Multi Factor Authentication

User Guide
If you have any comments about this document, please send them to the Manager of Training and Documentation at the following address or send e-mail to MIS.Training@metavante.com.

Oklahoma Solutions Center
FIS Image Solutions
1200 Sovereign Row
Oklahoma City, OK 73108
United States of America

Adobe® Acrobat® and Reader® are registered trademarks of Adobe Systems Incorporated in the United States and/or other countries. Microsoft®, Windows®, and Windows NT® are registered trademarks; and Windows Server™ and Windows Server System™ are trademarks of Microsoft Corporation in the United States and/or other countries. Other product and service names are used for identification purposes only and are the property of their respective owners.

© 2010 Fidelity National Information Services, Inc. and its subsidiaries. All rights reserved worldwide.

This document is protected as a trade secret and under the copyright laws as the property of Fidelity National Information Services, Inc. Copying, reproduction, or distribution to third parties is strictly prohibited.
# Table of Contents

**About This Manual** ........................................................................................................... v

Technical Support ................................................................................................................. ix

**Chapter 1**

**Introduction** ......................................................................................................................... 9

Overview .................................................................................................................................. 10
Getting Started .......................................................................................................................... 10
Requirements ............................................................................................................................. 10
  Operational Requirements ......................................................................................................... 10
  Installation/Setup Requirements ................................................................................................. 10
  System Requirements ................................................................................................................. 11
  Server Hardware Requirements ................................................................................................. 11
  Server Software Requirements ................................................................................................. 11

**Chapter 2**

**Workflow** .............................................................................................................................. 13

Workflow Process ....................................................................................................................... 14

Challenge Question Count and Response Length ...................................................................... 15

**Chapter 3**

**Scenarios** .............................................................................................................................. 19

New User Enrollment ............................................................................................................... 20
  Scenario 1 ................................................................................................................................ 20

Unregistered Enrolled User ......................................................................................................... 24
  Scenario 2 ................................................................................................................................ 24

Registered Enrolled User ............................................................................................................ 26
  Scenario 3 ................................................................................................................................ 26
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Registered Enrolled User Forgotten Password</td>
<td>28</td>
</tr>
<tr>
<td>Scenario 4</td>
<td></td>
</tr>
<tr>
<td>Unregistered Enrolled User Forgotten Password</td>
<td>31</td>
</tr>
<tr>
<td>Scenario 5</td>
<td></td>
</tr>
<tr>
<td>Registered Enrolled User Forgotten Challenge Questions</td>
<td>34</td>
</tr>
<tr>
<td>Scenario 6</td>
<td></td>
</tr>
<tr>
<td>Unregistered User Forgotten Challenge Questions</td>
<td>36</td>
</tr>
<tr>
<td>Scenario 7</td>
<td></td>
</tr>
<tr>
<td>Registered User Re-Enrollment</td>
<td>38</td>
</tr>
<tr>
<td>Scenario 8</td>
<td></td>
</tr>
<tr>
<td>Unregistered User Re-Enrollment</td>
<td>41</td>
</tr>
<tr>
<td>Scenario 9</td>
<td></td>
</tr>
<tr>
<td><strong>Index</strong></td>
<td>45</td>
</tr>
</tbody>
</table>
About This Manual

Multi Factor Authentication is a software solution designed to use forms authentication for authenticating users of its client applications. This manual is intended for users who have responsibility for using Multi Factor Authentication.

Assumptions

This manual assumes that you know how to work in the Microsoft Windows operating environment, and that you know how to use a web browser, like Internet Explorer. In particular, you need to know how to work with pull-down menus, dialog boxes, list boxes, and so on. This manual also assumes that you are using a mouse, and that you know how to use the mouse to select text or graphics.

For complete instructions and information about Microsoft Windows and the keyboard equivalents for mouse actions, see the documentation that comes with Microsoft Windows.

How to Use This Manual

This manual contains three kinds of information:

- **Overview** chapters explain what the product as a whole does. Such chapters cover critical concepts that are a prerequisite to information in the rest of the manual.

- **Procedural** chapters give step-by-step instructions for performing specific tasks with the product. Within these chapters, procedures are identified by a distinctive arrow and heading style, which is also used in the table of contents. For example:

  - Display the System Administration Menu

- **Appendixes** provide reference information about system configuration and related topics.
Text Conventions

This manual uses fonts and typefaces to connect what you read in this guide to what you see on the screen or what you need to type into the system. In particular:

◆ A sans serif font is used for text that is displayed on viewports, windows, or dialog boxes (the Close and OK buttons, the File menu) and for file names (/Etc/Hosts, C:\Windows\Win.ini) that appear within the text of paragraphs.

