



M86 Authenticator **USER GUIDE**

Software Version: 2.0.10
Document Version: 02.01.12

M86 AUTHENTICATOR USER GUIDE

© 2012 M86 Security
All rights reserved.

Version 1.03, published February 2012 for software release 2.0.10

Printed in the United States of America

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine readable form without prior written consent from M86 Security.

Every effort has been made to ensure the accuracy of this document. However, M86 Security makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. M86 Security shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. Due to future enhancements and modifications of this product, the information described in this documentation is subject to change without notice.

The latest version of this document can be obtained from <http://www.m86security.com/support/wf/download.asp>

Trademarks

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Part# WFA-UG_v1.03-1202

CONTENTS

M86 AUTHENTICATOR	1
Workstation requirements	2
Windows environment	2
Macintosh environment	2
Enable, download M86 Authenticator	3
M86 Authenticator Deployment Kit	4
Work flow in environments	5
Windows environment	5
Macintosh environment	6
Download and install the Deployment Kit	7
Access the Deployment Tool window	10
Configure a New Package set	11
Specify Package criteria	12
Specify Client Options	12
Save configuration settings, download files	15
View Package Configuration contents	17
Edit a Package Configuration	18

M86 AUTHENTICATOR

The M86 Authenticator ensures the end user is identified on his/her workstation, via an executable file that launches during the login process. To use this option in a Windows environment, the M86 Authenticator client can be installed on the user's workstation or launched from a network share during login. In a Macintosh environment, the application should be installed on the client machine, where it will be automatically launched when the user logs in.



TIPS: *When installing this application on multiple Macintosh workstations simultaneously, the Apple Remote Desktop product can be used to deploy the M86 Authenticator in bulk.*

See <http://www.m86security.com/software/8e6/hlp/auth/auth.html> for online help.

Workstation requirements

Windows environment

The M86 Authenticator client works with the following Windows operating systems:

- Windows XP Pro SP1 and 2
- Windows XP with Novell client v4.91
- Windows Vista (all editions except Home and Starter)
- Windows 7 (all editions except Home and Starter)



NOTES:

- *Windows XP and Vista and 7 Home/Starter Editions can be used if the Novell eDirectory client and M86 Authenticator are installed in a Novell network environment.*
- *Terminal Services must be enabled on Windows for Fast User Switching support.*
- *Remote Desktop Connections are not supported.*

Macintosh environment

The following minimum workstation components are required when using a Macintosh:

- Macintosh OS X 10.5 or 10.6
- Intel processor

Enable, download M86 Authenticator

Downloading, installing and configuring the M86 Authenticator Deployment Kit on a Windows machine results in the creation of a platform-specific package that can be installed on a network share accessible by an Active Directory domain controller, a Novell eDirectory server, or on a Windows or Macintosh workstation joined to a domain via Active Directory or OpenDirectory.

When installed on a workstation, the M86 Authenticator automatically authenticates the end user when the user logs into the workstation. If installing the deployment kit in a Macintosh environment, an Open Directory server should be used. The end user will be automatically authenticated when logging into the workstation.



NOTE: See the *M86 Web Filter Authentication User Guide* for information about enabling and configuring Authentication.

1. To enable the M86 Authenticator, in the Web Filter user interface, navigate to **System > Authentication > Enable/Disable Authentication**:

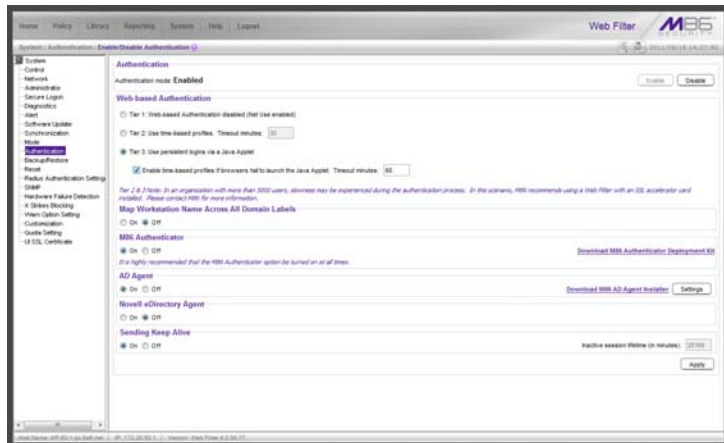


Fig. 1 Enable/Disable Authentication window

2. In the M86 Authenticator frame, click “On”.

3. To download the M86 Authenticator, click **Download M86 Authenticator Deployment Kit** to launch the M86 Authenticator Web page where you select the M86 Authenticator file you wish to download.

