AccessPoint and FireBase Installation Guide

Menlo Logic

Copyright Notice

Export

This software product and related technology is subject to U.S. export control and may be subject to export or import regulations in other countries. Purchaser must strictly comply with all such laws and regulations. A license to export or reexport may be required by the U.S. Department of Commerce.

Licensing

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes SSLeay cryptographic software written by Tim Hudson (tjh@cryptsoft.com) and Eric Young (eay@cryptsoft.com).

Contents

Preface ..... **iii**
Guide Overview iii
Conventions Used in This Guide iii
Related Documentation iv
Customer Support iv

1 Installation **1**
The FireBase Platform 1
AccessPoint and FireBase Modules 1
System Requirements 2
Installing the FireBase Platform 2
Installation Procedure 2
AccessPoint Files 4

2 Management and Certificate Setup **5**
Validating the Installation and Setup 5
Starting and Stopping the AccessPoint Software 6
AccessPointCtrl Options 6
Install an SSL Certificate 7
Generate a Self-Signed Certificate 7
Install an SSL Certificate Generated by a CA 8
SSH for FireBase Management 9
BIOS Security Configuration 9

3 File Management **10**
Configuration Files 10
Sample Configuration Files 10
Error Messages 13
Technical Support 14

Appendix A **15**

Index **17**

Preface

Welcome to Menlo Logic AccessPoint. The *AccessPoint Installation Guide* provides instructions for installing the Menlo Logic FireBase platform and the AccessPoint SSL VPN software.

Guide Overview

This *Installation Guide* is intended for networking professionals who are familiar with Linux or UNIX operating systems. This guide describes the system requirements, provides instructions for installing the AccessPoint software, and includes the initial configuration settings required to set up and test AccessPoint. This guide consists of a chapter describing the installation procedure on Linux followed by chapters on configuration and software validation.

Conventions Used in This Guide

Conventions for special information and procedures to enter or display data are given in the following table.

Convention	Description
`Monospaced type`	The syntax for system commands. Note that the `Enter` key is required to submit the command unless otherwise specified.
`[VARIABLE TERM]`	Variable term that should be substituted with an appropriate value. For example: `mv software.tar /tmp/[FILENAME]`
Bold type	The names of fields and selection options in the AccessPoint web user interface. For example: Type your password in the **Password** field.
NOTE:	Indicates a configuration note or warning. Notes include helpful suggestions and special instructions and information.
Italics	Denotes a reference guide, technical publication document or a chapter or section within a document.

Related Documentation

For full documentation on installing, configuring and managing AccessPoint SSL VPN software, please refer to the following documents:

- *AccessPoint Configuration Guide*
  Provides configuration information for the AccessPoint management interface.
- *AccessPoint User Guide*
  Provides instructions for using the AccessPoint SSL VPN portal to connect to Intranet resources.

For instructions on compiling the AccessPoint SSL VPN source code and modifying or integrating the source code, please refer to the following documents:

- *AccessPoint Source Code Installation Guide*
  Describes the build environment and the process for compiling and installing the AccessPoint source code.
- *AccessPoint Developer Guide*
  Provides information about the AccessPoint source code implementation, focusing on Developer Application Programming Interfaces (APIs).

If available, please also see the *Release Notes* for version specific information including new features and caveats.

Customer Support

Menlo Logic provides presales support to evaluation customers. Menlo Logic also offers a wide range of technical support and professional services programs to meet the unique requirements of our customers. Presales email support is provided during the evaluation period. Standard technical support is available to customers with a valid technical support contract.

Contact Menlo Logic Support at:

Email: support@menlologic.com
Phone: 650-922-6500
Web: www.menlologic.com/support.html

To obtain an evaluation version of the AccessPoint software in binary format, complete the registration form at:

www.menlologic.com/registration.html

To evaluate the AccessPoint source code, contact Menlo Logic Sales at:

Email: sales@menlologic.com
Phone: 650-922-6500

1 Installation

This chapter describes the system requirements and installation of AccessPoint and the FireBase platform. When finished with the tasks in this chapter, continue with the *Management and Certificate Setup* chapter.

For further information about AccessPoint configuration and use, refer to the *AccessPoint Configuration Guide* and *AccessPoint User Guide*.

