Undercover

User Guide

Contents

1. Installing and Registering Undercover

Undercover requirements

Undercover works with macOS Mountain Lion (10.8) and above. For users of Snow leopard (10.6) or Lion (10.7), the older version is still available at orbicule.com/undercover/mac/download.php

Setting up Undercover

Upon purchasing an Undercover license, you will receive an email with a link to set a password for your account. To add your Mac(s) to this account, please do the following (on each Mac you'd like to add):

Log in at undercoverhq.com using your email address and password

- Click on "Add Your Mac" , or the "+" button at the bottom left of your screen
- Download the Undercover installer, and double-click this installer after the download has completed
- Follow the instructions and reboot your Mac when prompted by the installer (if you don't want to restart your Mac immediately, you can minimize the installer)
- About 10 seconds after login, the Undercover registration window will appear
- Enter your account's email address and your password
- Your Mac will now appear in your account at undercoverhq.com
- Remove the undercover.pkg file (it's on your Desktop or in your Downloads folder)

2. Setting up your Mac

Creating a dummy account

We recommend you to create a dummy account that does not require a password. This way, the thief will be able to use your Mac to go online, which will trigger Undercover. Because this separate dummy account has no admin privileges, the thief will not have access to any of your personal files. You can either enable the macOS built-in guest account or you can create a dedicated dummy account - Undercover will work in both cases. The only difference is that in the guest account all files and settings will be deleted every time the guest logs off.

To enable the guest account:

- Go to the System Preferences and click the Users & Groups icon.
- Click the lock to make changes (if locked).
- Select the Guest Account from the list and enable the 'Allow guests to log into this computer' checkbox. There is no need to enable parental controls or Allow guests to connect to shared folders.

To set up a dedicated dummy account:

- Go to the System Preferences and click the Users & Groups icon.
- Click the + button to add a new (Standard) account
- Leave the password fields blank.
- This guest user should not be allowed to administer the computer.

Privacy Settings

Allow access for Undercover in the Privacy preferences on your Mac, so Undercover can obtain locations and key logs. Note that the tracking will also work fine when you don't have these settings enabled. Undercover can then still rely on the IP information for locations, and on photos and screenshots to identify the thief.

- Open System Preferences on your Mac
- Go to Security & Privacy
- Select the Privacy tab
- Select Location Services in the left-hand menu
- Unlock with your admin password to make changes
- Check the "uc" item in the list (you may have to scroll down to see it)
- Select Accessibility in the left-hand menu
- Check the "UCAgent" item in the list (you may have to scroll down to see it)

What happens when you check these items:

"uc" under Location Services will activate Apple's location database, which can allow Undercover to obtain a more accurate location for your Mac. If the item is not checked, Undercover will still always obtain the IP information, which the police can use to track the location of a stolen device.
"UCAgent" under Accessibility takes care of the key logging feature. Without key logging, Undercover can of course still rely on pictures, screenshots and locations for the recovery of a stolen Mac.

Setting up the Firmware Password

The Apple Firmware Password can be a very important tool to make your Mac more secure: it basically prevents anyone who does not know the password to reformat your hard disk. For Undercover users, this is particularly useful, since a reformat is the only way to disable Undercover. In spite of its usefulness, the firmware password utility is one of the most poorly understood Apple tools.

Before explaining how to enable the Firmware Password on your Mac, we first quash some common misconceptions.

Misconception 1 - If I enable the firmware password, I will need to enter a password every time I boot my Mac.
Only when booting from *another* disk than your default startup disk, the firmware password needs to be entered. This is what makes the firmware password very convenient: since most of us boot from our default startup disk 99% of the time, one will rarely need to enter a password. At the same time, this prevents thieves from reformatting the HD, because the current startup disk cannot be formatted while in use and booting from another drive without entering the password is impossible.

Misconception 2 - If I enable the firmware password, a thief cannot boot my Mac, making Undercover useless.
When enabling the password, a thief can still boot your Mac. The only restriction is that he can only boot your Mac from the default startup disk. As a result, a thief can still work and play with your Mac and Undercover can do its work.

Misconception 3 - With the firmware password enabled, I will not be able to troubleshoot my Mac in case of a problem.

Since you know the password, you will still be able to boot your Mac from any drive you want, including CDs, DVDs, ... and troubleshoot or reformat your drive. You just need to enter the firmware password when prompted.

You will find the Firmware Password Utility on the recovery partition on your Mac.
On macOS Lion and above you should follow these steps:

- Restart your Mac while holding the option (alt) key
- Select the recovery partition when prompted
- Choose Firmware Password Utility from the Utilities menu (in the top menu bar)

Alternatively, you can:

- Restart your Mac while holding the cmd + r keys
- After your computer finishes starting up, you should see a desktop with an OS X menu bar
- Choose Firmware Password Utility from the Utilities menu (in the top menu bar)

3. Undercover HQ

Undercover features

When you login to your account on undercoverhq.com, you will land on a page which lists your Macs. If you have multiple devices registered under the same email address, they will all appear on this page in your account.

