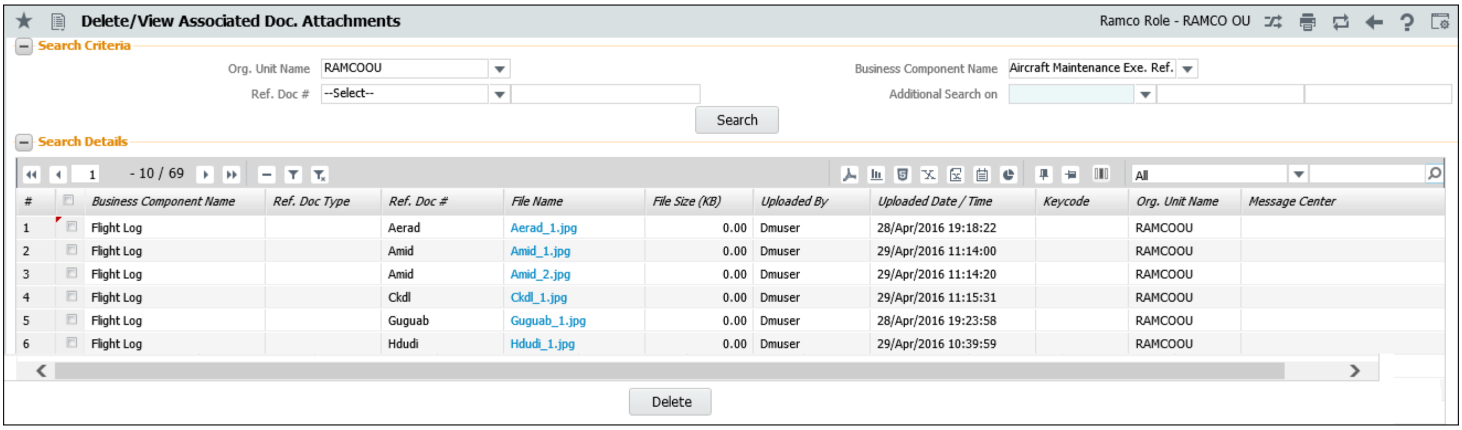


Figure 2. 4 Selecting file for upload

2. Enter some or all the fields in the search criteria, to retrieve files that you wish to delete or view.

Viewing files

1. Click the hyperlinked file name in the multiline.

Deleting files

2. Select the files in the multiline that you want to delete.
3. Click the **Delete** pushbutton.

Note: The 'Delete' pushbutton is available to only the login users who have access rights to the "Delete/View Associate Doc. Attachments" activity.

ELECTRONIC SIGNATURE

Electronic signature (e-signature) is the online equivalent of a handwritten signature of an individual. E-signature is affixed to or logically associated with a record/document, to indicate approval or authentication. An e-signature authenticates the creation, verification, approval or audit of electronic documents (e-documents) by an individual with the requisite authority.

An e-signature must possess attributes that guarantee the legitimacy of a handwritten signature. However, any information that identifies an individual found in an electronic/ computer system may not constitute a signature. For example, the entry of an individual's name in an electronic/computer system may not constitute an electronic signature.

Regulatory organizations have specified acceptable forms of e-signature. These include digital signature, digitized image of a paper signature, a typed notation, an electronic code or any other unique form of individual identification that can be used as a means of authenticating a record, record entry or a document.

The **Smart Card Interface** offered by Ramco enables an individual who intends to e-sign on e-documents to create his/her e signature. The Ramco e-signature solution is based on the smart card-based authentication technique.

When a user logs into Ramco Aviation Solution using a user name and password, the system verifies the user credentials and if found valid lists activities for which the user has been granted access rights. This constitutes the first-level of authentication.

After gaining access to Ramco Aviation Solutions, users typically navigate to activities of their choice and perform transactions such as creating, editing, authorizing, canceling, reversing and viewing records. Not all these transactions may require authentication of users. Typically, transactions such as authorizing, canceling or reversing of records mandatorily require an e-signature of the user. This constitutes the next level of authentication. The system validates the e-signature of the user and then routes the record to the next stage of the workflow/process. Let us take the instance of an employee who could apply for leave using the electronic/computer system. The leave application is routed to the designated supervisor of the employee, who can access and stamp approval on the leave application by inserting his/her e-signature.

The completion of any transaction/task that requires e-signature of an individual is linked to smart card-based authentication. The actual procedure of e-signature works in the following way.

The designated individual is issued a smart card that stores the personal identity (User ID) and personal identification number (PIN).

When the individual is required to sign a transaction/record electronically, he/she inserts the smart card into the smart card reader connected to the client computer and enters the user ID and PIN.

Thereafter, the system validates the user ID and PIN specified by the individual with that stored in the card.

If found valid, the system processes the transaction or routes it to the subsequent stage in the workflow. As users are in possession of their smart cards and the PIN is known exclusively known to them, the second level of authentication is deemed to be ultimate.

The e-signature process facilitated by Smart Card Interface business component involves the following tasks.

Configuration of smart cards
Enrollment of users
Administration of smart cards
Smart card issue

For information on client installation and smart card reader setup, refer to the Smart Card Interface – User Installation Guide.

Typically, the Smart Card Interface process in an organization requires two roles: Administrator and User

The Electronic Signature Administrator who enrolls users, issues cards, configures and manages smart card system.

Note: All the tasks in this process must be performed by administrators only.

The Electronic Signature User who uses the e-signature on e-documents.

Note: Users are granted access rights to components/activities that are enabled for electronic signature. Refer to the Annexure for a list of business components / activities / functions enabled for electronic signature.

3.1 CONFIGURATION OF SMART CARD INTERFACE

You can configure Smart Card Interface at the following levels:

- Installation: Enabling the smart card interface for all the applicable user interfaces across all the organization units and business components.
- Component: Enabling the smart card interface only for specific business components of each organization unit.
- Function: Enabling the smart card interface only for specific activities/functions in specific components.

1. Select the **Smart Card Configuration** link under the **Smart Card Interface** business component. The **Smart Card Configuration** page appears. *See Figure 3.1*.

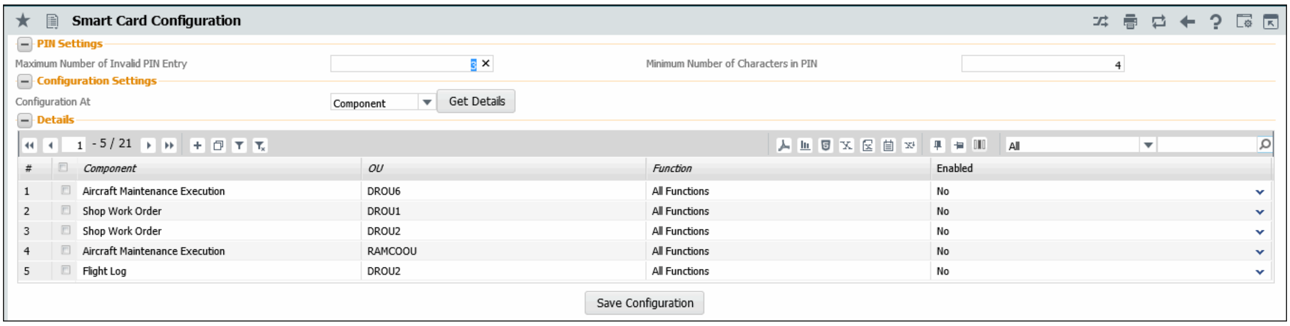


Figure 3.1: Configuring Smart Card process

In the PIN Settings group box, specify the following:

2. The maximum number of incorrect PIN entries that a user can make when inserting his/her e-signature in an e-document/activity/function in the Maximum Number of Invalid PIN Entry.