The FireBase Platform

To simplify installation and configuration, a hardened operating system has been bundled with the AccessPoint SSL VPN software. The operating system, FireBase, was developed from Linux, but it has been optimized to improve processing performance. All Linux packages not required by AccessPoint have been removed.

In addition to the packages required by AccessPoint, FireBase also includes an SSH server for remote management of the system. The SSH server is not managed through the AccessPoint web management interface and may be disabled or removed as desired by the AccessPoint administrator.

In addition, the FireBase operating system includes a system configuration program that can be launched from the console. To launch the system configuration program, type `setup` from the console prompt. The system configuration program enables the administrator to load new device drivers, set the root system password and other system settings. Some of these settings are also configurable through the web management interface.

AccessPoint and FireBase Modules

The AccessPoint application software consists of the following components and directories:

- `smm` - System Management Module for AccessPoint applications
- `firebase` - The operating system management module for IP and system configuration.
- `tunneld` - TCP tunnel termination module
- `httpd` - Modified version of Apache web server 1.3.28
- `ftpsession` - The FTP session handler module
- Library folder with system library files
- CGI, HTML, Java and Perl files

System Requirements

The minimum system requirements for installing AccessPoint with the FireBase platform:

- 600 MHz Processor x86/Pentium compatible processor - Multi-processor systems are not supported
- 128 MB RAM
- 60 MB Disk space
- One or more Ethernet interfaces

NOTE: *See Appendix A for a complete list of supported interface cards*

- CD-ROM drive

Installing the FireBase Platform

Installing FireBase with the AccessPoint SSL VPN software consists of downloading the FireBase ISO image, burning the image to a CD-ROM, and installing the FireBase operating system from the CD-ROM.

WARNING: *Installing the FireBase operating system will reformat your hard drive and erase all data on your system.*

If you do not have a bootable CD-ROM drive, you may also install the FireBase operating system from another bootable device, such as an external CD-ROM drive connected to your system via a USB port. If you boot from another bootable drive other than your system's CD-ROM drive, you will need to configure your server's BIOS settings to boot from the new drive before booting from the system's default hard drive.

If you are installing from a CD-ROM drive, confirm that the system BIOS is configured to boot from this drive before booting from other available drives. To configure the BIOS setup, refer to your computer hardware instructions. Typically, the BIOS configuration menu is displayed by pressing a key such as the `Delete`, `F2`, `F10` or `Escape` key while the machine is powered on. The BIOS setup feature is usually named "Boot Sequence".

Installation Procedure

Perform the following steps to install the FireBase and AccessPoint software.

1. Download the FireBase ISO from the Menlo Logic FTP site.

Contact sales@menlologic.com to request an evaluation version of the FireBase software.

2. Burn the FireBase ISO image to a CD.
3. Power down the machine that FireBase will be installed on.

4. Insert the CD with the FireBase ISO image into the CD-ROM drive.
5. Power on the machine.

   The machine should detect the FireBase installation CD-ROM and begin the installation of the FireBase operating system and the AccessPoint SSL VPN software.

   At the first prompt, if you press **RETURN**, you will begin the installation procedure and reformat your hard drive.

   WARNING: *All data on your system will be erased. If you do not wish to continue, then eject the FireBase CD and abort the installation immediately.*

   The installation consists of a menu-driven text-based installer. If you cancel the procedure at any point, the installation will end and your system will be rebooted.

   NOTE: Switch between options by using the `Tab` key. Click `Enter` to select.
6. The installer will initially partition your hard drive and install the FireBase operating system and the AccessPoint SSL VPN software. Click **OK** to partition the hard drive and continue with the installation.
7. The installer will configure the primary Ethernet interface. You may manually select the appropriate Ethernet driver from a list of available drivers or the installer can automatically probe the hardware and install a compatible Ethernet driver for the first Ethernet interface that it detects. The interface that the installer enables will be configured as the **eth0** interface in the FireBase operating system and will be shown as **eth0** in the AccessPoint web management interface.
8. The installer will then prompt you to enter an IP address and subnet mask for the system. Enter the appropriate values and click **OK**.
9. After the software has been successfully copied to your hard drive, the installer will eject the installation CD-ROM. Please remove the installation CD-ROM. If you do not remove the installation CD-ROM, your machine will try to reinstall FireBase again once you reboot your machine.
10. Enter the system Password and the confirmation Password and click **OK**.