◆ A monospaced font is used for listing the contents of files and certain programming terms.

◆ A bold monospaced font identifies actual characters you should type. For example, 
  … type exit at the DOS prompt …
  means you should type the characters e, x, i, and t.

◆ Italic identifies a variable that you should replace with the actual text or value appropriate for your system. For example,
  … the file D:\Directory\Filename …
  means you should replace D:, Directory, and Filename with the actual drive and full pathname of the file in question. For example,
  … the file C:\Windows\Win.ini …
  This variable is also used to identify viewports, windows, or dialog boxes. For example, 
  ….the Installation window will appear…..

Special Symbols

The caution symbol to the left of a paragraph indicates that you should carefully read and follow any directions in the paragraph to prevent serious errors or data loss.

The note pad symbol to the left of a paragraph highlights a helpful tip or technique.

This arrow is used to show a series of selections from a menu. For example,

Select File → Run

means you should expand the File menu and select Run.
Indexing Conventions

The index of this manual uses the following conventions to help guide you to other content:

- If more appropriate content is listed elsewhere in the index, the word See will be listed after the term (in italic type) and will be followed by the term you should look for instead. For example:
  creating, See adding

- If a related term is available for the content, the words See also will be listed as a subentry for the term (in italic type) and will be followed by the related term you should also look at. For example:
  defining

    extensions ............ 42
    recording profiles...... 181
    See also adding

Related Publications

Refer to the following manuals for additional information about Multi Factor Authentication. These files are available from your Installation..

<table>
<thead>
<tr>
<th>Document</th>
<th>Filename</th>
<th>Contains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct Suite Configuration Manager Utility Guide</td>
<td>Direct Suite v.5.0 Configuration Manager Utility Guide.pdf</td>
<td>Configuration of scanners, Branch Profiles, Capture Profiles, Display Profiles, IQA Profiles, and Notification Profiles.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Configuration and maintenance of Institutions, Branch Groups, Branches, Merchant Groups, Merchants, Users, User Roles, Alert Messages, Alert Groups, and Notification Groups.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Searching for Merchants and moving Merchants from institution to institution</td>
</tr>
<tr>
<td>Document</td>
<td>Filename</td>
<td>Contains</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Guide.pdf</td>
<td>Viewing and maintaining export jobs and deposits pending export.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Creating and maintaining deployment packages and tasks, including the configuration of Deployment Groups.</td>
</tr>
<tr>
<td><strong>Direct Aggregator System Deployment Guide</strong></td>
<td>Direct Aggregator v5.0 System Deployment</td>
<td>Pre-Installation Security information and configuration, product installation, post-installation security information and configuration, and overall maintenance.</td>
</tr>
<tr>
<td></td>
<td>Guide.pdf</td>
<td>Information regarding the Smart Deposit Manifest Utility, Direct Merchant configuration, CAR/LAR configuration, Multi-factor Authentication configuration, LDAP/Active Directory integration, the Direct Client Install directory, and reference information for all components.</td>
</tr>
</tbody>
</table>
Technical Support

FIS offers a product maintenance plan that includes use of a toll-free hotline and a technical support e-mail address. If your company has purchased a maintenance contract, you can contact FIS OneTouch Solutions in two ways:

- Call 1-800-454-4516
  Customer support representatives are available at this number, Monday through Friday, 7:00 AM to 8:00 PM, Central Time, excluding holidays observed by FIS.
  For emergency “system down” support, you may call any time.

- E-mail supportimage@fisglobal.com
  You can send messages to this address 24 hours per day, every day. Requests will be processed during the hours outlined above.

If your company does not have a current maintenance contract, you will be billed at an hourly rate for use of these services.
Chapter 1

Introduction

Topics

◆ Overview
◆ Getting Started
◆ Requirements
Overview

On October 12th, 2005 the Federal Financial Institutions Examination Council (FFIEC) released new guidelines aimed at overhauling security in Internet-based banking and financial services. The guidance entitled “Authentication in an Internet Banking Environment,” calls upon banks to upgrade current single-factor authentication processes with a stronger, second form of authentication or Multi-Factor Authentication.

