

ADPay

Payment Gateway

Version 3.3.1

This document describes the purpose of different modules and sub modules of ADPay Payment Gateway 3.3.1. Additionally, this document explains how a bank administrator user can use the different modules and sub modules.

Publishing Date: February 2020

**User Manual – Bank Administrator users**

##### Copyright Statement

**Copyright Notice**

This document is confidential and proprietary to Financial Software and Systems (P) Ltd. and no part of this material shall be reproduced, published in any form by any means, electronic or mechanical including photocopy or any information storage or retrieval system nor shall the material be disclosed to third parties without the express written authorization of FSS.

Copyright © 2020 FSS (P) Ltd. All rights reserved.

**Restrictions and Disclaimer**

The information contained in this document is confidential. This document shall not be disclosed, used or duplicated, in whole or in part, for any purpose other than to internally disseminate this information within FSS. The screens are captured in Demo version and are expected to change.

##### Version History

The following table displays the version history of this document:

| **Version No.** | **Created or Updated By** | **Reason for Change** | **Reviewer** | **Created or Updated on** |
| --- | --- | --- | --- | --- |
| 1.0.0 | FSS Documentation Team | Document Created. | Sharon Premkumar/Priyadarshini R | March 2020 |

##### Table of Contents

[Chapter 1 Getting Started 6](#_Toc34204199)

[Overview 7](#_Toc34204200)

[Log on to ADPay Payment Gateway 8](#_Toc34204201)

[Recover Forgotten Password 9](#_Toc34204202)

[Password Security 12](#_Toc34204203)

[Set up or Update your Answers for the Security Questions 16](#_Toc34204204)

[Change your Logon Password 17](#_Toc34204205)

[Regenerate and Resend a User’s Password 18](#_Toc34204206)

[Chapter 2 Customizing the Application 21](#_Toc34204207)

[Customize a Menu and Sub menu 22](#_Toc34204208)

[Modify Password Security Parameters 25](#_Toc34204209)

[Chapter 3 Configuring Roles and Users 29](#_Toc34204210)

[Introduction 30](#_Toc34204211)

[Create and Maintain User Menu 30](#_Toc34204212)

[Create User Menu 30](#_Toc34204213)

[View or Modify a User Menu 31](#_Toc34204214)

[Create and Maintain User Menu 33](#_Toc34204215)

[Create a User Role 33](#_Toc34204216)

[Assign or Remove Privileges from a Role 34](#_Toc34204217)

[View or Modify a User Role 35](#_Toc34204218)

[Create and Maintain User IDs 36](#_Toc34204219)

[Create a User ID 36](#_Toc34204220)

[View or Modify a User ID 38](#_Toc34204221)

[Chapter 4 Configuring the Institution 41](#_Toc34204222)

[Introduction 42](#_Toc34204223)

[Create and Maintain Institutions 42](#_Toc34204224)

[Modify or View the Details of an Institution 42](#_Toc34204225)

[Configure Institution Level Parameters 50](#_Toc34204226)

[Configure Data Encryption 53](#_Toc34204227)

[Add or Rotate the DEK 53](#_Toc34204228)

[Add or Rotate a KEK 54](#_Toc34204229)

[Change KeyStore Passwords 56](#_Toc34204230)

[Configure Brand Types 57](#_Toc34204231)

[Create a Brand Type 57](#_Toc34204232)

[View or Modify a Brand Type 58](#_Toc34204233)

[Configure External Connections 58](#_Toc34204234)

[Add an HTTPs External Connection 59](#_Toc34204235)

[Add a TCP/IP External Connection 62](#_Toc34204236)

[View or Modify an External Connection 67](#_Toc34204237)

[View or Modify a Listener 68](#_Toc34204238)

[Refresh the Settings on the Server 69](#_Toc34204239)

[Chapter 5 Configuring Dashboards 70](#_Toc34204240)

[Introduction 71](#_Toc34204241)

[Configure and Maintain Dashboard Templates 71](#_Toc34204242)

[Create a Dashboard Template 71](#_Toc34204243)

[View or Modify a Dashboard Template 72](#_Toc34204244)

[Configure and Maintain Parameters for Dashboard Templates 72](#_Toc34204245)

[Configure Panels for a Dashboard Template 72](#_Toc34204246)

[View, Modify, or Delete Dashboard Panel Configuration for a Template 74](#_Toc34204247)

[Chapter 6 Reload Settings 75](#_Toc34204248)

[Configure Reload Settings 76](#_Toc34204249)

[Chapter 7 GL Accounting 77](#_Toc34204250)

[Configure GL Accounting 78](#_Toc34204251)

[Index 80](#_Toc34204252)

# Getting Started

This chapter explains ADPay Payment Gateway 3.3.1. Additionally, it describes the procedures to log on, change your password, and recover your forgotten password.

[Overview 7](#_Toc33796506)

[Log on to ADPay Payment Gateway 8](#_Toc33796507)

[Recover Forgotten Password 9](#_Toc33796508)

[Password Security 12](#_Toc33796509)

[Set up or Update your Answers for the Security Questions 16](#_Toc33796510)

[Change your Logon Password 17](#_Toc33796511)

[Regenerate and Resend a User’s Password 18](#_Toc33796512)

## Overview

ADPay Payment Gateway is a robust, fast, secure, and cost-effective internet payment gateway that allows Financial Institution (FIs), payment processors, and merchants to accept and process electronic payments through internet. It offers a hybrid payment processing platform that supports multiple modes of payment, multiple payment channels, and efficient management of payments processing. It supports configuring multiple institutions.

It can process, verify, and accept the following modes of payment:

* Debit, prepaid, or credit cards
* Online and offline payments

The bank administrator user performs the bank specific configuration that is used throughout the application. The bank administrator user can perform the following tasks to configure the application for a bank:

* Customize the menus, sub menus, and password security parameters, if required
* Create the institution record
* Configure institution-level parameters
* Configure data encryption:
* Add or rotate the Data Encryption Key (DEK)
* Add or rotate the Key Encryption Key (KEK)
* Configure KeyStore passwords
* Configure brand types
* Configure external connections and listeners
* Configure risk alerts
* Configure and maintain dashboards
* Configure and generate reports

## Log on to ADPay Payment Gateway

You must log on the ADPay Payment Gateway before you can perform any tasks.

Perform the following steps to log on to the application:

1. Open a browser window, type the URL for ADPay Payment Gateway in the address bar, and then click **Go to** or press Enter. The **Pre-Login** page appears.
2. In the right top corner, click **Login** or at the bottom of the page, click **Process to Login** to open the **Login** screen.

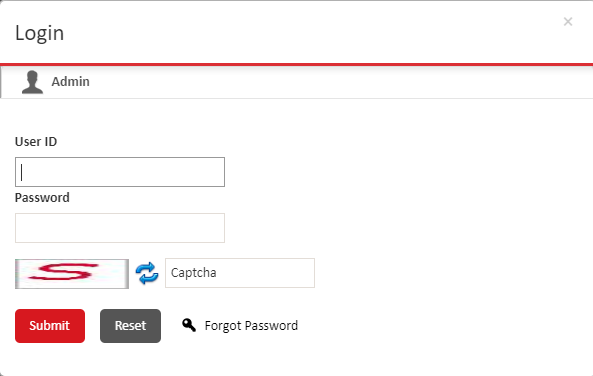


Figure : Login Screen

1. In the **User ID** box, type your user ID.
2. In the **Password** box, type your login password.

Note.png**Note**: If you have forgotten your password, then click **Forgot Password** to reset your password. For more information about how to recover a password, see [Recover Forgotten Password](#_Recover_Forgotten_Password).

1. In the **Captcha** box, type the captcha text that is displayed in the image. If you cannot read the captcha, click  to load another image.
2. Click **Submit** to log on to ADPay Payment Gateway.

Note.png**Note:** If you log on for the first time or after recovering your password, the **Change Password** page is displayed instead of the **Home** page. You must change your password and log on again. For more information, see [Change your Logon Password](#_Change_your_Logon).

## Recover Forgotten Password

You can recover your password in case you have forgotten your existing password. You must specify your institution code, user ID, captcha, email ID, and answer your account security question to recover your password.

Perform the following steps to recover your password:

1. On the **Login** screen, click **Forgot Password** to open the **Forgot Password** screen.

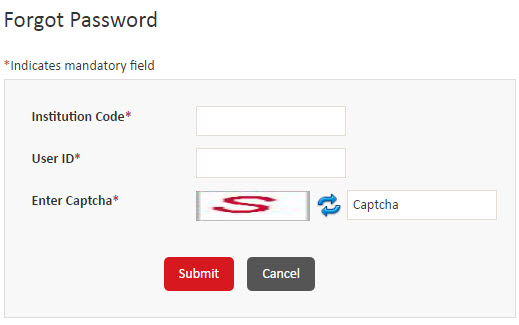


Figure : Forgot Password Screen

1. In the I**nstitution Code** box, type the unique three-digit identification code for your institution.
2. Type your user ID.
3. In the **Captcha** box, type the text that is displayed in the image. If you cannot read the captcha, click  to load another image.
4. Click **Submit**.

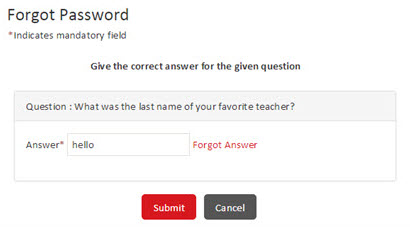


Figure : Answer your security question

1. In the **Answer** box, type the answer to the security question that is displayed, and then click **Submit**.
2. In the **Email Id** box, type your registered email ID.

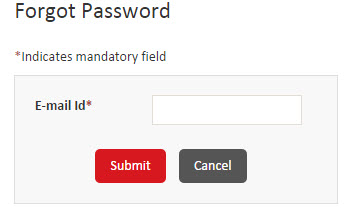


Figure : Specifying your registered email ID

1. Click **Submit**. After the password is reset, an email is sent to your registered email ID. The email contains a link that you can click to create your new password.

The following image displays a sample email that is sent to the user:

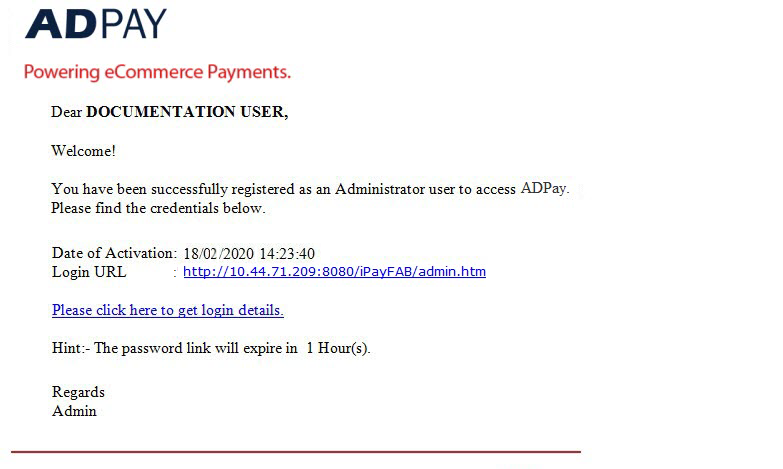


Figure : The email with password reset link

1. Click **Please click here to get login details** to display your new password.
2. Click **Please click here to Login to the application** link to log on to the application. For more information about how to log on to the application, see [Log on to ADPay Payment Gateway](#_Log_on_to_1).

## Password Security

You can view or modify the predefined password security parameters for a bank user type as per FAB requirements. You can specify the length, recurrence, expiration, lockout, allowed characters, and inactivity details for passwords.

Perform the following steps to view or modify the Password Security parameters:

1. Point to **My Accounts**, and then click **Password Security** to open the **Password Security** screen.

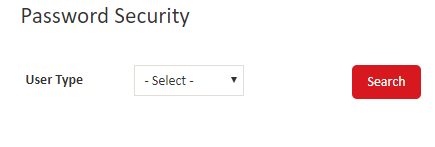


Figure : Password Security screen

1. Specify the search criteria to display the parameters by performing the following steps:
2. In the **User type** list, click one of the following options:

* **ALL** – Display the list of parameters for all user types.
* **ADMIN** – Display the password parameter record for FAB administrator users.
* **INSTITUTION** – Display the password parameter record for FAB users.
* **MERCHANT** – Display the password parameter record for Merchant users.

1. In the **Institution** list, select the institution to update the parameters.
2. Click **Search**. The **Password Security** screen is displayed with the filtered list of parameter records.

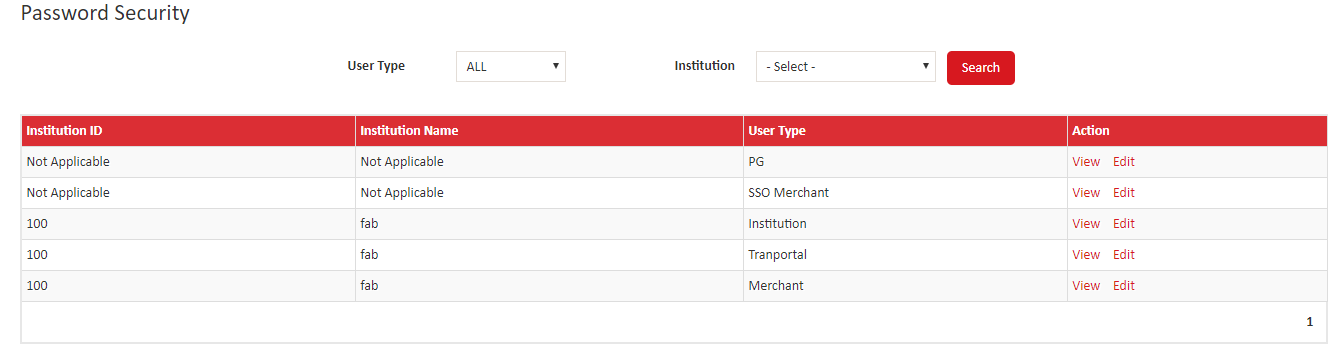


Figure : Password Security screen

1. Under the action column in the list of parameters, click **Edit**. The **Edit Password Security** screen is displayed.