    NOTE: *The system password is used to log into the server locally through a console or remotely using SSH. This is not the same password used to login to the AccessPoint web management interface. The default system user name is root and the default password is defined during installation. The AccessPoint administrative user name is admin and the default password is admin123.*

11. If additional Ethernet interfaces are available, the installer will allow these interfaces to be configured. To configure additional Ethernet interfaces click **OK**.

    Probe or manually select additional Ethernet interfaces. Then define the IP address and subnet mask for the additional interfaces.

    The initial interface configured in step 7 is the interface that will terminate SSL VPN connections.

12. The installer will display a message confirming that the installation is complete. Click **OK** to finish the installation and reboot the FireBase server.

Once you have completed the installation, you may log into the FireBase server. Enter the user name root and the password that you defined during the installation.

AccessPoint Files

The following AccessPoint files and executables will be saved to the `/usr/src/AccessPoint/` directory:

`bin/`	for binaries such as httpd, smm and tunneld.
`var/`	Various configuration and log file directory
`var/logs/`	log directory
`var/cert/`	certificate directory
`var/conf/`	config file; by default it contains smm.conf, tunneld.conf, smm.default, tunneld.default
`www/`	All Web CGI scripts and HTML files
`www/cgi-bin`	CGI Home
`www/htdocs`	HTML files

NOTE: *The* `/AccessPoint` *folder and its contents may be moved to another location, but the files should not be moved to a home directory. The Apache web server and other system daemons do not run with root privileges and will not be able to create log files if installed in a home directory.*

2 Management and Certificate Setup

This chapter describes how to verify that the AccessPoint software has been installed correctly and how to login and manage the FireBase operating system. It also provides SSL certificate management and SSH remote administration information.

Validating the Installation and Setup

Validate that AccessPoint and FireBase have been installed successfully. Log into the AccessPoint machine locally or use SSH for remote access. SSH is enabled by default on AccessPoint. Go to the end of this chapter for more information about SSH.

1. Enter the FireBase login user name and password to login. The FireBase user name is "root". The FireBase password was defined during the FireBase installation procedure.

NOTE: *The FireBase user name and password are not the same as the AccessPoint administrative user name and password. The FireBase user name is "root". The default user name for the AccessPoint web management interface is "admin" and the default password is "admin123".*

Refer to Chapter 2 of the AccessPoint Configuration Guide for instructions on logging into the AccessPoint web user interface.

2. To verify that the daemons are running use the following commands:

```
ps -e | grep httpd
ps -e | grep smm
ps -e | grep firebase
ps -e | grep tunneld
ps -e | grep ftpsession
```

All the AccessPoint daemons should be running, so all active processes should be displayed.

Starting and Stopping the AccessPoint Software

The FireBase installation includes a program named `AccessPointCtrl` saved in the `/usr/src/AccessPoint/bin/` directory that should be used to start, stop and restart the AccessPoint software.

By default, the AccessPoint software will be launched automatically when the system is rebooted. To manually start the AccessPoint software:

1. Go to the AccessPoint binary directory.

   ```
   cd /usr/src/AccessPoint/bin
   ```

2. To start the AccessPoint software, type:

```
./AccessPointCtrl start
```

When the software is started, a confirmation message will be displayed in the terminal window confirming that each process has started successfully.

AccessPointCtrl Options

For a full list of AccessPointCtrl options, type:

```
./AccessPointCtrl
```

Usage instructions similar to the following will be displayed:

```
Usage: ./AccessPointCtrl {start|stop|restart|status|condstart}
```

The AccessPointCtrl program may be used to start, stop, and restart all of the AccessPoint processes.

To start all AccessPoint processes that are not currently running, type:

```
./AccessPointCtrl condstart
```

To view the running processes, type:

```
./AccessPointCtrl status
```

Install an SSL Certificate

The AccessPoint administrator is required to create a SSL server certificate, either a self-signed certificate using the make certificates script, by purchasing a certificate from a third party Certificate Authority (CA) or by generating a certificate from the organization's authorized CA.

NOTE: *A default self-signed certificate is included with the AccessPoint software. The following instructions describe the procedure for creating additional SSL certificates.*

Generate a Self-Signed Certificate

1. To generate a self-signed certificate, from the `usr/src/AccessPoint/tools` directory, type:

   `mkcerts.sh`

You will be prompted to enter your contact and company information. Enter the appropriate information when prompted. You will also be prompted to enter the certificate key type. Select RSA as the key type.

