

Avira Mac Security

with AMC support

HowTo

Table of Contents

1. Introduction	3
1.1 Features	3
1.2 System Requirements	4
2. Installation	4
2.1 Installation with the install wizard	4
2.2 Installation using the command line	5
2.3 Installation with Avira Management Console	5
2.3.1 Silent installation with the Avira Management Console	9
2.3.2 Adjustments with an enabled firewall	10
3. Status overview	12
3.1 Your Mac is protected!	13
3.2 Your Mac is not protected	14
4. Scheduler	15
4.1 Scheduling Scans and Updates	15
4.2 Scheduling Scans	15
4.3 Scheduling Updates	16
5. Quarantine and Logs	17
5.1 Quarantine	17
5.2 Logs	18

1. Introduction

With this new Mac product, Avira brings the same high level security to the Mac OS X platform that was so far only available for Windows and UNIX operating systems.

1.1 Features

Your Avira product, delivered as a 64-bit package (.pkg), includes the following features:

- Event center for monitoring, managing and controlling the entire program
- Central preferences
- Event database (logs)
- Real-Time Protection scanner for continuous monitoring of all file access attempts
- System scanner for configurable search of all known types of viruses and malware
- Integrated scheduler for planning recurring jobs such as updates or scanning processes
- Integrated quarantine management to isolate and process suspicious files
- Extremely high virus and malware detection via innovative scanning technology (scan engine) including heuristic scanning method.
As an entity, the System Scanner searches for viruses in files and folders and writes the results back to the Graphical User Interface.
As a daemon the Real-Time Protection works in the background, monitors all file access attempts and blocks the access to infected files
- Detection of all conventional archive types including detection of nested archives and smart extension detection

1.2 System Requirements

- CPU: Minimum 64-bit Intel Core 2 Duo (Your Avira product does not support Intel Core Solo / Intel Core Duo because of their 32-bit system)
- At least 2 GB RAM
- At least 200 MB of free hard disk memory space
- Minimum system requirements: Version 10.6 or later
- The application does not support Mac OS X Server version
- Functioning Internet connection where appropriate (see Installation)
- Adobe Reader to view the User Manual, HowTo and other support documentation (www.adobe.com)

2. Installation

You will find the most recent version of Avira Mac Security in the [download section](#) on the Avira website.

Avira Mac Security is available as a 64-bit package.

- ▶ Download the package to a selected destination

2.1 Installation with the install wizard

- ▶ By clicking on the package you will start the install wizard that will guide you step-by step through the installation
- ▶ On the Welcome screen click on **Continue**
- ▶ Read the software license agreement and click again on **Continue**
- ▶ The next dialog will ask you to confirm that you have read and accepted the license agreement. To continue the installation, click on **Agree**
- ▶ The next screen will display the required space for the installation of Avira Mac Security on your hard drive. Make sure though that you have at least 200 MB of space available on your hard disk as stated in the system requirements. Click on the button **Install** to execute the installation

- ▶ The OS will ask you for your user name and password to allow the installation. Once you have entered your information, click on the button **Install Software**
- ▶ After the successful installation, click on the **Close**-button

2.2 Installation using the command line

- ▶ After download, login as root. Select the directory where the package has been saved.

Example:

```
cd /tmp
```

Now enter the following:

```
sudo installer -pkg ./avira_mac_security.pkg -target /
```

After a successful installation, the following message should be displayed:

```
installer: The install was successful.
```

