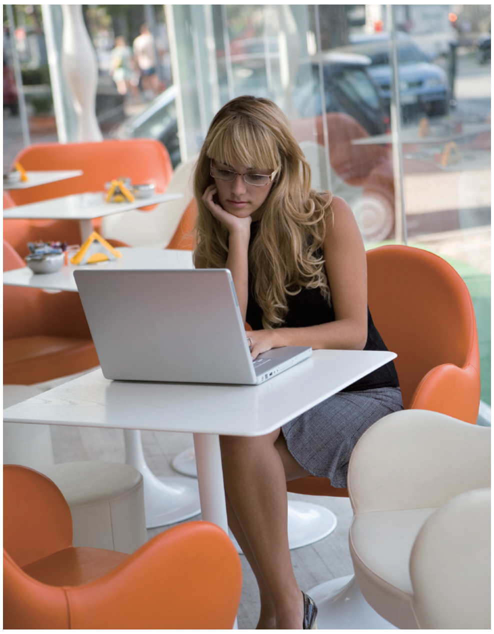
FLEXIBLE WI-FI AUTHENTICATION

FEATURE GUIDE

SUMMARY OF FEATURES

- BROWSER-BASED AUTHENTICATION
- 802.1X AUTHENTICATION
- EAP METHODS SUPPORTED
- IP/MAC-BASED AUTHENTICATION
- MULTIPLE ACTIVE AUTHENTICATION SERVERS
- CAPTIVE PORTAL CUSTOMIZATION
- WALLED GARDEN & ADVERTISEMENTS
- EASY GUEST ACCESS
- USER BLACKLISTING
- ON-DEMAND ACCOUNTS

INTRODUCTION



Nowadays when you attempt to connect to public Wi-Fi on your smartphone or tablet, there are a couple of things that you may notice. First, some SSIDs may have that pesky little lock icon next to it. Second, for the SSIDs that aren't locked with a passcode, you will most likely encounter some sort of terms of service page or login page when first attempting to access a website. Without the correct passcode or login credentials, none of these SSIDs (networks) can actually be used – so don't get excited too fast when you see a large list of SSIDs. But why do providers of Wi-Fi access set these limitations and restrictions on their networks? Why not just leave the networks open?

For organizations and establishments that provide Wi-Fi access, the tradeoff between ease-of-use and network quality has been an ongoing tug-of-war. On one hand, if the tasks required to get on Wi-Fi are too long and complex, users may feel annoyed, complain, or not use the service at all. On the other, if the Wi-Fi is left completely open, unauthorized users can easily leech off of the broadband and consume the entire available bandwidth. Therefore, open Wi-Fi is a luxury that organizations cannot provide, given the need to protect critical network resources and ensure an acceptable standard for network performance.

This feature guide aims to address the Wi-Fi access concerns of organizations, and will dive into all the facets of 4ipnet's user authentication features, explaining in detail how these features help organizations manage their Wi-Fi networks for security and QoS purposes. Features such as 802.1X and browser-based authentication via captive portals can be found on most enterprise-grade products today, but 4ipnet's solution goes above and beyond to provide an unparalleled flexibility that can suit the needs of any deployment.

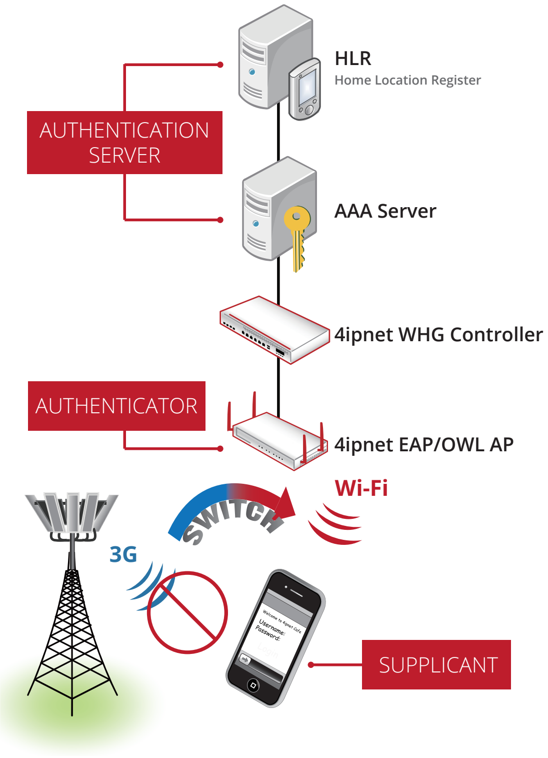
THE COMMONLY SEEN BROWSER-BASED LOGIN

If you've ever tried to log in to Wi-Fi at an airport, train station, or some other public location, you've probably already encountered **BROWSER-BASED AUTHENTICATION**. In simple terms, browser-based authentication is the process by which a user is not allowed access until authenticating (entering a correct username and password combination) in a web browser page. Even if Wi-Fi access at an establishment is free, the acceptance of a terms and conditions can still be interpreted as "authentication" – the denial of access until an action is performed.