Once you have entered your certificate information, a self-signed certificate will be saved to the `usr/src/AccessPoint/tools/ssl.crt/` directory. A test SSL key will be saved to the `usr/src/AccessPoint/tools/ssl.key/` directory.

2. Copy the cert from `/usr/src/AccessPoint/tools/ssl.crt/server.crt` to `/usr/src/AccessPoint/var/cert.`
3. Copy the key from `/usr/src/AccessPoint/tools/ssl.key/server.key` to `/usr/src/AccessPoint/var/cert.`

NOTE: *If you use a self-generated certificate, users will receive an error message when they log into the web user interface. These users will need to install the certificate manually to avoid receiving these error messages. Users can install the certificate by importing your self-signed certificate into their Java default keystore (jks) if they are using Sun Java Virtual Machine (JVM).*

To import a self signed certificate, provide the end user the `server.crt` file or instruct them to save the certificate from their web browser to their local disk. In Internet Explorer, users can view the certificate by double clicking the **HTTPS lock** in the browser status bar. In the Certificate window, click the **Details** menu and then select **Copy to File**. The certificate can then be saved to the local disk. Internet Explorer will add the extension "`.cer`" to the file name.

To import the certificate, type the following command from the Java keytool binary directory:

```
C:\Program Files\Java\j2re1.4.2_03\bin>keytool –import –file c:\server.cer
-keystore ..\lib/security\cacerts -storepass changeit -storetype jks
```

In the above example, substitute `c:\server.cer` with the appropriate name and path of the saved certificate.

Alternatively, with Sun JVM version 1.3 and greater, users may import self-signed certificates through the Java control panel. For Microsoft Windows users:

1. Open the Java plug-in control panel from the Windows control panel.
2. In the control panel, select the **Certificates** tab.
3. Select the radio button **Secure Site**.
4. Click the import button to import the self-signed cert from your machine. You may need to select **All files** from the **Files of type** menu if your browser saved the cert with a ".cer" extension.
5. Then click **Open**. You should see your self-signed cert in the Secure Site window.
6. Click **Apply** and then close the control panel.

Visit http://java.sun.com/j2se/1.3/docs/tooldocs/win32/keytool.html for more information.

Install an SSL Certificate Generated by a CA

You can also request an SSL certificate from a third party CA. To receive a certificate, you must generate a Certificate Signing Request (CSR) and a private key. The standard command to generate a CSR for Apache with OpenSSL and mod_ssl is:

```
openssl req -new -nodes -keyout myserver.key -out server.csr
```

NOTE: *The AccessPoint web management interface includes the ability to generate a CSR. For instructions on generating a CSR through the web management interface, please see* Chapter 3 *of the* AccessPoint Configuration Guide.

For more information, see http://www.openssl.org/docs/HOWTO/certificates.txt. In addition, confirm CSR requirements with your CA. Different CAs require different parameters to be defined before they will generate a certificate for you.

To install a certificate and certificate key generated by a CA to the FireBase system, save the two files to the server and then copy them to the appropriate directory:

```
cp [FILENAME].crt usr/src/AccessPoint/var/cert/server.crt
cp [FILENAME].key usr/src/AccessPoint/var/cert/server.key
```

SSH for FireBase Management

To manage the FireBase system remotely, FireBase includes an optional SSH server. Using SSH, administrators may securely authenticate to the FireBase system and configure the settings through a terminal prompt.

The SSH server may be accessed from any standard SSH client. A remote administrator should access the SSH server at an configured IP address or fully qualified domain name of the FireBase system. To login, the remote administrator must enter the FireBase user name, "root" and the password configured during the FireBase installation.

The SSH server is enabled by default. To disable SSH from starting when the FireBase system is rebooted, remove or rename the file that enables SSH.

1. Go to the SSH startup configuration directory.

```
cd /etc/fbase/remote
```

2. Remove the SSH startup flag file.

```
rm enablessh
```

3. Reboot the FireBase system.

NOTE: *Renaming the SSH startup flag file will also disable SSH.*

BIOS Security Configuration

For optimal security, the following BIOS configuration changes are recommended:

- Disable the "boot from floppy" option in the system BIOS. This will prevent booting from a floppy disk without permission and unauthorized system configuration changes.
- Configure a BIOS password to prevent changes to the BIOS configuration. Be sure to memorize the password or keep it in a secure place.

