



RFID Internet Security Pad User's Manual

ENETPAD USER MANUAL

Copyright Notice

Copyright 2005 by Macally Peripherals

This manual is furnished under license and may be used or copied only in accordance with the terms of such license.

Except as permitted by such license, no part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or any means, electronic, mechanical, recording, or otherwise, including translation to another language or format, without the prior written permission of Macally Peripherals.

The content of this manual is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Macally Peripherals. Macally Peripherals assumes no responsibility or liability for any errors or inaccuracies that may appear in this book.

Macally is a trademark of the Mace Group Inc. All other product names, trademarks and registered trademarks in this document are the property of their respective holder.

FCC Information

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communication. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Changes or modification made to this equipment not expressly approved by the manufacturer. May void the FCC authorization to operate this equipment.

Warranty

Macally Peripherals warrants that this product will be free from defects in materials and workmanship for period of time specified on the product packaging. This limited warranty shall commence from the date of purchase. Macally Peripherals warranty is not transferable and is limited to the original purchaser. If the product is found to be defective then, as your sole remedy and as the manufacturer's only obligation, Macally Peripherals will repair or replace the product. This warranty shall not apply to products that have been subjected to abuse, misuse, abnormal electrical or environmental conditions, normal wear and tear or any condition other than what can be considered normal use.

Warranty Disclaimers

Macally Peripherals makes no other warranties, expressed or implied, and specifically disclaims any warranty for merchantability or fitness for a particular purpose. The exclusion of implied warranties is not permitted in some states and the exclusions specified herein may not apply to you. This warranty provides you with specific legal rights. There may be other rights that you have which vary from state to state.

Limitation of Liability

The liability of Macally Peripherals arising from this warranty and sale shall be limited to a refund of the purchase price. In no event shall Macally Peripherals be liable for costs of procurement of substitute products or services, or for any lost profits, or for any consequential, incidental, direct or indirect damages, however caused and on any theory of liability, arising from this warranty and sale. These limitations shall apply not with standing any failure of essential purpose of any limited remedy.

Macally U.S.A

Mace Group Inc.
4601E. Airport Drive,
Ontario, CA 91761
Tel: 909. 230.6888
Fax: 909. 230.6889
e-mail: sales@macally.com
website: www.macally.com

Contents	3
Introduction	4
Systems and Environments	5
Software Installation	6
Using Login2Go	7
Configuration tab	8
Options tab	13
Favorite tab	16
Tips for Effective Learning	16
Known Issues	17
Using LoginEZ	18
LoginEZ Setup	18
LoginEZ Activation	20
Set back to Microsoft Login	22
eNetCard Management Tool	25
RFID Enabled Application Development	28
FAQs (Frequently Asked Questions)	28

Thank you for purchasing Macally eNetPad. The product package includes Macally eNetPad™ (a USB optical pad with built-in RFID reader/writer), an eNetCard (Philips mifare® Standard 1K RFID card), and a CD with Login2Go™, LoginEZ, software and pad driver. Before connecting eNetPad to your computer, please read the entire manual to understand how to install the pad driver and software, and use application Login2Go and LoginEZ.

More information about Macally products and services is available through following sources:

- The Macally Home Page on the World Wide Web URL <http://www.macally.com>
- Macally Tech Support:
In U.S.A., please call 1-909-230-6778 (9AM - 5PM PST, Monday - Friday) or
In other time and areas, E-mail us at techsupport@macally.com
- Please register your Macally product at <http://www.macally.com/register.html>

Introduction

The Login2Go™ software, an RFID enabled application, allows users to log in the various password protected web sites without having to remember and enter the user name and password every time. You only need to place RFID tags or eNetCard close to Macally eNetPad to invoke Login2Go for automatic web login.

First, user needs to configure and train the application Login2Go to log in a password protected web site. Once Login2Go learns the whole login process, it will be able to perform the automated login without user intervention thereafter. Since input of user name and password are not required in automated login, the risk of personal data being stolen by spyware is greatly reduced.

Certain information of automatic web login, mainly passwords, can be stored in the RFID tags for user identification and security purposes. Other information is stored in a local configuration file to minimize usage of memory space of a given RFID tag. The configuration file, whose file name is tag ID followed by suffix “.pas”, is created for each RFID tag.

For the convenience, users are allowed to store the complete sequence of actions for selected web sites on RFID tags, which are called portable web sites. These portable web sites can be automatically launched with RFID tag scanned(read) on any PCs having Login2Go and Macally eNetPad reader/writer installed. Due to limited memory space in RFID tags, it is strongly recommended to store no more than four portable web sites.

LoginEZ application allows user to login to Windows operating system with eNetCard and eNetPad.

The Macally eNetCard RFID card in this package is Philips mifare Standard with 1K Bytes space in transportation mode. Login2Go will initialize the card when used at the first time. This applies to any newly issued Philips mifare Standard 1K tags from manufacture. After the initialization, Login2Go can store information in those tags. On the other hand, for those RFID tags which only tag Id can be read, e.g., ISO 14443A RFID tag being initialized by other applications and not writable by Login2Go, users can still invoke Login2Go based on the RFID tag ID. However, all data can only be saved as local files.

