



# User Manual

This is the User Manual for Fingbox web interface.

It is intended to provide a complete description from the user's point of view: how to setup a Sentinel to monitor a remote network, how networks are added, managed and configured via Fing Apps and Fingbox Sentinels, how data is represented and alerts are notified.

8/21/2014

---

# TABLE OF CONTENTS

1	Introduction.....	3
2	Features .....	4
2.1	Synchronization and backup .....	4
2.2	Remote discovery and monitoring .....	4
2.3	Web access to your networks .....	4
2.4	Real time alerting .....	4
2.5	Merge Networks with multiple Access Points.....	5
2.6	Remote Wake On LAN.....	6
3	Security.....	7
4	Access from a mobile device .....	8
5	Access from a web browser .....	9
5.1	Web Application .....	9
5.2	Network list panel .....	10
5.3	Network content panel.....	10
5.3.1	The list view .....	10
5.3.2	The map view.....	11
5.3.3	The toolbar .....	11
5.4	The network details page .....	13
5.4.1	The toolbar .....	13
5.4.2	The ministats panel .....	14
5.5	The host details page .....	14
5.5.1	The TCP service panel.....	15
5.6	The settings panel .....	15
6	Sentinels.....	17
6.1	Configuration .....	17
6.1.1	Step by step: what do you want to do? .....	18
6.1.2	Step by step: Fingbox account.....	18
6.1.3	Step by step: network details .....	19
6.1.4	Step by step: summary .....	20
6.2	Service start up .....	20
6.2.1	Windows.....	21
6.2.2	Linux.....	21
6.2.3	Mac OS .....	22
6.2.4	Raspian .....	22
6.2.5	Manual start .....	23
6.3	Monitoring.....	23
6.4	Removing a monitored network.....	24

## 1 Introduction

Fingbox is a cloud system to monitor and manage your networks, based on Fing mobile and desktop Apps. It's a secure, cross-platform, comprehensive solution to discover, monitor, analyze and customize your networks, from anywhere. Intuitive and powerful, Fingbox will increase the operational efficiency of your business and reduce IT maintenance cost.

Any computer, smartphone and tablet become a powerful tool to manage your networks and contribute new data. Your account can be accessed from Fing apps and through an easy-to-use web user interface.



All network settings and customizations are automatically synchronized across all your devices. By installing Fing on a desktop workstation and logging into your account, you can perform operations on remote networks through the Fingbox cloud.

## 2 Features

### 2.1 Synchronization and backup

When a network is added to a Fingbox account, you get automatic synchronization and backup of networks status, customizations, and logs across as many devices as you want. With the increasing number of personal mobile devices, you would be free of the hassle of reporting any change back from one to another. Even if your device is lost, damaged or stolen, your data is safe on our Servers.

Pick the tool you choose it's best for your work today, and you'll be free to change it tomorrow. No other monitoring tool gives you this flexibility on such a great spectrum of platforms.

You decide what networks to move into the account and what networks to keep on your local device, because it's your data, and you shall always be in control of what to upload in the cloud.

### 2.2 Remote discovery and monitoring

Fingbox Sentinels help you monitor any remote network. They sit in the system on your behalf, constantly monitoring and automatically pushing the discoveries, events and alerts to the cloud. Just deploy a Sentinel, and enjoy the view of your networks that gets updated.

Sentinels rely on Fing for Console, a cross-platform version of Fing that is already available on Windows, OS X, and Linux. You are not tied to any technology, and you can choose the most convenient server or desktop that will be used to monitor your network. No extra cost, no extra hardware, no waste of time.

In case you need a dedicated device, Fing is also available for Raspberry Pi, a credit-card size PC that is available for less than \$50. Raspberry Pi are low-cost, low-consumption PCs that can be plugged into an Ethernet network to constantly monitor a remote system.

### 2.3 Web access to your networks

Apps are great, intuitive and convenient. There are times, though, when you don't have your own device with you, or you have to perform a long series of tasks that would just be much easier if you could use a keyboard.