In the next section another type of authentication, namely 802.1X, will be described. After understanding 802.1X you may wonder – why not just use 802.1X instead of browser-based authentication? For most users, logging in to Wi-Fi using a device's web browser is much more straightforward than using 802.1X. And in some cases, it's the only acceptable way. For example, 802.1X is not a viable option in public venues where there isn't a regular set of users/accounts, since creating an account in the back-end database for every temporary user (which may be up to hundreds or thousands of unique users per day) is just unrealistic and impractical.

802.1X: TRANSPARENT AND SECURE

Another form of user authentication commonly used today is **802.1X AUTHENTICATION**, where clients communicate with a backend RADIUS server that contains account information of all the network's users. In 802.1X, EAP (Extensible Authentication Protocol) is the framework used to perform authentication, with the supplicant and authentication server negotiating an appropriate EAP method to be used for authentication. If the authentication is successful, the authenticator (e.g. 4ipnet EAP/OWL-series access points) allows clients access to the network. If it fails, then the authenticator rejects the network access.



Both the WHG controllers and EAP/OWL-series access points support virtually all EAP methods. The following is a list of **EAP METHODS SUPPORTED** by 4ipnet access points and controllers:

1. EAP-AKA
2. EAP-FAST
3. EAP-GTC
4. EAP-MD5
5. EAP-SIM
6. EAP-TLS
7. EAP-TLV
8. EAP-TTLS
9. LEAP
10. PEAP

802.1X is the preferred method of authentication in environments where security is of the upmost concern, such as in enterprises and government facilities. Furthermore, given the explosion of mobile device traffic in recent years, carriers are increasingly using EAP methods such as EAP-SIM and EAP-AKA to automatically offload clients from their 3G networks to Wi-Fi.

In addition to security, one of the major benefits of 802.1X is the seamless & transparent login process. The user does not need to access a web browser after connecting to the 802.1X enabled access point – rather, he/she can directly start using all Internet services upon association to the AP.

AUTOMATIC DEVICE AUTHENTICATION

In deployments where a fixed set of devices access the network regularly, it may make sense to perform **IP/MAC-BASED AUTHENTICATION** of devices. The primary benefit of this type of authentication is convenience, as users do not have to enter a username and password every time they wish to gain access to the network. Although convenient, this type of authentication is not as secure – if the device were to get stolen or fall in the hands of others, those individuals would be incorrectly authenticated. Despite increasing the risk of a security breach, there are still many deployments that would place higher value on the convenience that this feature brings.

In a network managed by a 4ipnet WHG controller, devices that are authenticated via IP or MAC addresses can also be assigned to roles with associated access control profiles. This comes in handy when network administrators wish to assign a specific device or group of devices to a role that is unique from all other roles in the system. For example, when the user uses a MAC-authenticated device to log in, the policy assigned to the device can be different than if the user were to log in regularly using 802.1X or browser-based authentication.

Sometimes it is also necessary for certain network elements (e.g. servers providing specific network services) to be able to gain access to the external network or Internet without performing authentication. By tying the IP address and/or MAC address of that server to IP/MAC-based authentication, administrators can ensure that these servers can provide services normally and not be blocked due to lack of authentication.

ONE NETWORK, MULTIPLE AUTHENTICATION SERVERS

In each Service Zone (essentially a virtual controller consisting of individual network services, authentication settings, policy assignments, etc.), it is possible to configure **MULTIPLE SIMULTANEOUSLY ACTIVE AUTHENTICATION SERVERS**. The following authentication servers are supported by 4ipnet WHG controllers:

1. RADIUS
2. LDAP
3. NT Domain
4. SIP
5. POP3
6. Local accounts (internal database)
7. On-Demand accounts (internal database)
8. Guest

The primary benefit of having multiple active authentication servers at the same time is to cater to the different needs of each deployment. For instance, visitors at a public venue may be asked to purchase Wi-Fi accounts (using On-Demand authentication), while the staff who work at the venue day in and day out may have permanent accounts (using Local authentication). The network may also consist of SIP-based phones, which would require SIP authentication to also be active in the same Service Zone. In another example, a deployment may require two separate external RADIUS servers for authentication, as accounts for users of different roles may be stored at different locations. With the 4ipnet WHG controller, none of these cases will cause network administrators to even break a sweat – the configuration of authentication servers is extremely straightforward and flexible.