* Login2Go and LoginEZ are trademark of RFCyber Corp. eNetPad is a trademark of Macally Peripherals. mifare® is a trademark of Philips Semiconductors.

Systems and Environments

Operation Systems Supported:

- Microsoft Windows 2000, XP, Server 2003

Minimum PC Requirements:

- Pentium III 500MHz
- 256MB Main Memory
- 15MB Disk Space
- USB 1.1
- Screen Resolution 800x600
- An existing pad(to complete Login2Go software installation)

Web Browser:

- Microsoft Internet Explorer Version 6.0 and above

Languages:

- English

RFID Tags (Transponder, Proximity Integrated Circuit Card)

- Read/Write Tag Data and Read Tag ID operations:
ISO 14443A – Philips mifare® Standard 1K(including Macally eNetCard)
- Read Tag ID operation:
ISO 14443A – other Philips mifare® family such as Ultralight, 4K, ProX, DesFire
- RFID tags could be built into different products and form factors, such as credit card, debit card, bank card, phone card, watch, and cell phone etc.

Macally eNetPad:

- USB optical pad and RFID reader/writer integrated
- RFID Tag compatibility: all tags and form factors listed above
- Anti-collision support: multiple tags can be read simultaneously
- RFID reading distance: up to 0.78”(or 2cm) above eNetPad
- ISO 14443A compliant 13.56MHz frequency

Software Installation

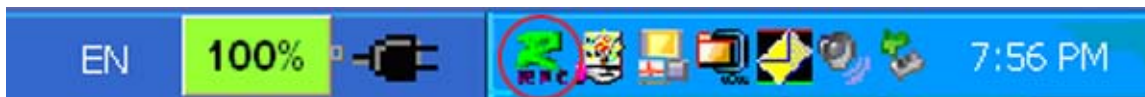
It is required to install the Login2Go and LoginEZ software first before plugging in the Macally RFID eNetPad. You must log in with administrator privilege to perform the following installation steps.

1. Insert the included software CD into your CD-ROM drive. Installation should start automatically, if not, please open the CD icon, locate and double click Login2Go_LoginEZ.exe to start.
2. Follow the on-screen instruction to complete the software installation. It is required to restart machine after the installation.
3. After reboot, a new icon appears in the system tray of taskbar to indicate status of Macally eNetPad. Red color "R" below means Login2Go is not ready.



Fig. 1

4. Plug in the Macally eNetPad into USB port. "Found New Hardware Wizard" window pops up, follow the on-screen instruction to complete pad driver installation.
5. Now, the "R" icon in task bar will change color to green as shown below. The top pad LED window will show blue color as well. If you don't see these, please try to reboot the system.



6. Congratulation! You have successfully installed Login2Go and Login2EZ software, and the Macally eNetPad.

If you accidentally plug in the eNetPad before installing software, the "Found New Hardware Wizard" window will pop up and ask for hardware device drivers, please unplug eNetPad, follow the step 1 through 6 above to install software first.

Using Login2Go

Login2Go is running on top of RFCyberOne, a runtime version of RFCyber application development platform RFCyberWork. The new “R” icon on system tray of taskbar mentioned in previous section is the RFCyberOne Console to indicate the status of the Macally eNetPad under RFCyberOne. The icon should be green color for normal operation. By right clicking on the RFCyberOne Console icon “R”, users get a pop-up window with a set of commands to control the RFCyberOne service shown in Fig. 3. Only Windows login user Ids with administrator privilege can invoke those commands successfully.

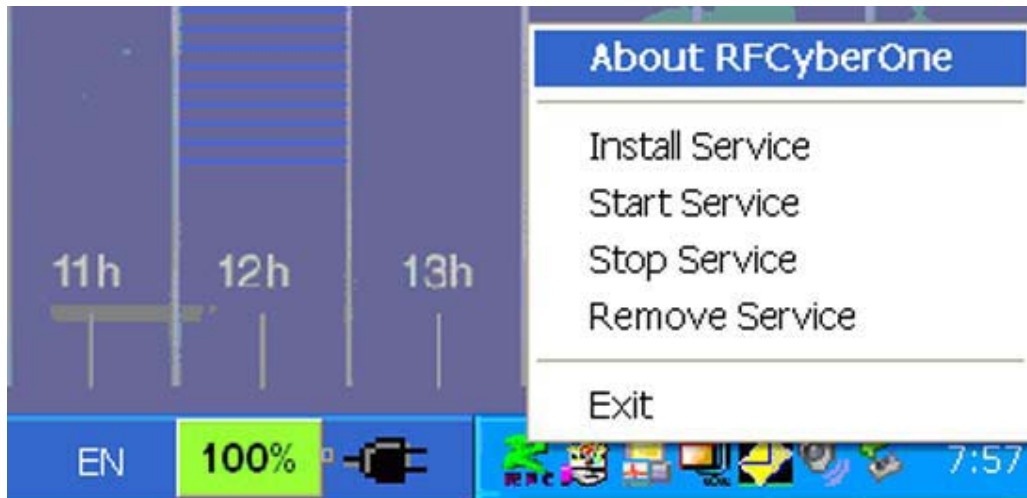


Fig. 3

If eNetPad is plugged in, the color of Console icon is not green yet, the RFCyberOne service should be restarted with the following order of commands: Stop Service, Remove Service, Install Service, Start Service. Depending on the system load, users might need to wait a few seconds after each command.