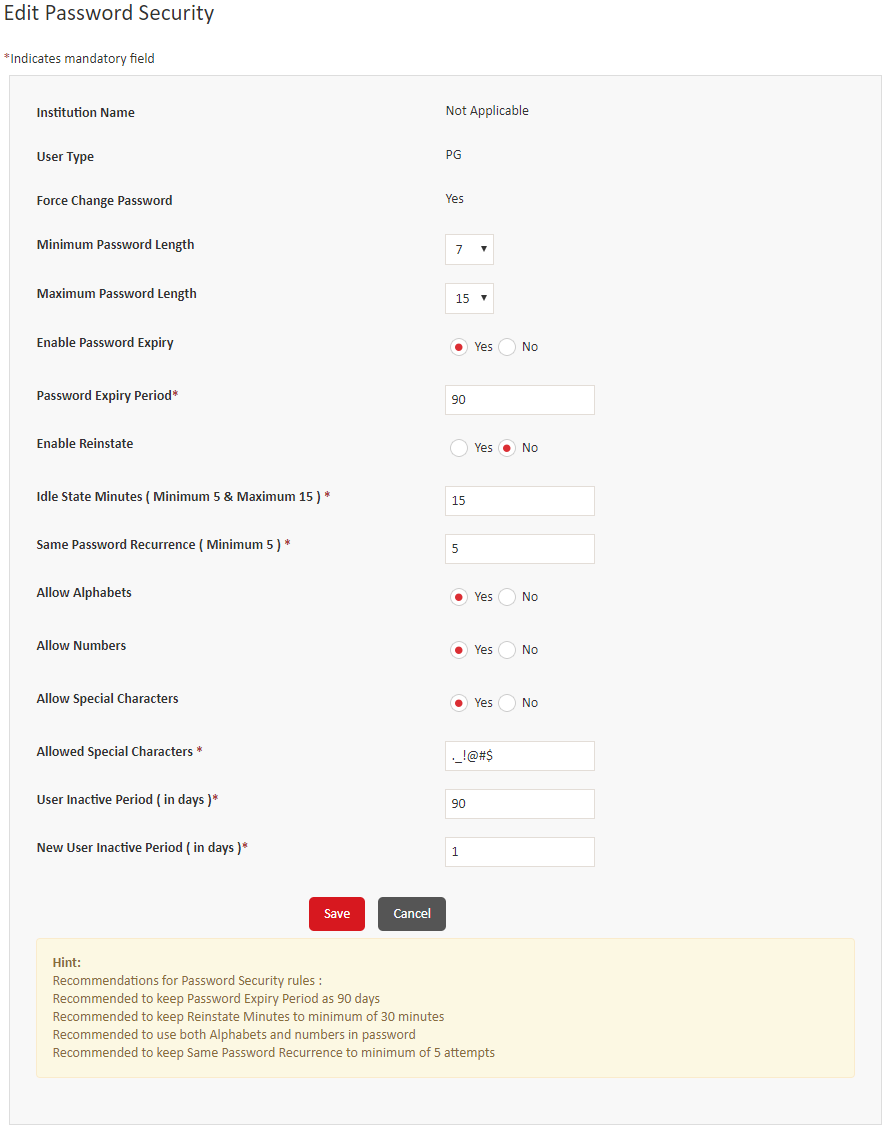


Figure : Edit Password Security

1. Specify values in the following fields:

| **Field** | **Description** |
| --- | --- |
| **Institution Name** | Displays the name of the institution for the password parameters. This is a read-only field. |
| **User Type** | Displays the user type for which the password parameters are displayed. This is a read-only field. |
| **Force Change Password** | Indicates that the password must be changed by the users when they first log on after user ID creation or password reset. This is a read-only field and displays Yes. |
| **Minimum Password Length** | Click a number to modify the minimum length of passwords. |
| **Maximum Password Length** | Click a number to modify the maximum length of passwords. |
| **Enable Password Expiry** | Click **Yes** or **No** to enable or disable password expiration after a specified period is lapsed. If you click Yes, then the Password Expiry Period list is displayed. |
| **Password Expiry Period** | Type or modify the number of days that indicates the period after which passwords expire and must be changed by the users. The recommended expiry period is of 90 days.  Note.png**Note**: This box is available only if you select Yes in the Enable Password Expires group. |
| **Enable Reinstate** | Click **Yes** or **No** to enable or disable reinstating passwords after the specified time period has elapsed. If you click Yes, then the Reinstate Minutes list is displayed. |
| **Reinstate Minutes** | Type or modify the number of minutes after which a password that was locked due to incorrect password attempts is automatically reinstated. The recommended minimum minutes to reinstate is 30 minutes.  Note.png**Note**: This box is available only if you select Yes in the Enable Reinstate group. |
| **Idle State Minutes (Minimum 5 & Maximum 15)** | Modify the number of minutes after which an inactive session is timed out. |
| **Same Password Recurrence (Minimum 5)** | Modify the number that indicates the count of unique new passwords that must be used by a user before an old password can be reused.  Note.png**Note**: It is recommended to keep same password recurrence to minimum of 5 attempts. |
| **Allow Alphabets** | Click **Yes** or **No** to allow or disallow using alphabets in passwords.  Note.png**Note**: It is recommended to use both, alphabets and numbers in the password. |
| **Allow Numbers** | Click **Yes** or **No** to allow or disallow using numbers in passwords.  Note.png**Note**: It is recommended to use both, alphabets and numbers in the password. |
| **Allow Special Characters** | Click **Yes** or **No** to allow or disallow using alphabets in passwords. |
| **Allowed Special Characters** | Modify the special characters that are allowed in passwords.  Note.png**Note**: This box is available only if you select Yes in the Allow Special Characters group. |
| **User Inactive Period (in days)** | Modify the number of inactive days after which a user ID is disabled. |
| **New User Inactive Period (in days)** | Modify the number of inactive days after which a new user ID is disabled. |

1. Click **Save** to save the changes.

To view a user menu, proceed the following steps:

1. In the action column, click **View**. The **View User Menu** screen is displayed.

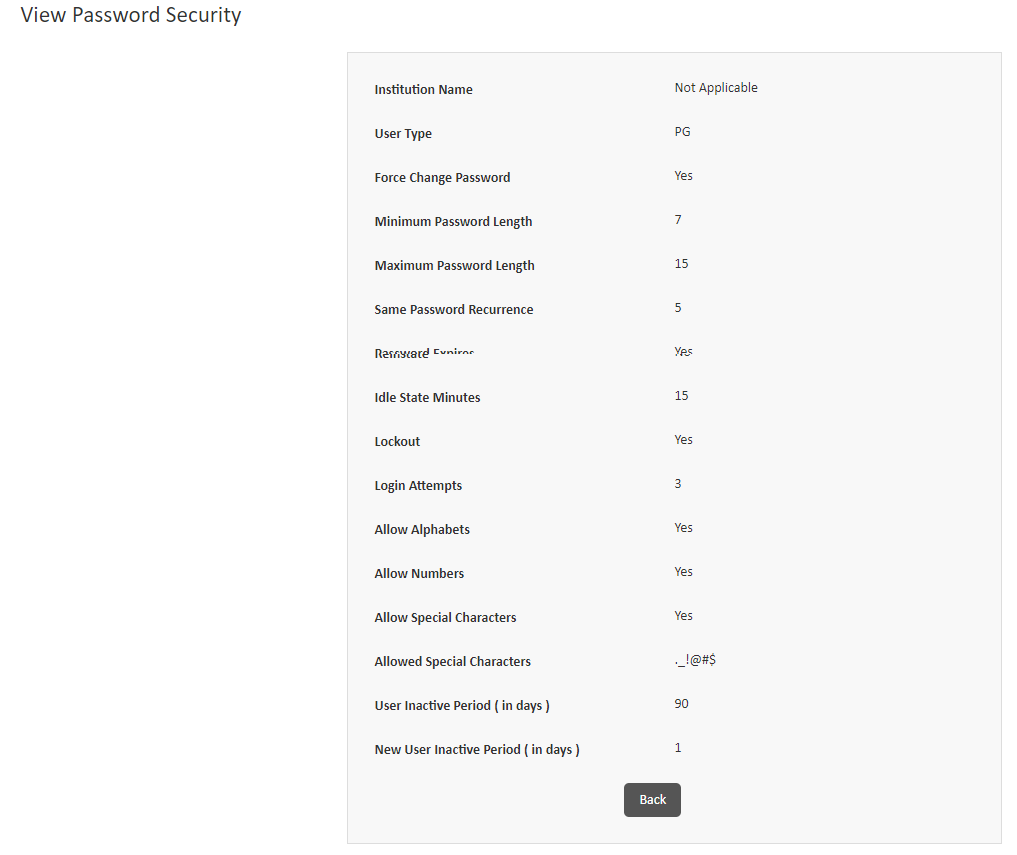


Figure : View Password Security

1. Click **Back** to return to the **Password Security** screen.

## Set up or Update your Answers for the Security Questions

The security questions are used to authenticate your user ID in case you forget your password. You can add or update answers for the security questions for your profile.

Perform the following steps to set up or update the answers:

1. Point to **My Accounts**, and then click **Security Questions** to open the **Security Questions** screen.

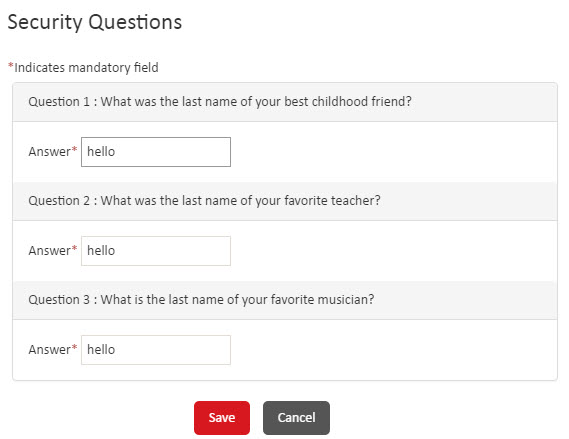


Figure 10: Security Questions Screen

1. In the **Answer** boxes, type or modify your answer for each of the security questions.
2. Click **Save** to save the answers.

## Change your Logon Password

You can change the existing password for your account. It is recommended that you change your password frequently. You must change your password at the first successful logon after your ID is created or after you have recovered your password.

Perform the following steps to change your password:

1. Point to **My Accounts** andclick **Change Password** to open the **Change Password** screen.

**Note.pngNote:** If you log on for the first time or after recovering your password, the **Change Password** page is displayed instead of the **Home** page.

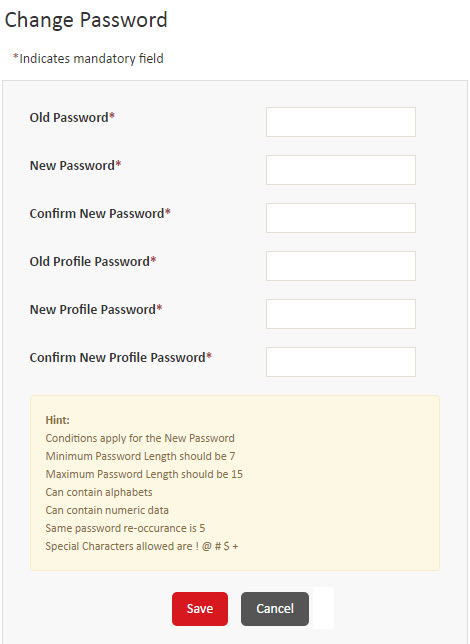


Figure : The Change Password screen

1. In the **Old Password** box, type your current password.
2. In the **New Password** and **Confirm New Password** boxes, type your new password twice.

Note.png**Note:** Ensure that your password adheres to the acceptable password criteria that are displayed on the screen.

1. In the **Confirm New Password** box, re-type the new logon password which you entered in step **3**.
2. In the **Old Profile Password** box, type your current profile password.
3. In the **New Profile Password** and **Confirm New Profile Password** boxes, type your new profile password twice.

Note.png**Note:** Ensure that your password adheres to the acceptable password criteria that are displayed on the screen.

1. Click **Save** to display the **Login** screen, where you can log on to the application using your user ID and new password.

## Regenerate and Resend a User’s Password

You can regenerate the default password for a user and send it to their registered email ID. Additionally, you can send a test email to validate a user’s email ID.

Perform the following steps to regenerate and resend a user’s password:

1. On the menu bar, point to **My Accounts**, and then click **Resend Password** to open the **Resend Password** screen.

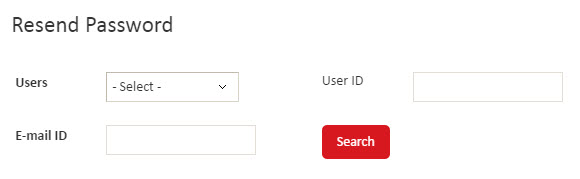


Figure : The Resend Password search screen

1. In the **Users** list, click one of the following search criteria:

* **ALL** – Select this option to display the list of all user IDs. If you select this option, you cannot specify the user ID and email ID to search.
* **Admin Users** – Select this option to display the list of administrator users. If required, specify the user ID in the **User ID** box and email ID in the **E-mail ID** box, and then click **Search** to further filter the list.
* **Institution Admin** – Select this option to display the list of Institution Admin users. If required, specify the user ID in the **User ID** box and email ID in the **E-mail ID** box, and then click **Search** to further filter the list.

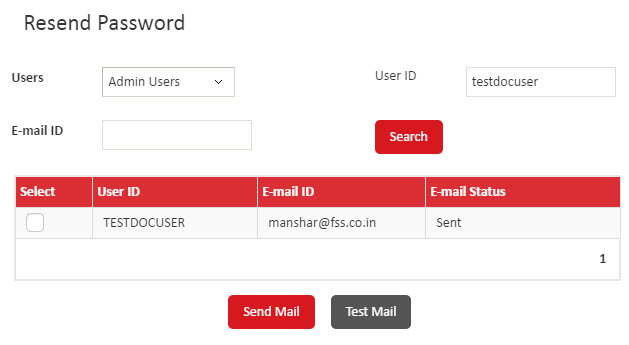


Figure : The Resend Password screen

1. To regenerate and resend the password to a user through email, in the **Select** column, select a check box, and then click **Send Mail**. You can select multiple user IDs.

Alternatively, to send a test email to an email address, click **Test Mail**. The **Test E-mail** dialog box is displayed, type the email address to send the test email to and click **OK** to send the test email.

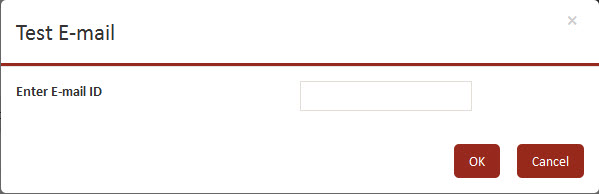


Figure : The Test E-mail dialog box

If you have regenerated and resent the password, the email is sent to user’s registered email address. If you send a test email, it is sent to the email address that you specify.

The following image displays a sample email that is sent to the user.

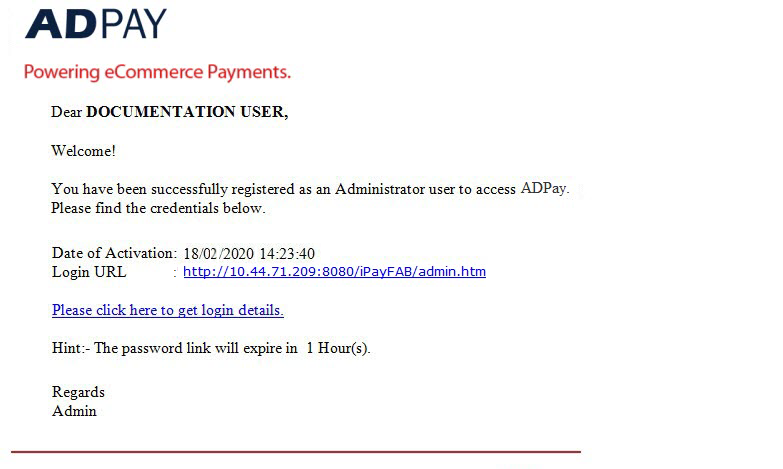


Figure : Sample email with the link to user’s credentials

# Customizing the Application

This chapter explains how to customize menus and sub menus. Additionally, it explains how to configure password security parameters for an institution and user type.