3 File Management

This chapter describes how to validate that the software has been installed correctly and that the daemons have been started.

Configuration Files

The AccessPoint settings are stored in three configuration files in the `/usr/src/AccessPoint/var/conf` directory: the `smm.conf`, `firebase.conf` and the `tunneld.conf` files.

The `smm.conf` file stores all the configuration settings for the System Management Module (SMM), including user, group, domain, access policy, and bookmark settings. The `firebase.conf` file includes IP address, route, host resolution and date settings. The `tunneld.conf` file contains TCP tunneling settings.

Settings may be configured through the web user interface or by directly editing the configuration files with a text editor. However, editing configuration settings through the web user interface is recommended because the format and syntax of the configuration files will always be modified correctly.

When AccessPoint is initially installed, the configuration files just contain the AccessPoint hostname with no other configuration settings.

Sample Configuration Files

The following is a sample `smm.conf` configuration file:

```
!This is the system name
hostname SSL VPN Server
!
save-options true
!
domain new_domain
auth-type radius
server 24.0.0.1
secret mypassword
exit
!
domain www.menlologic.net
auth-type radius
server new1.home.com
secret mypassword2
exit
```

```
!
group guest_group
comments AccessPoint authentication
exit
!
group sales_group
domain new_domain
comments Radius auth by 24.0.0.1
exit
!
user guest
password guest123
user-type normal
user-group guest_group
comments guest user
exit
!
bookmark global_telnet
bookmark-type global
host new1.home.com
service telnet
exit
!
bookmark rdp_word
bookmark-type global
host 192.168.168.5
service rdp
application word
comments bookmark2
exit
!
policy p1guest_user
policy-type user
policy-owner guest
host sales.mydomain.com
policy-action deny
service http
comments Deny web access to sales server
exit
!
end
```

The following is a sample `firebase.conf` configuration file:

```
!
lan-interface eth0
!
hostname firebase
!
save-options true
!
date-conf
ntp on
primary time.windows.com
secondary time.nist.gov
interval 64
time-zone 6
utc-log no
dst no
exit
!
dns-conf
primary 10.0.0.1
exit
!
wins-conf
primary 10.0.0.1
exit
!
interface eth0
address 10.0.0.70
mask 255.255.255.0
status enable
exit
!
route 0.0.0.0
mask 0.0.0.0
gw 10.0.0.1
interface eth0
exit
!
hosts-conf 10.0.0.70
name firebase
alias firebase
exit
!
hosts-conf 10.0.0.2
name Newaddress
alias
exit
!
sys-log
syslog-level 7
eventlog-level 7
alertlog-level 3
primary 10.0.0.101
alert-mail mail@menlologic.com
mta smtp.menlologic.com
mail-from mail@menlologic.com
```

```
exit
!
logrotate
email mail@menlologic.com
rotate size
history 8
exit
!
end
```

The following is a sample `tunneld.conf` configuration file:

```
!This is the system name
hostname SSL VPN Server
!
save-options true
!
tunnel smtp_tunnel
local-port 465
remote-port 25
remote-address mail.mydomain.com
protocol smtp
exit
!
tunnel webtunnel
local-port 8080
remote-port 80
remote-address intranet.mydomain.com
exit
!
end
```

NOTE: *TCP tunnels configured as standard TCP tunnels (not SMTP, POP3 or NTP) will not include a protocol type in the* `tunneld.conf` *file.*

Error Messages

In the event of operating system error message, consult a Linux user guide or refer to `/usr/include/errno.h` for more information. For error messages generated by AccessPoint, visit http://www.menlologic.com/support.html for troubleshooting information or contact Menlo Logic technical support.

Technical Support

If you are experiencing configuration problems or have a technical question, email a technical support request to:

support@menlologic.com

To best resolve your issue, include the following information:

- Indicate which operating system you are using.
- Include the results of running `ifconfig -a` from the shell prompt.
- Send the AccessPoint configuration file and a network diagram with the report.

Appendix A

Appendix A lists all Ethernet interfaces supported by FireBase.

