User Identification, Explained
# Table of Contents

- Introduction .................................................................................................................. 3
- Methods of User Identification .................................................................................... 5
- About Captive Portal (Web-Based Authentication) ....................................................... 6
- About RADIUS .............................................................................................................. 7
- About the Domain Controller Agent .............................................................................. 8
- About User Agents .......................................................................................................... 10
- Best Practices by OS ...................................................................................................... 12
- Pros & Cons Recap ......................................................................................................... 14
- Tips & Notes .................................................................................................................... 15
- About Lightspeed Systems ............................................................................................. 16
Introduction

Schools use web filtering and reporting to keep users safe, adhere to regulations (such as CIPA), and manage network activity. To ensure appropriate access without over-blocking, web filters also likely provide different policies for groups of users (e.g., teachers and students) or grade levels (e.g., first grade and twelfth grade).

There are two main elements to web filtering: blocking/allowing of sites by policy and reporting on user activity. To be effective, both of these pieces require accurate identification of users.

In this guide you’ll learn:

- Why accurate user identification is essential
- How mobile devices and user id work
- The methods the Lightspeed Rocket Web Filter provides to cover any device and need
- The best choices for your devices and your network

Overview of User Identification

When a user attempts to connect to the Internet through your school network, the network doesn’t know who that user is in order to determine if they can visit the requested site. User identification is the process of identifying the user.

Once a user is identified, the proper filtering policies (by user, group, etc.) can be applied. And with accurate user identification, you can report on who does what and drill into a specific user’s activity.

User identification is even more important in a world of mobile devices and regular use of the Internet for learning. You need to implement user identification that is as easy as possible for the user and that provides accurate and complete information for IT — regardless of user’s device or location.
One of the first things you need to think about as you prepare to set up web filtering is to choose how you’re going to do user identification. There are several ways to do this, each with its own benefits.

**Fig. 1: The goal of user identification is to know WHO the user is so appropriate policies can be applied and reporting can be associated with a user.**

**Considerations**

In addition to needing accuracy, schools need user identification to be as simple and painless as possible for users to log in. A single login process (and integration with existing directory services) is key in most environments. However, with the diversity of operating systems and user abilities, not to mention changing trends in technology, it’s almost impossible to do this transparently in every scenario. So, what is the best way to figure out who is logged into a particular device? A combination of techniques yields the best results.

**When choosing the method(s) of user identification, you need to consider:**

- Types of mobile devices in use
- Whether the devices are school- or student-owned
- Methods in place for pushing agents to school devices
- Directory services and desired integration

Lightspeed Systems Web Filter uses various authentication methods. Once a user is identified, the Web Filter uses rule sets and assignments to determine what types of content to allow or block. We have solutions to identify the user accurately and easily no matter your devices or network.
Methods of User Identification

User identification supplies Web Filter with each user’s credentials in order to provide the end user with the proper policy assignment and reporting.

Here are the four primary methods of user identification:

1. **Captive Portal/Web Authentication**: This agentless authentication works well in all environments. Similar to what you would see at a hotel or wi-fi hotspot, this option forces enabled users to identify themselves prior to accessing the Internet. This will work in all environments with any client device.

2. **Domain Controller User Agent**: The agent can be installed on Microsoft Active Directory Domain Controllers to supply Web Filter with user information when a user logs in or out of the network.

3. **Lightspeed Rocket RADIUS Integration**: The Rocket appliance can be set up as an accounting server with a school’s wireless RADIUS system. When users authenticate to the wireless network, this information can be transparently shared with the Rocket. This is ideal for BYOD environments in which a variety of personally owned devices connect to the network.

4. **User Agent**: Installed on Windows devices, PCs, Chromebooks and Macs, this agent provides transparent authentication for devices. The User Agent is often the most accurate, especially in environments in which a single device might have multiple IPs. It’s also the most seamless experience for the user, avoiding the need for web authentication.