   Note: The number of wrong PIN entries must be greater than 0 and less than 8.

3. The minimum size of a PIN in the Minimum Number of Characters in PIN. The number must be greater than '0' and less than '9'.

4. In the **Configuration Settings** group box, use the **Configuration At** drop-down list box to select the level at which **Smart Card Interface** must be enabled.

5. Select the **Get Details** pushbutton. The system retrieves all the business components, organization units and functions that enable **Smart Card Interface** in the multiline.

6. In the multiline, use the **Enabled** drop-down list box to enable or disable the Smart Card Interface for the business component, OU (organization unit) or function.

7. Click the Save Configuration pushbutton.

   Note: The system sets the Enabled field to "Partial", if 1) The Configuration At field is set to "Installation" and Smart Card Interface is not enabled for some of the business components. 2) The Configuration At field is set to "Component" and the Smart Card Interface is not enabled for some of the functions in the business component. Enrollment of users

3.1.1 ENROLLMENT

Smart Card Interface administrators can enroll users to enable them to use their e-signature.

You can also temporarily stop a user from using his/her e-signature for a specific function within a business component.

1. Select the **User Enrollment** link under the **Smart Card Interface** business component. The **Smart Card User Enrollment** page appears. *See Figure 3.2*.

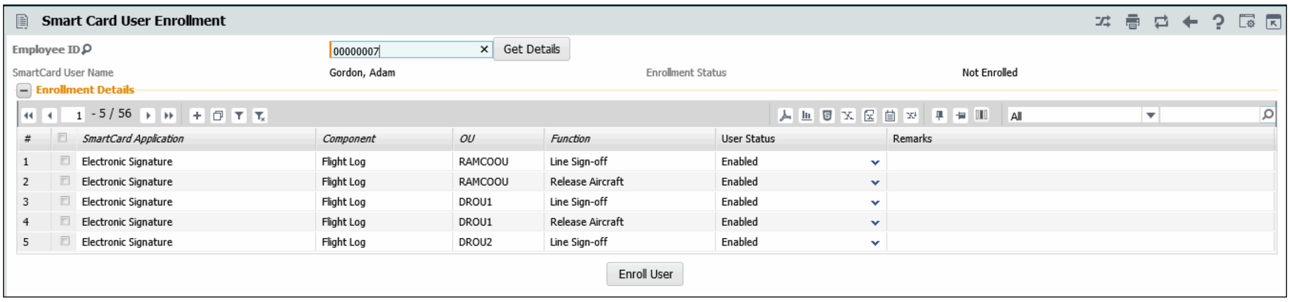


Figure 3.2: Enrolling users of smart cards

2. Specify the **Employee ID** of the Smart Card user.

3. Select the **Get Details** pushbutton to retrieve details of the specified Smart Card Interface user, if available.

In the **Enrollment Details** multiline,

4. Set the **User Status** to “Enabled”, to enable the employee to e-sign the function in the business component/OU.

5. Enter any **Remarks** on user enrollment.

To restrict the user temporarily from e-signing in the application

6. Set the **User Status** to “Hold”.

7. Enter **Remarks** on the reasons for withholding the user.

8. Click the **Enroll User** pushbutton to save the new information.

3.2 ISSUING SMART CARDS

You can issue smart cards to employees who are enrolled for e-signature. You can issue new smart cards, or reissue existing smart cards that were earlier used by other users. You can also set the expiry date for the smart card and specify the application for which the smart card must be used.

Before you start issuing smart cards, ensure that the smart card reader is connected to the computer and a new smart card is inserted. For more details on smart card reader installation, refer to the “Smart Card Interface-User Installation Guide”.

1. Select the **Smart Card Issue** link under the **Smart Card Interface** business component. The **Smart Card Issue** page appears. *See Figure 3.3.*

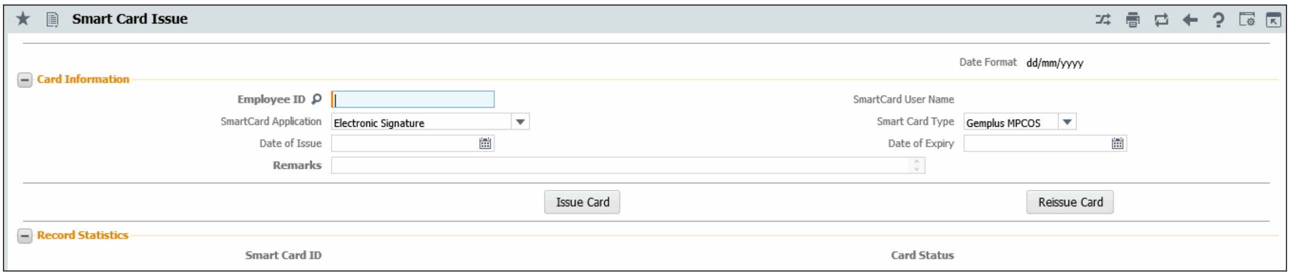


Figure 3.3: Issuing smart cars to e-signatories

2. In the **Card Information** group box, specify the **Employee ID** of the user to whom you want to issue the smart card.
3. Click the **Lens** icon positioned next to the **Employee ID** field, to retrieve the smart card user ID. Refer to the topic “Searching for smart card user IDs”, to know more on retrieving smart card user ID.
4. Set the **Smart Card Application** field to “Electronic Signature”.
5. Select the **Smart Card Type**.
6. Specify the date on which the smart card is issued, in the **Date of Issue** field.
7. Specify the date on which the smart card expires, in the **Date of Expiry** field.
8. Click the **Issue Card** pushbutton to issue a new smart card to the employee.

The system issues the smart card and assigns a unique ID to the smart card.

Note the following rules applicable to smart cards: 1) You can modify the PIN using the “Smart Card – Change User PIN” option provided in the “Start - Programs” menu. Refer to the topic “Changing user PIN in Smart Card Interface” for more details. 2) An employee can have any number of smart cards for a given application. Before issuing an additional card for an employee, all the existing smart cards issued to the employee must be set to “Blocked” status. 3) At any point of time, only one smart card can be active for usage in the application.

Reissuing existing smart card

9. Click the **Reissue Card** pushbutton to reissue an existing smart card.

The system will reissue the card to the selected employee, and assign a new smart card ID.

Note: You cannot reissue the smart cards that are in “Blocked” or “Cancelled” status to other employees.

3.3 ADMINISTRATION OF THE SMART CARD INTERFACE PROCESS

Administration of smart cards involves the following tasks,

- Configuring the Smart Card Interface and enabling business components/functions for the smart card interface.
- Settings the maximum number of invalid PIN entries and the minimum number of characters in a PIN.
- Enrolling users for Smart Car Interface and enabling them for components/activities
- Issuing smart cards to enrolled users

Further, administration of smart cards also includes activating, blocking, locking, unlocking, canceling and modifying the expiry date of smart cards on a need basis. You can activate, block, lock, unlock, and cancel smart cards by using the User Status attribute of the smart card. Similarly, you can reset the Date of Expiry of the card to extend the validity of the smart card.