2.3 Installation with Avira Management Console

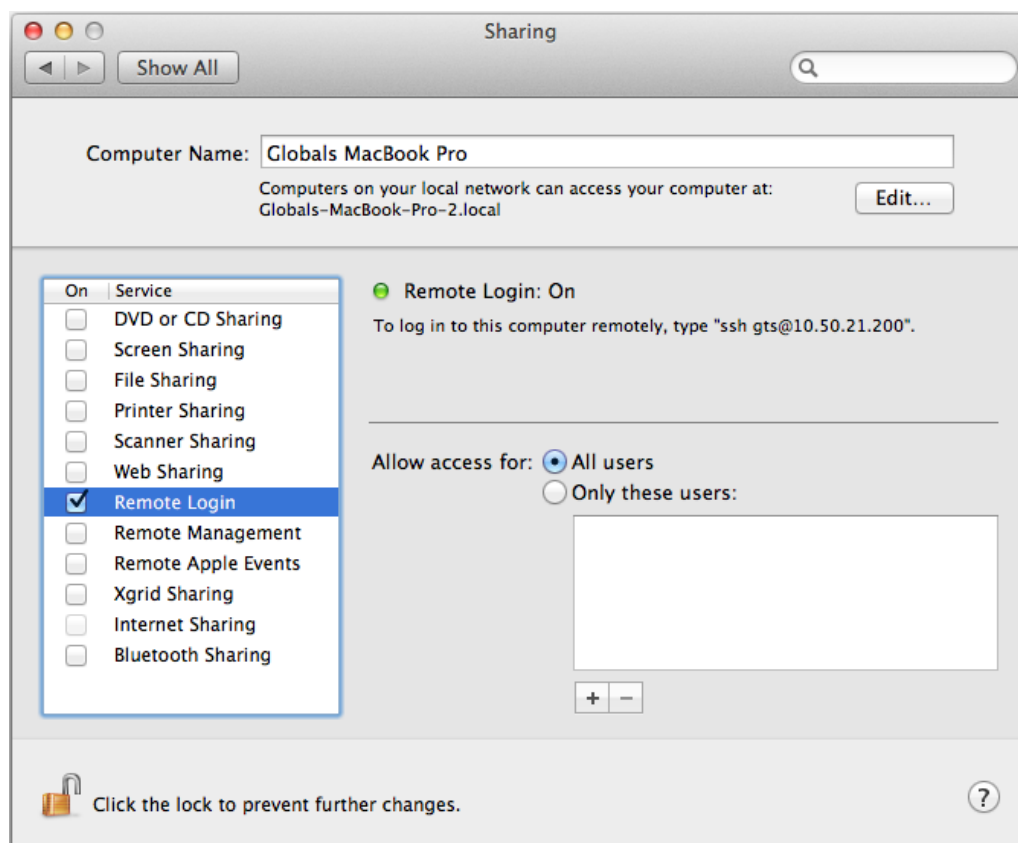
Note:

To manage Avira Mac Security via AMC you will need a license file that will be sent to you upon request.

For more details about handling software packages in the AMC, see the HowTo for the Avira Management Console.

If you want to manage one or more Mac-clients using the Avira Management Console, you need to go through the following steps so you can add the file „avira_mac_security.pkg“ like other packages to the software repository of the AMC:

- ▶ Activate SSH-support by starting the Terminal
- ▶ Open the file `/etc/sshd_config` (e.g. with vim, vi or nano) as root with `sudo -i`, activate the parameter `PermitRootLogin` (remove the #) and set it on `yes`
- ▶ Activate the Remote Login on your Mac by going to *System Preferences > Sharing* (see screenshot)



Once you have applied those changes, you need to restart the service SSH. To do this, you can either simply restart your Mac, or enter the following two command lines in the terminal:

```
$ sudo launchctl stop com.openssh.sshd  
$ sudo launchctl start com.openssh.sshd
```

Set root-password

You still might need to set the password for the user „root“ for a successful installation of Avira Mac Security.

To do this, enter the following command in the Terminal:

```
sudo passwd
```

Then, enter the desired password.

Adapting hosts

If you have installed the AMC based on host names, you need to ensure that the host name of your AMC server can be resolved as well during a remote installation of an AMC-agent. To do this, please enter the IP-address and the host name in `/etc/hosts`.