These methods are not exclusive, and, typically, a combination of methods works best. These methods can be combined to create the solution that best fits your school’s needs.
About Captive Portal (Web-Based Authentication)

With Captive Portal web-based authentication enabled, the Rocket prompts a user for their username and password when they access the Internet. This information is used to apply appropriate policies and reporting. Use the Captive Portal table to restrict Internet access to the portal until authentication requirements are satisfied.

There are a few options that you can use:

Exclusions
You can exclude users reported by an agent, RADIUS, proxy or Lightspeed Systems Mobile Filter Agent. This is a very useful setting, as it minimizes impact on your users if the Rocket knows them already, while ensuring proper identification if it doesn’t know them.

Authentication Lifetimes
You can configure authentication lifetimes for users, user groups, and user organizational units. Authentication lifetime determines how long a web-based authentication lasts before prompting the user to log in again.

Best practices for authentication lifetimes vary depending on your school’s needs. Typically, schools that have users sharing mobile devices set authentication lifetimes to last a single class period. That way, when a new class begins, the previous student’s authentication expires and the new student is asked to log in.

Exemptions
IP addresses or Domains to be exempt from any required authentication. This is useful for accessing resources that you want accessible without any hinderance (such as the school’s website) or for special purpose devices that need to access the internet but cannot provide the use interaction to login to the captive portal (such as printers or cameras).
Fig. 2: In Captive Portal method, a user authenticates by logging in before accessing the Internet.

Captive Portal Recap

*Works with any device with a Web browser*

*Benefits: Universal support*

*Issues: Requires end user interaction; IP changes require additional captive portal login*

About RADIUS

Rocket supports RADIUS accounting for user identification, which allows Rocket to act as an accounting server for an existing RADIUS implementation. You can use the Rocket’s accounting server to receive authentication information from wireless access points.
If wireless access points, or controllers, support RADIUS authentication, and have an option for sending a RADIUS accounting packet to our appliance, this option can be used. It creates a seamless experience for the end user on a mobile device. RADIUS is typically used on wireless networks.

**Fig. 3: In RADIUS authentication, the Rocket Web Filter gets the user identification from the RADIUS server.**

---

**RADIUS Recap**

*Available for any device that connects to an authenticated (802.1X/NAC) network*

*Benefits: No agent to install; transparent to the end user*

*Issues: Requires network support for NAC or 802.1X; only wireless devices*

---

**About the Domain Controller Agent**

*This feature does not require a client on every workstation; however, it requires the agent to be on every single domain controller on the network. If installing the User Agent on every device isn’t a viable solution, the Domain Controller Agent may be useful.*
Depending on your network, the Domain Controller Agent may not be as effective if you have any of the following situations:

1. **Terminal Services, nComputing or Citrix servers** – With thin clients, there is no way to differentiate at the domain controller level the identity of the user performing the web browsing functionality on the server. Because of this, the last person that logs into the server is registered as the person for all users on that system. So, if you use these types of servers, the domain controller agent by itself is not an effective solution for your network.

2. **Dual Internet connection devices** – When laptops switch between wired and wireless access, the user is not required to log in again, so the Domain Controller agent would not know who you are at this point and it will not be effective as a solution.

3. **Mobility devices** – When a device goes off-campus and back on, the network is re-logging the device into its previous session, so the domain controller is not notified that the user is on the device with that particular IP address.

4. **BYOD** – If you are supporting the option for users to bring their own devices on the network, then these devices are not members of the directory network; therefore, the user never logs into the domain itself.

Fig. 4: With the Domain Controller agent, the agent is installed on each DC rather then each client device.
Domain Controller User Agent Recap

Available for active directory-based networks

Benefits: Agents need to be deployed only to domain controllers, not every device

Issues: Admins only know about information that reaches the domain controller; can present challenges in mobile environments due to cached credentials and IP changes; cannot provide resolution for devices that do not log into Active Directory (iPads, Chromebooks)

About User Agents

A User Agent is a method of user identification in which an agent is installed on each device to transparently communicate user information to the Rocket Web Filter so it can deliver appropriate policies. For operating systems where a User Agent is available, this provides the best combination of accuracy and transparency.