The Exit command will terminate RFCyberOne Console and remove the icon from system tray of taskbar. To bring back the icon, please go through “Start -> All Programs -> RFCyber -> RFCyberOne -> RFCyberOne Console”.

To invoke Login2Go, users first put an RFID tag(eNetCard or other form factors) within 0.78” near the top of Macally eNetPad for couple of seconds, until Login2Go is invoked automatically. Please note, for security purpose, RFID tag is the only key to invoke Login2Go, there is no other way to run Login2Go. So if you lose eNetCard(i.e. RFID tag), you will not be able to invoke Login2Go application to automate web site login. Furthermore, please do not remove RFID tag from eNetPad too soon, otherwise tag reading will fail, error message will pop up, then you have to follow on-screen instruction to close error messages and put RFID tag on top of eNetPad again.

After a tag is scanned or read via eNetPad, a series of message windows pop up, Login2Go application is shown as Fig. 4. In title bar, it displays ID of your RFID tag, e2125332, and type of the RFID tag, (Philips) mifare 1K.

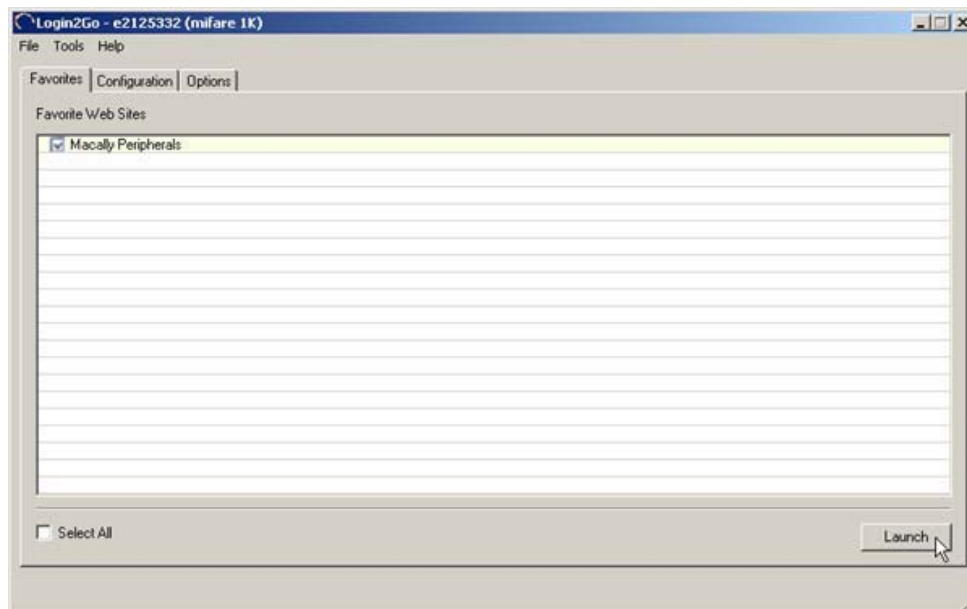


Fig. 4

The first tab displayed in Login2Go is “Favorites”, where you normally select preconfigured favorite web sites to launch. Detailed instructions on how to use Login2Go application are presented below.

Configuration tab

To configure your favorite web sites, you select “Configuration” tab, as shown in Fig. 5.

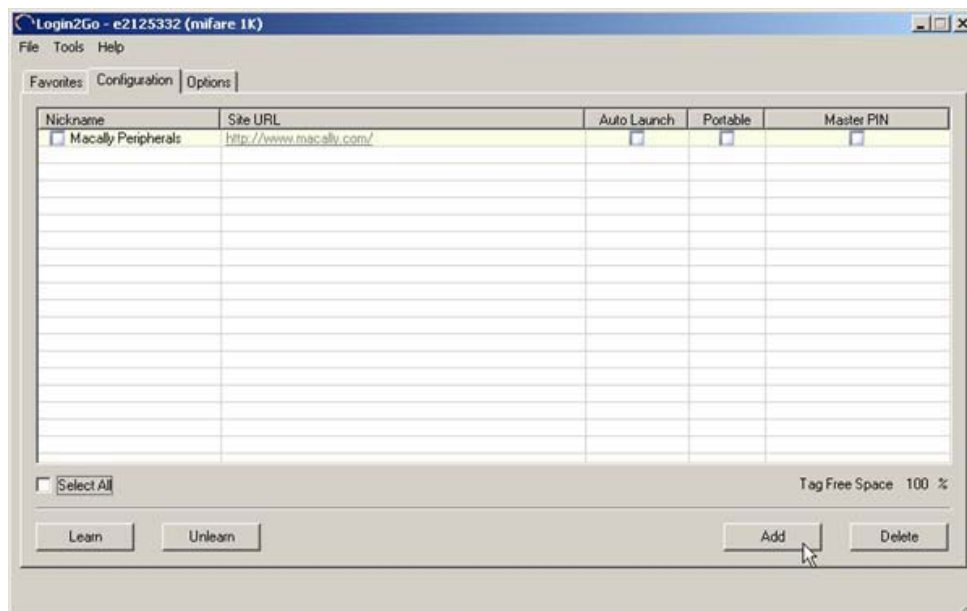


Fig. 5

Configuration tab has following fields:

- Nickname – The name you assign to a Favorites web site.
- Site URL – Login page URL of the favorite web site.
- Auto Launch – If this field box is checked, the favorite web site will be automatically launched once Login2Go is invoked.
- Portable – If this field box is checked, entire login process and login info of the favorite web site will be stored in the RFID tag instead of configuration file in computer, so that the web site will launch in any computer running Login2Go without further configuration.
- Master PIN (Personal Identification Number) – check this box to enable Master PIN verification whenever the web site is to be launched or configured. This feature adds extra level of security to prevent unauthorized access to your favorite web sites, in case eNetCard is lost or stolen.
- "Tag Free Space" indicates available space in percentage for the RFID tag. For example, if user chooses a favorite web site to be portable, the "Tag Free Space" percentage will be decreased. Please note, the data is not actually saved into the tag until the "Save" command is executed.

To start adding your own favorite web sites, click the "Add" button. A New Favorite Web Sites dialog window is popped up, for example, "Yahoo Mail" is entered as Nickname and "http://mail.yahoo.com" is entered in URL field as shown in Fig. 6 below.



Fig. 6

This Yahoo Mail URL is fairly short to input, and takes you to login page directly. However, some web sites do not display login screen in their home pages, users usually have to click through a few pages to find "Log in" or "Sign in" button to click in order to enter Login page. These unnecessary intermediate pages slow down every launching (automatic login) process of the web site. For example, if you start from the home page URL <http://www.troweprice.com>, it requires you to click through at least two intermediate pages to display actual login screen URL

<https://www3.troweprice.com/cda/public/common/indexLogin?scn=header> where to input login user name and password. To avoid errors, we recommend users to open a web browser separately, enter your web site to be configured, click through into login page where user name (or user ID) and password are asked. Then, in Address field, highlight and copy the exact URL of the login page as in Fig. 7, using the T. Rowe Price web site login as example,