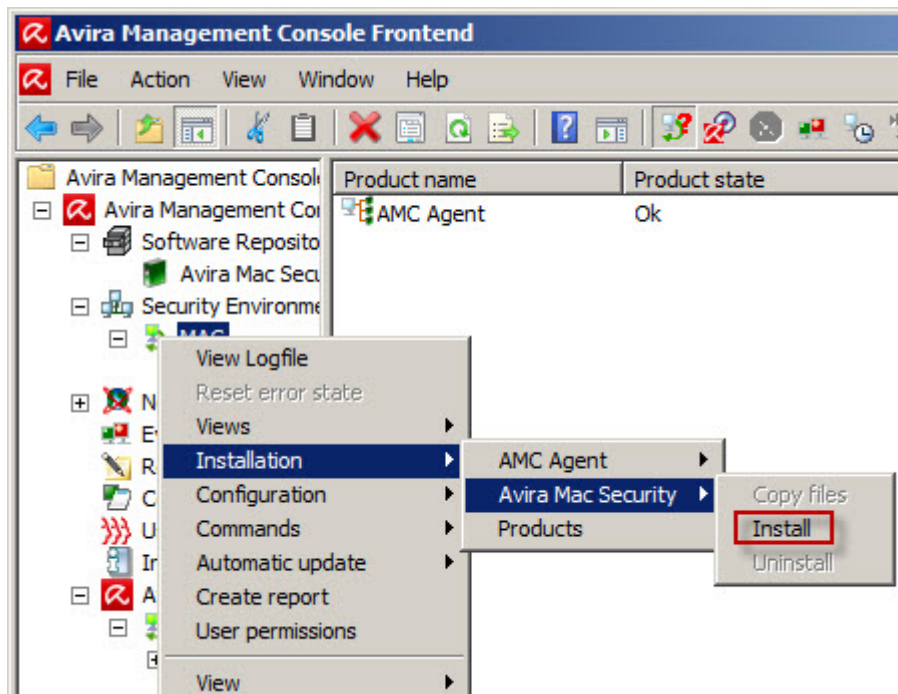
Example:

```
192.168.2.1          AMCSERVER
```

Once you have saved those changes, you should be able to execute a remote installation of the AMC-agent via the AMC console.

If everything works as desired, you will see your Mac with a green computer icon in the AMC frontend and you will also be able to install the Avira Mac Security package on your Mac.

As with other software packages, simply right-click on the computer and select *Installation > Avira Mac Security > Install*



Mac product not visible although installed

However, if the product is not shown in case you have already installed the Avira Mac Security product and added the agent later, you can enter this within

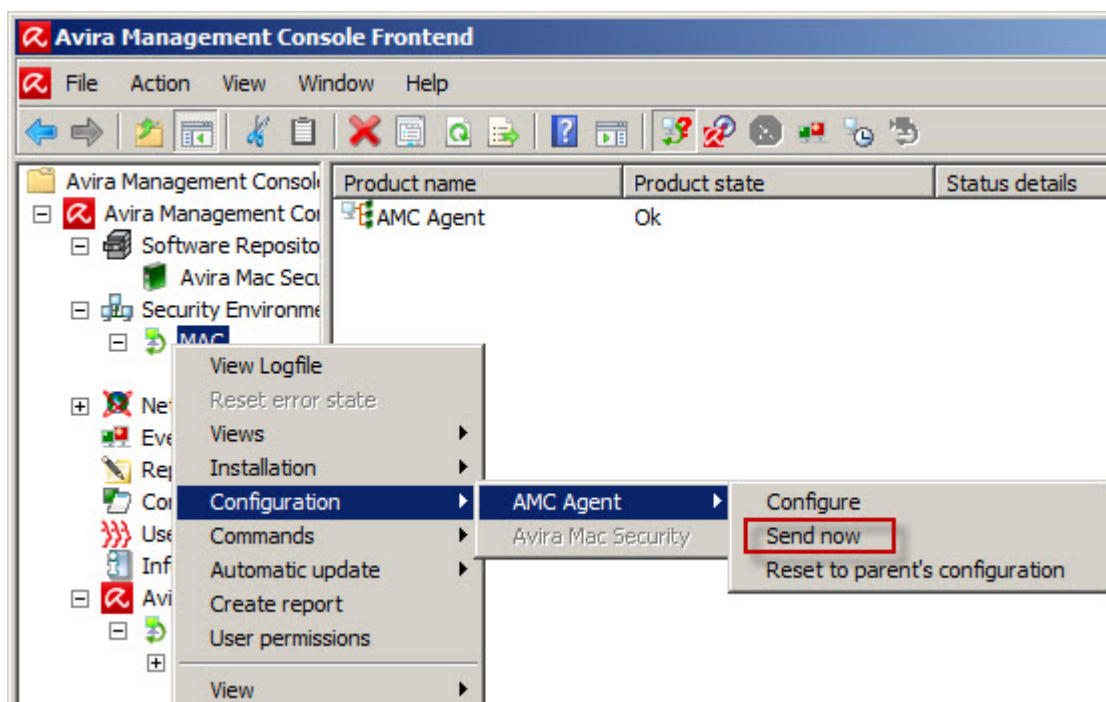
```
/opt/avira/etc/agent.ini
```

Open this AGENT.INI (e.g. with vim, vi or nano) and add the following entries at the very bottom

```
[plugins]
osxsrv=/Applications/Avira.app/Contents/guard/agent/libosxsrv.dylib
```

Save those changes and then perform a restart of the AMC-agent.