1. Select the **Smart Card Administration** link under the **Smart Card Interface** business component. The **Smart Card Administration** page appears. *See Figure 3.4.*

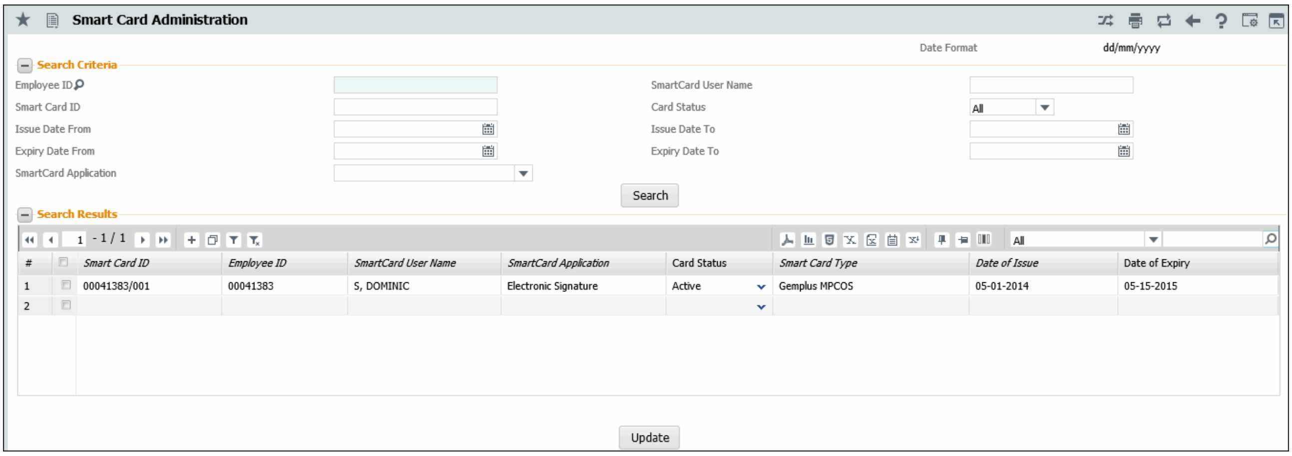


Figure 3.4 Administering smart card process

2. Specify the **Search Criteria**, and click the **Search** pushbutton to retrieve the smart card details based on the search criteria.

To lock/unlock smart cards

3. Set the **Card Status** field in the **Search Results** multilines to “Lock” to lock smart cards that are in “Active” status.
4. Set the **Card Status** field to “Unlock” to unlock smart cards that are in “Locked” status.

To block smart cards

5. Set the **Card Status** field in the **Search Results** multiline to ”Blocked” to block smart cards, which are in “Active”, “Locked” or “Unlock” status.

   @ *Note: You cannot block those smart cards that are in “Cancelled” status.*

To activate blocked or cancelled smart cards

6. Set the **Card Status** field in the **Search Results** multiline to ”Active”, to activate smart cards, which are in “Blocked” or “Cancelled” status.

To mark returned smart cards

7. Set the **Card Status** field in the **Search Results** multiline to “Returned”, to indicate that the smart card is returned by the user.

*Note: The returned smart card can be issued as a new card to another employee, in the **Smart Card Issue** activity.*

To cancel smart cards

8. Set the **Card Status** field in the **Search Results** multiline to "Cancelled", to cancel the smart cards that are in "Active", "Blocked", "Locked" or "Unlock" status.

To set / reset expiry date

9. Specify the Date of Expiry for the smart card.

To save details

10. Click the Update pushbutton, to save the modified details.

3.4 AFFIXING E-SIGNATURE IN E-DOCUMENTS/RECORDS/ FUNCTIONS

The e-signature process for end users/signatories would be as follows:

The smart card issued to a user will have the default Personal Identification Number (PIN) in it.

The user may change the default PIN to another PIN of his/her choice prior to using the smart card for e-signatures. (The Smart Card –Change User PIN screen facilitates changing the user PIN.)

The e-signature process begins with the launch of the **User Authentication** page. Henceforth, the user must undertake the following procedure for the successful completion of any activity/function that requires e-signature.

- The **User Authentication** page appears when the user clicks the relevant pushbutton in an application page (activity/function) enabled for e-signature.
- The user inserts the smart card into the Smart Card reader attached to the client system and types the PIN in the.
- **User Authentication** page. The system validates the PIN entry against the user ID and the PIN stored in the card. The transaction is processed / completed, if the validation is successful.

3.4.1 USER AUTHENTICATION

In a Ramco Aviation Solutions page, when you click on a pushbutton (task), which is enabled for e signature, the User Authentication page appears.

1. Enter your **Personal Identification Number (PIN)** for user authentication.
2. Click the **OK** pushbutton.

The entered PIN is validated against the PIN stored in the smart card and the transaction is completed on successful validation. On successful authentication, the system displays the message “Sign-Off Recorded successfully”. If an invalid PIN is entered, the system displays the error message “Incorrect Secret Code Submission” and the Electronic Signature cannot be completed.

3. Click the **Close** pushbutton to exit the page.

3.4.2 E-SIGNATURE AUTHENTICATION FAILURE

The user authentication can fail because of the following reasons:

- Inserting a smart card not issued to the user.
- Inserting the right smart card, but entering a wrong PIN.
- Inserting a smart card that is blocked, locked, cancelled or expired.

3.4.3 CHANGING USER PIN

The smart card issued to users has a default Personal Identification Number (PIN) that can be changed to a code of their choice, before using it for Electronic Signature. The “Smart Card –Change User PIN” screen facilitates changing the user PIN in the smart card interface.

1. Select the Smart Card – Change User PIN option in the Start – Programs menu. The Smart Card – Change User PIN page appears. See Figure 3.5.

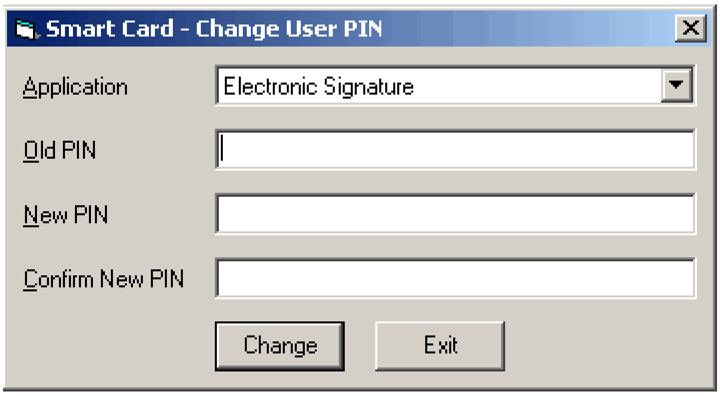


Figure 3.5 Changing user PIN in smart card interface

2. Insert the smart card into the smart card reader.
3. Select **Electronic Signature** in the Application field.
4. Enter the OLD PIN of the smart card.
5. Enter the New PIN for the smart card.
6. Repeat the new PIN value in the Confirm New PIN field.

    Note: The system does not differentiate between uppercase and lowercase letters in the Personal Identification Number (PIN).