It specifically addresses why financial institutions should conduct risk assessments, evaluate customer awareness programs, and implement multi-factor authentication.

The Multi Factor Authentication is a flexible, Multi-layered authentication solution designed to match security with transaction risk, customer need, preference and usability.

Getting Started

This manual is intended to provide instructions and descriptions for using the Multi-Factor Authentication application.

Before using the MFA application you will need an application UserID and a password, and you should meet or exceed the following requirements:

Requirements

Operational Requirements

The System Administrator/Web Client Administrator needs to set up the user ID's and passwords for login by the user. All password changes and locked out scenarios are handled by the System administrator at the Financial Institution level or by the merchant user with 'administrator' role using the web client. Procedures for these, and other possible actions, can be found in the Direct Suite Configuration Manager Utility Guide.

Installation/Setup Requirements

Two separate installs need to be executed - one for the DirectMerchant: Web Client and another separate install for the MFA application. They can either be installed on the same server or on separate servers as desired by the Financial Institution’s requirements.
System Requirements

The following areas have details in the General Information Document. Please refer to the appropriate sections for any questions or concerns that arise.

Server Hardware Requirements

This section is broken into two main parts; the Aggregator Server, and the External Web server. Reference the General Information Document Hardware Requirements section for all server hardware requirements.

Server Software Requirements

This section is broken into three main parts; the Aggregator Servers, the Database Server, and the External Web Server. Reference the General Information Document Software requirements section for all server software requirements.
Chapter 2

Workflow

Topics

- Workflow Process
This manual is intended to guide the user in using the Multi-Factor Authentication (MFA) application.

**Workflow Process**

1. Client initiates the login process by using the User ID set by the System Administrator.
2. Enrollment into MFA involves selecting the confidence factor picture and typing the user's text phrase.
3. The user must then answer all the challenge questions during initial registration.
4. After successfully answering the questions, the user's Cookie is placed on their computer and the user is logged into the system.
5. Forgot challenge questions and deleted Cookie flow helps the user re-register into MFA. Also, if the cookie is deleted by the user, only the challenge questions need to be answered and will be prompted to re-register the computer.
6. Login flow checks for the Cookie and if present, the password page is displayed. If the password matched for the User ID, the user is logged into the system and is presented the application page.

7. Register the Computer helps the user recover from the deletion of the Cookies.

8. The user is presented with a subset of challenge questions to be answered. If answered successfully, the user is logged in and presented with the DirectMerchant: Web Client application page.

9. If the user does not register the computer during initial login, a temporary session ID is created and once the user logs out that particular session is closed. The user during subsequent logins would continue to answer the challenge questions until he registers the computer.

**Challenge Question Count and Response Length**

The number of challenge questions presented is configurable. Valid configuration variables are 1-4. The default setting is 2.
During the MFA registration process, a default minimum length will be specified for each challenge question. The specified minimum length will be provided as a hint to the user as 'help' text for each question during the registration process, but not during login sequences.

If an answer does not meet the configured minimum length, an error message is provided to the user describing the problem and stating the required minimum length. The user is not be able to continue to the next step of MFA registration until all challenge question responses meet the configured minimum length requirement.

Default minimum lengths for challenge questions responses are specified in the table below:

<table>
<thead>
<tr>
<th>Challenge Question</th>
<th>Minimum Response Length</th>
</tr>
</thead>
<tbody>
<tr>
<td>In what year were you married?</td>
<td>4</td>
</tr>
<tr>
<td>In what month is your father’s birthday?</td>
<td>3</td>
</tr>
<tr>
<td>What is your oldest sibling’s middle name?</td>
<td>3</td>
</tr>
<tr>
<td>What was the first car you owned? (make-model)</td>
<td>5</td>
</tr>
<tr>
<td>In what state was your father born? (Spell out state.)</td>
<td>4</td>
</tr>
<tr>
<td>In what state were you born? (Spell out state.)</td>
<td>4</td>
</tr>
<tr>
<td>How many children do you have? (number)</td>
<td>1</td>
</tr>
<tr>
<td>What is the middle name of your first child?</td>
<td>3</td>
</tr>
<tr>
<td>What is your father’s middle name?</td>
<td>3</td>
</tr>
<tr>
<td>What year did you graduate from college? (YYYY)</td>
<td>4</td>
</tr>
<tr>
<td>In what town was your spouse born? (town name only)</td>
<td>5</td>
</tr>
<tr>
<td>In what month did you get married?</td>
<td>3</td>
</tr>
<tr>
<td>What is the first name of your youngest sibling?</td>
<td>3</td>
</tr>
<tr>
<td>What is your Zodiac sign?</td>
<td>3</td>
</tr>
<tr>
<td>What is your mother’s middle name?</td>
<td>3</td>
</tr>
<tr>
<td>In what city did you buy your first home (town name only)</td>
<td>5</td>
</tr>
<tr>
<td>What color was your first car?</td>
<td>3</td>
</tr>
<tr>
<td>What’s your shoe size? (just the number e.g. 6 or 10.5)</td>
<td>1</td>
</tr>
<tr>
<td>Where was your first child born? (town name only)</td>
<td>5</td>
</tr>
<tr>
<td>In what state was your mother born (spell out state)</td>
<td>4</td>
</tr>
<tr>
<td>What is your mother’s first name?</td>
<td>3</td>
</tr>
<tr>
<td>What did you name your first pet?</td>
<td>3</td>
</tr>
</tbody>
</table>
Challenge Question | Minimum Response Length
--- | ---
In what year did you buy your first home? (YYYY) | 3
What is your mother’s Zodiac sign? | 3
What is the house number of your last address? | 3
What is your father’s first name? | 3
In what year was your first child born? (YYYY) | 4
What musical instrument did you play in high school? | 4
In what year did you graduate from high school? (YYYY) | 4
In what month is your mother’s birthday? | 3
What is the first name of your first niece/nephew | 3
In what town were you born? (town name only) | 5

Set Up Secure Authentication

Step 2 of 3 - Set up confirmation questions
Select your confirmation questions. When you have provided answers for the questions, click “Continue setup.”
These questions may be asked when you sign on to confirm that an authorized individual is trying to access financial information online.
When asked, you must correctly answer these questions to sign on.

Question: What is the first name of your first niece/nephew?
Answer: 

Question: What is your shoe size? (just the number e.g. 6 or 10½)
Answer: 
This answer must be at least 2 characters long.

Question: What is your father’s first name?
Answer: 
This answer must be at least 3 characters long.

Question: What is your Zodiac sign?
Answer: 
This answer must be at least 4 characters long.
Answer for question 2 is too short.
Answer for question 3 is too short.
Answer for question 4 is too short.

Continue Setup
Chapter 3

Scenarios

Topics

- New User Enrollment
- Unregistered Enrolled User
- Registered Enrolled User
- Registered Enrolled User Forgotten Password
- Unregistered Enrolled User Forgotten Password
- Registered Enrolled User Forgotten Challenge Questions
- Unregistered User Forgotten Challenge Questions
- Registered User Re-Enrollment
- Unregistered User Re-Enrollment
New User Enrollment

Scenario 1

1. Enter the Login Screen. Click the Enroll in Multi-Factor Authentication link to go to the Secure Authentication Screen.

2. Click the Begin Setup button to continue to the next screen. Otherwise, click the Sign Off button to cancel this process and exit the application.
3. Choose a category, then choose a picture as an addition to the login data.

4. Enter the User ID and the Personal Pass-phrase corresponding to the selected picture.

   **NOTE**

   In addition, the previously chosen picture can be changed on this screen.

5. Click the Continue Setup button to continue to the Challenge Question selections.

6. Choose four challenge questions from the dropdown lists, and enter the answers.
7. Click the Continue Setup button to continue to the Computer Registration Selection.

8. The option to Register this computer or Do not register this computer will be available.

9. Click the Continue Setup button to continue to the Review screen.
10. Preview and change any data previously entered.

11. Click the Submit button to send the data for authentication and enrollment and for logging into the application.
Unregistered Enrolled User

Scenario 2

1. Enter the UserID.

![Image of login page]

2. Click the Login button to continue.

3. Answer the challenge questions, and click the Continue button to proceed, or click the Cancel button to quit the application.

In addition, an option to register the computer is available here.

If the computer isn't registered, challenge questions must be answered before the user can enter a password.
4. Type the password, and click the Login button to log into the DirectMerchant: Web Client application, or click the Cancel button to quit the application.
Registered Enrolled User

Scenario 3

1. Enter the User ID.

2. Click the Login button to continue.
3. Enter the password.

NOTE

If the computer isn't registered, challenge questions must be answered before the user can enter a password.