Either you send another configuration to the AMC-agent of your Mac (via *Configuration > AMC Agent > Send now*)



or you execute the following command in the terminal of your Mac:

```
sudo /opt/avira/agent/smcagent_restart.sh
```


2.3.1 Silent installation with the Avira Management Console

You can also integrate one or more Mac clients into the AMC with a silent installation of Avira Mac Security. This can be done e.g. by performing a rollout.

You do not need to configure a separate SSH-access for this.

Instead, you just need to ensure access to any desired network share that will make the agent package available.

The install script from the agent installation package must contain the target data of the AMC server to start the installation.

Also, an `--inf` parameter as well as an INF-file are necessary so that the script can run automatically.

The command line is as follows:

```
./install --server_uri=http://<dnsname_or_IP-address> --display_name=<name> --update_uri=http:// <dnsname_or_IP-address> --inf=./setup.inf
```

The SETUP.INF contains only the following entry:

```
LICENSE_AGREEMENT=y
```

The Setup will start now and install itself automatically on the system.

The start and the initialization (registration with the AMC) will run automatically, too.

2.3.2 Adjustments with an enabled firewall

In case a firewall is enabled, you need to configure it to guarantee a trouble-free communication between the agent and the AMC.

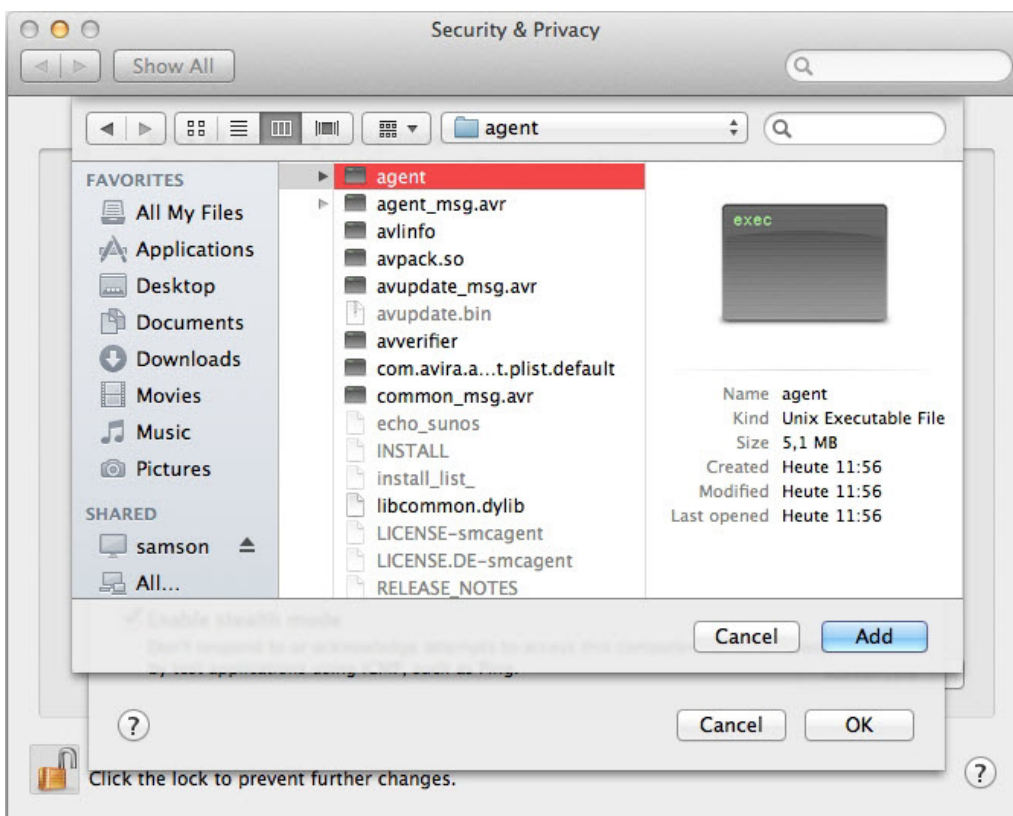
Open the firewall configuration at
System Preferences > Security & Privacy > Firewall ...