7. Click the Change pushbutton.

The system replaces the old PIN with the new PIN on confirmation.

8. Click the Exit pushbutton to exit the page

3.5 RETURNING SMART CARD BY USER

You can record the return of smart cards by users for various reasons such as change of department or role as a result of which they may no longer require the smart card or to acquire a new smart card. Cessation of association with the organization is another common reason for return of smart cards by employees.

Return of smart cards facilitates the reuse of these cards. Subsequent to the return of a smart card, the same card can be issued to another smart card user.

3.5.1 RECORDING RETURN OF SMART CARD

1. Select the **Smart Card Return** link under the **Smart Card Interface** business component. The **Smart Card Return** page appears. *See Figure 3.6*.

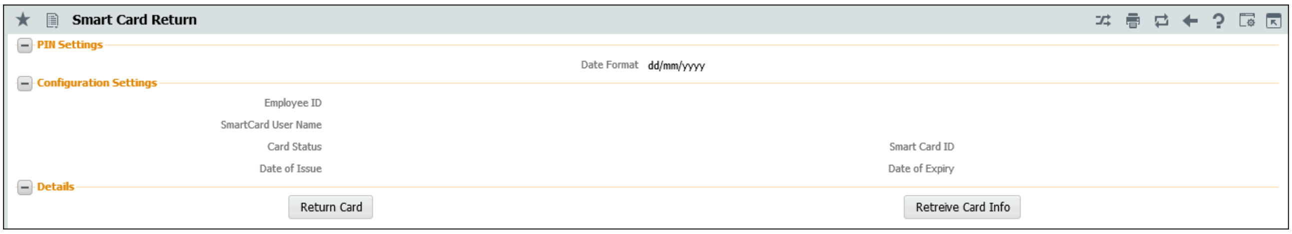


Figure 3.6 Recording return of smart card

2. Insert the smart card returned by the user into the Smart Card reader.
3. Click the **Retrieve Card Info** pushbutton to display details of the smart card from the Smart Card reader. The **Configuration Settings** group box displays smart card details.
4. Verify details of the smart card and ensure that the smart card is the one that is returned by the employee.
5. Click the **Return Card** pushbutton to indicate the return of the smart card.

3.6 TROUBLESHOOTING USER AUTHENTICATION PROBLEMS

Check for the following to avoid problems arising during user PIN authentication:

- The smart card client installation and the Internet Explorer (IE) settings.
- The smart card is inserted in the right direction in the smart card reader and the reader cable is inserted into the computer.

> *Note: For more details on smart card interface installation, refer to the "Smart Card Interface-User Installation Guide".*

The e-signature is carried out using the smart card issued to the user.

The Personal Identification Number (PIN) is entered correctly.

> *Note: If you enter a wrong PIN for more than the configured number of times, the smart card automatically gets into "Locked" status. Refer to the topic "Unlocking locked smart cards", for more details on unlocking the locked smart cards.*

The Date of Expiry of the smart card. Contact the administrator to extend the expiry date for the smart card.

The User Status of the smart card. The User Status must not be "Cancelled", "Blocked". Or "Help". Contact the administrator to activate a smart card that is in "Cancelled" or "Blocked" status.

How to block and activate smart cards

A smart card is blocked under the following circumstances:

- When the card is lost or misplaced.
- When more than one smart card is issued to an employee for e-signature.

The administrator must be contacted, who will set the User Status of the smart card to "Blocked" using the Smart Card Administrator activity. The administrator sets the User Status of the smart car to "Active" in the same activity, to enable the card fro e-signature once again.

How to cancel and activate smart cards

When a smart card is permanently lost or damaged, the User Status of the smart card is set to "Cancelled". Contact the administrator to set the User Status of the cancelled smart card to "Active", before using it for e-signature.

How to unlock locked smart cards

When a user tries to enter an invalid PIN for more than the configured number of times, the system locks the card automatically for security reason.

The administrator has to be informed, to unlock the card. The PIN of the unlocked card will be reset to the default PIN. Before the user can use the card again, the PIN must be changed using the Change User PIN screen.

How to extend the validity of smart cards

A smart card that has expired cannot be used any more for e-signatures. The administrator must be contacted, to extend the expiry date for the smart card.

How to return smart cards

When a user no longer needs the smart card, he/she must surrender the smart card to the administrator. The administrator sets the status of the smart card to "Returned". The returned smart card can be reused, and issued as a new card to another employee.

3.6.1 PREREQUISITES FOR E-SIGNATURE USING SMART CARD INTERFACE

- The smart card reader must be attached to the client system and configured to Ramco Aviation Solutions
- The smart card users must possess smart cards.
- The activities/functions that mandate e-sign must be enabled for smart card.
- The employees must have access rights to activities/functions that require them to e-sign, for completing the transaction

3.7 ANNEXURE

E-signature enabled user-actions in activities

Ramco Aviation Solution – Aircraft Maintenance Execution business component

Activity	Function/task/pushbutton
Record Aircraft Maintenance Execution Details	Record Sign-Off
Record Aircraft Maintenance Execution Details	Record Sign-Off & Completion
Record Aircraft Maintenance Execution Details	Sign-Off
Record Aircraft Maintenance Execution Details	Void Sub Task
Record Aircraft Maintenance Execution Details	Create / Edit CoM
Record Aircraft Maintenance Execution Details	Confirm CoM

Ramco Aviation Solution - Shop Work Order business component

Activity	Function/task/pushbutton
Record Shop Execution Details	Sign-Off Tasks
Record Shop Execution Details	Sign-Off
Record Shop Execution Details	Void Sub Task
Record Shop Execution Details	Create / Edit CoM
Record Shop Execution Details	Confirm CoM

DUAL ATHENTICATION

Dual authentication entails an additional level of verification over and above the authentication essential for logging into the Ramco Aviation suite.

An organization can make successful Dual Authentication of employees' mandatory for performing critical tasks, such as task signing off, certificate issue or task annulment.

To make Dual Authentication operational, you must complete the following tasks:

Configure Dual Authentication: This task helps to setup the Dual Authentication process. You may also disable the process anytime, if not required in the organization. Dual authentication types can be:

Login Password: Requires the employee to provide login password to be able to perform specific tasks.

PIN: Requires the employee to provide PIN to be able to perform specific tasks.

Login Password and PIN: Requires the employee to provide login password as well as PIN to be able to perform specific tasks.