M86 Authenticator Deployment Kit

The M86 Authenticator Deployment Kit, used for configuring the Authenticator for deployment via the Package Editor, is comprised of the following resources:

- Unconfigured packages containing the Authenticator software
- A tool for setting or modifying Authenticator packages (the “package editor,” CfgTool.exe)
- A script for uninstalling the Authenticator from a Macintosh workstation (Uninstall-Authenticator.sh)
- Link to an online help file providing an overview of this product

Work flow in environments

The administrator downloads and then installs the M86 Authenticator Deployment Kit on his/her machine. Then he/she uses the Package Editor application to configure packages for a Windows or Macintosh environment.

Windows environment

1. Once the M86 Authenticator client package for Windows is configured, the administrator installs that package on target workstations, or deploys it via a network logon script.
2. Using a Windows machine, an end user logs on the Active Directory domain, or logs on the eDirectory tree via a Novell client.
3. The Authenticator is launched in one of the following methods, based on the installation mode setup:
 - a. Netlogon Mode - If the Authenticator is deployed via a network login script, the script invokes Authenticat.exe from a network share.
 - b. User Mode - If installed in User Mode, Authenticator is launched from the user's local \Program Files tree via a startup registry key.
 - c. Service Mode - If installed in Service Mode, Authenticator starts with Windows, and detects the user login dynamically.



NOTE: *The Service Mode is not supported in Novell Client for Windows.*

4. Authenticator determines the authentication environment, then retrieves the username and related identifying information using either Windows or Novell APIs, and sends this information (via LOGON event) to the Web Filter.

5. The Web Filter looks up the group memberships for the user (via Windows AD, PDC, or eDirectory through LDAP), and determines the profile assignment.
6. The Web Filter sets the profile for the end user with username (including the group name, if it is available) and IP.
7. The M86 Authenticator client periodically sends a “heartbeat” packet to the Web Filter to sustain the connection and profile as long as the user is logged in and connected to the network.
8. The end user logs off, and the M86 Authenticator client sends a LOGOFF event to the Web Filter. The Web Filter removes the user's profile.

Macintosh environment

1. Once the Macintosh package is configured, the administrator installs the package on target workstations.
2. An end user logs on the domain, and OS X launches Authenticator.
3. Authenticator identifies the end user by using OS X Directory Services, retrieving the username and related identity information, which it sends to the Web Filter (via a LOGON event).
4. The Web Filter looks up the user's group memberships and determines the profile assignment.
5. The Web Filter sets the profile for the end user with username (including the group name, if it is available) and IP.
6. Authenticator client continually sends a “heartbeat” to the Web Filter until the end user logs off or disconnects.
7. If the user logs off, Authenticator sends a LOGOFF event to the Web Filter. The Web Filter removes the user's profile.

Download and install the Deployment Kit

1. In the Web Filter user interface, go to System > Authentication > Enable/Disable Authentication window (see Fig. 1).
2. In the M86 Authenticator frame, click **Download M86 Authenticator Deployment Kit** to launch the M86 Security Web page where you can select the M86 Authenticator Deployment Kit file to download to your machine.
3. Once the deployment kit .msi file is downloaded to your machine, click that file to launch the M86 Authenticator Deployment Kit Setup Wizard, with the End User License Agreement displayed:

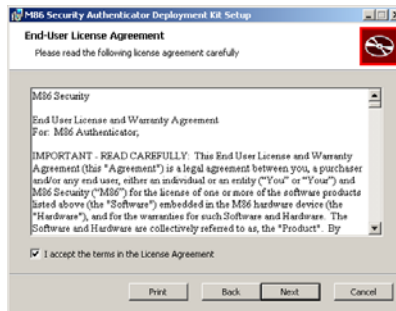


Fig. 2 End User License Agreement

4. After reading the EULA, click the checkbox corresponding to “I accept the terms in the License Agreement”, and then click **Next** to go to the Choose Setup Type step:

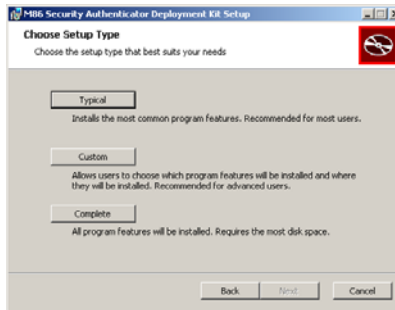


Fig. 3 Choose Setup Type

5. Select the setup option for installing the Authenticator (“Typical”, “Custom”, “Complete”), and then click **Next** to proceed with the option you selected for installing the application. If you chose the Custom option, you will need to specify where or how the main executable and support files will be installed on your machine, and/or where or how Windows and Macintosh packages for the Authenticator will be installed for distribution to user workstations.

