family zone | EDUCATION SOLUTIONS

TECHNICAL WHITE PAPER

Authentication and Identity Management

A guide to user authentication and identity management.

family zone | EDUCATION SOLUTIONS

Contents

Document Rev:A

Introduction

User authentication and identification are central to Family Zone Education Solutions. Identification facilitates flexible identity-specific filtering and reporting, and is crucial for network management in modern learning environments.

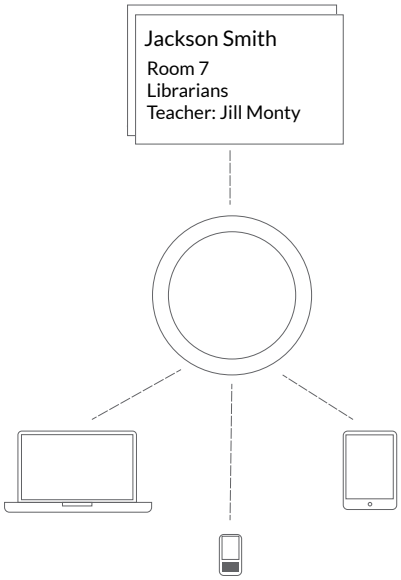
This guide introduces the concepts of authentication and identity management within the context of Family Zone School Manager.

Overview

When a user connects to the network they are normally unidentified. This means their browsing cannot be filtered specifically, and reporting can only be based on device heuristics. Authentication is the process of identifying the user.

Once identified, this user information can be used to filter traffic correctly and provide in-depth reporting on individual Internet usage.

User identification is becoming even more important in the world of Internet-enabled devices and BYOD. Correct user identification enables accurate and individualised filtering across all Internet-enabled devices, and helps facilitate BYOD in a learning environment.



A user identity bridges the gap between users, their devices and their identity.

The first step in authentication and identity management is deciding how you are going to identify various different users and different devices. Modern networks contain a wide range of different devices and operating systems, and it is paramount that you provide a painless authentication method for your users. We recommend a hybrid approach to authentication, making use of several different authentication methods for your different user groups and device types.

Considerations

When deploying authentication to your network with Family Zone School Manager, there are several key points to consider to ensure that the process is pain-free and accurate. These considerations will help you to create a hybrid authentication plan that best suits your network and environment:

- What kind of devices are your users connecting with - e.g. iPhones, Chromebooks, Windows laptops?
- How are they connecting to the network?
- Is your network segmented into VLANs?
- What age groups are using devices?
- Do you have a well defined group structure?
- What directory services are available on the network?

Once you have considered the points above, you can formulate a hybrid authentication plan. Family Zone School Manager supports many different authentication methods and a hybrid authentication plan consists of several of these.

An example hybrid authentication plan

Type of device	Authentication method	User experience
Domain joined - staff laptop	WMI Kerberos domain controller events	User logs into laptop with domain account and is authenticated with Family Zone School Manager automatically.
Domain joined - lab computer	WMI Kerberos domain controller events	User logs into laptop with domain account and is authenticated with Family Zone School Manager automatically.
BYOD iPhone	One-off captive portal log-in	User logs into the network via a captive portal, then saves their device permanently.
Shared Google Chromebook	Chrome extension	The Chrome extension identifies the user on a Chrome log-in and automatically authenticates with Family Zone School Manager.
Guest laptop	Captive portal guest log-in	Guest gets a pass from Reception then log in via the Guest Captive Portal

Once you have put together a plan for authentication, it's time to look at the implementation details. We recommend a gradual approach to avoid user frustration.

The User Session

The basis for authentication and identity management with Family Zone School Manager is the user session. When a user connects to the network and logs in, a user session is created in Family Zone School Manager and from that point onwards the user's network usage is mapped to their identity.

A user session is a mapping between a user identity and an individual network device. Normally this means mapping between Mac address, IP address and user.

Example Session Table

Username	Mac address	IP address	Log-in time	State
jill.sparrow	a1:f3:d1:a1:b2:c9	192.168.1.88	10:02AM	ACTIVE
jim.baggons	a7:f4:d2:a1:b2:dd	192.168.7.2	11:03AM	ACTIVE
michael.jackson	a2:c4:a2:a7:b1:a2	192.168.1.5	08:01 AM	INACTIVE

User sessions are created by authentication providers when a user signs in, and they have a finite lifetime. Family Zone School Manager supports many different providers like captive portal, 802.1x RADIUS, Windows domain controller log-ins and permanent associations. These providers are discussed in more detail in the following sections, but it's important to keep in mind that different providers can be used in tandem with each other. This functionality provides the basis for a hybrid approach to authentication.