Set/Change PIN: Dual or second-level authentication can be set for specific employees for execution of certain crucial jobs, such as Administer Dual Authentication Approve and Print Part Tags

Approve and Print Cert. of Maintenance

Approve and Print Cert. of Conformity o Approve and Print Cert. of Calibration o Task Sign-off

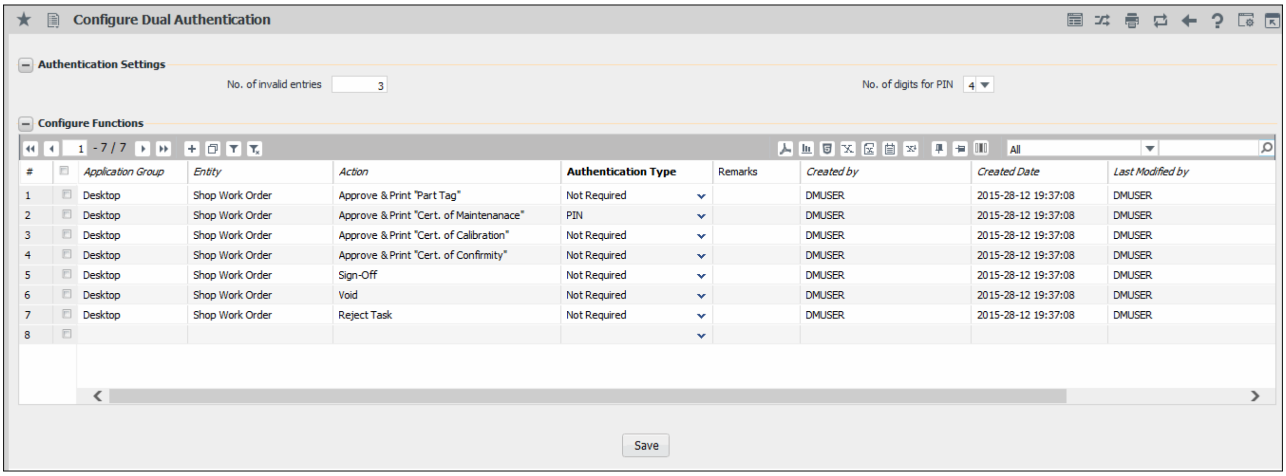
Reject Task

Void Task

Administer Dual Authentication: Typically, Security administrators grant Dual Authentication facility to mechanics to enable them to perform crucial tasks. This task can be used to reset PIN of locked/inactive employee accounts or inactivate Dual Authentication of employees.

4.1 CONFIGURING DUAL AUTHENTICATION

1. Select the **Configure Dual Authentication** link under the Smart Card Interface business component. The "Configure Dual Authentication" page appears. *See igure 4.1.*



Configure Dual Authentication

Authentication Settings

No. of invalid entries 3

No. of digits for PIN 4

Configure Functions

1 - 7 / 7

All

#		Application Group	Entity	Action	Authentication Type	Remarks	Created by	Created Date	Last Modified by
1		Desktop	Shop Work Order	Approve & Print "Part Tag"	Not Required		DMUSER	2015-28-12 19:37:08	DMUSER
2		Desktop	Shop Work Order	Approve & Print "Cert. of Maintenanace"	PIN		DMUSER	2015-28-12 19:37:08	DMUSER
3		Desktop	Shop Work Order	Approve & Print "Cert. of Calibration"	Not Required		DMUSER	2015-28-12 19:37:08	DMUSER
4		Desktop	Shop Work Order	Approve & Print "Cert. of Confirmity"	Not Required		DMUSER	2015-28-12 19:37:08	DMUSER
5		Desktop	Shop Work Order	Sign-Off	Not Required		DMUSER	2015-28-12 19:37:08	DMUSER
6		Desktop	Shop Work Order	Void	Not Required		DMUSER	2015-28-12 19:37:08	DMUSER
7		Desktop	Shop Work Order	Reject Task	Not Required		DMUSER	2015-28-12 19:37:08	DMUSER
8									

Save

Figure 4.1 Configuring dual authentication

4. In the **PIN Settings** group box, enter **No. of invalid Entries** to indicate the number of times a user is allowed to input incorrect PIN before the account gets locked and becomes inaccessible.
3. Use the **No. of digits for PIN** drop-down list box to specify the number of digits comprising PIN.
5. In the **Configure Functions** multiline, use the **Authentication Type** drop-down list box to select the type of authentication mandated for task signoff and issue of CoM. The drop-down list box displays: Not Required, Login Password, Login Password and PIN and PIN.

   Note: To disable the Dual Authentication process in the organization, set the authentication type as "Not Required".

5. Click the **Save** pushbutton to save details.

4.2 MAINTAINING PIN OF USERS

1. Select the **Set/Change PIN** link under the **Smart Card Interface** business component. The **Set/Change PIN** page appears. *See Figure 4.2.*

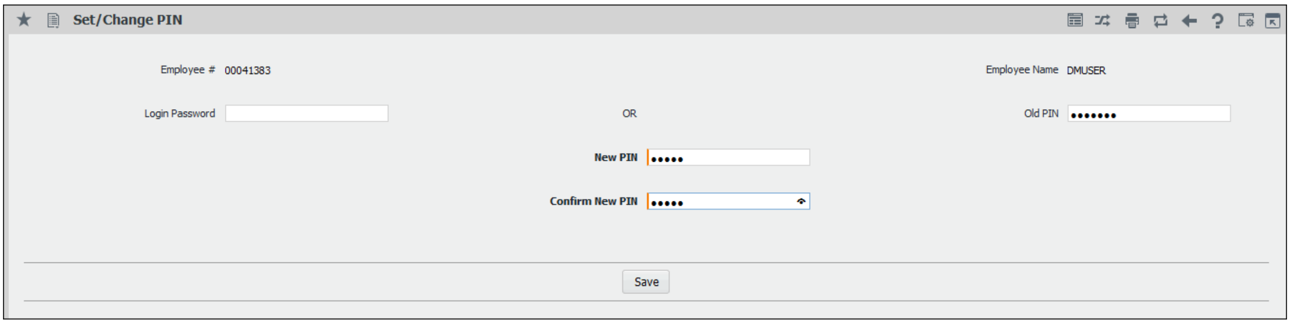


Figure 4.2 Maintaining PIN

2. Enter **Login Password** for the user.
3. Alternatively, enter **New PIN** for the employee.
4. Enter new PIN again in **Confirm New PIN** to validate.
5. Enter **OLD PIN**.

*Note: You must specify either **Old PIN** or Login **Password**.*

4.3 ADMINISTERING PIN

1. Select the **Administer Dual Authentication** link under the Smart Card Interface business component. **The Administer Dual Authentication** page appears. *See Figure 4.3.*

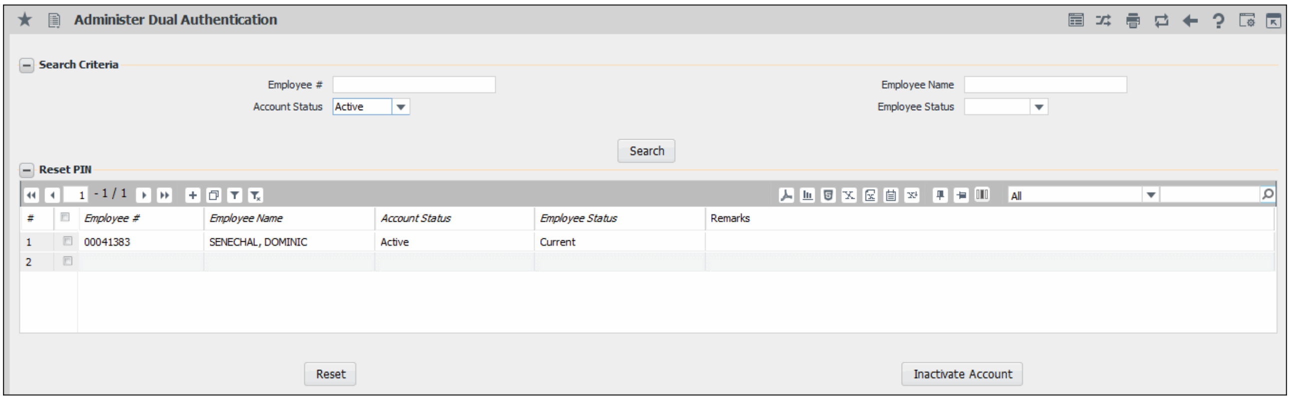


Figure 4.3 Administering PIN

2. Specify **Search Criteria** to retrieve employees for whom you wish to grant or prohibit Dual Authentication.

3. Click the **Search** pushbutton. The employees matching the search criteria are retrieved in the multiline.

4. In the multiline, enter **Remarks** for employees those who require PIN to be reset or account to be inactivated.

Activating Dual Authentication

5. Select the employee record in the multiline and then click the **Reset PIN** pushbutton.

> *Note: On reset of PIN, Account Status of the employee becomes 'Active' from 'Inactive' or 'Locked'. Now, you can reset PIN of the employee in the Set/Change PIN activity.*