Fingbox comes with a unique and amazing Web application, accessible from every HTML5-compatible browser. You can review all your networks, make customizations and add notes that will be synchronized on all your devices. It is also the main way to configure alerts that you will receive through our notification system.

### 2.4 Real time alerting

Let Fingbox do the heavy lifting, and get alerts in real-time about events in your networks. Just enable the feature for the networks and devices you want to monitor, and you will receive a notification when a new host is detected - perfect for intrusion detection - and host state change notifications - like a server turning off. The notification will report any changes in the last time frame, with convenient link to the affected devices. Just tap on the links and you will be able to see the full log of changes for that device, or the entire network if you need!

- ❖ Alert on new nodes in network: go to the network details and enable it. An alert is sent every time a new unknown device comes online in your network. This is great to detect network intrusions.
- ❖ Alert on state change: go to the node details and enable it. An alert is sent every time alert-enabled nodes change state. This is great for monitoring when a server shuts down or reboots.
- ❖ TCP service monitoring: an alert is sent every time your crucial services go down and come back online. Great to detect service outages like a web server going down. This feature is available only to PRO subscriptions.

## 2.5 Merge Networks with multiple Access Points

Every connection to a network takes place through an Access Point, either wired or wireless. Hubs, switches, routers, and Wireless Access Points are all used to connect computers together on a network. It is a common scenario to access the same network through different points, making them appear in Fing as separate networks. Sometimes a single Router may provide several access points at once.

With a Fingbox account, different kinds of networks may be merged into a single network profile: Wi-Fi (single access point), Wi-Fi (multiple access points) and Ethernet networks. Once merged, every scan performed by any device will contribute changes to that single network, making handling large and complex network much easier.

You may start analyzing a network with your mobile, then add the remote monitoring from a wired laptop, and see all the data as part of the same network.

Let's see a couple of examples:

- ❖ You have multiple access points, because your Wi-Fi needs more coverage, or because your Access Point supports multiple bandwidth standards like an Apple's Time Capsule. Using the web interface of Fingbox, open one of the Wi-Fi networks and then choose the 'Merge' action. A list of options will be prompted, and you just need to select the target network to merge it with.
- ❖ You discovered the same network via both Ethernet (Sentinel) and Wi-Fi (App): Using the web interface of Fingbox, open the Ethernet network and then choose the 'Merge' option. A list of options will be prompted, and you just need to select the target network to merge it with.

Once merged, the separate networks become a single one. Updates, Logs and Alerts coming from different sources will always apply to this single, monitored network.

## 2.6 Remote Wake On LAN

With professional account you also get the auto WOL feature: automatic Wake On LAN on your crucial hosts to make them stay online 24/7.

The feature is configurable at any time for any host, so you could also use it to just start the right server whenever you need it, without being physically there pressing the button.

### 3 Security

We take security seriously and take numerous measures to make sure your data is fully protected.

All your data is encrypted and all your private information is protected on our secure servers. Access to your information is restricted, so no one other than you can view your networks, not even us. All communication channels between the Fingbox Servers and Fing Clients (Apps, Sentinels, Browser) are encrypted via HTTPS or SSL.

In addition, we use advanced encryption to store your profile information and monitored networks in the Fingbox Secure Storage, with the industry-strong 256-bit SSL suite encryption algorithms.

With Fingbox security is all over the place, and you can trust us with your data.

## 4 Access from a mobile device

You don't need additional software to use Fingbox feature. Both Fing for Android (available in the [Google Play Store](#) and in the [Amazon Market](#)) and Fing for iOS (available in the [Apple App Store](#)) are already integrated with Fingbox.

Just go into the App settings, select *Fingbox*, and type your *account id* and *password* to log in. If you don't have an account yet, you may request one from the mobile device or from our website.

After you have successfully sign on, **My Networks** will look a bit different. Networks will be split in two sections: one group reports the networks stored in your device and one group those store in your Fingbox account.