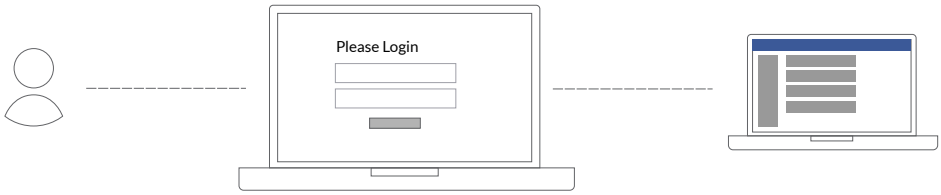
Log-in providers

As we've seen, Family Zone School Manager supports many different methods of authentication. This section explains the different methods of authentication and how they are integrated

- Captive portal log-in
- Domain controller WMI events
- 802.1x RADIUS authentication
- Chrome extension
- Permanent associations

Captive portal log-in

A captive portal is what a user sees when they first associate with a Wi-Fi SSID, or when they join the network and open a web browser to surf the Internet. When a captive portal is configured, all Internet traffic will be redirected to a particular URL and a user will be required to log in before they are allowed to connect to the Internet.



As the base authentication mechanism, Family Zone School Manager provides a secure captive portal hosted in our cloud environment. When deploying the captive portal, there are several considerations to keep in mind:

- Access to HTTPS sites will be disabled while the user is not authenticated.
- Sessions are only temporary and will time out after a period of inactivity.
- Servers, printers and Internet-enabled devices may need access without log-in.

Family Zone School Manager supports the use of different captive portals for different network subnets or VLANs. If your network is segmented into logical VLANs we recommend creating different captive portals for each segment. This segmentation allows you to customise time-outs, enable or disable user-driven permanent associations, exceptions and also log-in method.

Example of captive portal configurations:

Portal name	Network	Log-in method	Permanent	Time-outs
Student BYOD	192.168.1.1-192.168.1.254	LDAP credentials	YES	
Lab computers	192.168.10.1-192.168.20.254	LDAP credentials	NO	10 minutes Idle
Guest network	172.16.1.1-172.16.1.254	Guest token	NO	1 day lifetime
Servers	10.7.1.1-10.7.1.255	Not required		

Deploying specific captive portals gives you a degree of flexibility and eases pain for your users.

There are several different authentication back-ends that can be configured for log-in to the captive portal. Integrating with these providers is remarkably simple, and the group membership and information that these providers supplies becomes part of the user identity and is used in filtering rules.

SSO provider	Authentication mechanism
LDAP or active directory	Users must enter a username and password that is checked with the LDAP server.
Google OAuth	Users are redirected to the Google authentication servers and asked to approve the log-in.
Azure AD	Users are redirected to the Office365/AzureAD servers to log in.
Guest token	Users enter a guest token that has been created previously in the Family Zone School Manager cloud.
Local UserDb	Users are asked to log in with username and password.

Different methods can be configured and used in different portals, and in different VLANs and networks.

To help facilitate log-ins via the captive portal, there are several important URLs that can be bookmarked and shared to forcibly trigger the log-in and log-out processes.

Link	Description
http://log-in.linewize.net	Present the user with the option to log-in/logout of Google.
http://autolog-in.linewize.net	Open the relevant captive portal for that network and prompt the user to log-in.
http://autologout.linewize.net	Trigger a manual log-out. This can only be used if the user session has originated from the captive portal.

On shared machines these links can be deployed to open on start-up to assist in ensuring the correct user is authenticated on the device.

Exceptions and exclusions
Devices and applications/websites can be configured to be exempt from any required authentication. This is useful for resources you want to have easily accessible (such as the school's website), or for special-purpose devices that need to access the Internet (such as printers or cameras)

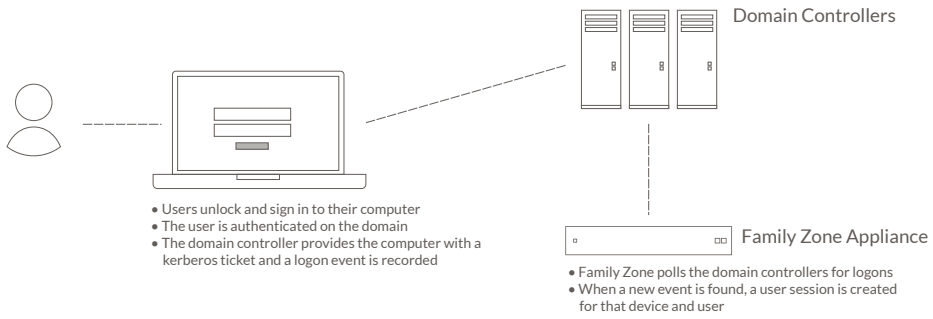
Permanent associations
Permanent associations are discussed in more detail later in this document, but it's worth noting here that a captive portal can be configured to allow users to "save their device" permanently. This removes the need for future log-in attempts and streamlines the user's experience.