When your machine is ready to install the Deployment Kit, the page that confirms the installation process is ready to begin displays:



Fig. 4 Installation process ready to begin

6. Click **Install** to begin the installation process. The following page displays when the installation process is complete:

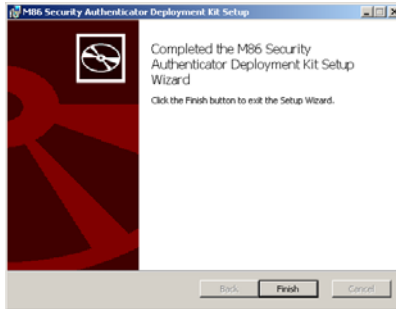


Fig. 5 Installation complete

7. Click **Finish** to close the wizard dialog box.

Access the Deployment Tool window

Once the Authenticator Deployment Kit is installed on your machine, the Authenticator Deployment Tool window (see Fig. 6) and Authenticator Package Configuration window (see Fig. 8) are used for configuring packages for Windows or Macintosh.

The Authenticator Deployment Tool window is accessible via **Start > All Programs > M86 Security Authenticator Deployment Kit > Package Editor**:

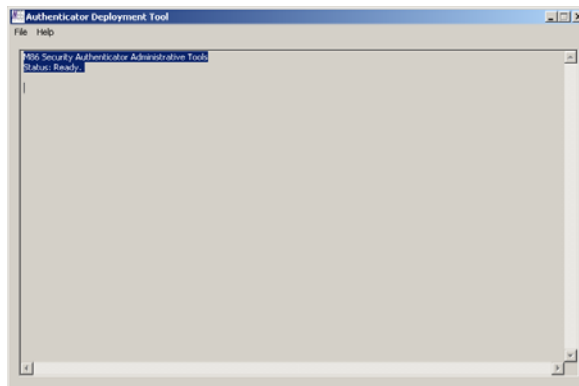


Fig. 6 Authenticator Deployment Tool window

The Authenticator Deployment Tool's package editor log window displays the operations performed when creating and configuring packages.



NOTE: Before exiting the Authenticator Deployment Tool and Package Configuration windows, be sure to save all entries you intend to save for packages you've configured. To exit the Authenticator Deployment Tool window, with the Package Configuration window closed, go to **File > Exit**.

Configure a New Package set

1. In the Authenticator Deployment Tool window, go to **File > New Package...** to open the Choose Product Version dialog box:

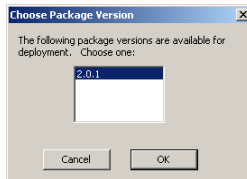


Fig. 7 Choose Product Version dialog box

2. Select the Authenticator software version from the available choices, and then click **OK** to close the Choose Product Version dialog box and to open the Package Configuration window:

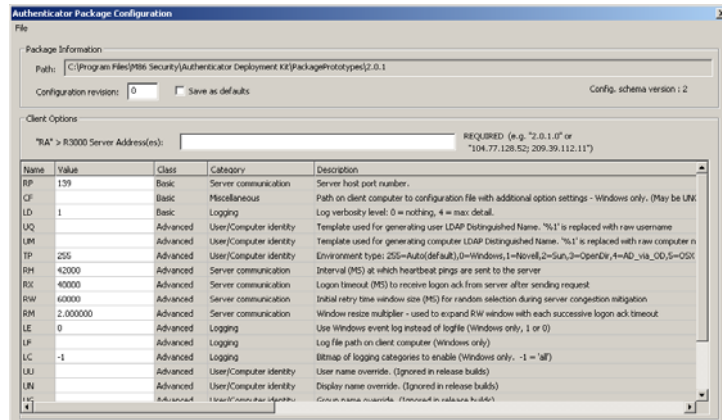


Fig. 8 Package Configuration window

The Package Configuration window is comprised of the Package Information and Client Options frames.



NOTE: To exit the Package Configuration window at any time before saving your edits, select **File > Cancel** from the menu.

Specify Package criteria

The Package Information frame includes the following information: Path on the system where the current package is located, Configuration revision number, Configuration schema version number, and package version numbers.

The following fields are editable:

- **Configuration revision:** This number is automatically incremented by “1” each time changes made to the package configuration are saved. When deploying the Authenticator to end user workstations, the installer uses this revision number to determine whether a newer configuration is already installed on the workstation.