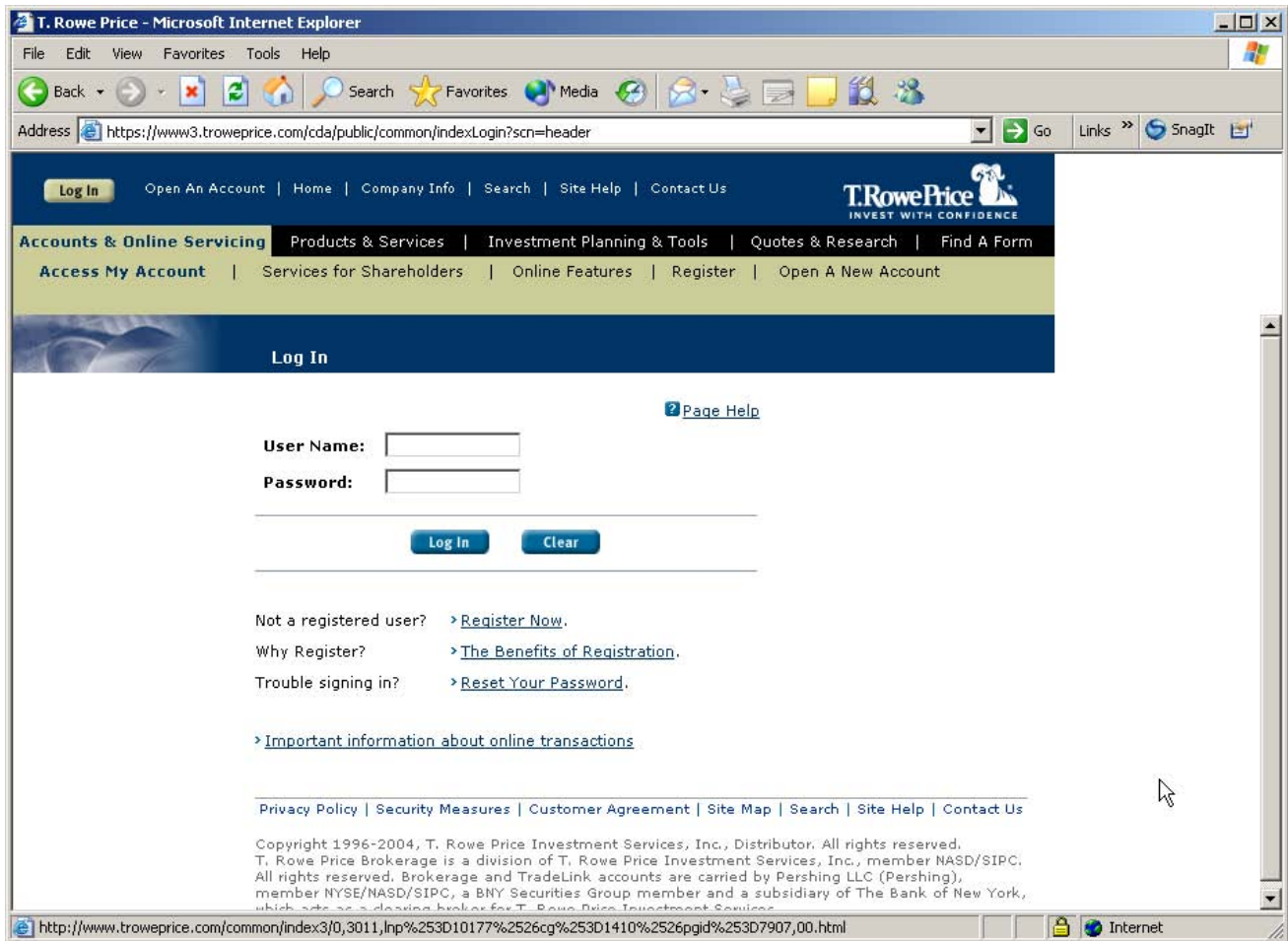


Fig. 7

then switch to Login2Go, paste the login URL in URL field in New Favorite Web Sites window.

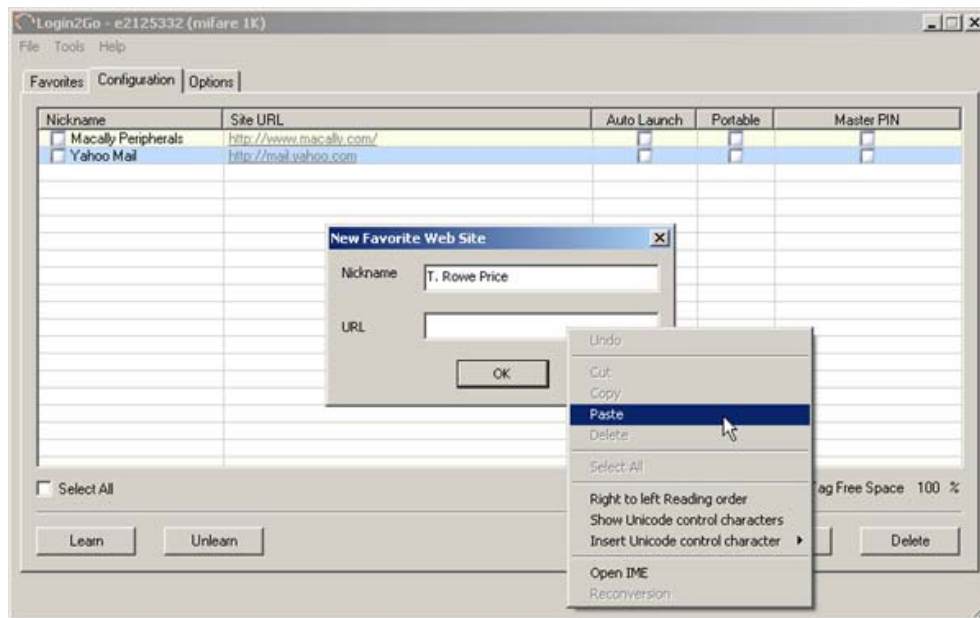


Fig. 8

This copy-and-paste approach is quite effective, you can avoid memorizing the long login URL and typing error, and reduce chance for web site login incompatibility. But if you encounter any problem by following this approach, such as dynamically generated login web page URL, you can still start from beginning, enter home URL of the web site, instead of login page URL, in New Favorite Web Site. Please unlearn and learn login sequence again whenever Site URL is updated.

Let's return to example of added favorite web site "Yahoo Mail".

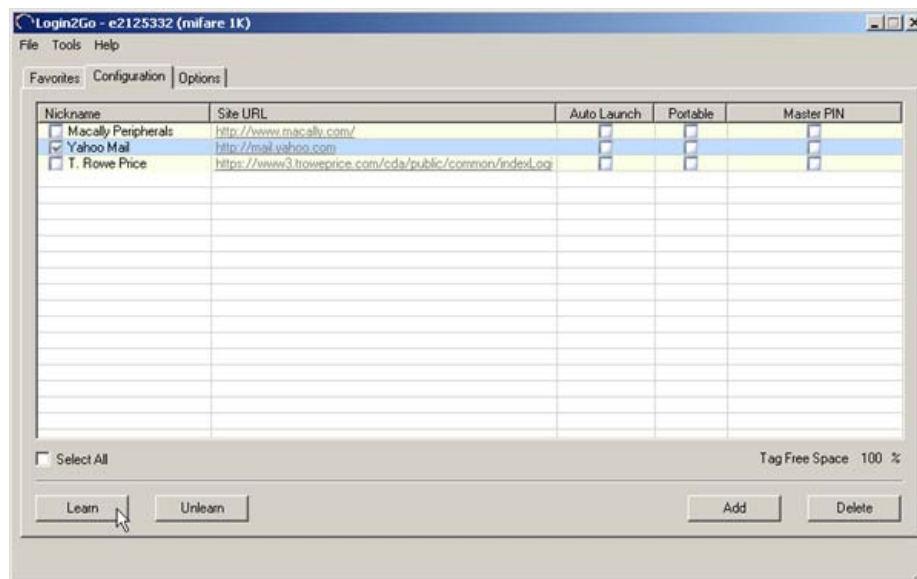


Fig. 9

To learn the login sequences, user can check the square box in front of the site nickname, click the "Learn" button to teach Login2Go the sequence of login actions of selected web sites. As shown in Fig. 10, an embedded IE (Microsoft Internet Explorer) is popped up with title "Learn Login – Yahoo Mail" to track and record sequence of login actions as user enters user name and password to logon into the favorite web site. At end, "Done" or "Downloading (100%)" message is displayed on lower left corner of the embedded IE indicating login is successful, the sequence of login actions has been recorded. User can click "Finish" button to complete the learning process.