In the top menu bar, you can see 9 different tabs:

- **Info** - Here you can find some important information about your Mac and about Undercover: the version that is installed, the Ethernet and Wireless ID, the serial number, and the name of your Mac. You can use this pane to remove, transfer or rename your Mac, and you can also check on its status, and on recent activity in your account.

- **Theft Report** - Use this pane to mark your Mac as stolen and to start tracking. When the Mac is reported stolen, you can enter the police details here, and download a package with all tracking information that Undercover has gathered.

- **Location** - Here you can see the location of your device. This location will get updated every 30 minutes. The slider at the bottom will show you the history of recorded locations. When you click on the location indicator on the map, you will get a popup with all details and IP information.
  If you don't want Undercover to obtain your location, you may change the settings in the Privacy tab.
  You can also click the "Locate Now" button at the bottom right of the page to get an updated location.

- **Photos** - When your Mac is marked as stolen, Undercover will collect photos from the camera every 8 minutes. You can filter these photos to show only those photos with a face.
  In additon, you may snap pictures on-demand , giving you a live view of the thief.

- **Screenshots** - Undercover will take a screenshot every 8 minutes when the Mac is reported stolen. This feature is also available on-demand.

- **Key Logs** - Undercover will start collecting key logs when your Mac has been reported stolen. All text typed on your Mac will be recorded here, except for text entered in password fields.

- **Plan B** - If the police fail to recover your Mac, you can fall back on Plan B. This feature can simulate a hardware failure on your Mac, which should urge the thief to bring the Mac in for repair or sell it. It can also block the Mac and show a full screen message, which can be customized.

- **Privacy** - Use this tab to control which information Undercover gathers.

When you click your email address at the top right corner of the screen, you can see and change your login and personal details, and you can check how many license seats are left.

Important! Note that the email address you use to login at undercoverHQ.com will be used for all communication, including the tracking information that is sent to you when a Mac is marked as stolen. If you don't want that to happen, make sure to change your login to an email address that is not accessible from the Mac that's being protected, or from the dummy/guest account on that Mac.

Testing Undercover

You may test Undercover by reporting your device as stolen under the "Report Theft" tab in your account. Please make sure not to enter any police information during a simulation!

After marking your Mac as stolen, you will start receiving information every 8 minutes: photos from the built-in camera, screenshots, location information and key logs.

Remember that even when there's no location information on the map, it will still be no problem for the police to track the exact location of your Mac with the IP information (which is always available). Allow Undercover to gather tracking info for at least 30 minutes.
After the test, please mark the Mac as recovered again under "Theft Report".

Plan B

You can also test the different options of Plan B, but make sure you have another computer nearby which you can use to deactivate Plan B again. Once Plan B has been activated on your Mac, your Mac will be effectively blocked!

4. In case of theft

Theft report

You can report your Mac as stolen by logging in to your account at undercoverhq.com, choosing the "Theft Report" tab, and clicking the Report Stolen button.
You will then be invited to enter all police details. If you enter an email address for the police, they will also automatically be notified when your stolen Mac gets connected.

Theft follow-up

As soon as your stolen Mac connects to the internet, Undercover will start sending information to your account. You will automatically be notified by email when that happens.
The first time Undercover sends information, the police officer handling your case will receive an email with this information as well.

Every 8 minutes, Undercover will take photos and screenshots and every 30 minutes IP/location information is gathered from the stolen Mac. Everything the thief types will appear under Key Logs. If a push connection is available, you will also be able to take pictures, screenshots and request location information on demand.

The complete theft file can be downloaded under Theft Report. This file contains all information gathered by Undercover, and can easily be passed on to the police officer who is handling your case. The police can track the exact location of your Mac with the IP location information. Since internet service providers consider computer theft as network abuse, they will reveal the thief's identity to the police.

Plan B

If law enforcement fails to recover the stolen Mac, you can activate Plan B.
In Plan B mode, Undercover can simulate a hardware (backlight) failure. At this point, we think the thief has two options: to send the computer to a reseller for repair, or to try to sell it.

Undercover can also show a full-screen message alerting the reseller or someone who bought the Mac from the thief that the Mac has been stolen, that it has become unusable and that it needs to be returned as soon as possible.
This message can be fully customized by the user and if the thief tries to dismiss it, it will instantly reappear.
You can decide when Undercover switches to Plan B and what message is displayed.

Plan B can not be disabled by the thief. If you installed Apple's firmware password, (see above) your Mac's Hard Disk also can't be wiped by someone who doesn't know your firmware password.

Here if you need us

On our website, we have compiled a list of frequently asked questions.
The F.A.Q. is available at: http://orbicule.com/undercover/support.php

If you have a question that is not in the F.A.Q., feel free to contact us at:
support@orbicule.com.

We value our relationship with you and we want you to be 100% satisfied with Undercover.

Stay informed

If you want to keep up with the latest Undercover news, make sure to visit our company weblog at http://orbicule.com/blog, or follow us on Twitter or Facebook.

Company Information

Orbicule BVBA
Middelweg 129
3001 Heverlee
Belgium, Europe
http://www.orbicule.com