To add a network into your Fingbox account on Android, select a network from your local device and long-tap the network name until a menu appears with the "Add to Fingbox" option. Similarly on iOS, tap the "Edit" button, select the network and then tap on "Add to Fingbox".

Once a network has been added to Fingbox, it will be automatically synchronized every time you refresh or customize it. You can discover, view or edit from any mobile device and from the web interface, and the data will be backed-up and synchronized to all your devices.

Your networks are updated automatically by the system. In case you want to force a refresh on the mobile device, just tap on the "Fingbox" logo in the main view, and data will be synchronized immediately.



## 5 Access from a web browser

Fingbox has a comprehensive and nice looking web interface, allowing you to have under control your entire network and devices.

Your Fingbox account is accessible from any modern web browser supporting HTML5, including Chrome, Internet Explorer, Firefox, Safari and Opera. You may access your account at the following link:

<https://www.fingbox.com>

All communication is encrypted with Secure Socket Layer (SSL) to protect your privacy. Fingbox for Web looks and feels like one our Apps, with an easy-to-use, polished interface that requires no training. Every change to networks and nodes will be synchronized back to all your mobile devices.

### 5.1 Web Application

Once you have successfully signed in, the Fingbox Web App is displayed. The layout of its visual elements is arranged to display the most critical details in a single window in two distinct areas.



Both areas have a dedicated toolbar to interact with the view below.

On the left side, the network list panel, showing the networks in your account. At the center, the content panel, reporting essential data about the selected network. It is also used to display account settings.


When a page is dedicated to a specific network, node or activity, the window is rearranged in a simpler layout with just a toolbar on top and a content area.



The toolbar operates on just the specific element that is being displayed to customize the settings and perform actions. A “Back” icon allows going back to the previous level of detail, up to the Main Window.





## 5.2 Network list panel

This panel has two logical areas: the toolbar on top and the list of networks as main content. Please refer to the following table for the toolbar actions

	<p>Clicking on the Fingbox logo will Manage your Account options and actions, including:</p> <ul style="list-style-type: none"> <li>❖ Your account's name and password</li> <li>❖ The subscription period, its renewal and payments</li> <li>❖ The global settings and options</li> <li>❖ A page to send us direct feedback</li> <li>❖ A page to invite friends to try Fingbox</li> </ul> <p>Use this action to logout from your Account: the working session will expire and you will be redirected to the login page.</p>
---	---

The list reports all the networks currently added into your account. Every network is represented by an icon, its name, the address expressed as "IP address/mask" ([CIDR notation](#)), the date and time of last change date and the number of active devices vs. the total number of devices found.

The icon represents the different types of network that Fingbox supports:

-  **Wi-Fi:** networks that are discovered from your mobile device
-  **Ethernet:** network created/monitored by your sentinel using the data-link discovery
-  **IP:** network created/monitored using the network-layer discovery engine
-  **Merged:** a mix of Ethernet and Wi-Fi, obtained by merging two networks of those types

A network that is actively monitored by a Sentinel reports a green **Monitored** tag below network's address. If the updates from the sentinel have timed out (based on the discovery timeout that you have applied for the network), an orange **Not Responding** tag is displayed. Non-responding networks are usually an indication of missing connectivity and network failure.

## 5.3 Network content panel

Selecting a network in the network list panel will automatically display in the content panel an overview of its content, in multiple forms.

### 5.3.1 The list view

The default view is the “List View”, which displays the list of hosts in the network. The most relevant details of the hosts, like the number of devices and the most frequent type of devices, are summarized in the header.

For every host, the icon, host “best” name (evaluated among DNS name, NetBIOS name and custom name), IP and MAC addresses, device manufacturer and host tags are displayed.

If the network identifies elements by MAC address, then it may happen that a single network bridge respond to several IP addresses. In that case, a small badge marked “+N” will be displayed, reporting the number of additional IP addresses connected with the same device. As a convenience, if the host has notification alerts enabled, a special orange tag “Alerted” is displayed.