[Customize a Menu and Sub menu 22](#_Toc33796513)

[Modify Password Security Parameters 25](#_Toc33796514)

## Customize a Menu and Sub menu

You can view or modify the predefined menus and sub menus that are available in the ADPay Payment Gateway. This allows you to customize the application for each user type as per your requirement, thereby making ADPay Payment Gateway more user-friendly.

Note.png**Note:** You cannot modify the menu ID and menu type for a menu or sub menu.

Perform the following steps to customize a menu or sub menu:

1. Point to **My Accounts**, and then click **User Menu** to open the **User Menu** screen.

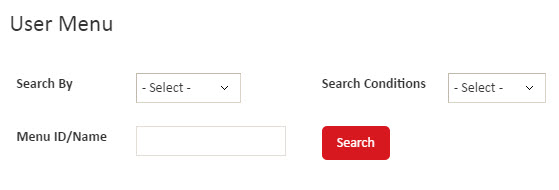


Figure : The User Menu screen

1. Specify the search criteria to display the predefined menus and sub menus by performing the following steps:
2. In the **Search By** list, click one of the following options:

* **ALL** – Display the list of all of the menus and sub menus.
* **Menu ID** – Search for a specific menu or sub menu using its menu ID.
* **Menu Name** – Search for a specific menu or sub menu using its name.

1. If you select **Menu ID** or **Menu Name** in the **Search By** list, perform the following steps:
2. In the **Search Conditions** list, click **Exact**, **Starts With**, **Ends With**, or **Contains** to indicate the search conditions to use.
3. In the **Menu ID/Name** box, type the ID or name of the menu or sub menu to search for.
4. Click **Search**.

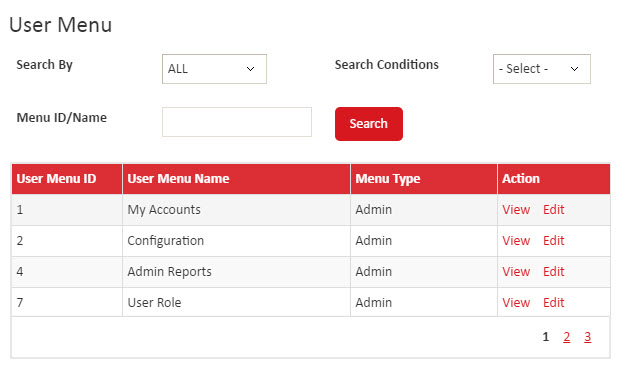


Figure : The list of menus and sub menus

1. In the list of menu and sub menus that are displayed, click **Edit** to open the **Edit User Menu** screen.

Alternatively, you can click **View** to open the **View User Menu** screen, where you can view the details of a menu or sub menu.

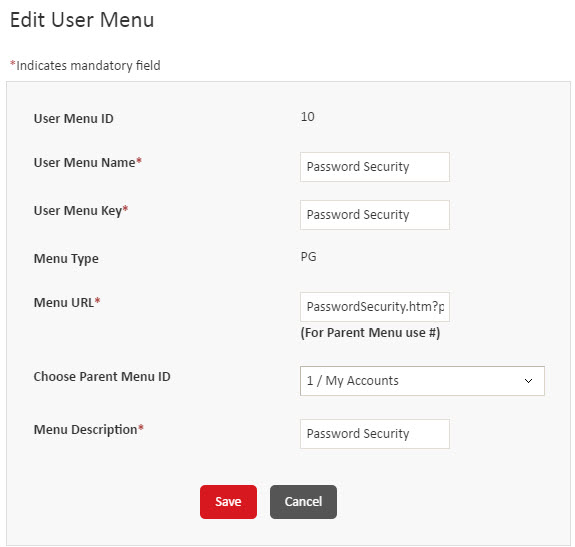


Figure : The Edit User Menu screen

1. In the **User Menu Name** box, modify the name of the menu or sub menu.
2. In the **User Menu Key** box, modify the key for the menu or sub menu.
3. In the **Menu URL** box, modify the URL for the menu or sub menu.

Note.png**Note:** You must specify **#** as the menu URL for all parent menus.

1. If you are customizing a sub menu, then in the **Choose Parent Menu ID** list, click the parent menu for the sub menu. This field is not available for parent menus.
2. In the **Menu Description** box, modify the description for the menu or sub menu.
3. Click **Save** to save the changes.

## Modify Password Security Parameters

You can view or modify the predefined password security parameters for a user type for an institution. You can specify the length, recurrence, expiration, lockout, allowed characters, and inactivity details for passwords.

Perform the following steps to view or modify the parameters:

1. Point to **My Accounts**, and then click **Password Security** to open the **Password Security** screen.



Figure : The Password Security screen

1. Specify the search criteria to display the parameters by performing the following steps:
2. In the **User type** list, click one of the following options:

* **ALL** – Display the list of parameters for all user types.
* **ADMIN** – Display the password parameter record for administrator users.
* **INSTITUTION** – Display the password parameter record for institution users.
* **MERCHANT** – Display the password parameter record for merchant users.
* **TRANPORTAL** – Display the password parameter record for tranportal users.

1. In the **Institution** list, click the institution to update the parameters for.
2. Click **Search** to display the filtered list of parameter records.
3. In the list of parameters that are displayed, click **Edit** to open the **Edit Password Security** screen.

Alternatively, you can click **View** to open the **View Password Security** screen, where you can view the parameters.

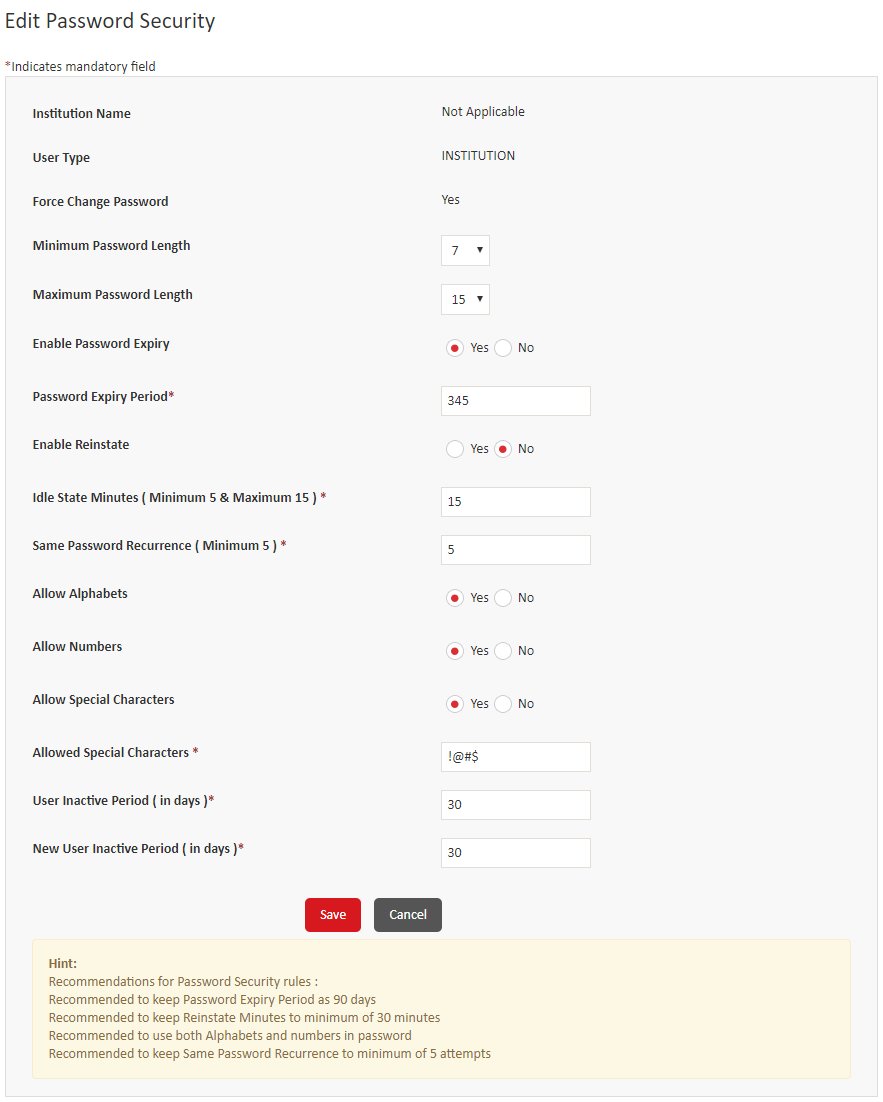


Figure : The Edit Password Security screen

1. View or modify values in the following fields:

|  |  |
| --- | --- |
| Field | Description |
| **Institution Name** | Displays the name of the institution for the password parameters. This is a read-only field. |
| **User Type** | Displays the user type for which the password parameters are displayed. This is a read-only field. |
| **Force Change Password** | Indicates that the password must be changed by the users when they first log on after user ID creation or password reset. This is a read-only field and displays **Yes**. |
| **Minimum Password Length** | Click a number to modify the minimum length of passwords. |
| **Maximum Password Length** | Click a number to modify the maximum length of passwords. |
| **Enable Password Expiry** | Click **Yes** or **No** to enable or disable password expiration after a specified period is lapsed. If you click **Yes**, then the **Password Expiry Period** list is displayed. |
| **Password Expiry Period** | Type or modify the number of days that indicates the period after which passwords expire and must be changed by the users. The recommended expiry period is of 90 days.  Note.png**Note**: This box is available only if you select **Yes** in the **Enable Password Expires** group. |
| **Enable Reinstate** | Click **Yes** or **No** to enable or disable reinstating passwords after the specified time period has elapsed. If you click **Yes**, then the **Reinstate Minutes** list is displayed. |
| **Reinstate Minutes** | Type or modify the number of minutes after which a password that was locked due to incorrect password attempts is automatically reinstated. The recommended minimum minutes to reinstate is 30 minutes.  Note.png**Note**: This box is available only if you select **Yes** in the **Enable Reinstate** group. |
| **Idle State Minutes (Minimum 5 & Maximum 15)** | Modify the number of minutes after which an inactive session is timed out. |
| **Same Password Recurrence (Minimum 5)** | Modify the number that indicates the count of unique new passwords that must be used by a user before an old password can be reused.  Note.png**Note**: It is recommended to keep same password recurrence to minimum of 5 attempts. |
| **Allow Alphabets** | Click **Yes** or **No** to allow or disallow using alphabets in passwords.  Note.png**Note**: It is recommended to use both, alphabets and numbers in the password. |
| **Allow Numbers** | Click **Yes** or **No** to allow or disallow using numbers in passwords.  Note.png**Note**: It is recommended to use both, alphabets and numbers in the password. |
| **Allow Special Characters** | Click **Yes** or **No** to allow or disallow using alphabets in passwords. |
| **Allowed Special Characters** | Modify the special characters that are allowed in passwords.  Note.png**Note**: This box is available only if you select **Yes** in the **Allow Special Characters** group. |
| **User Inactive Period (in days)** | Modify the number of inactive days after which a user ID is disabled. |
| **New User Inactive Period (in days)** | Modify the number of inactive days after which a new user ID is disabled. |

1. Click **Save** to save the changes.

# Configuring Roles and Users

This chapter describes how to create and maintain user roles and user IDs. Additionally, it explains how to regenerate and resend a user’s password.

[Introduction 30](#_Toc34152081)

[Create and Maintain User Menu 30](#_Toc34152082)

[Create User Menu 30](#_Toc34152083)

[View or Modify a User Menu 31](#_Toc34152084)

[Create and Maintain User Menu 33](#_Toc34152085)

[Create a User Role 33](#_Toc34152086)

[Assign or Remove Privileges from a Role 34](#_Toc34152087)

[View or Modify a User Role 35](#_Toc34152088)

[Create and Maintain User IDs 36](#_Toc34152089)

[Create a User ID 36](#_Toc34152090)

[View or Modify a User ID 38](#_Toc34152091)

## Introduction

You can perform the following tasks to create user IDs:

1. Create a user role and assign privileges to the role
2. Create a user ID and assign a role to it. Each user ID that is created must be attached to a user role. The user ID inherits the same privileges as the user role.

Additionally, if the password link for a user has expired, then you can resend the email that contains regenerated password.

The following sections explain each of these tasks in detail.

## Create and Maintain User Menu

You can create user Menus, and then assign menus to user roles. Additionally, you can view or modify user menus. You cannot delete user menus.

### Create User Menu

You can view or modify the predefined menus and sub menus that are available in the ADPay. Also, you can customize the application for each user type as per the requirement.

1. Point to **My Accounts** and click **User Menu** to open the **User Menu** screen. The User Menu Screen is displayed.

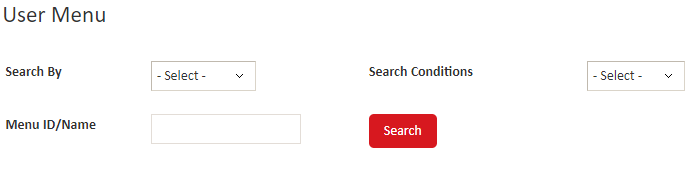


Figure : User Menu

1. Specify the search criteria to display the predefined menus and sub menus by performing the following steps:
2. In the **Search By** list, click one of the following options:

* **Search By** – Display the list of all the menus and sub menus.
* **Menu ID/** – Search for a specific menu or sub menu using its menu ID.
* **Menu Name** – Search for a specific menu or sub menu using its name.

1. If you select **Menu ID** or **Menu Name** in the **Search By** list, perform the following steps:
2. In the **Search Conditions** list, click **Exact**, **Starts With**, **Ends With**, or **Contains** to indicate the search conditions to use.
3. In the **Menu ID**/**Name box**, type the **ID** or name of the menu or sub menu to search for.
4. Click **Search**.