Inactivating Dual Authentication

6. Select the employee record in the multiline and then click the **Inactivate Account** pushbutton.

> *Note: The employee Account Status becomes 'Inactive'.*

Dual authentication procedure

7. During execution of tasks that require dual authentication, the **User Authentication** window opens up to display the Employee information. See Figure

8. Based on **Authentication Type** set for the Application Group, Entity and Action combination in the **Configure Dual Authentication** activity, you are required to enter either **Login Password** or **PIN** or **both** to proceed with task signoff and Issue of CoM.
9. Click the **Save** pushbutton. On successful authentication, the system executes the pushbutton (for example, Task Sign Off or Issue CoM) task.

4.4 ANNEXURE

Dual Authentication enabled user-actions in activities

Ramco Aviation Solution – Aircraft Maintenance Execution business component

Activity	Function/task/pushbutton
Record Aircraft Maintenance Execution Details	Task Sign-Off
Record Aircraft Maintenance Execution Details	Task Void
Record Aircraft Maintenance Execution Details	Bulk Sign-off

TECHNICAL DOCUMENT INTERFACE

Aircraft Original Equipment Manufacturers (OEMs) such as Boeing and Airbus provide guidelines for the maintenance and upkeep of aircraft. These guidelines are made available to the fleet operators and aircraft maintenance companies in electronic digitized form. The guidelines cover comprehensive documents like Aircraft Maintenance Manuals (AMMs), Illustrated Parts Catalogues (IPCs) and intermediate directives like Service Bulletins (SBs) and Airworthiness Directives (ADs). Usually aircraft maintenance personnel are provided access to the maintenance documents through the OEM's Technical Document Systems. For example, Airbus provides its maintenance documents through Airnav / ADOC Navigator while Boeing provides its maintenance documents through PMA and MyBoeingFleet.com. Similarly, independent third party document management systems such as "Jouve" and "Enigma", which host the OEM documents, can also be used.

The **Technical Document Interface** business process comprises the **Set Tech Doc System Options,** and **View Technical Documentation** activities.

The **Set Tech Doc System Options** activity allows you to set options for accessing the Technical Document Systems.

The **View Technical Documentation** activity invokes the Technical Document System for viewing maintenance documents.

5.1 SET TECH DOC SYSTEM OPTIONS

The maintenance documents provided by the Original Equipment Manufacturers (OEMs) are made available through external Technical Document Systems. This activity allows you to set the options for connection information and authentication for accessing the technical document systems. You can select a particular technical document system and map the various manufacturers whose source documents must be viewed through the selected technical document system.

5.1.1 SETTING OPTIONS FOR TECHNICAL DOCUMENT SYSTEM

1. Select the **Set Tech Doc System Options** link under the **Technical Document Interface** business component. The **Set Tech Doc System Options** page appears. *See Figure 5.1.*

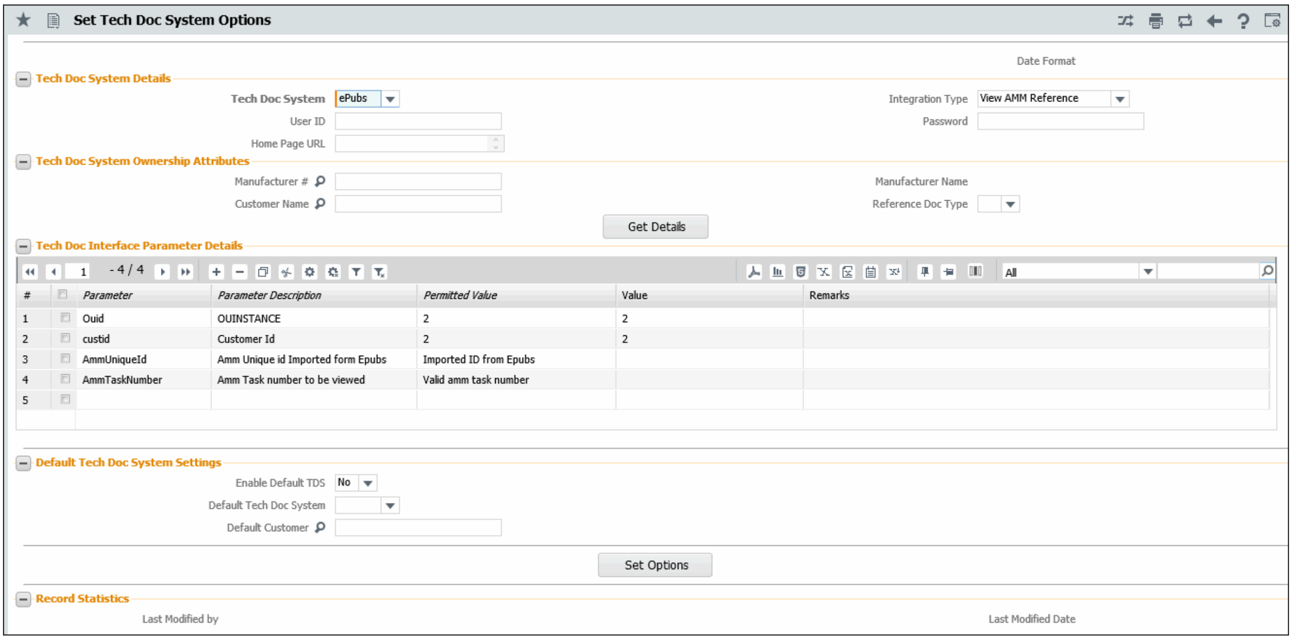


Figure 5.1 Setting options for Technical Document System

2. In the **Tech Doc System Details** group box, select the **Tech Doc System** as “Jouve”, “Airnav” or “ePubs”, through which you wish to view the source document details.

3. Select the **Integration Type** of the Tech Doc System with the Maintenance & Engineering Application. The system lists the options “View AMM Reference” and “View Task Card” if the Tech Doc System is set as “Airnav” or “Jouve”. If the Tech Doc System is set as “ePubs”, the system lists the options “View AMM Reference”, “View Task Card” and “Print Task Card”.

4. Enter the **User ID** and **Password** for accessing the technical document system.

5. Enter the **Home Page URL** indicating the URL of the document which the user intends to view. In the **Tech Doc System Ownership Attributes** group box,

6. Enter the **Manufacturer #** and **Manufacturer Name** whose source document details must be viewed through the selected technical document system.