CUSTOMIZED EXACTLY THE WAY YOU WANT

Users using browser-based authentication will typically encounter a captive portal, a special web page that is displayed to a user for authentication purposes, before the user is granted access to the network or Internet. Some network providers may want this page to simply show a service disclaimer, while others may want this page to provide a full-fledged login with terms of service, username and password, etc. Due to the vastly different requirements of each network provider or organization when it comes to what information is to be displayed on this page, the page must support fine-grained and extensible customization.

A 4ipnet-powered wireless LAN supports customization of all the different types of pages that may be encountered by Wi-Fi users. The login page, login success page, login failed page, and logout page are just some examples of pages that can be completely customized. However, what truly distinguishes 4ipnet's captive portal customization from that of other vendors is the ability for each page to be customized independent of one another.

4ipnet WHG controllers support four types of **CAPTIVE PORTAL CUSTOMIZATION**:

1. 4ipnet Default – the most basic page design with no customization required
2. Customize with Template – page elements (e.g. the action that occurs when "submit" is pressed) are pre-defined, but colors of buttons and wordings can be modified
3. Upload Page – the entire page is written externally in html and uploaded to the WHG
4. External Page – the entire page resides on another location reachable by the WHG; users that need to be authenticated will be redirected to this location

Each page (e.g. login success, login failed, etc.) can be assigned a type individually, such that some pages can be uploaded, while others can simply be customized with template. Even the page that tells users (briefly) that they are being redirected can be completed customized. Whether for hotels, enterprises, coffee shops, or public venues, network administrators can easily adapt the authentication-related pages to fit the needs of the each deployment.

ALLOWING ACCESS BEFORE AUTHENTICATION

Sometimes it is necessary to universally allow access to certain network locations even when devices have not yet been authenticated, as these locations may be essential towards some basic function of the device. In other cases, these locations may simply be web pages containing general information, such as the map of a mall or hotel. As another example, carriers may wish to utilize the high traffic flow [of people] generated by their Wi-Fi hotspots to sell advertisements that users see during the Wi-Fi login process.

To support these different needs, the WHG controller contains a **WALLED GARDEN** feature, which allows network administrators to specify a whitelist of IP addresses and/or domain names – locations that are allowed prior to authentication. To round off the feature, each entry can be individually configured to either be displayed on the Wi-Fi login page as **ADVERTISEMENTS**, or hidden as an intrinsic property. As mentioned previously, network operators can use the advertisement feature as an additional source of revenue by selling ad space to other organizations, or simply use this feature as a method to provide Wi-Fi users with relevant information.

QUICK AND FREE GUEST WI-FI

In many public venues the ability to provide **EASY GUEST ACCESS** without users having to enter login credentials is a much desired feature. For organizations offering Wi-Fi service, creating guest accounts can be a big hassle, especially if there are an immense number of guests each day. For the guests, obtaining a set of account credentials just to use the Wi-Fi can also be an irritating task. Thus, these venues ultimately opt to provide Wi-Fi that can be easily accessed by the guests themselves. However, just because the users aren't asked to login with a username and password doesn't mean that their usage shouldn't be managed. As previously mentioned, it is imperative to manage users' usages, otherwise malicious activities cannot be prevented and Wi-Fi quality cannot be guaranteed.

The WHG controller allows network administrators to provide guests with an easy method to login – the guests only have to enter their e-mail address before gaining access to the Internet. Furthermore, the guest accounts can be limited by time, and have the same comprehensive access control profiles as regular users (e.g. bandwidth limitations, firewall rules, etc.). In the event that the account is limited by time, it doesn't make much sense if the user can simply enter another e-mail address after the account has expired and continue surfing the web. To address this issue, administrators can define a reactivation time, which is the minimum amount of time that the device must wait before being allowed access again.

4ipnet's guest access system ensures that even when authentication is more lax, all of the Wi-Fi users are still being managed with the same level of detail, maintaining a fine balance between ease-of-use with quality of service.

BLOCKING UNWANTED USERS

No matter how tightly a network is managed or how completely the security is enforced, there will still be users who try to bypass security measures and use the network in an illegal manner. For example, students will often use a university's high-speed network to illegally download music or movies, and even when given warnings, continue to act in the same manner. For users such as these, it is simply not enough to just perform bandwidth limitations or apply firewall rules that block access to applications and sites. In these cases, more extreme measures are required.

USER BLACKLISTING, or the banning of a user from a network, is the most absolute method for safeguarding the network from malicious users. In this feature guide we discussed all the various methods that a user can be authenticated onto a Wi-Fi network secured by a 4ipnet WHG controller. Regardless of which authentication type and server used, each user will have a unique account that distinguishes him/her from others on the network. If this account is blacklisted, the user will have no means to get on the network, and consequently will not be able to perform any illegal activities.