Please note, some well-known web mail services, such as Yahoo Mail, Hotmail and Gmail will download cookies into your computer after a successful login for quicker future login. This practice affects Login2Go relearn process, it is not a bug in Login2Go. As a message at bottom left corner of the learning window reminds you, if you observe a web site is logged in unexpectedly even without your input of user name and password, please log off your web mail account from all IE browsers including embedded one, and learn again.

To learn more tips, please refer to subsection “Tips for effective learning” later.

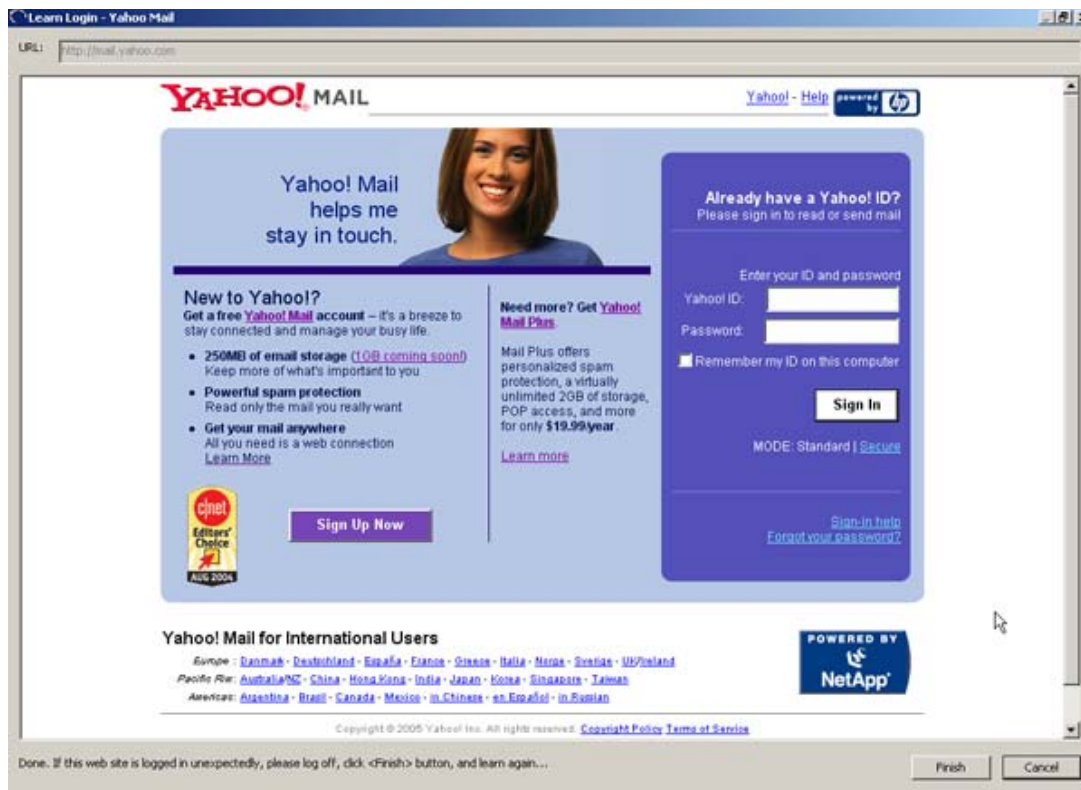


Fig. 10

After the successful learning process, “Site URL” field of the web site turns into dark blue color in Fig. 9.

Users can click the “Unlearn” button to erase previously learned sequence of login actions for a favorite web site. “Site URL” field of the web site changes back to grey color.

If users change password for the favorite web site later, they can update the password stored in Login2Go without repeating the learn process. This is done by right clicking on, for example, the “Yahoo Mail” row in “Configuration” tab in Fig. 11, and changing password.

Generally, web sites are updated frequently. It is possible that certain stored Login URL or info are no longer valid, launching such web site will result in failure. If you experience this problem, find out what the changes are from the web site, configure and learn the login process again with updated information.

The “Delete” button lets users delete selected favorite web sites from Login2Go.