Here, click on **Advanced** and remove the check mark in the next dialog at „Block all incoming connections“:



Then, add the agent binary with „+“ (you can find it at `/opt/avira/agent/agent`):



Please make sure that all incoming connections are allowed now:



Click on **OK** to confirm.

3. Status overview

The Status window is a control center for information and events. In addition to the sidebar sections that can be selected individually, it offers a number of options that can be accessed from the Mac menu bar as well.

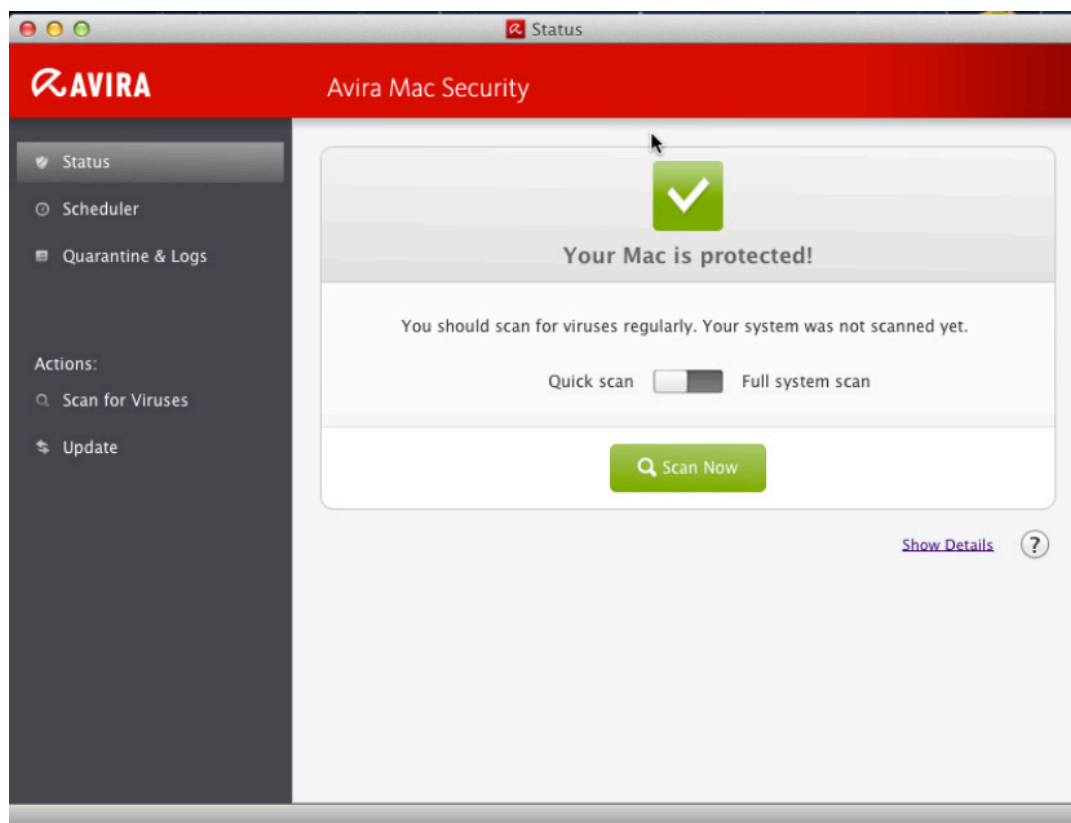
- ▶ To open the **Status** window of the event center, click the Avira logo in the Dock. Alternatively, click the logo in the menu bar and select **Open Avira** from the short-cut menu.

The **Status** window enables you to see at a glance whether your Mac is protected and displays the period of time since your last search for malware.

- ▶ To see more details about your security status, click on the link **Show details**. More information will be displayed on the panes of the two tabs: *Status* and *Statistics*. Click on **Hide Details** to close the tabs *Status* and *Statistics* again.

3.1 Your Mac is protected!

If the message in your Status window displays the information *Your Mac is protected!*, you may launch a scan process literally by just one click.