When a user logs in, the agent notifies the Rocket Web Filter immediately that the user is on that particular device, so appropriate policies are applied. If the user decides to go from wired to wireless connection, the agent updates the appliance that there has been a change and the user will have a transparent experience.

A User Agent may be the best method for you if:

- you want transparent authentication (without the need for users to identify themselves through web authentication)
- you need complete IP information for devices with multiple IP addresses
- you want the most complete and reliable web traffic reporting
- you have primarily school-owned (not student-owned) mobile devices
User Agents are available for Macs, PCs, Chromebooks, and Thin Clients.

Because this is a client-side agent, it also provides the Web Filter with IP information for all the interfaces on the device. There are many conditions in which a device may have multiple IP addresses that it switches between; machines with both wired and wireless conditions, and dual-stack environments in which both IPv4 and IPv6 are in use, are a couple examples.

A thin client agent is available if you are using a terminal server, nComputing device or Citrix server in which multiple users are logging into a single system. In order to get proper username information, Lightspeed Systems has created a special thin client agent that will install on these types of servers. This client passes the session information to the Lightspeed Systems Web Filter, allowing the appliance to give the correct policy to the individual user session.

![Diagram](image)

**Fig. 5:** With the User Agent on the device, user identification information is passed to the Rocket for appropriate web filtering.

---

**User Agents Recap**

*Available for Mac, Windows, ChromeOS, Thin Client*

*Benefits: Completely transparent to the end user; highly reliable with network transitions*

*Issues: Agent needs to be deployed; challenging for BYOD environments*
Best Practices by OS

User Identification for iOS

All our agents identify themselves to Web Filter by using a combination of a unique device identifier and user information obtained from the device. This identifier allows the Web Filter module to perform many types of authentication, including cached credentials, captive portal/web authentication, and forced registration.

User identification for iOS devices is different because the nature of the device does not permit a user agent to operate. There are a couple of reasons for this. First, these devices are user-less devices from a network perspective meaning there is no forced user login in order to use the device. Second, the sandbox nature of the iOS operating systems does not allow for a user agent to run that can monitor the network usage, changes and reporting necessary to provide identity information to the Rocket appliance.

For transparent authentication on an iOS device, we recommend RADIUS integration. By forcing the device to provide user credentials as part of joining the network the two restrictions of the iOS operating system are removed. Through 802.1x or NAC the device is now logging into the network whenever it joins the wifi. And because these same technologies also alert when a device joins, drops, or has an IP change on the network, this integration provides the transparent end-user experience that a User Agent can provide on other operating systems.

User Identification for Windows

The PC User Agent provides user identification for Windows devices when they are used on a network filtered by Web Filter v2.x. The LMA provides user identification for Windows devices when they used on a network that is filtered by Web Filter 3.x. The LMA (Lightspeed Management Agent) combines multiple functions, including user identification, into a single agent for easy deployment and updates.

User Identification for Chromebooks

The User Agent extension for Chrome provides seamless single sign-on capabilities for ChromeOS devices when they are used on a network filtered by Web Filter. It transparently authenticates users within your tier address space to your tier’s
Google authentication source. (Users must be valid members of your Google Authentication domain.)

**User Identification for BYOD**

There are many cases in which you may find it beneficial to identify users, such as with BYOD or an unsecure network that is provided for the public at your school. Perhaps you need to identify mobile devices that leave your network or you want to log in through the Web to access your profile. Whatever the case, authentication settings help you to define who, what, and when authentication takes place on the Internet.

You can require users to web authenticate before they are allowed to browse the Web. The authentication process allows Internet access for a specified time period. When the time period elapses, users must log in again before continuing.