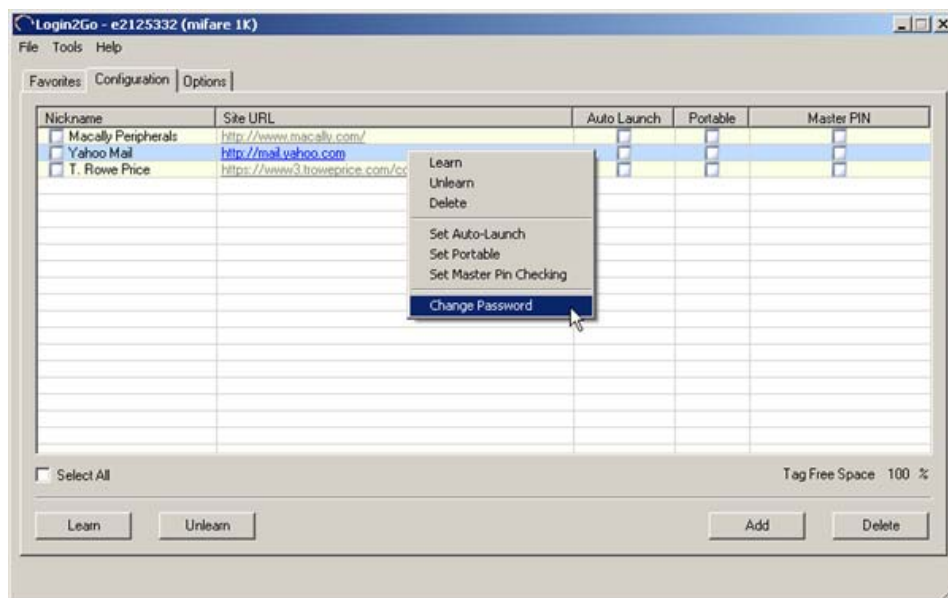


Fig. 11

Options tab

The “Options” tab in Fig. 12 offers more features in using Login2Go application.

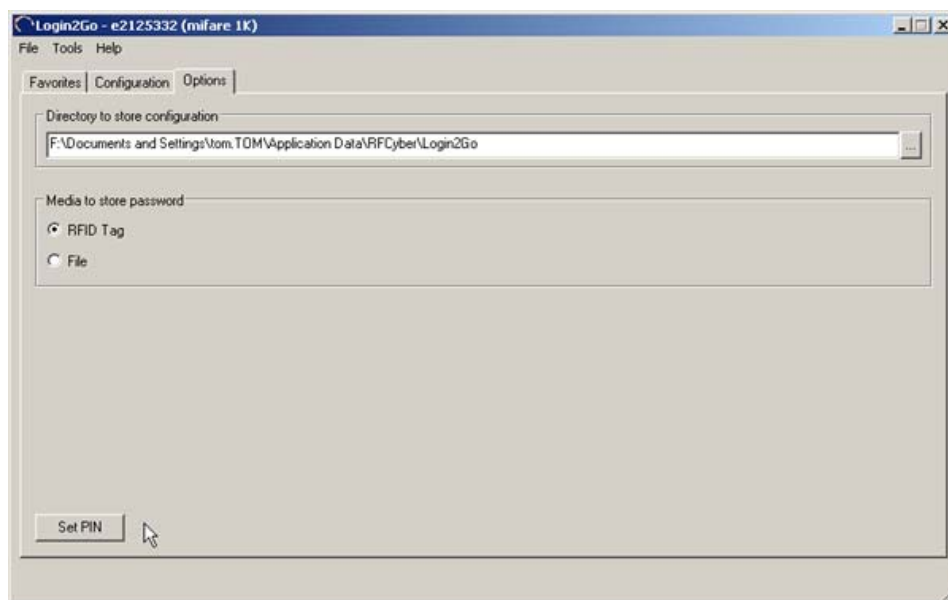


Fig. 12

It provides you with following choices for a given RFID tag:

Directory to store configuration,
Media to store password,
Set PIN.

We recommend you to keep default directory path to store the configuration. The “Media to store password” gives you the choice to store password in either the given RFID tag or the configuration file in computer. For the former case, the RFID tag must be writable. If the “Media to store password” setting is changed from “RFID Tag” to “File”, users will be asked to put the RFID tag near Macally RFID eNetPad to clean passwords information from the memory of RFID tag and transfer them into the configuration file of the RFID tag.

By default, RFID tag PIN(personal identification number) is blank, no PIN is set. “Set PIN” button allows user to enter a Master PIN for the given RFID tag. As shown in Fig. 13, a dialog window is popped up to confirm the change of PIN.