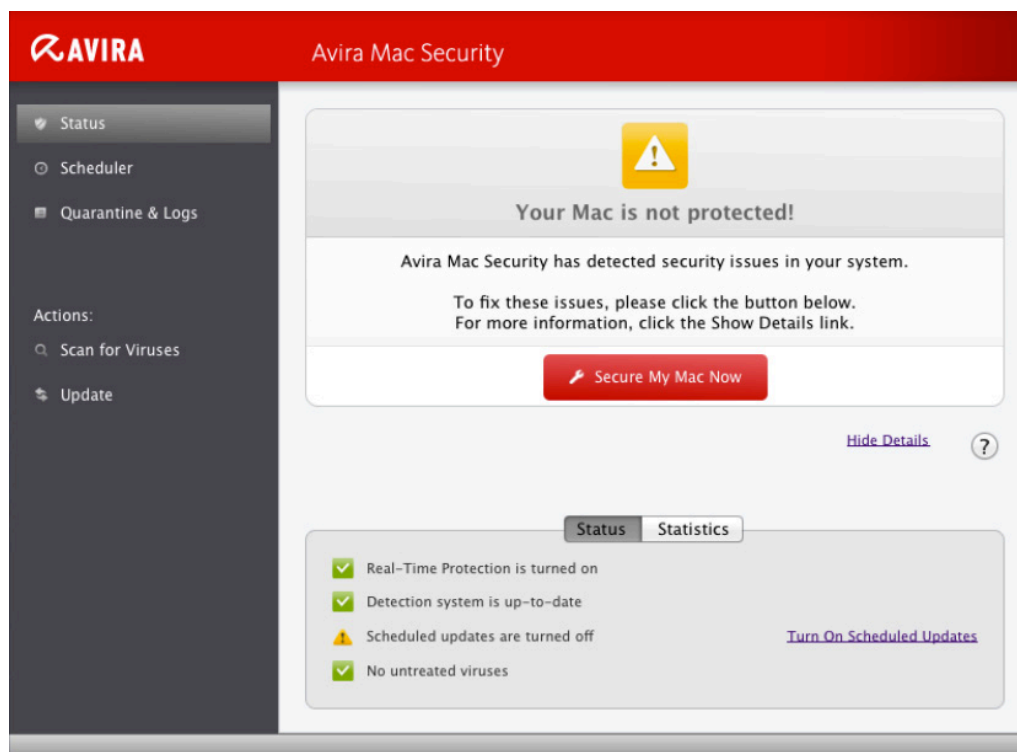


- ▶ To select between a **Quick scan** and **Full system scan**, click on the switch. Switch to **Quick scan** for a virus scan on sensitive parts of your Mac, or switch to **Full system scan** to scan the entire system for malware.
- ▶ To trigger a security check immediately, click **Scan Now**. The scanning process is displayed with a blue moving indicator. The result window will show the duration of the scan, the number of files that have been scanned and the number of viruses found.
- ▶ To pause the running scan process, click **Pause**.
- ▶ To stop and abort the scan, click **Cancel**.

Alternatively, you can also trigger a scan process at any time by clicking on **Scan for Viruses** in the left pane below the category *Actions*:

3.2 Your Mac is not protected

However, if the message in your **Status** window displays the information *Your Mac is not protected!*, you can fix this problem simply by clicking on the button **Secure My Mac Now**.



Once those problems have been fixed successfully, Avira Mac Security will tell you so.

In the rare case that the security risks remain, please consult the manual or the Avira support website.

Again, you can click on the link **Show Details**, to see in this case which feature of Avira Mac Security is reporting the problem.