Active directory WMI domain log-in

Family Zone School Manager offers automatic authentication for Domain joined machines. This solution provides seamless automatic log-in for Windows desktops, terminal server clients and Apple OSX computers that are joined to the domain.

Once configured, the Family Zone Appliance will poll your Windows domain controllers every few seconds for Kerberos log-in events via the WMI API. This is the simplest and most seamless method of authentication

with Family Zone School Manager because it requires no intervention from the user. Users will log in to their domain-joined PC and will be instantly authenticated with Family Zone School Manager.



Domain controller log-ins

Users will log-in to their domain joined PC and are instantly authenticated with Family Zone School Manager. Unlike other solutions, Family Zone School Manager does not require that an agent be installed on the Domain Controller. Family Zone School Manager does requires an account on your domain and will then poll the DC remotely. The only downside of AD WMI log-in is that it does not normally extend to BYOD devices. For this reason, in a BYOD environment, a hybrid approach with a RADIUS 802.1x or a captive portal log-in for BYOD users is almost always required.

When deploying AD WMI integration it's important to keep the following in mind:

- On large networks it is common practise to have several domain controllers. Ensure that each DC is configured with Family Zone School Manager.
- Terminal servers need to be configured for multiple IP addresses based on sessions.
- In most cases you will also need to configure the LDAP directory service in Family Zone School Manager as well.
- Active Directory WMI log-in is the least intrusive authentication method by far. Where possible we recommend it be used as the primary log-in method.

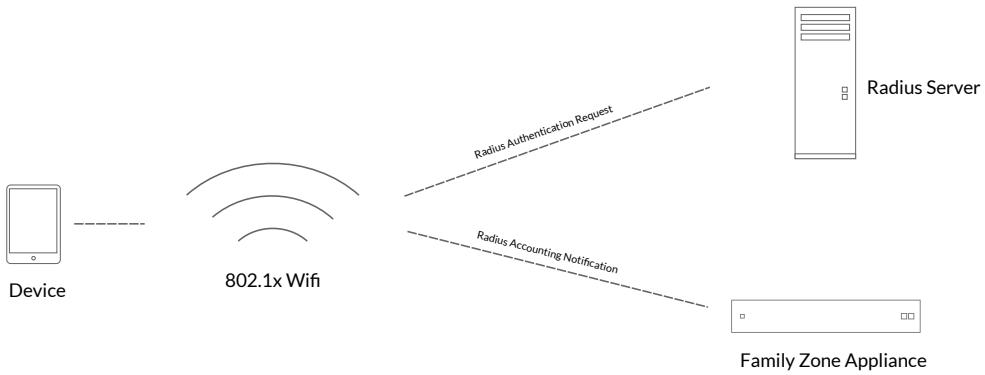
NPS RADIUS authentication

Similar in concept to the Active Directory WMI log-ins, Family Zone School Manager's 802.1x support hooks into the WMI API of your Microsoft NPS server and identifies users using 802.1x wireless authentication.

802.1x is an authentication protocol widely used on wireless networks today. It offers secure and very flexible username- and password-based log-in for networks. Prior to 802.1x, access to wireless networks was normally reliant on a shared key. This new approach extends the notion of single sign-on to wireless and enables profile-based layer 2 connectivity.

Because users signing onto a 802.1x wireless network are identified by their LDAP credentials, Family Zone School Manager is able to utilise this information and provide automatic touchless authentication.

Keep in mind: One caveat with NPS integration for 802.1x is that the security event provided by the NPS WMI events do not contain the IP address of the client device. If traffic is routed before our appliance we will not be able to correctly identify the client device and the log-in events will fail.



RADIUS Accounting with 802.1x wireless networks

802.1x RADIUS Accounting proxy

Family Zone School Manager can also be configured as a RADIUS Accounting endpoint for wireless networks using 802.1x authentication. Normally configured on your wireless controller, Family Zone School Manager intercepts the RADIUS Accounting events when users log in to the wireless network, and they are automatically signed in with Family Zone School Manager.