A grayed-out row represents hosts that have been found in the network, but were not responding during the latest discovery. Clicking on one row will display the

### 5.3.2 The map view

The alternative view is the “Map View”, which displays a pin on a geographical map for every network in your account. The currently selected network is highlighted and a popup is displayed by default, reporting the custom name, notes and location.




Details can be edited directly from the popup; if you type a new location address, e.g. “34th Street, New York, NY”, the pin will move to the new location.

Clicking on a pin changes the current selection, allowing you to move quickly from one network to another, based on their proximity.



### 5.3.3 The toolbar

The toolbar contains icons to execute the main actions on the network, and a text area for the free-text search.

Name	The name of the network. Clicking on the name will display the Network details page.
Search Box	<p>Searches the hosts matching the given criteria. Clicking on the search box will enlarge the text area.</p> <p>Just type any free-text and then ENTER. Fingbox will match the text with any property of the hosts - like name, mac address, vendor, IP address - and display in the table only the matching nodes. The match is always case-insensitive.</p> <p>Searching on specific properties is supported as well, using appropriate keywords. You may search by:</p> <ul style="list-style-type: none"> <li>❖ host state, e.g. <b>state:up</b> or <b>state:down</b></li> <li>❖ IP address, e.g. <b>ip:196.22.43.21</b></li> <li>❖ host name, e.g. <b>name:webserver</b></li> <li>❖ note, e.g. <b>note:No password</b></li> <li>❖ location, e.g. <b>location:34th Street, New York, NY</b></li> </ul>

	<ul style="list-style-type: none"> <li>❖ NetBIOS name, e.g. <b>netbios:MYSERVER</b></li> <li>❖ tag: e.g. <b>tag:mytag</b>, the tag can be defined in the host detail page</li> <li>❖ device type e.g.: <b>type:server</b>. Every time you assign an icon, it implicitly defines a kind of device, displayed as a green tag below the host name.</li> <li>❖ alert state, e.g. <b>alert:on</b> or <b>alert:off</b>.</li> <li>❖ mac address, e.g. <b>hw:00:18:4D:CC:AB:A2</b></li> <li>❖ vendor, e.g. <b>vendor:Cisco</b></li> </ul> <p>Wrap the filter in double quotes (“”) if the filter contains any space.                  Negative searches are supported by prefixing the minus (-) symbol, e.g. <b>state:up -vendor:Apple</b> will return all nodes that are up, except those whose device manufacturer is Apple.</p>
	<p>Allows to configure the order in which the hosts will be sorted in a network:</p> <ul style="list-style-type: none"> <li>❖ by IP address</li> <li>❖ by MAC address</li> <li>❖ by name, alphabetically</li> <li>❖ by state, hosts that are UP first</li> <li>❖ by vendor, alphabetically</li> <li>❖ by last change, hosts that changed their state recently first</li> </ul>
	<p>Advanced management of the current network. A list of action you can do with your network:</p> <ul style="list-style-type: none"> <li>❖ Delete the network</li> <li>❖ Merge with other networks: if you networks can be merged with some of your Wi-Fi networks, a list of possible selections will be prompted to you, just select one of them and the network will be merged</li> <li>❖ Split in separate networks: a previously merged network can be split out again in separate networks</li> <li>❖ Sync customizations: the customizations from other networks can be applied to the current one</li> <li>❖ Disable all alerts: disable the alert on state change for the current node</li> <li>❖ Enable all alerts: enable the alert on state change for the current node</li> </ul>
	<p>Export the hosts contained in the network as:</p> <ul style="list-style-type: none"> <li>❖ XML file</li> <li>❖ CSV file</li> <li>❖ HTML file</li> </ul>

A segmented section allows changing the way you analyze the current network.

	<p>Switches to the table view, showing all the hosts, one per row.</p>
	<p>Switches to the map view, showing all networks in your account.</p>

## 5.4 The network details page

This panel is displayed by clicking the network name link in the main window.

It displays all the network details and it allows you to customize the network name, its notes, its location address and to specify space-separated tags.

You don't have to manually save after a modification: any change is persisted into Fingbox when the input focus leaves one the text areas.