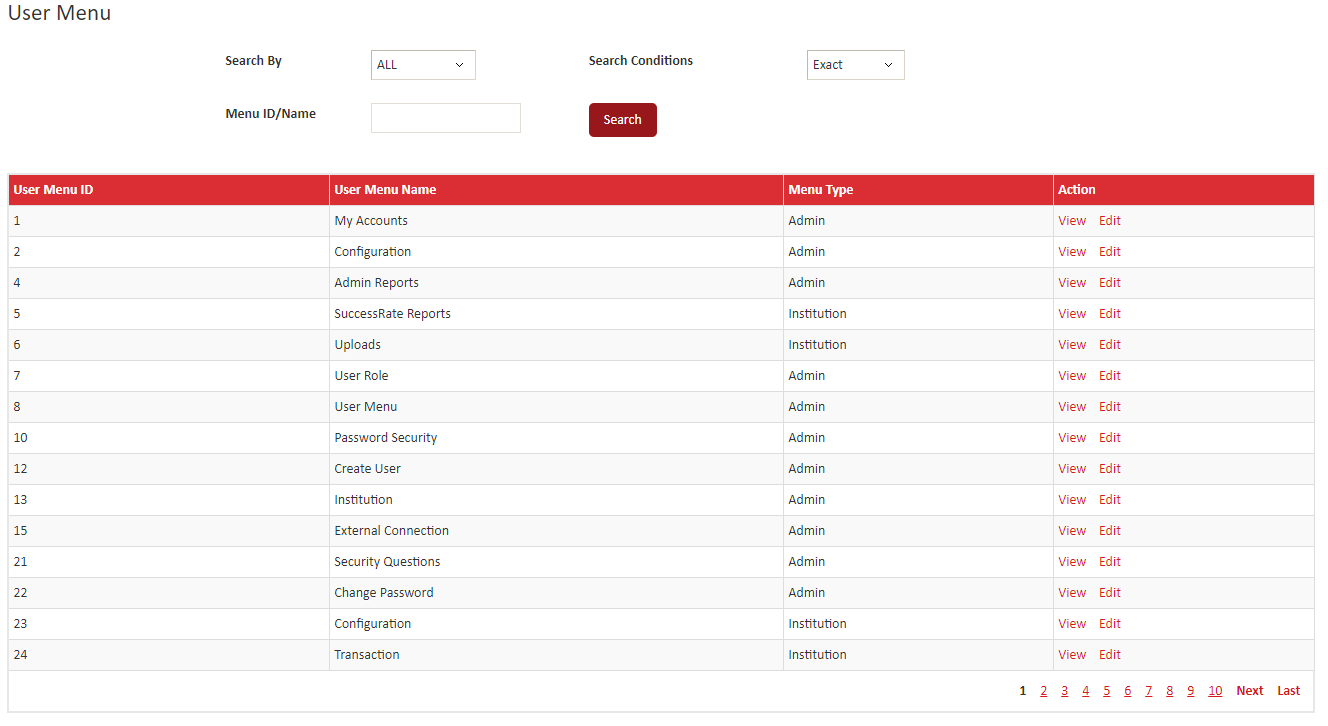


Figure : User Menu – List Screen

### View or Modify a User Menu

You can view or modify a user menu that you have created. You can only modify the User Menu Name, User Menu Key, Menu URL and Menu Description for a menu. You cannot edit the menu ID and menu type.

The screens to modify and view the user role are similar to the **Add User Menu** screen. Depending on the task, follow of one of the menu paths to open the screen:

To modify a user menu, proceed the following steps:

1. In the action column, click **Edit**. The **Edit User Menu** screen is displayed.

A screenshot of a social media post

Description automatically generated

Figure : Edit Screen

1. In the **User Menu Name** box, modify the name of the menu or sub menu.
2. In the **User Menu Key** box, modify the key for the menu or sub menu.
3. In the **Menu URL** box, modify the URL for the menu or sub menu.

Note.png**Note:** You must specify **#** as the menu URL for all parent menus.

1. If you are customizing a sub menu, then in the **Choose Parent Menu ID** list, click the parent menu for the sub menu. This field is not available for parent menus.
2. In the **Menu Description** box, modify the description for the menu or sub menu.
3. Click **Save** to save the changes.

To view a user menu, proceed the following steps:

1. In the action column, click **View**. The **View User Menu** screen is displayed.

A screenshot of a cell phone

Description automatically generated

Figure : View Screen

1. Click **Back** to return to the **User** **Menu** screen.

## Create and Maintain User Menu

You can create user roles, and then assign menus to user roles. Additionally, you can view or modify user roles. You cannot delete user roles.

### Create a User Role

You can create a user role. When you create a user role, a role ID is automatically generated and assigned to the user role by ADPay Payment Gateway.

Perform the following steps to create a user role:

1. Point to **My Accounts**, and then click **User Role** to open the **User Role** screen.
2. Click **Add** to open the **Add User Role** screen.

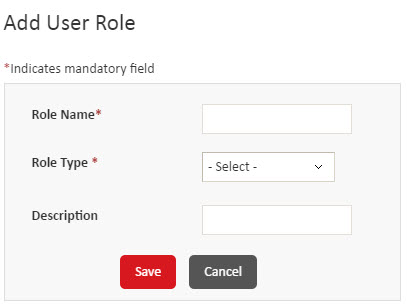


Figure : The Add User Role screen

1. In the **Role Name** box, type the name of the role to create.
2. In the **Role Type** list, click the type of role to create.
3. In the **Description** box, type the description of the user role.
4. Click **Save** to create the user role. An identification code is generated and assigned to the role and the role is added to the list on the **User Role** screen.

### Assign or Remove Privileges from a Role

After you create a user role, you can assign access to menus and sub menus to the user role. Alternatively, you can remove access to menus and sub menus from existing roles. This allows restricting access of the users who belong to a selected role.

Perform the following steps to assign or remove access from a user role:

1. On the menu bar, point to **My Accounts**, and then click **User Role** to open the **User Role** screen.
2. In the list of roles that are displayed, click **Assign Menu** to open the **Assign Menu** screen, where you can assign or remove access for the user role.

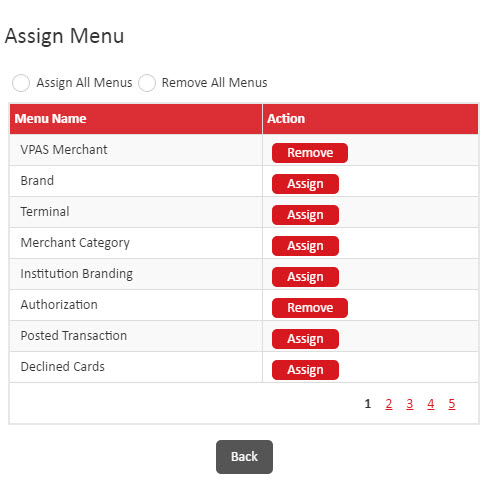


Figure : The Assign Menu screen

1. Depending on the menus or sub menus to assign, perform one of the following steps:

|  |  |
| --- | --- |
| Objective | Action |
| To assign all of the menus and sub menus | On the top of the screen, click **Assign All Menus**. |
| To remove all of the menus and sub menus | On the top of the screen, click **Remove All Menus**. |
| To assign access to specific menus and sub menus | In the **Action** column, click **Assign** for the menus or sub menus to remove. |
| To remove access for specific menus and sub menus | In the **Action** column, click **Remove** for the menus or sub menus to remove. |

1. Click **Back** to save the changes.

### View or Modify a User Role

You can view or modify a user role that you have created. You can only modify the name and description for a role. You cannot edit the role ID and type of role.

The screens to modify and view the user role are similar to the **Add User Role** screen. Depending on the task, follow of one of the menu paths to open the screen:

* To modify a user role, on the menu bar, point to **My Accounts**, and then click **User Role** > **Edit**. For more information about the fields and their descriptions, see [Create a user role](#_Create_a_user).
* To view a user role, on the menu bar, point to **My Accounts**, and then click **User Role** > **View**.

## Create and Maintain User IDs

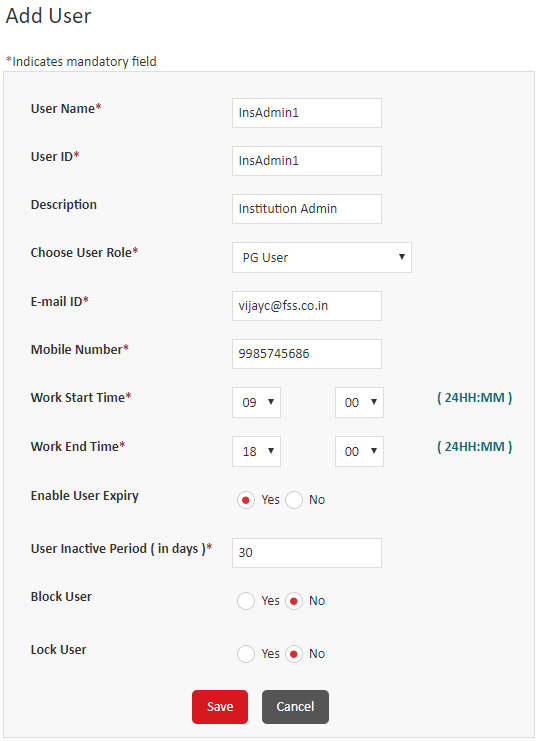
You can create user IDs and assign user roles to the IDs. Additionally, you can view or modify user IDs. You can change the status of a user from **Active** to **Inactive** or **Inactive** to **Active**.

You cannot delete user IDs.

### Create a User ID

Perform the following steps to create a user ID:

1. Point to **My Accounts**, and then click **Create User** to open the **User** screen.
2. Click **Add** to open the **Add User** screen.



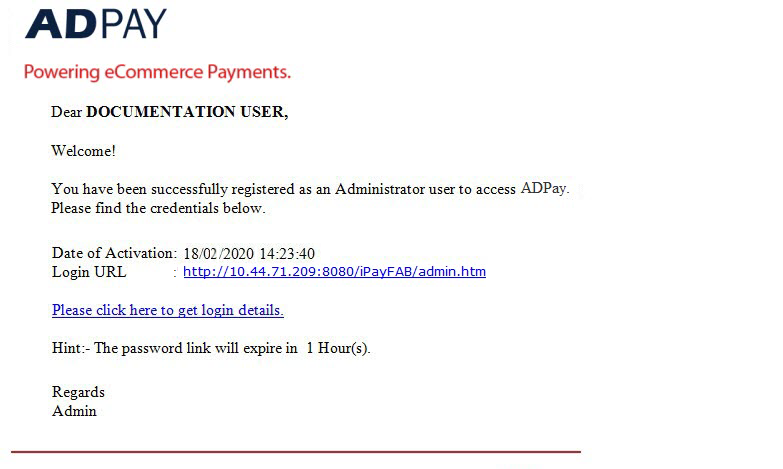
**Figure 27: The Add User screen**

1. Specify values in the following fields:

|  |  |
| --- | --- |
| Field | Description |
| **User Name** | Type the name of the user. |
| **User ID** | Type a unique alphanumeric user ID for the user. The user ID cannot contain special characters and spaces. |
| **Description** | Type the description of the user. |
| **Choose User Role** | Click the role to assign to the user. The access for the user is restricted based on the role. |
| **E-mail ID** | Type the email ID of the user. |
| **Mobile Number** | Type the 10-digit mobile number of the user. |
| **Work Start Time** | Click the hour and minute to indicate the beginning of work time for the user. |
| **Work End Time** | Click the hour and minute to indicate the ending of work time for the user. |
| **Enable User Expiry** | Click **Yes** or **No** to enable or disable user expiration after the expiry period elapses. |
| **User Inactive Period (in days )** | Type the number of inactive days after which the user ID is blocked.  Note.png**Note**: This box is available only if you select **Yes** in the **Enable** **User Expiry** field group. |
| **Block User** | Click **Yes** or **No** to block or unblock the user ID. |
| **Lock User** | Click **Yes** or **No** to lock or unlock a user account. |

1. Click **Save** to save the user ID.

When you create a user ID, a welcome email is sent to the user that contains the link to access their logon credentials. The following images display a sample email and the screen that displays the logon credentials of a user after the user clicks the **Please click here to get login credentials** link.



**Figure 28: Sample email that is sent to the user after user ID creation**

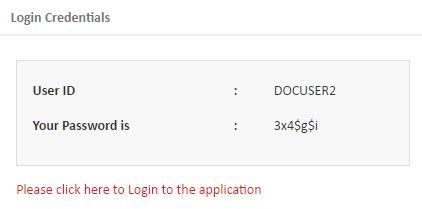


Figure : The Login Credentials screen

### View or Modify a User ID

You can view or modify a user ID that you have created. You must search for the record before you can view or modify its details. You can modify all of the details for a user ID, but you cannot modify the user ID. You can also change the status of a user ID from **Active** to **Inactive** or **Inactive** to **Active**.

**Note.pngNote:** You can modify only an active record.

Perform the following steps to view or modify a user ID:

1. On the menu bar, point to **My Accounts**, and then click **Create User** to open the **User** screen.

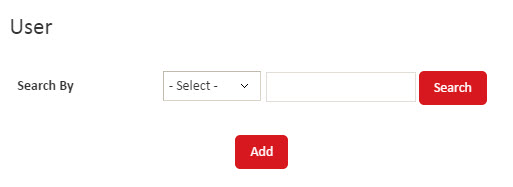


Figure : The User search screen

1. In the **Search By** list, click one of the following search criteria:

* **ALL** – Select this option to display the list of all user IDs.
* **User Name** – Select this option to search using the name of a user, and then in the box, type the name of the user to search for. Click **Search**.
* **User Role** – Select this option to search using the user role, and then in the list, click the user role to search for. Click **Search**.
* **User ID** – Select this option to search using the unique user ID, and then in the box, type the user ID to search for. Click **Search**.

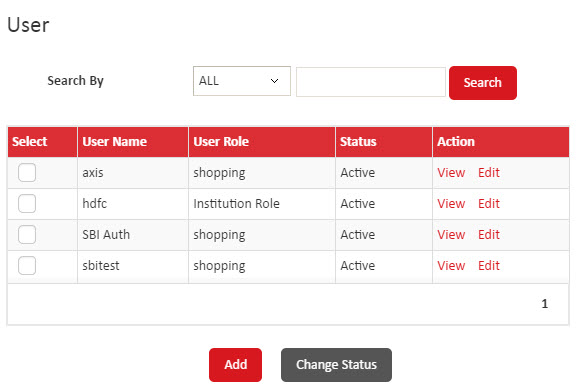


Figure : The User screen

1. Depending on the requirement, perform one of the following steps:

* To view the details of a user, click **View** to open the **View User** screen.
* To modify the details of a user ID, click **Edit** to open the **Edit User** screen. Modify the required details. For more information about the values to specify in the fields, see [Create a User ID](#_Create_a_user_1).
* To change the status of a user ID, in the **Select** column, select a check box or multiple check boxes to select records, and then at the bottom of the screen, click **Change Status**. If a confirmation message is displayed, then click **OK**.

# Configuring the Institution

This chapter describes how to create and maintain institutions. Additionally, it explains how to configure institution parameters, brand type, encryption, external connections, listeners, and risk alerts in ADPay Payment Gateway.

