



ePDQ Logical Access Controls Password Security Policy

Version 2.0 Issued March 2009

COPYRIGHT NOTICE

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means electronic or mechanical, including photocopying and recording, for any purpose, without the prior written permission of Product Development, Barclaycard Payment Acceptance, Barclays Bank PLC.

Contents

Contents	2
Introduction	3
Purpose of this Document.....	3
Audience	4
Contacting Us	4
Managing the Security Policy	5
Managing Users	5
Security Policy defined.....	7
Password reset	7
Password expiration	8
Setting up the Security Policy	9
Security policy best practice	10

Introduction

Changing passwords on a regular basis can help tighten security, and the best way to ensure that passwords are changed regularly is to have them expire regularly. ePDQ is equipped with a password security policy so that when a user's password expires, that user cannot sign-on to the ePDQ store until they change their password.

The policy is defined as follows:-

- User must reset initial password
- User must reset password assigned by an administrator Expire passwords after 30 days
- Warn user within 10 days of expiration

Purpose of this Document

This document details the procedure and policy for ePDQ Logical Access Controls. It will assist you with the usage of the security policy to meet the needs of your own business security policy requirements.

It is important that you understand how the policy may affect the use of your ePDQ store and we strongly recommend that you read the instructions on how to use the password policy.

Audience

This document should be read by all users or integrators of the ePDQ Payment Service this includes, but is not limited to:

- ePDQ Cardholder Payment Interface (CPI) users
- ePDQ Merchant Payment Interface (MPI) users
- ePDQ Lite users

If you are not sure which product you are using, please contact us.

Contacting Us

Telephone Number – 0844 822 2099*

Email Address – epdq@barclaycard.co.uk

Opening hours - 8:00am to midnight, Monday to Sunday.

**** Calls may be monitored or recorded to maintain high levels of security and quality of service***

Managing the Security Policy

To manage password expiration, you must first assign yourself with an Administrator who is responsible for managing your ePDQ account together with the configuration of the security policy and management of allocation and editing of user accounts. Typically this can be the initial ePDQ user ID that is allocated to you upon set up.

Managing Users

When your ePDQ store is initially set up, we will provide you with a user ID that allows full permissions across your store. The set of permissions allocated to the user is defined by which Role we have allocated. Typically we will allocate an "ePDQ Level 4" role which gives you full permissions including managing the security policy.

You can create new users with different role allocations, allowing different access levels throughout the store. However, the User account required to manage the security policy for your store must be allocated an "ePDQ Level 4" role.

Store users only have access to the store they are allocated to. As long as you have the correct permissions, you can set up new store users. When you add a new user to your store, the most important consideration is which role profile you wish to assign to the user. You may wish to consider restricting access to your store for particular members of staff. This is useful to ensure that no confidential or company sensitive data is accessed by an unauthorised user.

Follow the procedure below to add a new user to your ePDQ store.

1. From the User List Page, select Add.
2. The Add User page will be displayed. Enter the details as required. Mandatory fields are marked with *.
 - The User ID must be at least 8 alpha/numeric characters and can be up to 32 characters. It must not contain any special characters (such as *,/, \, _ , -).
 - The Password must be at least 8 alpha/numeric characters and must not contain any special characters (such as *,/, \, _ , -).
 - Enter the Password again for validation purposes.
 - Enter a Password Hint. This must not be your password and must not compromise the password (i.e. "same as user ID").
 - Password never expires is optional if the password security policy is enabled within your ePDQ store. Always select this if the password is going to be used for the integration of ePDQ
 - Account Name and Account Description are optional, and can be used to identify a user, or store (i.e. Northampton Store).

- The Role is the level of permissions you wish to assign to the user. Use the drop down list to select an appropriate role.
 - Set Pagination size according to how much data you wish to have displayed on each page.
3. You can elect for an email to be sent to the user (or an alternative recipient) confirming set up of the new user.
 4. Once you have entered all the details correctly, select Add. If you have entered any details incorrectly and wish to clear all fields, select Reset.
 5. The new user will now be created, and can be viewed from the User List.

IMPORTANT! Please remember that the functionality described in this document may not be available to all users. The role assigned to them may prohibit access to certain functionality. Please ensure you and your staff are familiar with your role privileges.

TIP! If you make any changes to an existing user to change the password, page display size or role assigned to them, that user will have to sign off and back in again before the changes are effective.

Security Policy defined

With the security policy you can define the following:

- User must reset initial password
- User must reset password assigned by an administrator
- Expire password after X days
- Warn user within X days of expiration

Active	Description
<input type="checkbox"/>	User must reset initial password
<input type="checkbox"/>	User must reset password assigned by an administrator
<input type="checkbox"/>	Expire passwords after 90 days

Warn user within 7 days of expiration

[Apply changes](#)

[Restore policies to default](#)

[Reset form values](#)

Password reset

User must reset initial password or User must reset password assigned by an administrator

A user's password can be configured to expire at the first login or after the password is reset by an administrator. The initial password issued by an administrator is valid for the user's first login only. At that time, ePDQ prompts the user to choose another password before any other work can be done. This way only the person assigned the User ID knows the password. An example of the password reset screen is on the following page

Password reset screen

Your password must be reset. Please enter a new password below.

User ID	jotest
New Password	
Confirm Password	
Password Hint	

Password expiration

A user's password can be configured to expire after a number of days. You can define the amount of time that a password can be used on the ePDQ store for example, if the password expiration is set to a 30-day time interval, a user cannot use a password for more than 29 days. You can also set the ePDQ Administration Tool to warn the user within a configurable time that the password is going to expire.

[Sign Off](#) | [Help](#)

Note: Your password is about to expire. Please update your password before your account becomes disabled.

I would like to update my password now

Proceed without updating my password

Setting up the Security Policy

Before setting the security policy it is important that you update the user account you have allocated for transaction processing, with either the ePDQ Cardholder Payment Interface or ePDQ Merchant Payment Interface, to avoid changes impacting the ability for these accounts to process payments.

To amend the security policy for a specific user

1. After you have logged into the store, click Administration from the top four options.
2. Select Users from the menu on the left. The User List is displayed.
3. Select the User profile and then select update. The Update User screen is displayed.
4. Apply the relevant changes e.g. select Password never expires then select update.
5. The changes will be applied and you will return to the User list.

To set or change the User Security Policy

1. After you have logged into the store, click Administration from the top four options.
2. Select Security Policy from the menu on the left. The User and Password Expiration Policy screen is displayed.
3. Select the Policy options that are appropriate for your own security policy then select Apply these changes.
4. The Policy will now apply to all Users within your ePDQ store

Important – If you are creating a new password we recommend that you do not use the option to 'Allow the system to create the password'

Note - Please be aware that on all new stores the security policy comes enabled by default.

Security policy best practice

1. Changing passwords on a regular basis can help tighten security
2. Encourage regular expiration of passwords e.g. monthly
3. Never set a password to expire if it is used within
 - a. the configuration of transaction processing for the ePDQ Cardholder Payment Interface (CPI)
 - b. the configuration of transaction processing for the ePDQ Merchant Payment Interface (MPI)
 - c. the configuration and set up of Periodic Billing Orders
 - d. the configuration and set up of MPI reports

IMPORTANT - If the password security policy is enabled within your ePDQ store you must ensure that the specific CPI and MPI user set up to perform transaction processing, that the password never expires. Always select the 'Password never expires' option to avoid this user and password expiring.

This user will be required for the "behind the scenes" transaction processing performed by ePDQ and must be maintained at all times (it must not be deleted or modified).