This is very similar to the NPS RADIUS authentication, with a couple of key differences. Whereas NPS RADIUS authentication is tied to the Microsoft network policy server, Microsoft's standard RADIUS implementation, the accounting proxy can be configured to work with any RADIUS server. The RADIUS Accounting endpoint also supports authentication based on the client IP address through the use of the framed-IP parameter passed in accounting events from most wireless controllers.

Chrome extension

Chromebook offer a unique challenge for agentless authentication. In a school environment, Chromebooks are commonly shared between users so a normal approach of one-off captive portal-based log-in or wireless authentication is not suitable. Chromebooks are built with an identity in mind. Users sign in to the Chromebook with their Google account and are automatically logged into Google's suite of applications.

The Family Zone School Manager Chrome extension builds on this sign-in process and automatically notifies the Family Zone appliance when a user has signed in. This removes the need for the captive portal on Chromebooks and ensures that the correct user is always authenticated with Family Zone School Manager. The Chrome extension can be deployed automatically to all users in your Google apps domain.

Directory services

Directory services are services like Active Directory that provide information on users such as first name, last name and groups and membership. The Family Zone Appliance will sync with the directory provider and retrieve all user and group information.

Family Zone School Manager supports several different directory services:

Provider	Method
Active Directory	LDAPv3
OpenLDAP	LDAPv3
Novell eDirectory	LDAPv3
Google apps	Google Rest API
Azure AD/Office 365	Azure AD Rest API
Local DB	

The Family Zone Appliance will sync with the directory provider and retrieve all user and group information. This information is then tied to a user's identity when they log in.

Family Zone School Manager supports several different directory services, but we recommend using only one at a time. Once configured, a directory service is queried on a daily basis for new groups and updated user information. This ensures that changes in the directory service are quickly reflected in Family Zone School Manager. A manual sync can also be triggered from the cloud dashboard.

Time-outs

User sessions are temporary and will eventually time out. Without a time-out, users could be associated with a device incorrectly and security would be compromised. The trade-off with time-outs is that users may frequently have to sign in if not using an automatic authentication mechanism. This sign-in process disrupts network access and is intrusive.

Family Zone School Manager offers two solutions to this problem. Where BYOD devices are in use, we offer permanent associations. For shared devices, session time-outs can be configured in varying ways.

Custom session time-outs

Administrators can also configure different time-outs for different user groups and VLANs. This facilitates appropriate time-outs for shared and individual devices. There are three different types of time-outs:

- **Session idle time-out.** The idle time-out is default and invoked after a certain period of inactivity.
- **Session elapsed time-out.** The elapsed time-out is hit when a session has existed for a certain period of time.
- **Absolute time-out.** The absolute time-out is invoked for all sessions regardless of activity or state at a certain time.

Permanent associations

- Permanent associations are a permanent mapping between a MAC address and user identity. For networks with BYOD devices it is ideal.
- When a permanent association is created either from the Family Zone School Manager interface, or after a user signs in, a mapping is created on the appliance. This mapping is then cross-checked against new devices that appear on the network. When a device matching the MAC address stored in the permanent association joins the network, a new session is created. This bypasses all other authentication mechanisms.
- For devices that are shared as part of pods or carts, like iPads for example, permanent associations can be bulk imported in CSV form into the cloud dashboard.

Routing

Network routing is beyond the scope of this document, but be aware it is a significant factor in how you deploy your authentication.

As mentioned in previous sections, user sessions are normally composed of a combination of MAC address and IP address. Layer-3 routing obfuscates the MAC address of the client device and prevents the Family Zone Appliance and other devices that are more than one hop away from seeing the correct client MAC address.

This means for authentication types that are solely dependent on MAC address, like 802.1x and permanent associations, a network topology change is sometimes needed to enable these features.

We recommend that you terminate/route BYOD VLANs on either the Family Zone Appliance itself or the Edge firewall on the WAN side of the Family Zone Appliance. This prevents the obfuscating and enables the use of permanent associations and 802.1x.

Summary

User authentication is a complex topic and there is no right or wrong approach. The general guideline is that you should try to avoid user interaction by taking advantage of the automatic authentication means and use the captive portal as a fail back when users cannot be identified via other means.

About Family Zone Education Solutions

Family Zone Education Solutions is committed to making student internet management easy, and keeping students safe online on any device, anywhere, any time.

Learn more

Email sales@familyzone.com
Visit us at familyzoneschools.com