[Introduction 42](#_Toc34204253)

[Create and Maintain Institutions 42](#_Toc34204254)

[Modify or View the Details of an Institution 42](#_Toc34204255)

[Configure Institution Level Parameters 50](#_Toc34204256)

[Configure Data Encryption 53](#_Toc34204257)

[Add or Rotate the DEK 53](#_Toc34204258)

[Add or Rotate a KEK 54](#_Toc34204259)

[Change KeyStore Passwords 56](#_Toc34204260)

[Configure Brand Types 57](#_Toc34204261)

[Create a Brand Type 57](#_Toc34204262)

[View or Modify a Brand Type 58](#_Toc34204263)

[Configure External Connections 58](#_Toc34204264)

[Add an HTTPs External Connection 59](#_Toc34204265)

[Add a TCP/IP External Connection 62](#_Toc34204266)

[View or Modify an External Connection 67](#_Toc34204267)

[View or Modify a Listener 68](#_Toc34204268)

[Refresh the Settings on the Server 69](#_Toc34204269)

## Introduction

You can perform the following tasks to configure an institution in ADPay Payment Gateway:

* Create the institution record
* Configure institution-level parameters
* Configure data encryption:
* Add the Data Encryption Key (DEK)
* Add or rotate Key Encryption Key (KEK)
* Configure KeyStore passwords
* Configure brand types
* Configure external connections and listeners

## Create and Maintain Institutions

You can view or modify the details of an institution. Additionally, you can change the status of an institution and configure institution level parameters.

### Modify or View the Details of an Institution

You can modify or view the details of an institution. You cannot modify the institution ID, name, institution user ID, user role, and data encryption key for an institution.

**Note.pngNote:** You can modify only an active record.

You cannot delete an institution record, but you can change the status of the institution.

Perform the following steps to modify an institution:

1. On the menu bar, point to **Configuration**, and then click **Institution** to open the **Institution** screen.



Figure : The Institution search screen

1. In the **Search By** list, click one of the following search criteria:

* **ALL** – Select this option to display the list of all institutions.
* **Institution ID** – Select this option to search using an institution ID, and then in the box, type the identification code of the institution. Click **Search**.
* **Institution Name** – Select this option to search using the name of an institution, and then in the box, type the name. Click **Search**.

1. Depending on the action to perform, follow one of the following steps:

* To view a record, click **View** to open the **View Institution** screen.
* To change the status of a record, in the **Select** column, select the check box to select a record. You can select multiple records. At the bottom of the screen, click **Change Status**, and then click **OK** on the confirmation message.
* To modify a record, click **Edit** to open the **Edit Institution** screen.

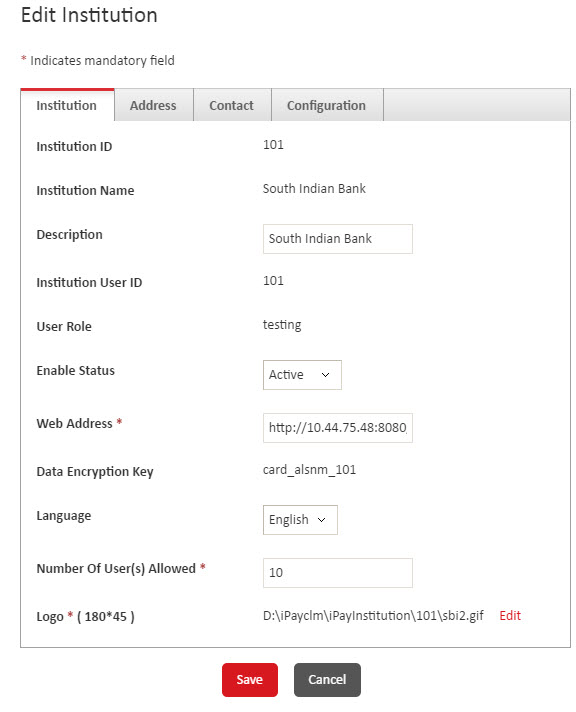


Figure : The Institution tab

Perform the following steps to modify the institution details:

1. On the **Institution** tab, specify the following information:

|  |  |
| --- | --- |
| Field | Description |
| **Institution ID** | Displays the identification code of the institution. You cannot modify this value. |
| **Institution Name** | Displays the name of the institution. You cannot modify this value. |
| **Description** | Modify the description of the institution. |
| **Institution User ID** | Displays the user ID of the administrator user of the institution. You cannot modify this value. |
| **User Role** | Displays the role that the administrator user belongs to. You cannot modify this value. |
| **Enable Status** | Click **Active** or **Inactive** as the status of the institution. |
| **Web Address** | Modify the web address of the institution. |
| **Data Encryption Key** | Displays the data encryption key for the institution. You cannot modify this value. |
| **Language** | Click the language to use for the institution. |
| **Number of User(s) Allowed** | Modify the number of users that can be created by the institution. |
| **Logo (180\*45 )** | Click **Edit** to modify the logo of the institution. The **Logo** box and **Browse** button are displayed. Click **Browse** to select and upload a different logo. |

1. Click the **Address** tab.

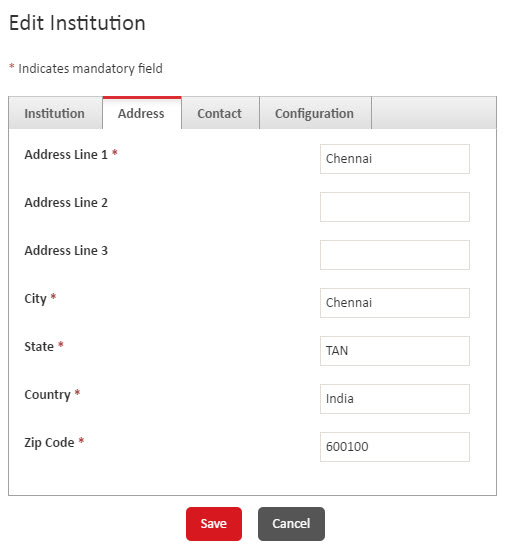


Figure : The Address tab

1. Update the address details of the institution.
2. Click the **Contact** tab

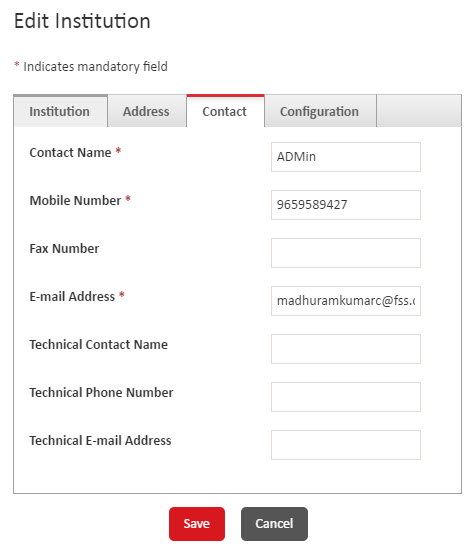


Figure : The Contact tab

1. Specify the following details of the contact person for the institution:

* Name
* Contact number
* Fax number
* Email address
* Name of the technical contact person
* Contact number of the technical contact person
* Email address of the technical contact person

1. Click the **Configuration** tab.

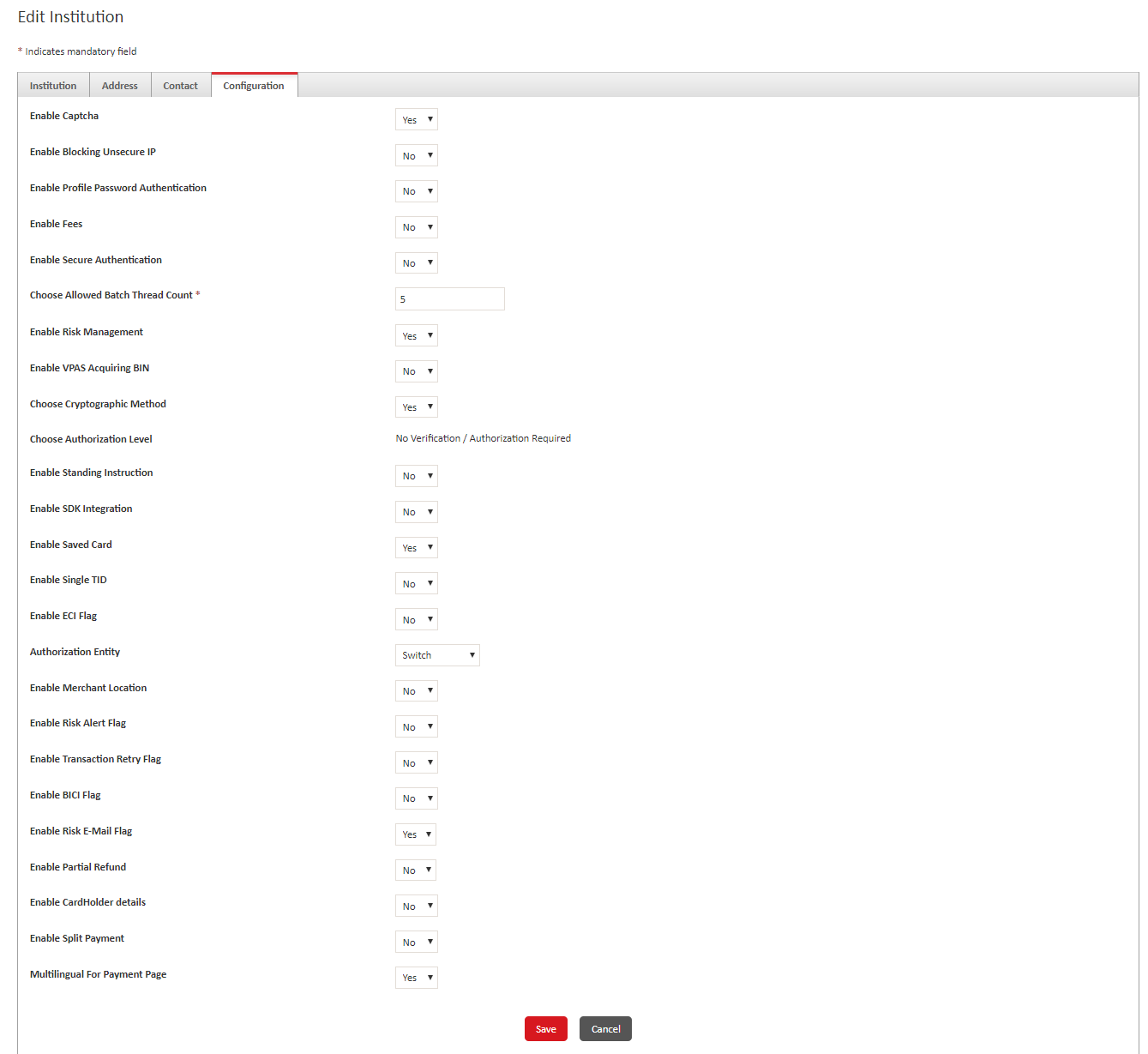


Figure : The Configuration tab screen

1. Specify the following information:

|  |  |
| --- | --- |
| Field | Description |
| **Enable Captcha** | Click **Yes** or **No** to enable or disable captcha to be displayed at logon. |
| **Enable Blocking Unsecure IP** | Click **Yes** or **No** to enable or disable blocking unsecure IP addresses. |
| **Enable Profile Password Authentication** | Click **Yes** or **No** to enable or disable profile password authentication for the bank and merchant users of the institution. If you click **Yes**, then the bank and merchant users must specify the profile password to access transaction and configuration modules. |
| **Enable Fees** | Click **Yes** or **No** to enable or disable fees on transactions. |
| **Enable Secure Authentication** | Click **Yes** or **No** to enable or disable secure authentication. |
| **Choose Allowed Batch Thread Count** | Type the number of batch transaction threads that are allowed for the institution. A single thread runs a single batch process. |
| **Enable Risk Management** | Click **Yes** or **No** to enable or disable risk management for the institution. |
| **Enable VPAS Acquiring BIN** | Click **Yes** or **No** to enable or disable Visa Pont of Sale (POS) Authentication Server (VPAS) acquiring BIN for multi-currency transactions. If you click **Yes**, then one VPAS acquiring BIN for each currency will be used for 3D secure authentication. |
| **Choose Cryptographic Method** | Click **Yes** or **No** to allow or block merchants from choosing cryptographic method. If you click **Yes**, then FI can select a cryptographic method for merchants. The cryptographic method can be **Plain Text**, **Hashing**, or **Encryption**. |
| **Choose Authorization Level** | Displays the authorization level for the institution. You cannot modify this value.  If this field displays the values **Only Verification Required** or **Verification and Authorization Required**, then maker, checker, and authorizer functionality is enabled for the institution. |
| **Enable Standing Instruction** | Click **Yes** or **No** to enable or disable standing instruction transactions. |
| **Enable SDK Integration** | Click **Yes** or **No** to enable or disable SDK Integration. |
| **Enable Saved Card Checkout** | Click **Yes** or **No** to enable or disable merchants from allowing customer to save and use Saved Card payment option. |
| **Enable Single TID** | Click **Yes** tomanage multiple merchants on a single terminal ID. Alternatively, click **No**. |
| **Enable ECI Flag** | Click **Yes** or **No** to enable or disable the 3-D Secure authentication for debit card transactions. |
| **Authorization Entity** | Click one of the following options to indicate the authorization entity to use for the institution:   * Switch * Interchange * Both |
| **Enable Merchant Location** | Click **Yes** to display the first two characters of the ISO defined merchant location code. Alternatively, click **No** to display the all three characters. |
| **Enable Risk Alert Flag** | Click **Yes** or **No** to enable or disable risk alerts for the institution. |
| **Enable Transaction Retry Flag** | Click **Yes** or **No** to enable or disable the flag for Transaction Retry. |
| **Enable BICI Flag** | Click **Yes** or **No** to enable or disable the configuration of an external connection for the Switch/Interchange. |
| **Enable Risk E-mail Flag** | Click **Yes** or **No** to enable or disable the risk e-mail flag for the transaction. |
| **Enable CardHolder details** | Click **Yes** or **No** to display the cardholder’s details on the payment screen. |
| **Enable Partial Refund** | Click **Yes** or **No** to display the Partial Refund amount. |
| **Enable Split Payment** | Click **Yes** or **No** to display the split payment option. |
| **Multilingual For Payment Page** | Click **Yes** or **No** to display the multilingual for the payment page. |

1. Click **Save** to save the changes.

### Configure Institution Level Parameters

You can configure the institution level parameters in ADPay Payment Gateway. You can specify threshold values, batch directories, and enable or disable various features for institutions.

Perform the following steps to configure institution level parameters:

1. Point to **Configuration**, and then click **Institution Configuration** to open the **Institution Configuration** screen.