If a valid location address is set, the map will be centered on the given address. Without a specific address, Fingbox will center the map based on a geo-referenced database of IP addresses of the Internet Provider, if any.

Network details collected by Fing apps and Fingbox Sentinels are reported below that area. The details report the network Access Points (Wi-Fi BSSID), the Internet Provider and other key addresses the network is configured with.

A summary of the latest events is also displayed, allowing a quick overview of the devices that were turned on and off or services that have been started and stopped (when TCP monitoring is enabled). A link allows to browse the full log.

### 5.4.1 The toolbar

The toolbar contains icons to execute the main configuration on the network.

	<p>Goes back to the main window.</p>
	<p>Enable and disables the alert on new nodes. When enabled, you will be notified if a new device is connected to your network, and also the new device will have the alert on state change enabled by default.</p>
	<p>Enable and disables the discovery timeout alert. When enabled, if the sentinel does not send updates to the cloud and you have set a timeout of 2 minutes, you will be notified whenever a Sentinel update has not been received for more than 2 minutes. This feature is really useful to be informed if your network lost the Internet connectivity.</p>
	<p>Changes the way in which Fing uniquely identifies host during the discovery process. Alternatives are:</p> <ul style="list-style-type: none"> <li>❖ by MAC address. (default)</li> <li>❖ by IP Address</li> </ul> <p>Beware of the impact that changing this setting implies. When the identification key is the MAC address, the same machine will always be recognized; the downside is that network bridges may present several IP addresses as a single device, and</p>

	<p>you cannot customize the single devices the bridge is connected to.</p> <p>The opposite is the identification by IP Address: every IP becomes a host that can be edited; the downside is that unstable IP assignments coming from a DHCP will mess up your customizations.</p> <p>Networks discovered using the network-layer discovery engine will always identify by IP Address.</p>
--	---

### 5.4.2 The ministsats panel

Fingbox calculates and displays a minimal set of statistics, based on the hosts found on your network. It's a useful tool to understand at a glance the composition of the devices, e.g. how many laptops vs. fixed PC vs. servers you might have in a network to monitor.

It also displays a distribution of device manufacturers, giving you a simple but immediate idea of the type of vendors you might have to manage.




## 5.5 The host details page


This panel is displayed by clicking the host row in the main window's list view.

It displays all the host details and it allows you to customize the host name, its notes, its location address and to specify space-separated tags.

You don't have to manually save after a modification: any change is persisted into Fingbox when the input focus leaves one the text areas.

A summary of the latest events is also displayed, allowing a quick overview of the devices that were turned on and off or services that have been started and stopped (when TCP monitoring is enabled). A link allows browsing the full log.

	<p>Goes back to the Main window.</p>
	<p>Enable and disables the alert on state changes. You will be informed every time a host changes its state i.e. from UP to DOWN and vice versa.</p>
	<p>Enables and disables the automatic Wake on LAN feature. If you expect a machine to be always on, Fingbox can re-boot the device when it is detected as being DOWN after a network discovery.</p> <p>The Fingbox Sentinel will send a <a href="#">WOL (Wake on LAN) packet</a> targeting the</p>

	specific device. Usually, a BIOS setting enables the machine to be remotely powered on. Please refer to the Operator Manual of the specific device.
	Advanced management of the current host. A list of action you can do with on the current host: <ul style="list-style-type: none"><li>• Delete this node. It removes the host from the network</li><li>• Push node customization: you can apply the customization to another network if the node is present on multiple networks, e.g. a mobile device.</li></ul>

### 5.5.1 The TCP service panel

Fingbox TCP service monitoring, available only for PROFESSIONAL accounts, lets you to configure what services Fingbox shall verify on this host. A text fields accepts port numbers and service descriptions; the text is automatically completed using an internal database of service names and ports, but you can also enter a custom port and description to be monitored.

Just type a port or a service name and click ENTER and the service will be added to the list. The remote Sentinel will discover perform the service check at the next round of discovery. The current state and the date and time of last change is reported in the table and logged as a network event.