7. Enter the login ID of the customer, using which the Tech Doc System can be viewed, in the **Customer Name** field.

8. Use the **Reference Doc Type** drop-down list box to specify the type of the reference document as “AMM”.

9. Click the **Get Details** pushbutton, to retrieve the details (if any) for the selected technical document system. On clicking the **Get Details** pushbutton, the system automatically retrieves the following details for the selected “Tech Doc System”, in the **Tech Doc Interface Parameter Details** multiline:

- Parameter - The parameter specific to the Tech Doc System.
- Parameter Description **-** The description of the parameter.
- Permitted Value **-** The permitted value of the parameter. If the Tech Doc System is selected as "Airnav" and the
- Integration Type is selected as "View AMM Reference", the system displays the string **Enter '1' for 'True' and '0' for 'False'** for the parameters "Force" and "Open Administrator".

10. Enter the **Value** defined for the parameter.
11. Enter any additional **Remarks** pertaining to the technical document system. In the **Default Tech Doc System Settings** group box,
12. Use the **Enable Default TDS** drop-down list box and select "Yes" to specify whether the technical document must be defaulted on launch of the page or not. Otherwise select the option "No".
13. Select the **Default Tech Doc System** as "Jouve", "Airnav" or "ePubs".
14. Enter the name of the **Default Customer.**
15. Click the **Set Options** pushbutton to update the options for the technical document system.

5.2 VIEW TECHNICAL DOCUMENTATION

Maintenance documents provided by the Original Equipment Manufacturers (OEMs) will be available through the technical document systems. This activity allows you to view the source documents by invoking the technical document system set for the manufacturer in the **Set Tech Doc System Options** activity. You can select a manufacturer and launch the corresponding technical document system for viewing the source document details.

5.2.1 VIEWING MAINTENANCE DOCUMENT DETAILS

Note: The manufacturer must have been mapped to a technical document system in the "Set Tech Doc System Options" activity.

1. Select the View Technical Documentation link under the Technical Document Interface business component. The **View Technical Documentation** page appears. *See Figure 5.2.*

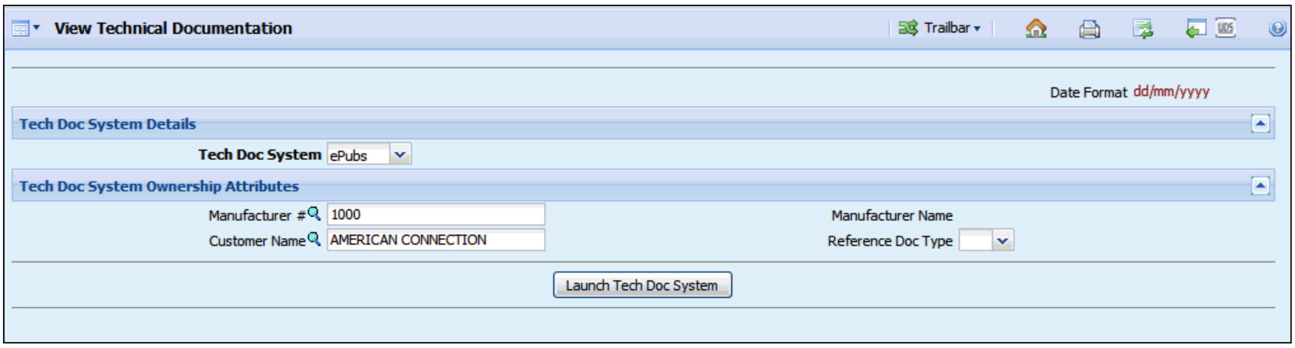


Figure 5.2 Viewing maintenance documents

2. Select the **Tech Doc System** as "Jouve", "Airnav" or "ePubs", through which you wish to view the source document details.
3. Enter the number identifying the manufacturer whose source documents must be viewed, in the **Manufacturer # field**. The system displays the **Manufacturer Name**.
4. Enter the login ID of the customer, using which the Tech Doc System can be viewed, in the **Customer Name** field.
5. Use the **Reference Doc Type** drop-down list box to specify the type of the reference document as "AMM". Based on the mapping done in the **Set Tech Doc System Options** activity, the system invokes the technical document system corresponding to the manufacturer, for viewing the source document details.

LineAnywhere

The LineAnywhere process in the desktop Ramco Aviation system under Utilities enables the users to validate and process pending work packages transferred from LineAnywhere before they are saved to Ramco Aviation. However, processed work packages are right away to Ramco Aviation. The work packages transferred from LineAnywhere hold one of the following transfer statuses: Pending and Processed. The processed work packages can only be viewed while users can validate process or shortclose pending work packages in this activity. The users can retrieve / view the work packages based on varied and specific criteria. The details of retrieved work packages including aircraft, arrival flight, transfer, validation and error are on display for the users. With the available information, the users can choose to perform the following actions on the work packages.

- View processed work packages
- Validate an then process pending work packages
- Process or shortclose pending work packages

Processed packages are uploaded to the Ramco Aviation online database from the offline LineAnywhere app. This process provides a facility that highlights the errors encountered in the work packages. The users can rectify the errors by providing valid data to rectify errors and then process them.

6.1 PROCESSING WORK PACKAGES TRANSFERRED FROM LineAnywhere

1. Click on the **Transfer Work Package Log** link under the **LineAnywhere** business component. The **Transfer Work Package Log** page appears. *See Figure 6.1*.