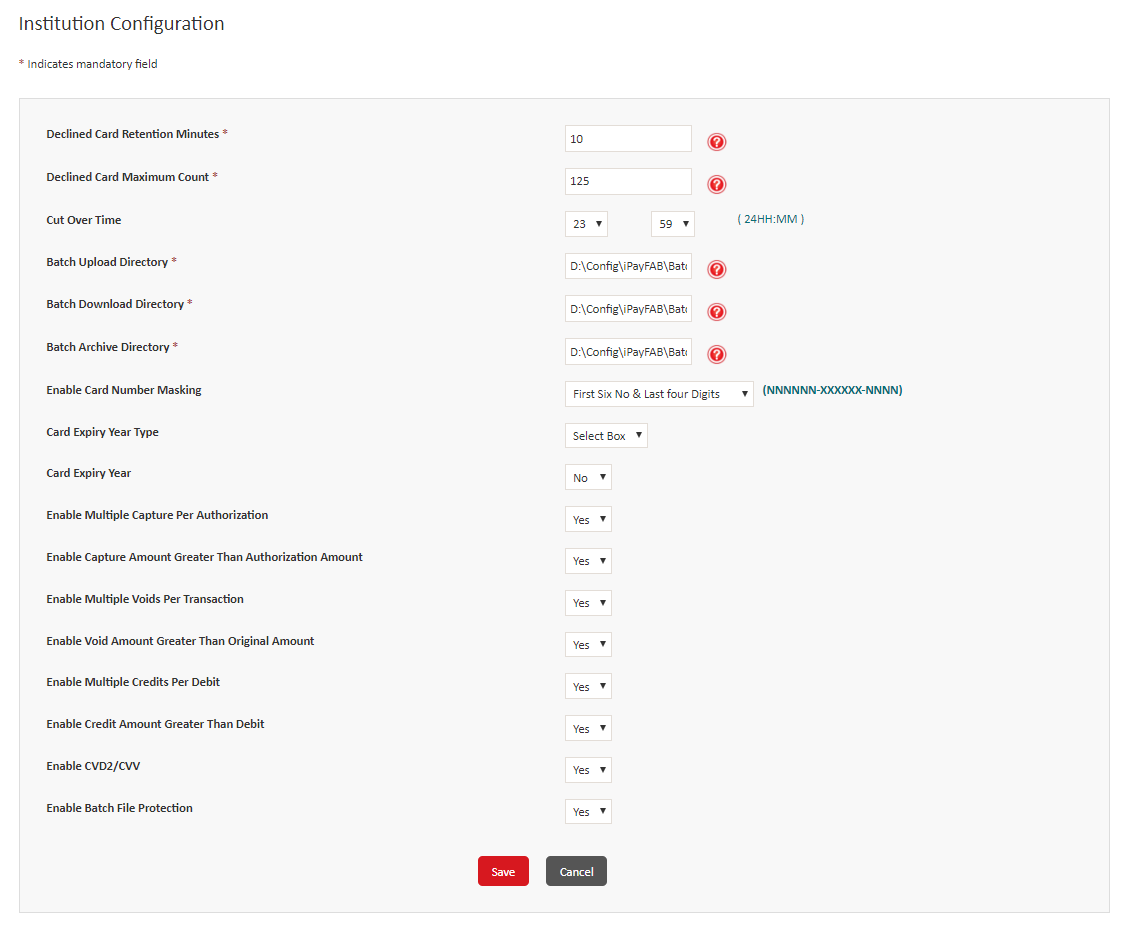


Figure : The Institution Configuration

1. Specify values in the following fields:

|  |  |  |
| --- | --- | --- |
| Field | | Description |
| **Declined Card Retention Minutes** | | Type or modify the number of minutes to specify the maximum transaction count for. |
| **Declined Card Maximum Count** | | Type or modify the maximum number of transactions allowed in the time you specified in the **Declined Card Retention Minutes** box. Any transaction above the maximum count is declined until the retention duration has elapsed or the count for the retention period duration is less than or equal to the limit. |
| **Cut Over Time** | | Click the hour and minutes to indicate the daily cut over time for the institution. |
| **Batch Upload Directory** | | Type or modify the path and name of the directory from where batch processes are uploaded. |
| **Batch Download Directory** | | Type or modify the path and name of the directory to which batch processes are downloaded. |
| **Batch Archive Directory** | | Type or modify the path and name of the batch processes archive directory. |
| **Enable Card Number Masking** | | Click one of the following options:   * **Show All** – Display all the digits of the card numbers. * **Last Four Digits** – Display only the last four digits of the card numbers. The first 12 digits are masked. * **First Six No & Last four Digits** – Display the first six and last four digits of the card numbers. The remaining six digits are masked. |
| **Card Expiry Year Type** | | Click one of the following options to indicate the type of card expiration date field that is displayed to the customer on the institution's payment page:   * Text Box * **Select box -** If you click this, then the **Card Expiry Year** list is displayed. |
| **Card Expiry Year** | | Click **Yes** to define the starting year. Alternatively, click **No** to display the default year list.  Note.png**Note**: If you click **Yes**, then the **Select Year** list is displayed. |
| **Select Year** | | Click the starting year to be displayed in the list. |
| **Enable Multiple Capture Per Authorization** | Click **Yes** or **No** to enable or disable multiple captures for each authorization. | |
| **Enable Capture Amount Greater Than Authorization Amount** | Click **Yes** or **No** to enable or disable capturing an amount greater than authorization amount for transactions. | |
| **Enable Multiple Voids Per Transaction** | Click **Yes** or **No** to enable or disable multiple void transactions for each transaction. | |
| **Enable Void Amount Greater Than Original Amount** | Click **Yes** or **No** to enable or disable creating a void transaction for an amount greater than the original amount. | |
| **Enable Multiple Credits Per Debit** | Click **Yes** or **No** to allow or block multiple credits for a single debit transaction. | |
| **Enable Credit Amount Greater Than Debit Amount** | Click **Yes** or **No** to enable or disable crediting an amount greater than the debit amount. | |
| **Enable CVD2/CVV** | Click **Yes** or **No** to enable or disable Card Verification Data 2 (CVD2) or Card Verification Value (CVV) for authenticating transactions. | |
| **Enable Batch File Protection** | Click **Yes** or **No** to enable or disable protection of batch files. | |

1. Click **Save** to save the changes.

## Configure Data Encryption

ADPay Payment Gateway uses the following types of encryption:

* DEK – The DEK is used to encrypt the sensitive data, such as card numbers.
* KEK – The KEK is used to encrypt the DEK.
* KeyStore passwords – The DEK and KEK are stored in a KeyStore that is protected using two KeyStore passwords.

### Add or Rotate the DEK

The DEK is generated and added to the institution when the institution is created. You can add a DEK in case when the DEK was not generated. The **Card Alias Name** column is updated as **No Card Key** for the institutions for which DEK is not added.

Alternatively, you can rotate the existing DEK.

Note.png**Note**: You must change the KeyStore passwords when you rotate the DEK.

Perform the following steps to add or rotate the DEK:

1. Point to **Configuration**, and then click **DEK** to open the **Data Encryption Key** screen.
2. In the **Institution** list, click an institution name and then click **Search**.

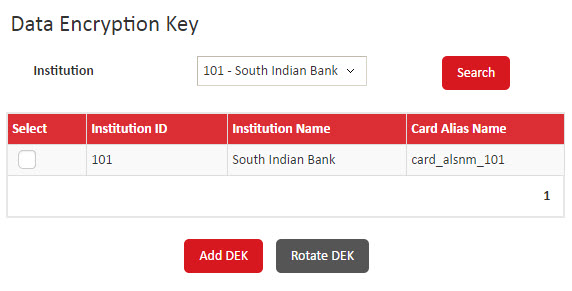


Figure : The Data Encryption Key screen

1. Depending on the task, perform one of the following steps:

* To add a DEK, click **Select** to select a record, and then click **Add DEK**.

Note.png**Note**: You can add the DEK for institutions for which DEK has not been generated. The **Card Alias Name** column for such institutions is updated as **No Card Key**.

* Alternatively, to rotate the DEK, click **Select**, and then click **Rotate DEK**, and perform the following steps:

1. In the **Verifying KeyStore Password** screen, in the **KeyStore Password Part1** and **KeyStore Password Part2** boxes, type the two KeyStore passwords, and then click **Validate** to validate.
2. If a confirmation message is displayed, then select the user to change the passwords for, and then click **OK**.
3. The **Change KeyStore Password** screen is displayed. You must change the KeyStore password in order to complete the DEK rotation. To do so, in the **New** **KeyStore Password Part1** and **New** **KeyStore Password Part2** boxes, type the new KeyStore passwords, and then click **Save** to rotate the DEK.

### Add or Rotate a KEK

You can add a KEK if one is not already added for an institution. The **Card Alias Name** column is updated as **No Card Key** for the institutions for which KEK is not added. Alternatively, you can rotate an existing KEK for an institution to remove the old KEK and adds a new KEK.

Note.png**Note**: You must change the KeyStore passwords when you rotate the KEK.

Perform the following steps to add or rotate the KEK:

1. Point to **Configuration,** and then click **KEK** to open the **Key Encryption Key** screen.
2. In the **Institution** list, click an institution name and then click **Search**.

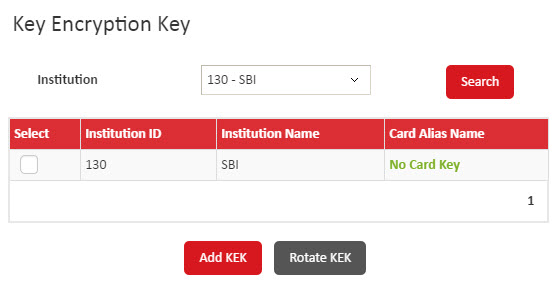


Figure : The Key Encryption Key screen

1. Depending on the task, perform one of the following steps:

* To add a KEK, click **Select** to select a record, and then click **Add KEK**.

Note.png**Note**: You can add the KEK for institutions for which KEK has not been generated. The **Card Alias Name** column for such institutions is updated as **No Card Key**.

* Alternatively, to rotate the KEK, click **Select**, and then click **Rotate KEK**, and perform the following steps:

1. In the **Verifying KeyStore Password** screen, in the **KeyStore Password Part1** and **KeyStore Password Part2** boxes, type the two KeyStore passwords, and then click **Validate** to validate.
2. If a confirmation message is displayed, then select the user to change the passwords for, and then click **OK**.
3. The **Change KeyStore Password** screen is displayed. You must change the KeyStore password in order to complete the KEK rotation. To do so, in the **New** **KeyStore Password Part1** and **New** **KeyStore Password Part2** boxes, type the new KeyStore passwords, and then click **Save** to rotate the KEK.

### Change KeyStore Passwords

Perform the following steps to change the KeyStore passwords:

1. Point to Configuration, and then click Change KeyStore Password to open the Change KeyStore Password screen.

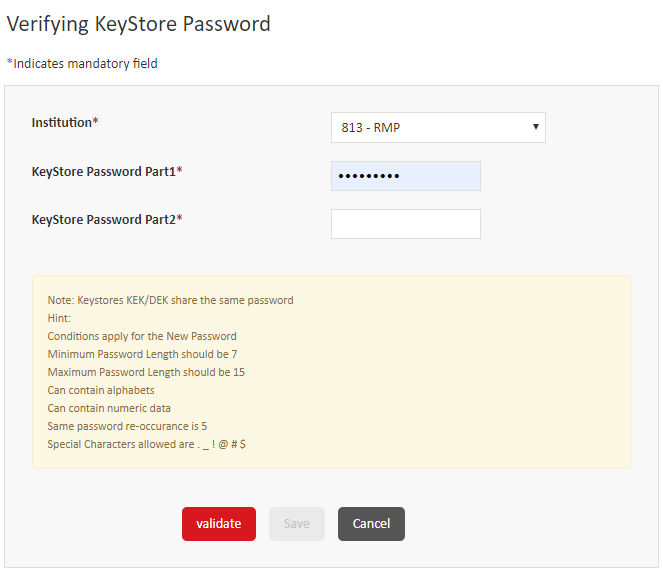


Figure : The Verifying KeyStore Password screen

1. In the **Institution** list, click the institution to change the KeyStore Passwords for.
2. In the **KeyStore Password Part1** and **KeyStore Password Part2** boxes, type the two KeyStore passwords.
3. Click **Validate**, and then click **OK** in the **Confirm Password Change** dialog box.
4. The **Change KeyStore Password** screen is displayed, type the new KeyStore passwords one by one in both the boxes.
5. Click **Save** to save the new passwords.

## Configure Brand Types

A brand type indicates a group of payment instruments’ BIN ranges that are configured to be processed similarly at terminals for an institution. You can create, view, or modify brand types.

### Create a Brand Type

Perform the following steps to create a brand type:

1. Point to **Configuration**, and then click **Brand Type** to open the **Brand Type** screen.
2. Click **Add** to open the **Add Brand Type** screen.

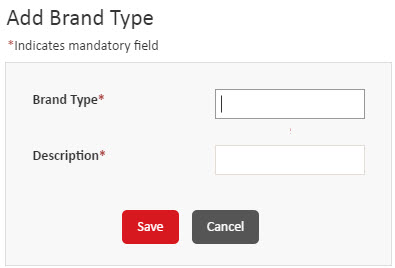


Figure : The Add Brand Type screen

1. In the **Brand Type** box, type the identification code of the brand type.
2. In the **Description** box, type the description of the brand type.
3. Click **Save** to create the brand type.

### View or Modify a Brand Type

You can view the details of a brand type or modify the description of a brand type. You cannot modify the identification code of a brand type.

**Note.pngNote:** You can modify only an active record.

You cannot delete a brand type, but you can change the status of the brand type.

Perform the following steps to view or modify a brand type:

1. Point to **Configuration**, and then click **Brand Type** to open the **Brand Type** screen.
2. Depending on the action to take, perform one of the following steps:

* To view the details of a brand type, click **View**. Click **Back** to return to the **Brand Type** screen.
* To modify the description of a brand type, click **Edit**, and then modify the description. Click **Save**.
* To change the status of a brand type, in the **Select** column, select a check box or multiple check boxes to select records, and then at the bottom of the screen, click **Change Status**. If a confirmation message is displayed, then click **OK**.

## Configure External Connections

You can configure the details of an external system that ADPay Payment Gateway connects to. For example, a transaction switch, Visa directory, or MasterCard directory.

You can create an external connection with Transmission Control Protocol/Internet Protocol (TCP/IP) protocol for socket connection or Hyper Text Transfer Protocol Secure (HTTPs) protocol for web URL connectivity. The TCP/IP connection can be created for Base 24, Aggregator, or Aggregator Echo Application Programming Interface (API) connection types. A connection can be created for each application instance.

Note.png**Note**: You must configure all three types of API Connections (Base24, Aggregator, or Aggregator Echo).

You can create a new external connection. Alternatively, you can view or modify an existing record. You can also change the status of an external connection.

### Add an HTTPs External Connection

You can create an HTTPs external connection for web URL connectivity with or without Secure Socket Layer (SSL).

Perform the following steps to add an HTTPs connection:

1. Point to Configuration, and then click External Connection to open the External Connection screen.
2. Click **Add** to open the **Add External Connection** screen.