***TIP:** To ensure updates to end user workstations are properly applied, if you are making configuration-only changes, it is better to edit the previous package rather than create a new one.*

- **Save as defaults:** By checking this box, your configuration will be saved in a central defaults file for use in the next “Save” command.



***TIP:** By enabling this feature, if creating a new package you can apply these saved default settings to the new package by choosing **File > Apply Defaults** from the menu.*

Specify Client Options

The Client Options frame includes fields used for specifying configuration settings.

1. In the field "RA" > **R3000 Server Address(es)** enter the virtual IP address(es) of the Web Filter server(s), separating more than one IP address by a semi-colon (;). Typically this entry is just a single IP address for each server, but the full syntax is:

```
{server_spec};{server_spec};...  
server_spec= {hostname or IP addr} [: port]
```


- Review the Basic class parameter fields and make any necessary modifications in the corresponding **Value** fields:

Name	Value	Category	Description
RP	139	Server communication	Server host port number: This value is used for any server_spec which does not contain an explicit port number. If this value is changed from the default value, the new port number must be entered via a command line change in the Web Filter. (Contact Technical Support for assistance in making this change in the Web Filter.)
CF		Miscellaneous	Path on client computer to configuration file with additional option settings; Windows only. (May be UNC)
LD	1	Logging	Log verbosity level: 0 = nothing, 4 = max detail.

- For advanced users, if necessary, make modifications in the corresponding **Value** field for any of these Advanced class parameters:

Name	Value	Category	Description
UQ		User/Computer identity	Template used for generating user LDAP Distinguished Name. '%1' is replaced with raw username.
UM		User/Computer identity	Template used for generating computer LDAP Distinguished Name. '%1' is replaced with raw computer name.
UT	255	User/Computer identity	Environment type: 255=Auto(default), 0=Windows, 1=Novell, 2=Sun, 3=OpenDir, 4=AD_via_OD, 5=OSX
RH	42000	Server communication	Interval (MS) at which heartbeat pings are sent to the server.

Name	Value	Category	Description
RX	40000	Server communication	Logon timeout (MS) to receive logon ack from server after sending request.
RW	60000	Server communication	Initial retry time window size (MS) for random selection during server congestion mitigation.
RM	2.0	Server communication	Window resize multiplier: Used for expanding RW window with each successive logon ack timeout.
LE	0	Logging	Use Windows event log instead of logfile. (Windows only, 1 or 0)
LF		Logging	Log file path on client computer. (Windows only; operates from the command line)
LC	-1	Logging	Bitmap of logging categories to enable. (Windows only. -1 = 'all')
UU		User/Computer identity	User name override. (Ignored in release builds)
UN		User/Computer identity	Display name override. (Ignored in release builds)
UG		User/Computer identity	Group name override. (Ignored in release builds)
UD		User/Computer identity	Domain name override. (Ignored in release builds)
UL		User/Computer identity	User LDAP DN override. (Ignored in release builds)
UC		User/Computer identity	Computer name override. (Ignored in release builds)
WI		User/Computer identity	Computer LDAP DN override. (Ignored in release builds)

Save configuration settings, download files

In the Package Configuration window, the following options are available from the File menu for saving the package configuration:

- **Save** - Saves the current package
- **Save as...** - Launches the Save Package window in which you specify the **Package Name**, click **OK** and then **Yes** in a dialog box to close both the box and window
- **Save and Quit** - Saves your edits and closes the Package Configuration window

When the package is saved the Configuration revision number in the Package Configuration window is automatically incremented to the next sequential number, and the Authenticator Package Contents local Web page launches, providing a summary of package contents with links to various components generated in the package:

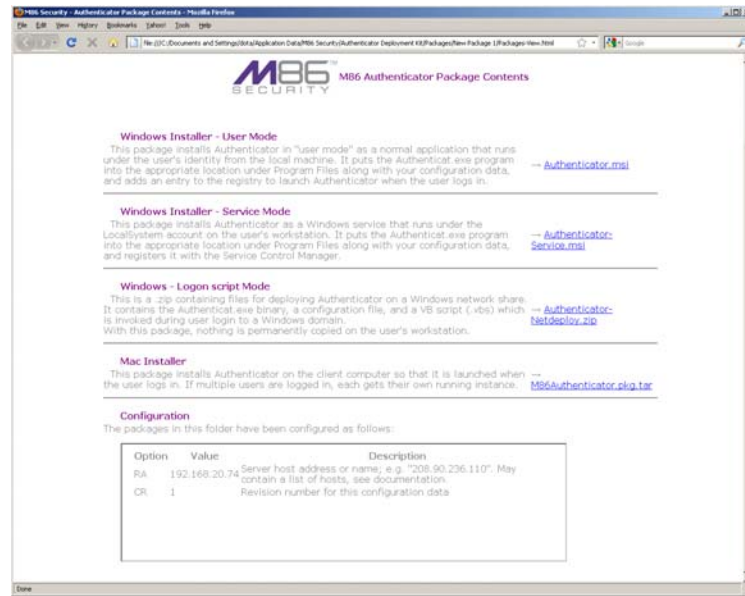


Fig. 9 Authenticator Package Contents page

The Authenticator Package Contents page includes the following information, with links to files generated for the package:

- **Windows Installer - User Mode (Authenticator.msi):** This package installs Authenticator in "user mode" as a normal application that runs under the user's identity from the local machine. It puts the Authenticat.exe program into the appropriate location under Program Files along with your configuration data, and adds an entry to the registry to launch Authenticator when the user logs in.
- **Windows Installer - Service Mode (Authenticator-Service.msi):** This package installs Authenticator as a Windows service that runs under the LocalSystem account on the user's workstation. It puts the Authenticat_s.exe program into the appropriate location under Program Files along with your configuration data, and registers it with the Service Control Manager.
- **Windows - Logon script Mode (Authenticator-Netdeploy.zip):** The .zip file contains files for deploying Authenticator on a Windows network share. It contains the Authenticat.exe binary, a configuration file, and a VB script (.vbs) which is invoked during user login to a Windows domain. With this package, nothing is permanently copied on the user's workstation.
- **Mac Installer (M86Authenticator.pkg.tar):** This package installs Authenticator on the client computer so that it is launched when the user logs in. If multiple users are logged in, each user gets his/her own running instance.
- **Configuration** - Package configuration Options and their corresponding Values and Descriptions.



NOTE: More information about these tools is provided in subsequent pages in this section of the user guide.

View Package Configuration contents

In addition to viewing a summary of package contents using the Authenticator Package Contents page, actual package contents are accessible via the Authenticator Deployment Tool window.

1. From the Authenticator Deployment Tool window, select **File > Explore packages...** to launch the Authenticator Deployment Kit's Packages folder containing all packages created for the Authenticator:

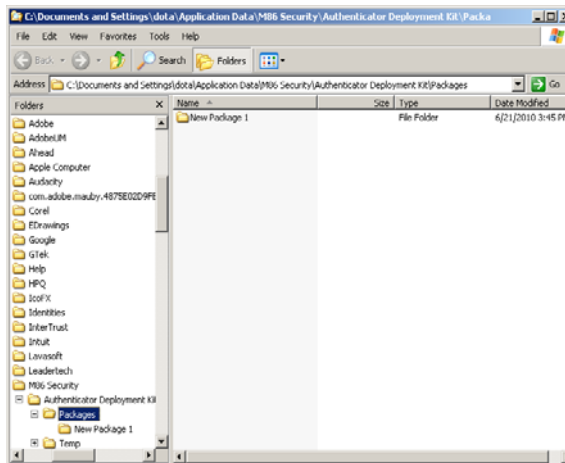



Fig. 10 Packages folder for Authenticator

 **TIP:** The Packages folder is also accessible from the Select Package window (see Fig. 11) by clicking the **Explore packages...** button.

2. Double-click the selected package to display its contents.
3. When you are finished, click the “X” in the upper right corner of the folder to close it.

Edit a Package Configuration

1. From the Authenticator Deployment Tool window, select **File > Edit Package...** to open the Select Package window:

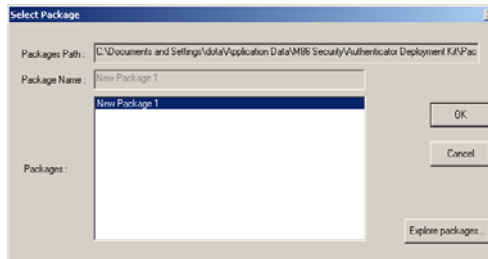




Fig. 11 Select Package window

2. From the Packages list box, choose the package to be edited; this action populates the Packages Path and Package Name fields with pertinent criteria about the package.

 **TIP:** Click **Explore packages...** to open the Authenticator Deployment Kit's Packages folder and choose the package to be edited from the available selections.

3. Click **OK** to close the Select Package window and to launch the Authenticator Package Configuration window displaying the last saved edits made for the package.

 **NOTE:** The "Configuration revision" is incremented to the next sequential revision number.

4. After making your edits, choose a Save option for saving the configuration package.