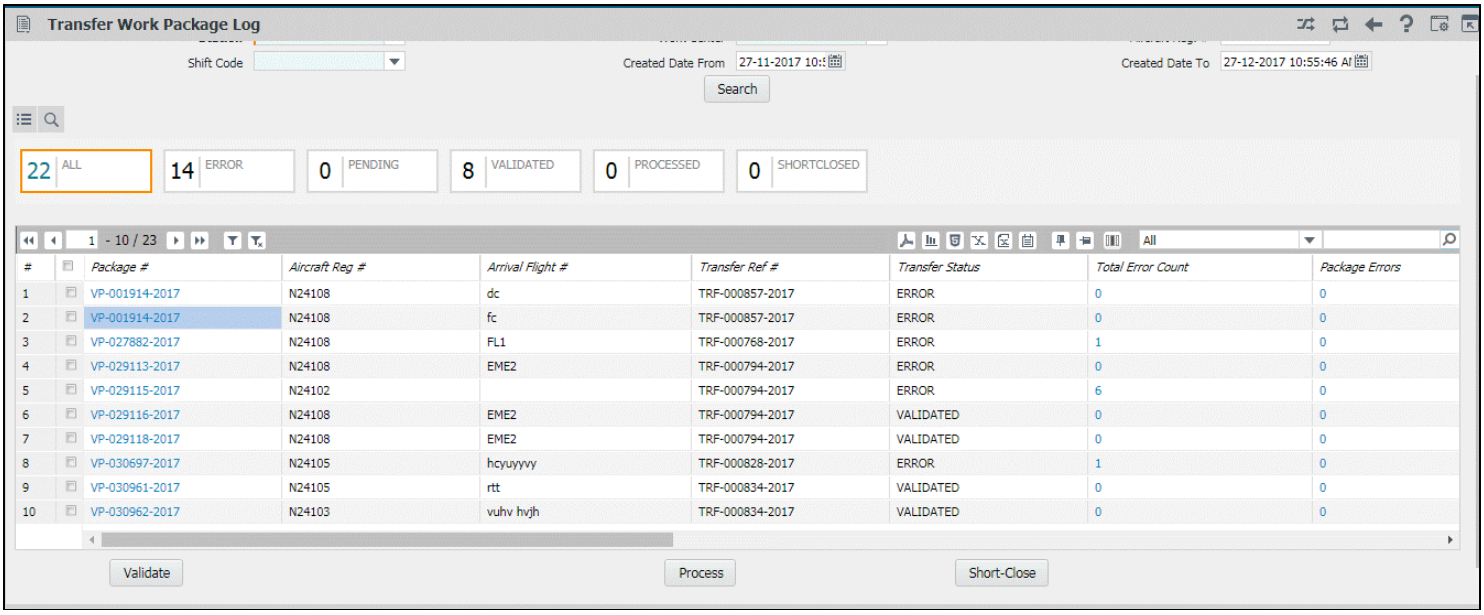


Figure 6.1 Setting options for Technical Document System

2. Specify search criteria to retrieve work packages transferred from **LineAnywhere** to the desktop **Ramco Aviation** application.
3. Click the **Search** pushbutton to retrieve work packages that meet the user-specified criteria.

Status search

4. Click the  icon.

The following filter cards appear with the count of work packages in specific status.

All	Shows the count of work packages retrieved on the basis of the specified criteria. On click of the filter card, these work packages are displayed in the multiline. This filter card becomes active on launch of the screen.
Error	Shows the count of work packages retrieved on the basis of the specified criteria with the transfer status as 'Error'. On click of the filter card, these work packages are displayed in the multiline.
Pending	Shows the count of work packages retrieved on the basis of the specified criteria with the transfer status as 'Pending'. On click of the filter card, these work packages are displayed in the multiline.
Validated	Shows the count of work packages retrieved on the basis of the specified criteria with the transfer status as 'Validated'. On click of the filter card, these work packages are displayed in the multiline.
Processed	Shows the count of work packages retrieved on the basis of the specified criteria with the transfer status as 'Processed'. On click of the filter card, these work packages are displayed in the multiline.
Shortclosed	Shows the count of work packages retrieved on the basis of the specified criteria with the transfer status as 'Shortclosed'. On click of the filter card, these work packages are displayed in the multiline.

Specific search

5. Click the icon.
6. Under **View Level,** select the relevant radio button to view requisite work packages.
7. If you wish to retrieve work packages, select the **Package** radio button.
8. If you wish to retrieve the errors from the work packages, select the **Error** radio button.
9. Enter search criteria in the **Search By** drop-down list box on the basis of which you wish to retrieve work packages.
10. Click the **Go** pushbutton to display work packages in the multiline.

Additional search criteria in Package view level

11. Select the **Package** radio button and then enter search criteria in addition to the specific search criteria to retrieve work packages.

Additional search criteria in Error view level

12. Select the **Error** radio button and then enter search criteria in addition to the specific search criteria to retrieve work packages.

Data Retrieval and processing

The multiline displays details of the work packages.

13. You must validate work packages in the “Pending” transfer status to ascertain and rectify errors in them. Click the **Validate** pushbutton.
14. You can process validated work packages; validated work packages with errors can also be processed. Alternatively, transferred work packages can be straightaway processed without validation. Click the **Process** pushbutton to save the work packages in the Ramco Aviation database.

    Note: The transfer status of the work packages becomes “Processed”, if no errors are found in the work package. However, if remain in the work packages, the transfer status is set as “Validated”.
15. You can shortclose the work packages in the “Pending” transfer status. Alternatively, you can shortclose work packages with/without resolving the errors subsequent to validation, if the errors do not adversely affect the aircraft operability. Click the **Shortclose** pushbutton to shortclose transfer work packages.

    Note: The transfer status of the work packages becomes “Shortclosed”.

Manage Transfer Info popup

This popup primarily aims to pinpoint the source of the errors to users who can then quickly rectify them and proceed to process or shortclose the package. Alternately, users select the work package they want to work with by using search criteria as explained next

1. The **Manage Transfer Info** popup appears with the details of the work package selected in the **Manage Transfer Package Log** multiline *See Figure 6.2*.

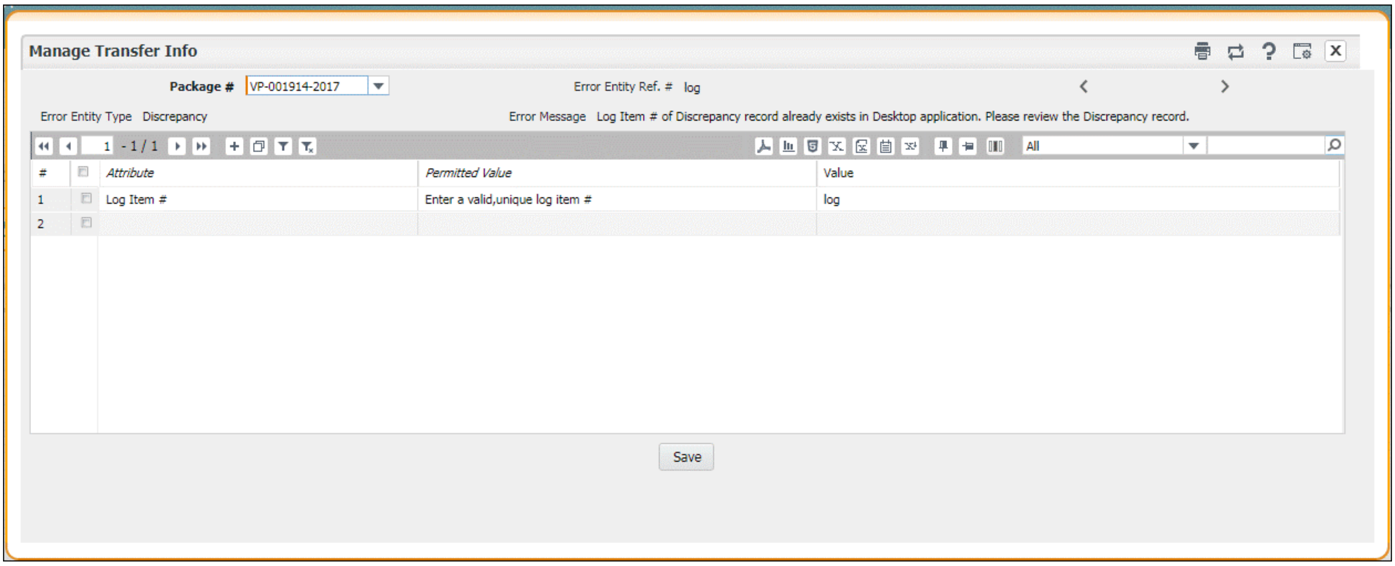


Figure 6.2 Setting options for Technical Document System

2. Use the **Work Package #** drop-down list box to select the work package you want to work with. The drop-down list box displays the work packages
3. Enter a valid **Value** for the attribute in the multiline.
4. Click on the **Save** pushbutton.

Index

Corporate Office and R&D Center

RAMCO SYSTEMS LIMITED

64, Sardar Patel Road, Taramani,

Chennai – 600 113, India

Office : + 91 44 2235 4510 / 6653 4000

Fax : +91 44 2235 2884

Website : www.ramco.com