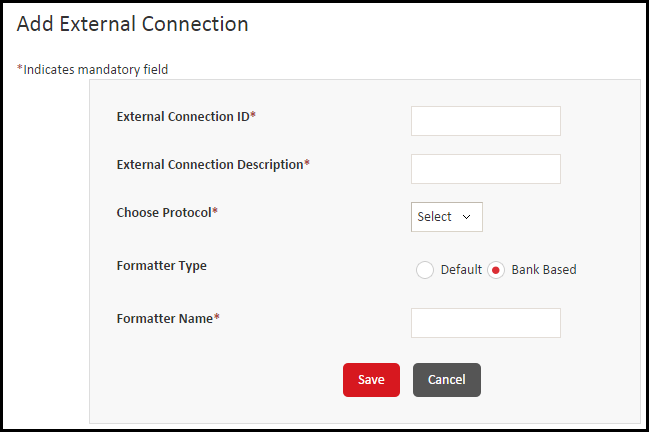


Figure : The Add External Connection screen

1. In the **External Connection ID** box, type unique identification code of the external connection.
2. In the **External Connection Description** box, type the description of the external connection.
3. In the **Choose Protocol** list, click **Https**. The remaining fields on this screen are displayed.
4. In the **Formatter Type** field group, click one of the following options to indicate the transactions that are supported by the connection:

* **Default**
* **Bank Based**

1. In the **Formatter Name** box, type the name of the formatter.

Note.png**Note**: This field is displayed only if you click **Bank Based** in the **Formatter Type** field group.

1. In the **Choose Connectivity Mode** list, click a connectivity mode to use for the external connection. Based on the value that you select, the remaining fields on this screen may vary.

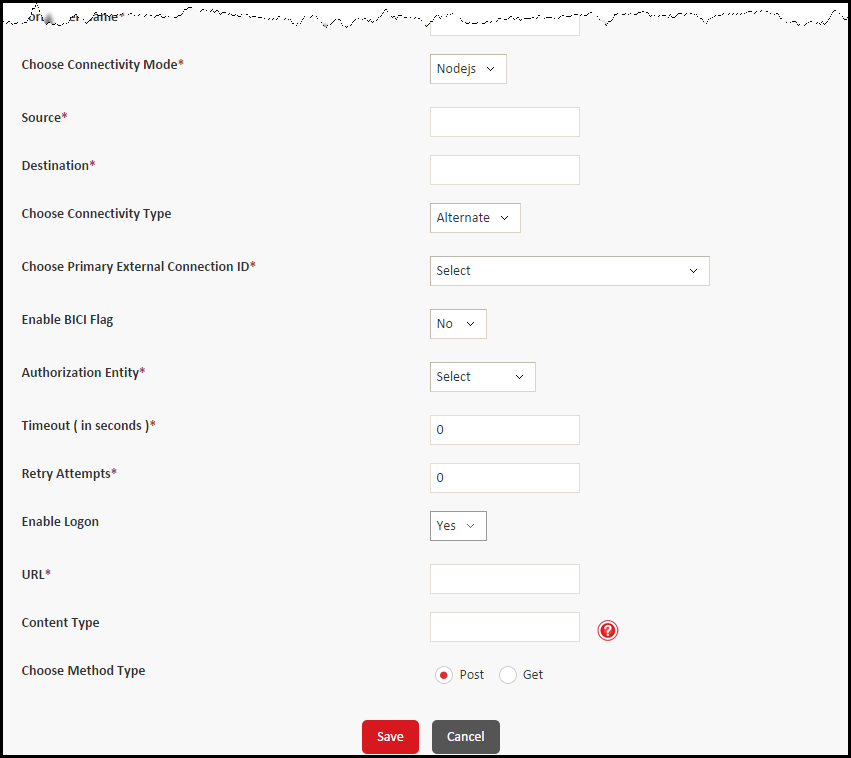


Figure : Adding an HTTPs connection

1. Specify values in the following fields for the HTTPs connection:

|  |  |
| --- | --- |
| Field | Description |
| **Source** | Type the source URL to use for the external connection.  Note.png**Note**: This field is displayed only if you select **Nodejs** in the **Choose Connectivity mode** list. |
| **Destination** | Type the destination URL to use for the external connection.  Note.png**Note**: This field is displayed only if you select **Nodejs** in the **Choose Connectivity mode** list. |
| **Choose Connectivity Type** | Click **Primary** or **Alternate** to indicate the type of connection. If you click **Alternate**, then the **Choose Primary External Connection ID** list is displayed. |
| **Choose Primary External Connection ID** | Click the connection to use as the primary connection.  Note.png**Note**: This list is displayed only if you select **Alternate** in the **Choose Connectivity Type** list. |
| **Enable BICI Flag** | Click **Yes** to enable the payment gateway to connect directly to BICI switch. Alternatively, click **No** to connect through an intermediate switch. |
| **Authorization Entity** | Click **Switch** or **Interchange** to indicate the authorization entity for the key. |
| **Authorization Type** | Click the type of authorization to use for the external connection. |
| **Timeout (in seconds)** | Type the time in seconds after which an idle connection is timed out. |
| **Retry Attempts** | Type the number of retry attempts for the connection. |
| **Enable Logon** | Click **Yes** to check the connectivity. Alternatively, click **No**.  Note.png**Note**: This field is displayed only if you select **Nodejs** in the **Choose Connectivity mode** list. |
| **URL** | Type the URL to connect to. |
| **Content Type** | Type the type of content or file that is sent to the external system. For example, application/XML or application/TXT. |
| **Choose Method Type** | Click **Post** or **Get** to indicate the type of method to use for the connection. |

1. Click **Save** to save the connection and display a confirmation message.

### Add a TCP/IP External Connection

You can create a TCP/IP external connection for socket connectivity to Base 24, Transaction Engine, or Transaction Engine Echo APIs.

Perform the following steps to add a TCP/IP external connection:

1. Point to **Configuration**, and then click **External Connection** to open the **External Connection** screen.
2. Click **Add** to open the **Add External Connection** screen.

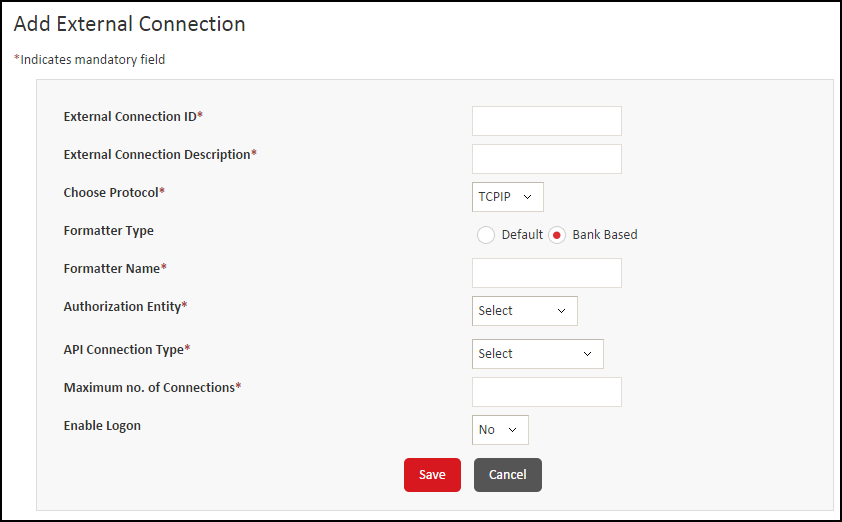


Figure : The Add External Connection screen

1. In the **External Connection ID** box, type a unique identification code of the external connection.
2. In the **External Connection Description** box, type the description of the external connection.
3. In the **Choose Protocol** list, click **TCPIP**. The remaining fields on this screen are displayed.
4. In the **Formatter Type** field group, click one of the following options to indicate the message formats supported by the connection:

* **Default** – ISO defined message format
* **Bank Based** – Bank defined message format

1. In the **Formatter Name** box, type the name of the formatter.

Note.png**Note**: This field is displayed only if you click **Bank Based** in the **Formatter Type** field group.

1. In the **Authorization Entity** list, click one of the following options to indicate the authorization entity for the key:

* **Switch**
* **Interchange**
* **HSM**

1. In the **Authorization Type** list, click **Visa** or **Master** to indicate the interchange that will authorize the key.

**Note.pngNote**: This list is displayed only if you selected **Interchange** in the **Authorization** **Entity** list.

1. In the **API Connection Type** list, click one of the following options to indicate the API connection type:

* **Base 24**
* **Aggregator**
* **Aggregator Echo**

The remaining fields on this screen are displayed depending on the API connection type.

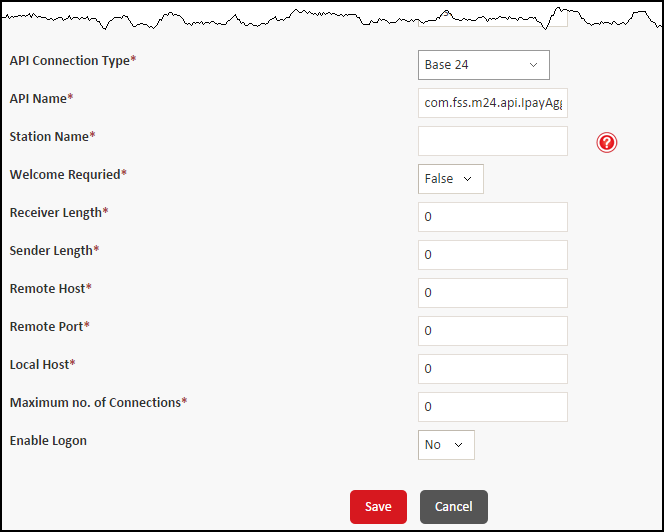


Figure : Adding a Base 24 external connection

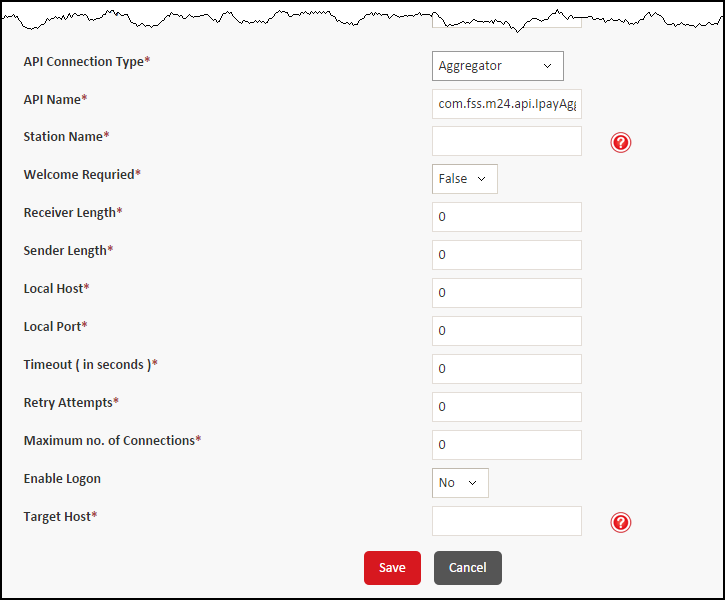


Figure : Adding an Aggregator external connection

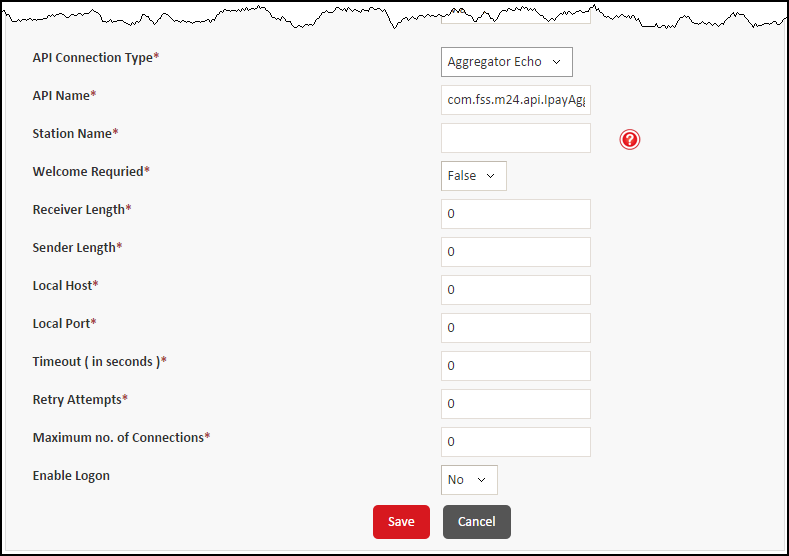


Figure : Adding an Aggregator Echo external connection

1. Depending on the connection type that you clicked, specify the following details:

|  |  |
| --- | --- |
| Field | Description |
| **API Name** | Displays the URL where the APIs are available for the connection. The value in this box depends on the authorization entity that you selected. This is a read-only field. |
| **Station Name** | Type com.ipayfab.m24.api.IpayAggAPI as the name of the station. |
| **Welcome Required** | Click **True** or **False** to enable or disable logon for Base 24, Visa, and MasterCard. |
| **Receiver Length** | Depending on the type of connection, type one of the following values:   * For **Base24** API connection, type 2 * For **Aggregator** API connection, type 2 * For **Aggregator Echo** API connection, type 4 |
| **Sender Length** | Depending on the type of connection, type one of the following values:   * For **Base24** API connection, type 2 * For **Aggregator** API connection, type 2 * For **Aggregator Echo** API connection, type 4 |
| **Remote Host** | Type the Base 24 host address for the connection.  **Note.pngNote**: This field is available only for **Base 24** API connection type. |
| **Remote Port** | Type the Base 24 port number for the connection.  **Note.pngNote**: This field is available only for **Base 24** API connection type. |
| **Local Host** | Type the manager server IP address for the connection. |
| **Local Port** | If you clicked **Aggregator** or **Aggregator Echo** in the **API** **Connection Type** list, then type the manager server port number.  **Note.pngNote**: This field is not available for **Base 24** API connection type. |
| **Timeout (in seconds)** | If you clicked **Aggregator** or **Aggregator Echo** in the **API** **Connection Type** list, then type the time in seconds after which a connection request is timed out.  **Note.pngNote**: This field is not available for **Base 24** API connection type. |
| **Retry Attempts** | If you clicked **Aggregator** or **Aggregator Echo** in the **API** **Connection Type** list, then type number of times a connection should be retried.  **Note.pngNote**: This field is not available for **Base 24** API connection type. |
| **Maximum no. of Connections** | Depending on the type of connection, type one of the following values:   * For **Base24** API connection, type 1 for each manager server * For **Aggregator** API connection, type 50 or more each manager server * For **Aggregator** **Echo** API connection, type 1 or more for each manager server |
| **Host Event** | Click **Yes** or **No** to indicate that host event is triggered or not triggered by the connection. |
| **Event Interval (in seconds)** | If you clicked **Yes** in the **Host Event** list, then type the time period interval between host events, in seconds. |
| **Target Host** | Type the URL of the target host.  **Note.pngNote**: This field is available only for **Aggregator** API connection type. |
| **Enable Logon** | Click **Yes** to check the connectivity. Alternatively, click **No**. |
| **Logon Interval (in seconds)** | Type the time interval in seconds to check the connectivity status.  **Note.pngNote**: This field is available only if you click **Yes** in the **Enable Logon** list. |

1. Click **Save** to add the external connection and display a confirmation message.

### View or Modify an External Connection

You can modify the details of an active external connection. Alternatively, you can change the status of an external connection.