4. Scheduler

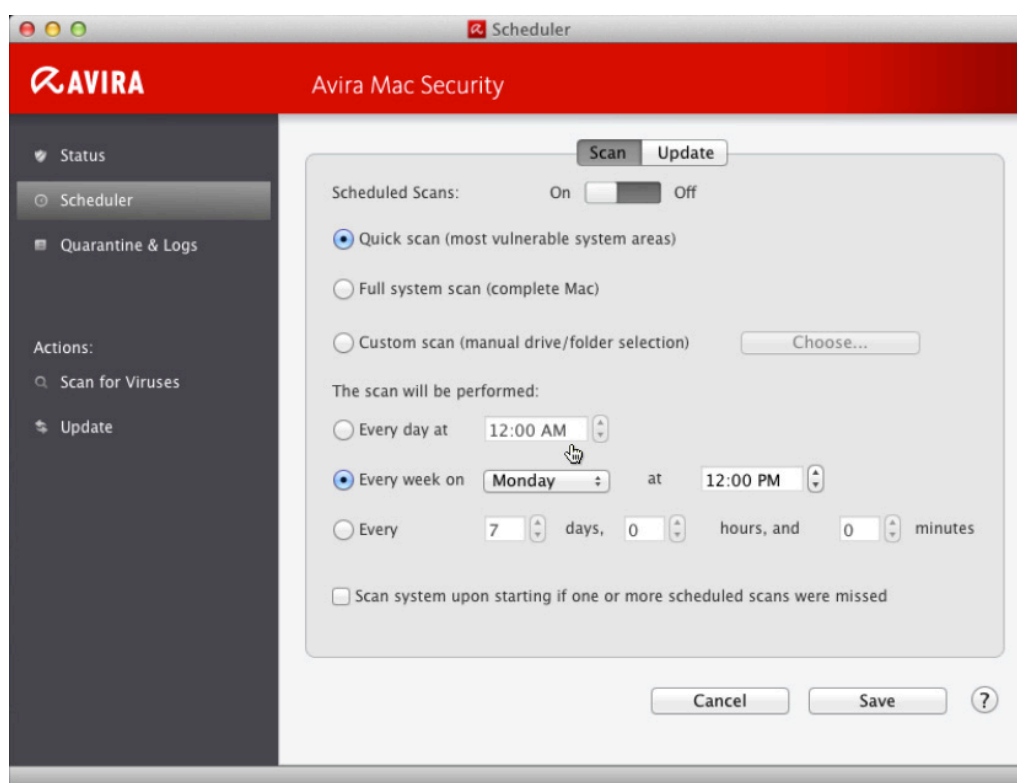
4.1 Scheduling Scans and Updates

Select the **Scheduler** from the sidebar to schedule a periodic scan or update task. The **Scheduler** window has two tabs:

- Scan with the option to switch **Scheduled Scans On** or **Off**.
- Update with the option to switch **Scheduled Updates On** or **Off**.
- ▶ Click the appropriate tab to open the specific pane.
- ▶ Select what kind of default job you want to perform and specify the timeline for this job.

4.2 Scheduling Scans

With the **Scheduler** feature of the sidebar, you schedule targeted scans for viruses and unwanted programs. Choose *Scheduler > Scan > Scheduled Scans > On*.



- ▶ To turn on the **Scheduled Scans**, switch the default button to **On**.
- ▶ Turn on **Quick scan** for a virus search on the most vulnerable parts of your Mac.

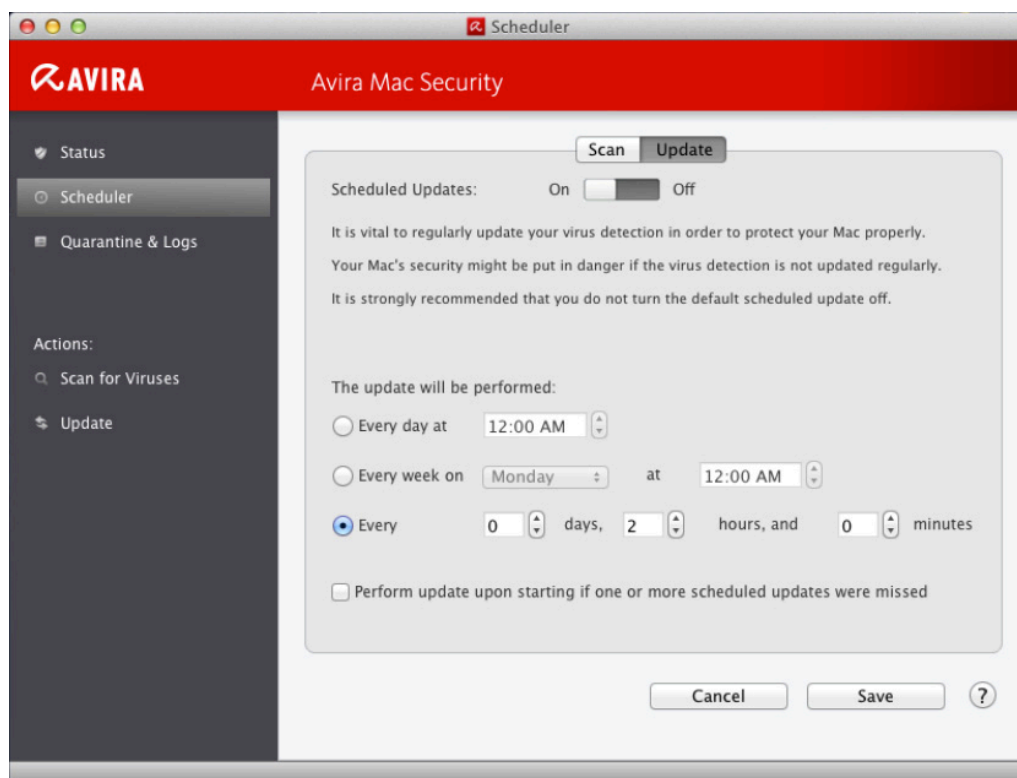
- ▶ Turn on **Full system scan** for a complete malware search on your system.
- ▶ Alternatively, you can select the **Custom scan** and specify the drive and the folders you want to get scanned.