- 100VG-AnyLan Network Adapters, HP J2585B, J2585A
- 3Com EtherLink III
- 3Com 3c501
- 3Com ISA EtherLink XL
- 3Com 3c503 and 3c503/16
- 3Com EtherLink MC (3c523)
- 3Com EtherLink MC/32 (3c527)
- 3Com EtherLink Plus (3c505)
- 3Com EtherLink 16
- 3Com \Corkscrew\ EtherLink PCI III/XL, etc.
- 3Com Typhoon Family (3C990, 3CR990, and variants)
- Adaptec Starfire/DuraLAN
- Alteon AceNIC/3Com 3C985/Netgear GA620 Gigabit
- AMD8111 based 10/100 Ethernet Controller
- AMD LANCE/PCnetAllied Telesis AT1500, J2405A
- AMD PCnet32 and AMD PCnetPCI
- Ansel Communications EISA 3200
- Apricot 680x0 VME, 82596 chipset
- AT1700/1720
- AX8817x USB Ethernet
- Broadcom 4400
- Broadcom Tigon3
- Cabletron E2100 series ethercards
- CATC USB NetMate-based Ethernet
- CDC USB Ethernet
- Crystal LAN CS8900/CS8920
- Compaq Netelligent 10/100 TX PCI UTP
- D-Link DL2000-based Gigabit Ethernet
- Digi Intl. RightSwitch SE-X EISA and PCI
- Digital 21x4x Tulip PCI ethernet cards, etc.
- Digital DEPCA & EtherWORKS,DEPCA, DE100
- DM9102 PCI Fast Ethernet Adapter
- EtherWORKS DE425 TP/COAX EISA, DE434 TP PCI, etc.
- EtherWORKS 3 (DE203, DE204 and DE205)

- HP PCLAN/plus
- HP LAN ethernet
- IBM LANA
- ICL EtherTeam 16i/32
- Intel i82557/i82558 PCI EtherExpressPro
- Intel i82595 ISA EtherExpressPro10/10+ driver
- Intel EtherExpress 16 (i82586)
- Intel Panther onboard i82596 driver
- Intel PRO/1000 Gigabit Ethernet
- KLSI USB KL5USB101-based
- MiCom-Interlan NI5010 ethercard
- Mylex EISA LNE390A/B
- Myson MTD-8xx PCI Ethernet
- National Semiconduct DP8381x ,
- National Semiconduct DP83820 ,
- NE/2 MCA
- NE2000 PCI cards, RealTEk RTL-8029
- NE1000 / NE2000 (non-pci)
- NI50 card (i82586 Ethernet chip)
- NI6510, ni6510 EtherBlaster
- Novell/Eagle/Microdyne NE3210 EISA
- Packet Engines Hamachi GNIC-II
- Packet Engines Yellowfin Gigabit-NIC
- Pegasus/Pegasus-II USB ethernet
- PureData PDUC8028,WD8003 and WD8013 compatibles
- Racal-Interlan EISA ES3210
- RealTek RTL-8139 Fast Ethernet
- RealTek RTL-8139C+ series 10/100 PCI Ethernet
- RealTek RTL-8150 USB ethernet
- RealTek RTL-8169 Gigabit Ethernet
- SiS 900 PCI
- SKnet MCA
- SMC 9000 series of ethernet cards
- SMC EtherPower II
- SMC Ultra/EtherEZ ISA/PnP Ethernet
- SMC Ultra32 EISA Ethernet
- SMC Ultra MCA Ethernet
- Sundance Alta
- SysKonnect SK-98xx
- Toshiba TC35815 Ethernet
- VIA Rhine PCI Fast Ethernet
- Winbond W89c840 Ethernet

Index

Configuration File, 10
Configuration file, sample, 10
Create SSL Certificate, 7
Daemons, AccessPoint, 1
Install an SSL Certificate, 8
Installation, 1, 2
Menlo Logic Support, contact, iv
Sample configuration file, 10
smm.conf, 10
System requirements, 2
tunneld.conf, 10
Untar AccessPoint tarball, 2
Validate installation, 5

Menlo Logic

Menlo Logic LLC
488 University Ave. Suite 212
Palo Alto, CA 94301
Telephone: 650-922-6500
Fax: 650-649-1953
Email: sales@menlologic.com
www.menlologic.com

Part #: 10-0005-04
Rev. A 5/04