**Identification by Device**

<table>
<thead>
<tr>
<th>Device</th>
<th>Recommended Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Laptops/Desktops</td>
<td>Mac User Agent</td>
</tr>
<tr>
<td>PC Laptops/Desktops</td>
<td>Captive Portal, RADIUS</td>
</tr>
<tr>
<td>Chromebooks</td>
<td>ChromeOS Extension Agent</td>
</tr>
<tr>
<td>Thin Clients</td>
<td>Thin Client User Agent</td>
</tr>
<tr>
<td>Android Devices</td>
<td>Captive Portal, RADIUS</td>
</tr>
<tr>
<td>iOS Devices</td>
<td>RADIUS, Captive Portal</td>
</tr>
<tr>
<td>Windows Devices</td>
<td>PCUA (WF v2.x), LMA (WF v3.x), Captive Portal, RADIUS</td>
</tr>
</tbody>
</table>
Pros & Cons Recap

**Web Authentication/Captive Portal**

*Works with any device with a web browser*

*Benefits: Universal support*

*Issues: Requires end user interaction; IP changes require additional captive portal login*

**User Agents/LMA (Lightspeed Management Agent)**

*Available for Windows, Mac, ChromeOS, Thin Clients*

*Benefits: Completely transparent to the end user; highly reliable with network transitions*

*Issues: Agent needs to be deployed, which is challenging for BYOD environments*

**Domain Controller Agent**

*Available for Active Directory–based networks*

*Benefits: Agents need to be deployed only to domain controllers*

*Issues: Admins only know about information that reaches the domain controller; can have challenges in mobile environments due to cached credentials and IP changes; cannot provide resolution for devices that do not log into Active Directory (iPads, Chromebooks)*

**RADIUS**

*Available for any device that connects to an authenticated (802.1X/NAC) network*

*Benefits: No agent to install, transparent to the end user*

*Issues: Requires network support for NAC or 802.1X*
Tips & Notes

There are many ways to get a username from a device on the network, and there is no single correct solution. The Rocket Web Filter supports multiple methods of user identification so you can maximize accuracy and transparency for whatever devices and systems you have on your network.

Here are some tips and notes:

• The user agent is usually the best choice for Mac, PC and ChromeOS devices, as it provides the most accurate information with the least user interaction.

• It is usually a good idea to turn on Captive Portal authentication and exclude users reported by a User Agent, RADIUS, proxy or mobile filter. (This way, if an agent is present, and the filter knows who user is, he doesn’t need to authenticate; if the filter doesn’t know who the user is, he has to authenticate.)

• If the network has any terminal servers, nComputing or Citrix devices on the network, push out the thin client user agent to those devices (but note that then the Domain Controller agent isn’t an option).

• If your wireless access points or controllers support RADIUS, use of the RADIUS authentication integration with our appliance.

• All our authentication methods integrate with the school’s Active Directory, Open Directory, eDirectory, LDAP or local users database. Multi-directory environments are also fully supported.

• The user identification methods listed work only with a Rocket Web Filter, not a hosted mobile filter.

• There may be times when an authenticated user isn’t provided a log-out link. In these situations, the user can log out at any time by entering the following URL: http://lsaccess.me/logout
About Lightspeed Systems

Lightspeed Systems builds smart solutions for school networks

Since 1999, Lightspeed Systems has partnered with schools around the world to help them manage, secure, filter, and report on their school networks. All of our products are made just for schools with the features and services schools need. That’s why our award-winning web filter, MDM, and classroom management solutions are happily used in more than 6,500 districts, making technology integration easy and safe for IT.

The Lightspeed Systems Rocket Web Filter gives you easy and accurate user identification for any device – so you can get the most effective filtering and reporting.

Contact us:

www.lightspeedsystems.com
sales@lightspeedsystems.com
support@lightspeedsystems.com
1 877.447.6244