Perform the following steps to view or modify an external connection:

1. Point to Configuration, and then click External Connection to open the External Connection screen.
2. Depending on the action to take, perform one of the following steps:

* To view the details of an external connection, click **View**. Click **Back** to return to the **External Connection** screen.
* To modify the details of an external connection, click **Edit**, and then modify the details. Click **Save**. For more information, see [Add an HTTPs external connection](#_Add_an_HTTPs) or [Add a TCP/IP external connection](#_Add_a_TCP/IP).
* To change the status of an external connection, in the **Select** column, select a check box or multiple check boxes to select records, and then at the bottom of the screen, click **Change Status**. If a confirmation message is displayed, then click **OK**.

## View or Modify a Listener

ADPay Payment Gateway 3.3.1 is deployed in different servers. However, the servlet listeners should run only in one managed server. These listeners are added in the ADPay Payment Gateway from the backend. However, you can modify these listeners, if required. You cannot modify the name of the listener.

Perform the following steps to view or modify a listener configuration:

1. On the menu bar, point to **Configuration**, and then click **Listener Configuration** to open the **Listener Configuration** screen.
2. Depending on the task, perform one of the following steps:

* To view the details of a listener, click **View**.
* To modify the details of a listener, click **Edit**, and then perform the following steps:

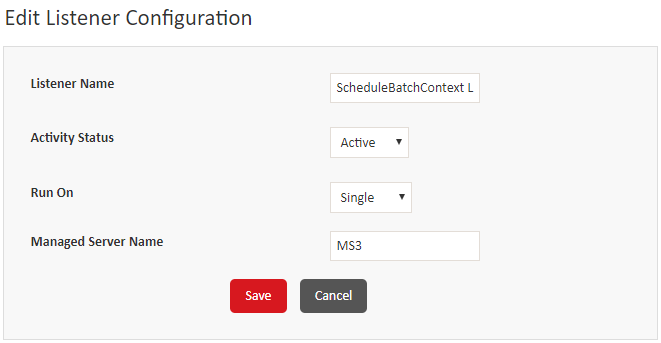


Figure : Editing the Listener Configuration

1. In the **Activity Status** list, click **Inactive** or **Active** to change the status of activities.
2. In the **Run On** list, click an option toindicate the number of managed servers to run the listener on. The listener for Payment Gateway 3.3.1 must be run only one managed server, therefore click **Single**. The **Managed Server Name** box is displayed.
3. In the **Managed Server Name** box, modify the name of the managed server to run the listener on.
4. Click **Save**.

## Refresh the Settings on the Server

You can use this option to refresh the server to update all of the configuration information on the server. This is required only if the property file has been updated by the administrator.

Perform the following steps to reload the settings:

1. Point to **Configuration,** and then click **Reload Settings** to open the **Reload Settings** screen.

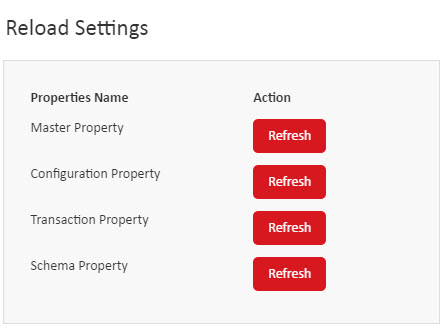


Figure : The Reload Settings screen

1. Click **Refresh** to refresh a set of properties of the application and display a confirmation message.

# Configuring Dashboards

This chapter describes how to configure dashboard templates and panels.

[Introduction 71](#_Toc34152184)

[Configure and Maintain Dashboard Templates 71](#_Toc34152185)

[Create a Dashboard Template 71](#_Toc34152186)

[View or Modify a Dashboard Template 72](#_Toc34152187)

[Configure and Maintain Parameters for Dashboard Templates 72](#_Toc34152188)

[Configure Panels for a Dashboard Template 72](#_Toc34152189)

[View, Modify, or Delete Dashboard Panel Configuration for a Template 74](#_Toc34152190)

## Introduction

You can create a dashboard template, and then configure parameters for each dashboard panel for the template. The number of panels for a dashboard is defined in the template.

## Configure and Maintain Dashboard Templates

You can perform the following tasks:

* Create a dashboard template
* View or modify a dashboard template

You cannot delete a dashboard template.

### Create a Dashboard Template

Perform the following steps to create a dashboard template:

1. Point to Configuration, and then click Dashboard Template to open the Dashboard Template screen.
2. Click **Add** to open the **Dashboard Template - Add** screen.

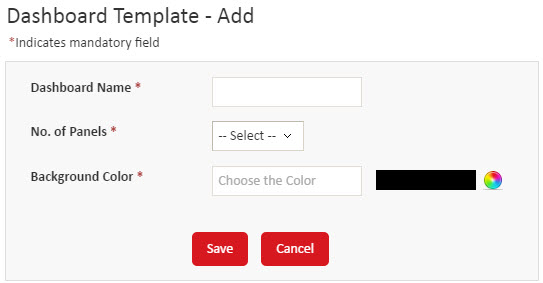


Figure : The Dashboard Template - Add screen

1. In the **Dashboard Name** box, type the name of the template.
2. In the **No. of Panels** list, click a number to indicate the number of panels in the template.
3. In the **Background Color** field group, click the color bar, and then drag the dot to select a color or type the color code in the box. Click **choose** to select the color. The code of the color is updated in the **Background Color** box.
4. Click **Save** to add the template

### View or Modify a Dashboard Template

You can view the details of a dashboard template or modify all of the details of a dashboard template.

Perform the following steps to view or modify a dashboard template:

1. Point to Configuration, and then click Dashboard Template to open the Dashboard Template screen.
2. Depending on the action to take, perform one of the following steps:

* To view the details of a dashboard template, click **View**. Click **Back** to return to the **Dashboard Template** screen.
* To modify a dashboard template, click **Edit**, and then modify the details. Click **Update**.

## Configure and Maintain Parameters for Dashboard Templates

After you create a dashboard template, you must configure the parameters for each panel for the dashboard.

You can configure the parameters for a new template, or view, modify, or delete an existing panel configuration.

### Configure Panels for a Dashboard Template

Perform the following steps to configure panels for a dashboard template:

1. Point to **Configuration**, and then click **Dashboard Parameter** to open the **Dashboard Panel** screen.
2. To configure panels for a dashboard template, click **Add**.The **Dash Board: <Dashboard template name>** screen opens. The screen contains the same number of panel configuration sections as the number of panels you specified when creating the template.

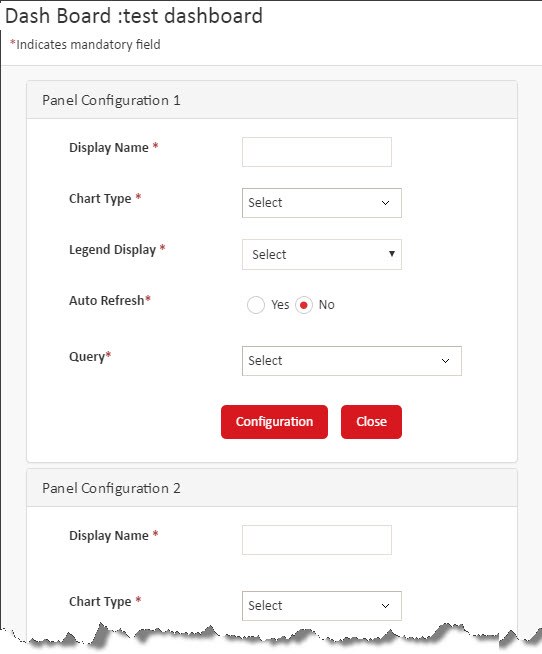


Figure : The Dash Board: <Dashboard template name> screen

1. In each panel section, perform the following steps:
2. In the **Display Name** box, type the display name of the panel.
3. In the **Chart Type** list, click the type of chart to display in the panel.
4. In the **Legend Display** list, click **Yes** or **No** to display or hide legend in the chart.
5. If you clicked **Yes** in the **Legend Display** list, then in the **Legend Position** list, click the position of the legend.

Note.png**Note**: This list is displayed only if you click **Yes** in the **Legend Display** list.

1. In the **Auto Refresh** field group, click **Yes** or **No** to enable or disable automatic refreshing of data in the chart.
2. If you clicked **Yes** in the **Auto Refresh** field group, then in the **Refresh Interval (in Minutes)** box, type the number of minutes after which the data in the chart is refreshed.

Note.png**Note**: This box is displayed only if you click **Yes** in the **Auto Refresh** field group.

1. In the **Query** list, click the query to use to add data to the chart.
2. Click **Configuration**.
3. Repeat step 3 to configure parameters for additional panels, if any.

### View, Modify, or Delete Dashboard Panel Configuration for a Template

Perform the following steps to view, modify, or delete the parameters for the panels for a template:

1. Point to **Configuration**, and then click **Dashboard Parameter** to open the **Dashboard Panel** screen.
2. Depending on the action to take, perform one of the following steps:

* To view the details of a record, click **View**. Click **Cancel** to return to the **Dashboard Template** screen.
* To modify the details of a record, click **Edit**. Modify the required details. For more information, see [Configure Panels for a Dashboard Template](#_Configure_panels_for).
* To delete a record, click **Delete** to open the **Dash Board: <Dashboard template name>** screen. The screen contains the same number of panel configuration section as the number of panels you specified when creating the template. In the dashboard panel section, click **Confirm** to delete the dashboard panel. You can delete multiple panels.

# Reload Settings

You can use this option to refresh the server to update all the configuration information on the server. This is required only if the property file has been updated by the administrator.

[Configure Reload Settings 76](#_Toc34152191)

## Configure Reload Settings

Perform the following steps to reload the settings:

1. Point to **Configuration** and click **Reload Settings**. The **Reload Settings** screen is displayed.

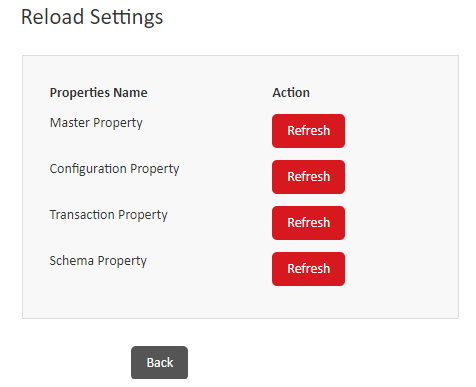


Figure : Reload Settings Screen

1. Click **Refresh** to refresh a set of properties of the application and display a confirmation message.
2. Click **Back** to return to the Reload Settings screen.

# GL Accounting

You can view or modify the predefined GL (General Ledger) Accounting records for a bank user as per FAB requirements. You can specify the fixed charges, variable charges, VAT charges, exception duration and hold duration for the account to keep track of the bank’s financial transactions and to prepare the financial reports.

[Configure GL Accounting 78](#_Toc34152192)

## Configure GL Accounting

Perform the following steps to view or modify the Password Security parameters:

1. Point to **Configuration** and click **GL Accounting**. The GL Accounting screen is displayed.

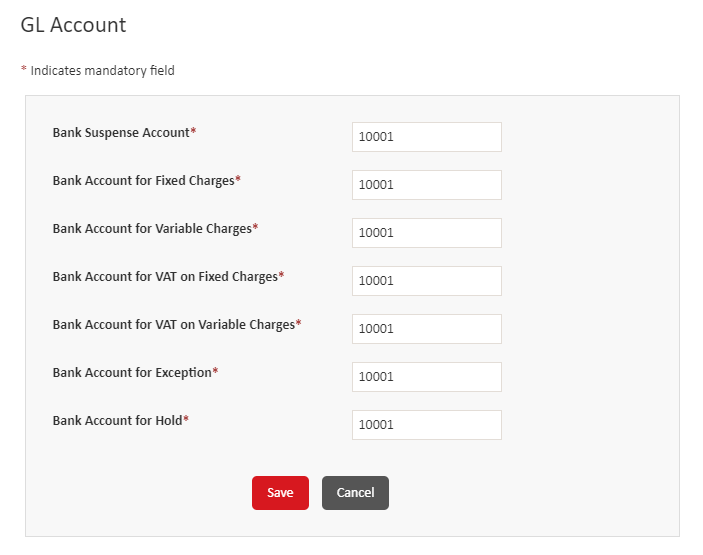


Figure : GL Accounting Screen

1. Specify values in the following fields:

|  |  |
| --- | --- |
| Field | Description |
| **Bank Suspense Account** | Type the unique alphanumeric user account number which needs to be closed temporarily or permanently. |
| **Bank Account for Fixed Charges** | Type the fixed charge amount for the user account. |
| **Bank Account for Variable Charges\*** | Type the Variable charge amount for the user account. |
| **Bank Account for VAT on Fixed Charges\*** | Type the VAT charge over Fixed Charges for the user account. |
| **Bank Account for VAT on Variable Charges\*** | Type the VAT charge over Variable Charges for the user account. |
| **Bank Account for Exception** | Type the user account number which exceeds their transaction limit. |
| **Bank Account for Hold\*** | Type the user account number which has any fraudulent or suspicious transaction or have any history of overdrafts. |

1. Click **Save** to update the changes.

# Index

A

ADPay Payment Gateway 7

B

Bank administrator users 7

Base 24 connection 65

Brand types 58

C

Change your logon password 17

Configure Institution Level Parameters 51

Configure Reload Settings 78

Create institutions 43

Create User Menu 30

Customize menus 22

D

Dashboards 71

Panels 74

Templates 72

Data encryption 54

DEK 54

KEK 55

KeyStore 57

E

External connections 59

HTTPs 60

TCP/IP 63

F

Forgot password 9

G

GL Accounting 79

H

HTTPs 60

HTTPs connection 60

I

Institution configuration 42

Introduction 30, 43, 72

L

Listener 69

Log on 8

M

Modify or View the Details of an Institution 43

O

Overview 7

P

Password Security 12

Passwords

Recover 9

Security parameters 25

R

Refresh server 70

Regenerate and resend a user’s password 18

Reload Settings 77

S

Sample emails 11, 20, 39

Security questions 16

Servlet listener 69

Socket connectivity 63

T

TCP/IP 63

TCP/IP connection 63

Transaction Engine connection 65

Transaction Engine Echo connection 66, 69

U

User IDs 37

User roles 30, 33

V

View or modify a User Menu 31

W

Web URL connectivity 60