

Setting up your WhoFi Agent

A WhoFi Deployment can be implemented in 3 Steps.



Step 1

Running a Local Agent on your network to Detect Devices

A WhoFi detection agent needs to be running on your local network in some manner to be able to detect all devices. WhoFi detection agents are available as Windows and Android software downloads, as well as a router plugins for Meraki, Aruba, and Aerohive access points. We also have custom API plugin solutions for systems with 5 or more locations or subnets.

NETWORK REQUIREMENT By default, each downloadable WhoFi detection agent needs to be on the same subnet as other devices that you would like to detect. This is because each agent uses an ARP request probe to detect other devices on the same network. ARP is not usually a routable protocol. This means that if you have multiple VLANs, you will need to have a software agent on each VLAN that you would like to monitor for the detection agent to be able to see the

other devices. This also means that if your router or access point runs in AP isolation mode, where each device is given their own micro-network, then the detection agent will not be able to see other devices on the network. In those cases, a DHCP or SNMP based solution, a configuration change, a router plugin, or other API solution is recommended.

HARDWARE REQUIREMENT Each downloadable WhoFi detection agent also needs to be on a device that is always on. Because it is periodically scanning the network for device inventory, the device turning off occasionally would cause data to be missing in your online reports. A dedicated computer, server, or tablet is recommended to run the detection agent.

WhoFi downloadable detection agents are available as Free downloads by logging into your analytics account at <https://whofi.com>

Step 2

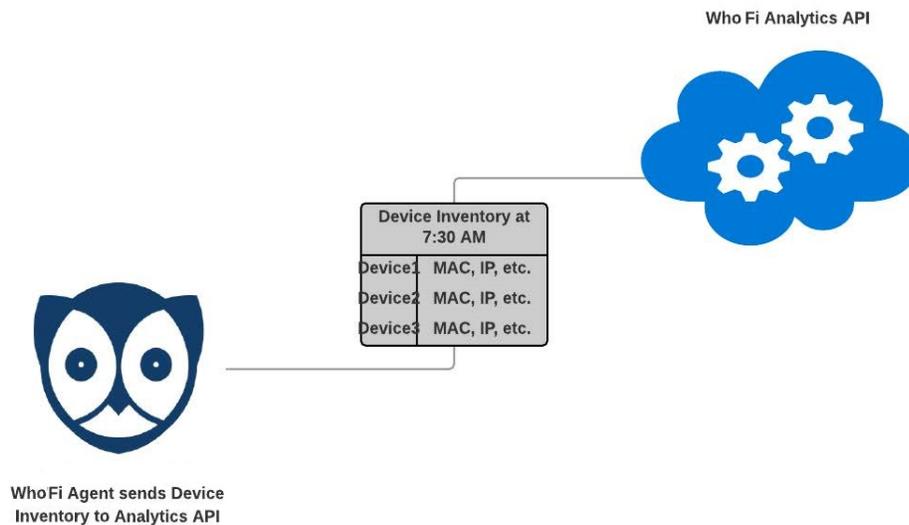
Ensuring Detection Agent Can Connect to WhoFi Analytics API

WhoFi detection agents are designed to store small amounts of data over time. To handle historical reporting, the WhoFi detection agent sends point in time inventory data to the WhoFi Analytics API.

To ensure proper connectivity please make sure that whatever device will be running a WhoFi detection agent needs to be able to access this website: <https://api.whoisonmywifi.net>

INBOUND PORTS There are no inbound ports required to use WhoFi detection agents or WhoFi Analytics.

OUTBOUND PORTS Outbound Port 443 to <https://api.whoisonmywifi.net> is required to send device inventory data to the WhoFi Analytics API over ssl/tls.