The port number of the service is also used to represent the status. When it is **green**, the service is up; when it is **red**, the service has not been detected; when it is **black**, the status is unknown.

Fingbox may send notifications when the service changes its state. If you want to enable/disable the alert for service state change just click on the small alert icon: when the icon appears filled, the alert will be sent.

## 5.6 The settings panel

The settings panel contains the application wide customization. Here is possible to configure the time zone for the alert's date and time, the email address that Fingbox will send the alerts to, and the alerting type:

- “Do not send”  
the alerts are temporarily disabled
- “A summary email with multiple events”  
an email containing all network events detected at each refresh; all events, even of different nature, are summarized in the single email

- “A separate email for each event”  
an email for each single event happened, with self describing subject, e.g.: *Node DOWN: Webserver-Main @ CentralSite*

It allows also to configure the order in which networks are listed in the Network List panel: by Name, by the time of the last change (most-recently change will be on top), by the time of the last discovery (most-recently discovered will be on top).



## 6 Sentinels

Fingbox Sentinels remotely monitor your networks. Discoveries, events and alerts are automatically pushed to the cloud using a secure connection.

Once deployed, a Sentinel will constantly monitor your network. Changes are synchronized into your Fingbox account, providing real time updates to Fing on Android, iOS and the Web. Moreover, when you configure alerts on the network and related hosts, you'll receive real-time email notifications of the changes.

Sentinels are part of Fing 2.x for Windows, Mac, Linux and Raspberry. You may start monitoring a network in two very simple steps.

### 6.1 Configuration

First, you need to install Fing on your computer/server where you have administrative rights.

This means that on Windows Vista and Windows 7 you must make sure to run it as Administrator, or to have the UAC (User Access Control) turned off.

On Linux and OS X, you must make sure to run it with sudo or as root.

The configuration of the network discovery and linked Fingbox Account is a one-time-only guided procedure.

On Windows, you may select Overlook Fing from the Start Menu, or open a Command Prompt and type:

```
fing -interactive
```

On OS X and Linux, open a Terminal/Shell and type:

```
sudo fing --interactive
```

You'll be prompted to enter the target network details. A valid Fingbox account will be requested and validated against our servers.

The Fingbox Sentinel works using HTTPS so you should make it possible for outgoing HTTPS (TCP port 80 and 443) to fingbox.com to take place. Fingbox Sentinels also support HTTP proxy, which can be configured in the Fing configuration file (fing.properties).

Once the interactive configuration procedure is complete, a Fingbox profile is saved to an encrypted file on your local file system in Sentinel configuration folder; on Windows you have

a link to Sentinel folder from Start Menu shortcuts, while on OS X and Linux you it's placed in the folder mentioned below.

The created profiles are then placed in the Sentinel configuration folder:

- On Windows you have a link to from Start Menu / Overlook Fing
- On Linux/MAC you can find it at `/var/data/fing/sentinel`

The Sentinel service automatically runs each profile found in the above folder.

Please note that you can skip the following sections and directly try the interactive procedure of configuring your sentinel, as it's a guided procedure. However, if you don't feel confident, just read the systematic chapters below to understand what you'll be asked by the sentinel configuration facility.

If you want to skip this, just jump to Service start up chapter.

### 6.1.1 Step by step: what do you want to do?

First of all you are prompted about your main purpose, as fing is not only the Fingbox Sentinel but also a command line utility, capable of performing network discovery, TCP service scan, ping, show network information.

```
Do you want to (D)iscover, (S)can, (F)ingbox, (P)ing or display
(I)nfos?
> f
```

So just, type the letter **f** to the question above.

### 6.1.2 Step by step: Fingbox account

You are prompted to enter your Fingbox credentials: username and password. The username is the email address you used to register to the service.

```
Please enter Fingbox account username.
> johndoe@mydomain.com

Please enter Fingbox account password.
>
```

You must enter your email address, press enter, then your password, and again enter. Please note that when you are entering your password you are not going to read the characters on the screen, as they are being hidden for privacy reasons.