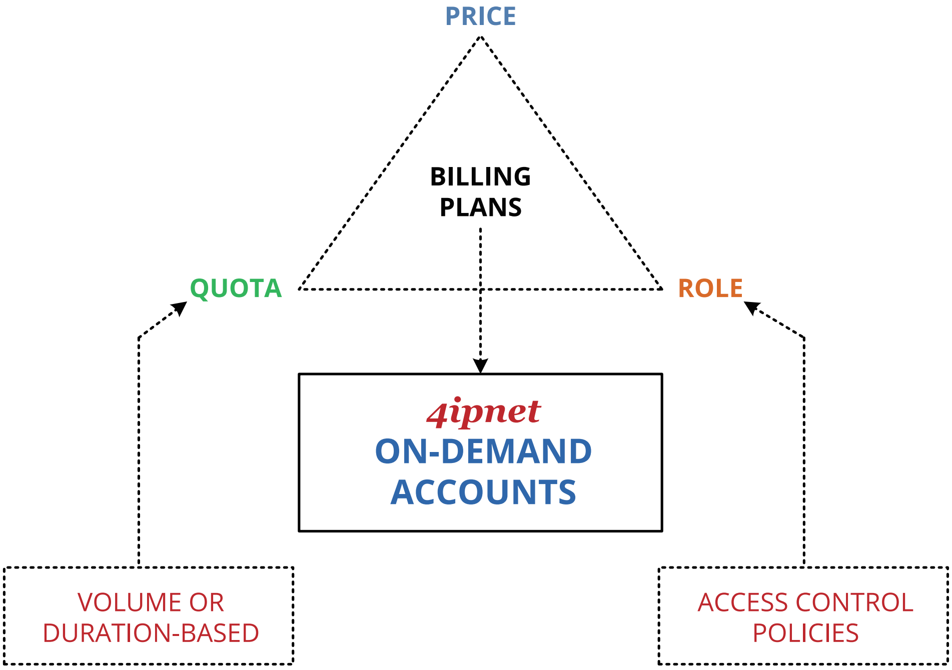
In summary, user blacklisting is an effective method that network providers have at their disposal when they need to enforce the usage rights of their network. Users will also be deterred from attempting to infract on these rights, and encouraged use the network respectfully.

QUOTA-BASED, BILLABLE WI-FI ACCOUNTS

Although free Wi-Fi is a growing trend in recent years, it is not ideal for every environment. For example, coffee shops have begun to realize that Wi-Fi is both an advantage and a drawback. Many coffee-goers will not buy their daily cup of coffee at a shop that does not provide free Wi-Fi, but when a shop does provide free Wi-Fi, people become "Wi-Fi squatters", taking up all the seats and turning away potential paying customers.

4ipnet's **ON-DEMAND ACCOUNTS** provide the perfect solution to address the Wi-Fi squatter dilemma. An on-demand account is an account generated from a billing plan, which is a set of parameters that define characteristics of the account, such as usage quota, price, and access control policy applied. What makes these accounts even friendlier for public environments such as coffee shops is the ability for the account to be quickly printed via 4ipnet's Hotspot Ticketing System or any conventional printer connected to a PC.

Of the On-Demand account characteristics mentioned, some can be utilized to directly alleviate the Wi-Fi squatter dilemma. Firstly, coffee shop owners can provide accounts that are only active for a limited period of time. For example, after purchasing a cup of cappuccino, a user may be given an account that allows him to use Wi-Fi for 1 hour – it's not unreasonable to think that a cup of coffee can be consumed in a 1 hour time span. Secondly, as accounts can be billed, coffee shop owners can make up for some of the revenue lost due to Wi-Fi squatters. Although billed Wi-Fi is not very popular amongst users, shop owners do have a business to run and bills to pay. Lastly, accounts can be redeemed, allowing owners to extend the Wi-Fi usage of specific guests that continue to purchase items.



Some coffee shops have stopped providing Wi-Fi altogether to avoid the Wi-Fi squatter dilemma. However, with 4ipnet's On-Demand accounts, coffee shop owners can mix and match quota, price, and access control policies to strike a balance between keeping Wi-Fi in their stores (which attracts customers) and preventing Wi-Fi squatters (which turns away customers).

The applications of On-Demand accounts reach far beyond just coffee shops. For instance, many premium hotels that want to offer differentiated Wi-Fi services also rely on On-Demand accounts with different access control policies and prices. On-Demand accounts are key to any deployment where billable, quota-based, and manageable accounts are needed.

CONCLUSION

Throughout this feature guide, you have been introduced to the comprehensive user authentication features that a 4ipnet managed Wi-Fi solution provides. The key takeaway is that all these features bring about one major benefit: **flexibility**. From the multitude of authentication servers offered to the highly customizable captive portal pages and extremely adaptable On-Demand accounts, network administrators using 4ipnet's solution will not need to worry about not being able to find a solution with features to fit their Wi-Fi needs.