4.3 Scheduling Updates

The effectiveness of antivirus software depends on how up-to-date the program is, in particular the virus definition file and the scan engine. The **Scheduled Updates** component has been integrated into your Avira product for the execution of frequent updates. **Scheduled Updates** ensure that your Mac security is always up-to-date and able to deal with the new viruses that appear every day.

The default update interval is 2 hours.

Select *Scheduler > Update > Scheduled Updates > On*.



Note

We strongly recommend that you do not turn off the default update job **Scheduled Updates**.

5. Quarantine and Logs

5.1 Quarantine

Detected viruses, malware or unwanted programs are stored in the quarantine directory.

Files cannot be added manually to the quarantine directory. Once a file has been sent to quarantine, it cannot be executed as long as it remains there.

If one or more infected files are residing in the quarantine, you have several options available to deal with them.

In the menu *Action for selected item(s)*, you may select the following actions:

- **Delete:** The infected file is irrevocably removed.
- **Rescan:** The infected file is scanned again by the **Real-Time Protection** scanner. Rescanning a file is recommended if the virus definition file of your Avira product has been updated and a false positive report is suspected. This enables you to confirm a false positive with a rescan and possibly restore the file, otherwise it remains in quarantine. If verified as virus, you receive an Antivirus ALERT dialog that provides more detailed information.
- **Restore:** The detected malware will be relocated to its original folder, if the original location still exists.
- **Send file to Avira:** You may send files to Avira for further examination. The path of the file you wish to send is written automatically to the subject line of the sending form. Fill in the form with your personal data as name and email address and select an assumption from the menu. Don't forget to choose a file format for Avira's reply email.
To send the file, click **Upload**. The progress indicator shows the upload process. A copy of the sent file will remain in the quarantine.

You can apply the following steps for all the actions mentioned above:

- ▶ Click **Apply** to perform the selected action.
You are asked to enter your password, allowing Avira to perform the selected action.
- ▶ To allocate only one action to all quarantined files, click **Select All**. Each action is written to the event database and displayed in the pane of the Logs tab of the **Quarantine & Logs** window.

- ▶ Click **Refresh** to update the Quarantine manager.
Each recently found malware is added to the table of the Quarantine manager.
Each quarantined malware with the assigned action **Delete** or **Restore** is removed from the Quarantine manager's table.

5.2 Logs

All information from the different modules of Avira Mac Security are displayed in the pane of the **Logs** tab in the **Quarantine & Logs** window.

All relevant issues such as updates, upgrades, scans, detection results, quarantine directory, status of modules or product errors are written to the event database called **Logs**.

You may want to reduce the size of the log database by decreasing the time period that defines how long those events are being recorded.

On the Avira menu bar, click on **Avira > Preferences**. Then, within the category *General*, click on the tab **Logging**.

Here you can select the length of time for recorded events in the log database from 1 up to 12 months.

Please consult the manual of Avira Mac Security for more information about the various settings, preferences and detailed descriptions of the features. You will find the manual and additional information in our support section.

This manual was created with great care. However, errors in design and contents cannot be excluded. The reproduction of this publication or parts thereof in any form is prohibited without previous written consent from Avira Operations GmbH & Co. KG.

Issued Q2-2012

Brand and product names are trademarks or registered trademarks of their respective owners. Protected trademarks are not marked as such in this manual. However, this does not mean that they may be used freely.



live free.™