The configuration program connects to one of our remote servers and checks your account. The outcome is dumped on screen, showing your account details, as per example below.

```
Logging in to FingBox... OK

FingBox details:
  Account:      johndoe@mydomain.com (John Doe)
  Account type: PROFESSIONAL until 2014/05/22
```

### 6.1.3 Step by step: network details

It's time to decide which network you want to monitor. The configuration utility checks your system and shows you the current active local networks, as per text below:

```
Please select the network to be monitored and added to Fingbox.
Type a letter or a network.

(A) NIC Gigabit Ethernet Adapter
    192.168.1.100/24 - Ethernet

(B) VirtualBox Host-Only Ethernet Adapter
    192.168.56.1/24 - Ethernet
>
```

In most cases, you will just type the letter of the corresponding network that you want the sentinel to monitor. E.g. in the case you chose the first one, you just type letter **a** and enter. If you are interested in monitoring a non-local network, like a WAN or a VPN, just can write it directly at the prompt, e.g.:

```
> west-site.mydomain.com/24

Please enter a name to identify the network.
Leave blank for default: 192.168.1.0/24
>
```

You are then prompted to enter a custom network name, but you can leave the default one. Then you must provide the monitoring refresh interval in minutes. Home account owners have a limit down to 10 minutes interval, while professional accounts can rely on much lower granularity.

```
Please enter refresh interval in minutes.
Leave blank for default (15 minutes). Minimum is 10.
> 10
```

### 6.1.4 Step by step: summary

A summary shows you the configuration details of your network to be added to the Fingbox sentinel.

```
FingBox configuration:
  Account:      johndoe@mydomain.com (John Doe)
  Account type: PROFESSIONAL until 2014/05/22
  Network:     192.168.1.0/24 (Ethernet)
  Network name: west-site
  Refresh:    10 minutes
  NUI:        eth-90E6BAD87156-192.168.1.0-24
  Conf file:   west-site.fingbox

Automatic configuration dumped above. Choose No to customize Fingbox
NUI/file.
Do you want to keep it, (Y)es or (N)o?
```

In the common case, you will answer **y** to question to commit the configuration and you can skip the rest of the chapter, jumping straight on the *Service start up* section.

You should answer **n** and customize the NUI if you are configuring a network that was previously being monitored by another server/computer. NUI is Network Unique Identifier and in Fingbox is used, as the name says, to uniquely identify a network in your account. If you are in the case above, of deploying a sentinel in a new server but willing to keep all existing configuration, you should now go to the Web User Interface, select the network and go to the network panel details; there you find a line providing you the needed information:

**NUI: eth-90E6BAD87156-192.168.1.0-24 (Support Code #234815042)**

Copy the NUI and use it to configure the sentinel; the support code is not needed here, it is used instead in cases you need us to investigate specific issues and our support team need to read your network details to debug the issue.

Using the NUI of an existing Fingbox network makes sure that there won't be any duplication and the newly installed sentinel will update the same network.

## 6.2 Service start up

The Fingbox Sentinel automatically runs all configured profiles placed in its Sentinel configuration folder. The Sentinel can run as:

- Windows service
- Linux/Unix System V init service (RedHat/Centos/RPM-based)
- Upstart service (Ubuntu/Debian-based)
- OSX Launchd (Mac OS)
- Raspian (Raspberry Pi)
- Manually started

### 6.2.1 Windows

On Windows, the interactive procedure of creating a profile also manages the service installation and startup. Just answer yes when requested to register and start the Fingbox sentinel service. That's all.

### 6.2.2 Linux

On Linux the Sentinel service can be installed, according to the target platform:

- Linux/Unix System V init service (RedHat/Centos/RPM-based)
- Upstart service (Ubuntu/Debian-based)

#### 6.2.2.1 System V

The following section applies to Linux distributions supporting System V init.d  
Red-hat, Centos, and other RPM based distributions support it.