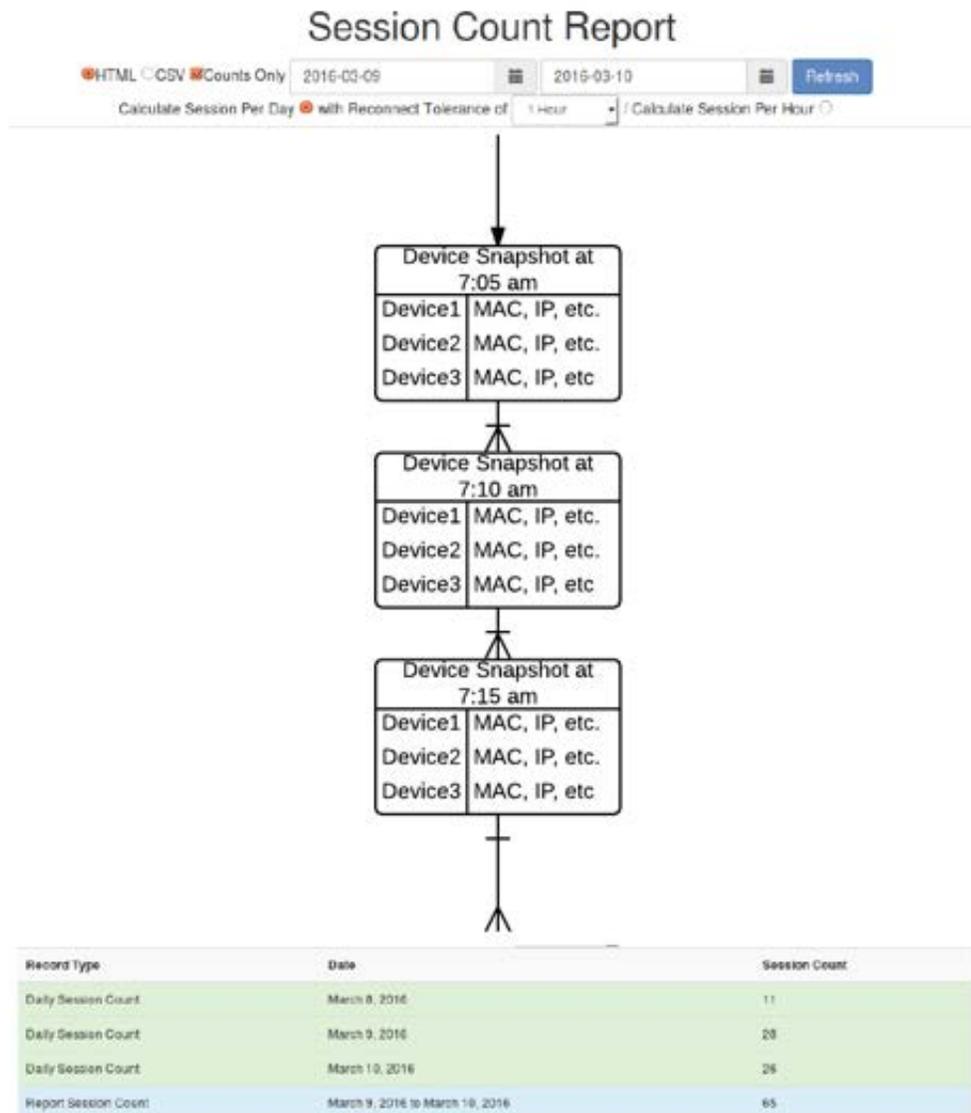


Step 3

Decide who will view Online Reports

Once the device inventory data is stored in the online analytics system, the reports can be viewed by any user that has been given access, from anywhere. They do not need to be on the same local network as the access points to view reports.

You will need to set the privileges for the users who have been given access to WhoFi's Analytics system. Go to the Admin tab to see the reports vs. who should be an administrator on the account. Sometimes these are the same people, and sometimes they are different.



Multi-Network and Multi-Location Considerations

WhoFi downloadable detection agents are set to detect device inventory on a single subnet by default. WhoFi Analytics is built to receive data from multiple agents across different subnets or locations.

This means that if you have several VLANs, and you'd only like to monitor a single VLAN, then your setup is simple. You would simply need some kind of always on device on the VLAN you'd like to monitor, install one of the software agents onto this device, make sure it can connect to the internet, and you'll start to see device data connect to your online analytics account.

If you'd like to monitor several VLANs, often the best result is to have a single agent per VLAN. Android Tablets are a good solution for this. Each agent on each VLAN would need to be able to connect to the WhoFi API.

In our technology's view, there is no difference between a Multi-Network and Multi-Location setup.

If you have more than 5 locations or VLANs that you would like to monitor, we have additional agent types that you might want to consider. The first multi-location agent option is a plugin for Meraki, Aruba, and Aerohive access points. The second multi-location option is an agent that works directly on a Windows DHCP Server with multiple scopes. Finally, we have custom SNMP API agents that can connect to various Wireless Controllers, to detect all devices across multiple locations.

If you have more than 5 locations or VLANs, please contact us, and we'll be happy to discuss a solution that will work for your needs.

DEVICE PRIVACY OPTIONS

In the settings section of the agent under **DEVICE PRIVACY OPTION** (*Online Users*)—Click on **PUBLIC NETWORK/ANONYMIZE UNKNOWN DEVICES** this will then anonymize and encrypt all patron information being sent to the cloud.

ADMIN SECTION

Setting up Additional Users for the same account. Go to the **ADMIN TAB** and click on **USERS** and then click **ADD USERS** and then enter all pertinent information and select the Permission Group they should be assigned.

SETTING UP A USER ACCESS GROUP

Setting User Access Privileges by group. Go to the **ADMIN TAB** and click **USER ACCESS GROUP** and then click **ADD ACCESS GROUP** then enter in the Group name and select the privileges you would like the members to have access too.

FILTER VIEW

Viewing a specific network through the filter view. First go the **MY ACCOUNT** tab and then click **NETWORK FILTER** and then check the box that says **ENABLE NETWORK FILTERING**. You may now select the Network you would like to view.

MULTI-LOCATION VIEW

Multi-locations systems will see a Location drop down under their My Account section. To see analytics reports per location, simply choose the location from the drop down menu and view the report you'd like to see.

INTERNAL EQUIPMENT SESSION MONITORING SETTINGS

To ignore the session counts of internal equipment first click on **DEVICE** then identify the MAC Address or IP Address of the device you would like to ignore the session counts of. Once you have identified the device click the + sign next to the device and then check the box that says **HIDE FROM SESSION COUNT**. To save your changes click the **UPDATE** button.

Contact Us

At WhoFi, our goal is to provide you with the best possible user experience. We are here to answer any questions you may have about our services, so feel free to reach out to us and we will be happy to assist you.

Technical Support

For questions about the product, or technical support, please visit the Support Knowledge Base at <http://whofi.zendesk.com> For support, e-mail us at support@whofi.com, or call one of our support lines.

Phone Support

Toll Free: 1-800-278-5099
Direct Line: 1-405-415-0434

Hours of Operation

Our Regular Business Hours are Monday – Friday, 9 am to 5pm CST.

Mailing Address

WhoFi
4005 NW Expressway,
Suite 610
Oklahoma City, OK 73116
USA