4. Click the Login button to begin the session, or click the Cancel button to exit the application.
Registered Enrolled User Forgotten Password

Scenario 4

1. Enter the User ID.

2. Click the Forgot your password link to continue to the challenge questions.
3. Answer the challenge questions.

4. Click the Continue button to go to the Change Password screen, or click the Cancel button to exit the application.

5. Enter the new password data, and click the Save button to log into the application.
6. If the password is forgotten or the user cannot answer the challenge questions, it is necessary to re-enroll into MFA. The System Administrator will need to be contacted for re-enrollment.

7. If a user is locked out after three unsuccessful attempts, the System Administrator will need to unlock the account. After the System Administrator unlocks the account, steps 1 through 3 of the scenario needs to be completed. The same password can be used once the account is unlocked.
Unregistered Enrolled User Forgotten Password

Scenario 5

1. Enter the User ID.

2. Click the Login button to continue to the Challenge Questions.
3. Answer all four pre-set questions correctly.

4. The password screen displays.

5. Click the Forgot your password? link to continue to the Enter New Password dialog.
6. The user is prompted to “Enter New Password and Confirm Password since the challenge questions have already been successfully answered.

![Change Password](image)

7. If a user is locked out, the Merchant Administrator will need to unlock the user in the Configuration Management Administrator Tool. The user will then need to repeat steps 1 through 3.
Registered Enrolled User Forgotten Challenge Questions

Scenario 6

1. Enter the User ID.

2. Click the Login button to continue to Password Entry.
3. Click the **Forgot your password** link to continue to the challenge questions. Three attempts are given to answer all four challenge questions correctly.

![Challenge Questions Image]

4. After three unsuccessful attempts, the user is prompted with the error message **If you have forgotten answers to your challenge questions, contact your system administrator to get your account activated.**

5. The user will be locked out, and any previous enrollment will be cleared. The user needs to contact the System Administrator to unlock the User ID, and be required to re-enroll using the re-activated user id and a valid password to access the application.
Unregistered User Forgotten Challenge Questions

Scenario 7

1. Enter the User ID.

2. Click the Login button to continue to Challenge Questions. Answer all four pre-set questions correctly.
3. After three unsuccessful attempts, the user is prompted with the error message If you have forgotten answers to your challenge questions, contact your system administrator to get your account activated.

4. The user will then be locked out and be required to contact the System Administrator to re-enroll using the re-activated User ID and a valid password to access the application.
Registered User Re-Enrollment

Scenario 8

1. Click the Enroll in Multi-Factor Authentication link.

2. Click the Begin Setup button to continue to the next screen. Otherwise, click the Sign Off button to cancel this process and exit the application.
3. Choose a category, and then choose the picture as an addition to the login data.

4. Enter the User ID and the Personal Pass-phrase corresponding to the selected picture.

5. Click the Continue Setup button to continue to the Challenge Question selections.
6. If the user has already enrolled into MFA, the following error message displays:
   User ID- <username> has already enrolled in Multi Factor Authentication. Please contact your
   System Administrator if you wish to re-enroll with the same User ID.

7. The user must contact the system administrator to re-enroll or continue to use the
   existing user name for logging in to the application.
Unregistered User Re-Enrollment

Scenario 9

1. Enter the Login Screen. Click the Enroll in Multi-Factor Authentication link to be taken to the Secure Authentication screen.

2. Click the Begin Setup button to continue to the next screen. Otherwise, click the Sign Off button to cancel this process and exit the application.
3. Choose a category, then choose the picture as an addition to the login data.

4. Enter the User ID and the Personal Pass-phrase corresponding to the selected picture.

NOTE

The previously chosen picture can be changed on this screen.
5. Click the Continue Setup button to move to the Challenge Question selections.

6. If the user has already enrolled into MFA, the following error displays: User ID-<username> has already enrolled in Multi Factor Authentication. Please contact your System Administrator if you wish to re-enroll with the same User ID.

7. Contact the system administrator to re-enroll. In this scenario, the user is locked out and needs to contact the System Administrator. The user is required to re-enroll using the re-activated User ID and a valid password to access the application.
Index

C

challenge questions ........................................ 15, 16, 21
change password ........................................... 29, 33
Cookie ......................................................... 14

D

documentation ............................................... vii

F

Federal .......................................................... 10
FFIEC ............................................................ 10

P

Personal Pass-phrase ......................................... 21

R

register .......................................................... 22
registration .................................................... 16