Copy or link the init.d script from `/usr/lib/fing/init.d/fingbox-sentinel` to your `/etc/init.d` folder.

Then add to your services with:

```
chkconfig --add fingbox-sentinel
```

To manually control the service:  
start:

```
service fingbox-sentinel start
```

stop:

```
service fingbox-sentinel stop
```

restart:

```
service fingbox-sentinel restart
```

#### 6.2.2.2 Upstart service

The following section applies to Linux distributions supporting Upstart, Ubuntu and other Debian based.

Copy the upstart script from `/usr/lib/fing/upstart/fingbox-sentinel.conf` to your `/etc/init` folder.

To manage the service with upstart:  
start:

```
sudo start fingbox-sentinel
```

stop:

```
sudo stop fingbox-sentinel
```

### 6.2.3 Mac OS

The Sentinel is compatible with OSX Launchd, as follows.

Copy or link the launchd script from `/usr/lib/fing/launchd/com.overlooksoft.FingSentinel.plist` to your `/Library/LaunchDaemons` folder.

To copy:

```
sudo cp /usr/lib/fing/launchd/com.overlooksoft.FingSentinel.plist  
/Library/LaunchDaemons
```

To manually load and start the service in background:

```
sudo launchctl load com.overlooksoft.FingSentinel.plist
```

To unload:

```
sudo launchctl unload com.overlooksoft.FingSentinel.plist
```

### 6.2.4 Raspian

The following section applies Raspberry pi distribution supporting System V init.d  
Raspbian based distributions support it.

Copy or link the init.d script from `/usr/lib/fing/init.d/fingbox-sentinel.raspberry` to your  
`/etc/init.d/fingbox-sentinel`

Make sure you have installed chkconfig:

```
sudo apt-get install chkconfig
```

Then add to your services with:

```
chkconfig --add fingbox-sentinel
```

To manually control the service:

start:

```
service fingbox-sentinel start
```

stop:

```
service fingbox-sentinel stop
```

restart:

```
service fingbox-sentinel restart
```

### 6.2.5 Manual start

If you really need to manually start the FingBox Sentinel, it is a simple and straightforward command on Windows:

```
fing --sentinel
```

On OS X and Linux:

```
sudo fing --sentinel
```

The command runs Fing in Fingbox Sentinel mode, thus it's neverending; if you close, kill or interrupt it, you are actually stopping the sentinel.

## 6.3 Monitoring

By default the Sentinel doesn't log, but it can be easily enabled by means of a configuration setting: in `fing.properties` configuration file:

- On Windows you have a link to from Start Menu / Overlook Fing / Fing configuration
- On other platforms it is placed in `/etc/fing`

Edit configuration as follows:

```
overlook.fing.logging.enabled = true
overlook.fing.logging.level = INFO
```

The log is stored:

- On Windows you have a link to from Start Menu / Overlook Fing / Fing logs
- On other platforms it is placed in `/var/log/fing`

In case you are experiencing issues Overlook Support team might ask you for even more verbose logs, in that case you should set log level to `DEBUG`.

## Tuning

In some rare cases, you should tune the `fing` discovery engine to better fit your needs.

Discovery engine configuration is placed in `fing` configuration folder, in `discovery.properties` file; you can tune default profiles to change the engine behavior.

E.g. if you experience some frequent up/down state change, you could want to increase the timeouts and discovery thresholds for `data-link` discovery engine:

```
# native (data-link) discovery configuration for default profile
profile.default.data-link.round.interval = 60000
profile.default.data-link.packet.interval = 6
profile.default.data-link.timeout = 3000
profile.default.data-link.retries = 3
```

## 6.4 Removing a monitored network

To remove a previously configured network discovery added to your Fingbox Sentinel you should stop the Sentinel service and manually remove its configuration file in Sentinel folder.

As mentioned above, to find the Sentinel configuration folder:

- On Windows you have a link to from Start Menu / Overlook Fing
- On Linux/MAC you can find it at `/var/data/fing/sentinel`

Just remove the file of the network you want to erase and then restart the service.