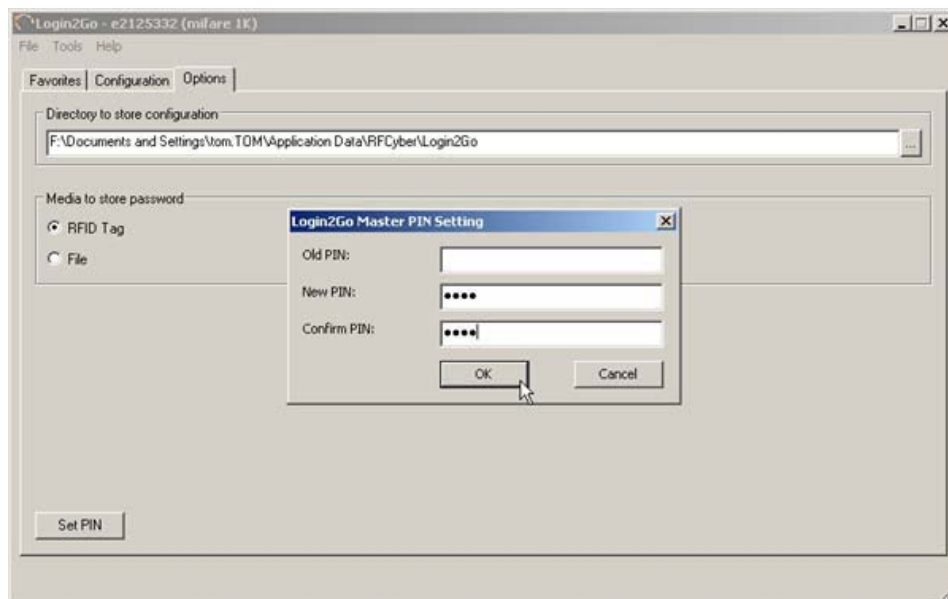


Fig. 13

Once the Master PIN is set, Login2Go will ask for the PIN for the following two situations. First situation is when users select the “Configuration” tab to configure favorite web sites, the second when user wants to launch a favorite web site with “Master PIN” field checked.

To remove Master PIN, users just need to set PIN, leave blank in the “New PIN:” and “Confirm PIN:” fields.

Fig. 14 shows Save and Load commands under the File in pop down menu.

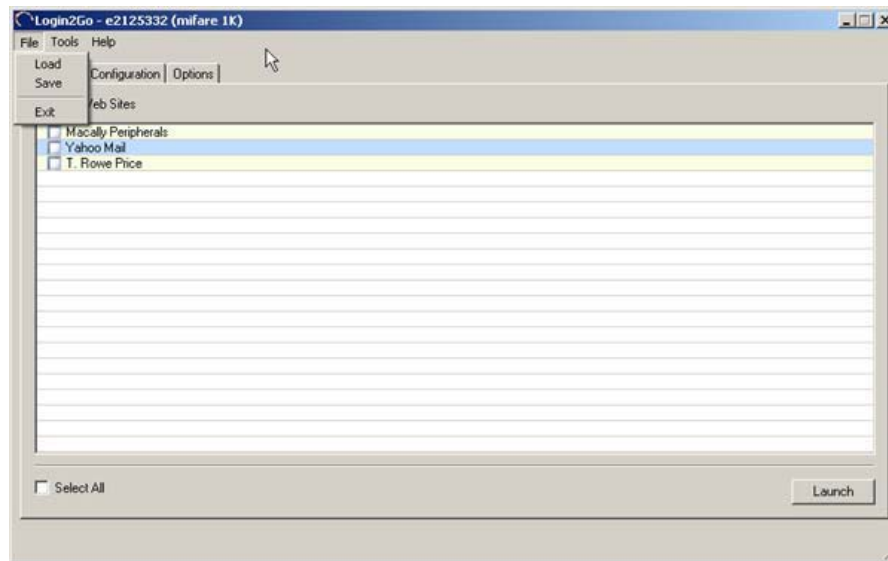


Fig. 14

“Save” command lets you save any changes or updates taken place in Login2Go. “Load” command allows you to scan another RFID tag to load its configuration file without exiting and opening Login2Go application again. When “Load” is executed, Login2Go will prompt you to put another RFID tag near the eNetPad.

When users exit Login2Go application, by either clicking “Exit” command or closing the main application window, a dialog window will pop up to confirm whether to save the change if there is any change associated with the current RFID tag.

Fig. 15 shows Reformat command under Tools menu.

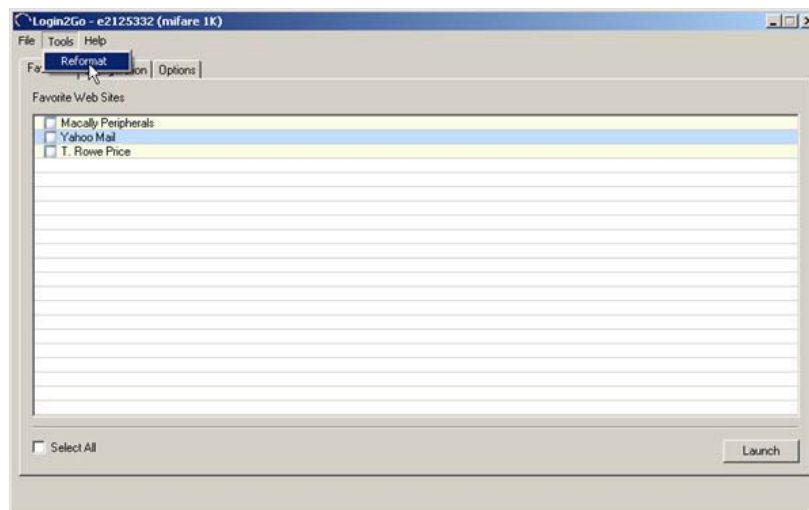


Fig. 15

“Reformat” command will reformat the given RFID tag, delete the corresponding TagId.pas file, and exit Login2Go application. This command is used if there is corrupted data in the given RFID tag and/or the corresponding TagId.pas file. The RFCyberOne Service must be up running while invoking the reformat operation, i.e., the RFCyberOne Console icon “R” in task bar needs to be green color.