# Authenticating Your Internet Users

When users attempt to connect to the Internet, their identity usually needs to be verified to support the company's Acceptable Use Policy (AUP) for monitoring and policy enforcement. IT administrators can accomplish this by employing authentication methods. There are many to choose from, and more than one type may be configured depending on the needs of the organization. An authentication method will authenticate the connection request before allowing or denying access to the Web site. Here, we will discuss authentication using a captive portal and why it may be a suitable choice for your organization.

Authenticating With a Captive Portal

Captive portals can be set up in different ways. In this authentication method, the user's logon credentials are used to authenticate the user. When the user tries to visit a Web site, a captive portal redirects the user to a logon page allowing him to provide his credentials. The user interaction with the logon page is a benefit of this authentication method. It is a stable option in today's modern mixed environment of devices.

After the user enters his logon information and accepts the AUP (if required), his credentials are stored, and he will not be prompted to log on again for as long as his identity is confirmed. The user logs on once per session. The IT administrator configures the length of time before authentication is necessary again. Whereas NTLM supports Windows operating systems primarily, authentication with a captive portal supports a wide range of devices, such as smartphones, tablets, and laptops as well as your employees' workstations.

The following diagram illustrates a possible setup of devices in your managed corporate network with CyBlock Software. This authentication method will also work with CyBlock Appliance and CyBlock Cloud.
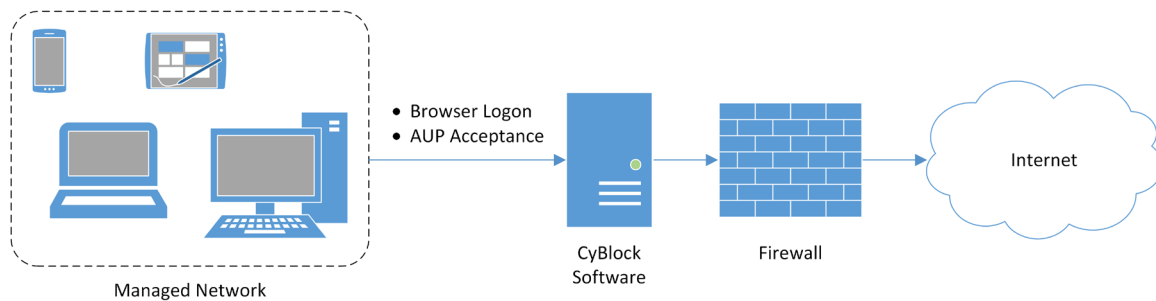
Authentication Using a Captive Portal With CyBlock Software

Customizing the Logon Page

A captive portal allows the logon page that is presented to the user to be customized to fit your company's needs. You can specify the acceptance text for the AUP check box, include your company logo, and add the AUP message that you want to display on the logon page.

<logo> **ACME CORPORATION**

E-Mail: [_____]

Password: [_____]

This Sample Internet Usage Policy applies to all employees of who have access to computers and the Internet to be used in the performance of their work. Use of the Internet by employees of is permitted and encouraged where such use supports the goals and objectives of the business…

☐ I have read and agree to the AUP.

[Logon]

Forgot Password Create Account

Logon Page

Conclusion

A captive portal offers an easy setup and may be a viable solution to support your organization. It works well for users who want to access your network with devices, such as laptops, tablets, and smartphones. That is, it can be used in a mixed environment of Windows and non-Windows based devices. It requires users to provide credentials through a customizable logon page and accept your AUP, if configured, before they can browse the Internet. Users only need to log on once per session, and the length of the session is controlled by the IT administrator. Authentication using a captive portal is a reliable type of authentication that confirms the identity of users accessing the Internet through your network.

About Wavecrest Computing

Since 1996, Wavecrest Computing has provided business and government clients with reliable, accurate employee Web-access security, monitoring, and analytics solutions. IT specialists, HR professionals, and business managers trust Wavecrest's Cyfin and CyBlock products to manage employee Internet usage with today's distributed workforce in mind–monitoring VPN use, following roaming and remote users, managing and monitoring Web usage for hybrid work environments, comprehensive reporting on Microsoft 365 use, and more. Focused on our customer's needs–reducing liability risks, improving productivity, managing cloud services, saving bandwidth, and controlling costs.

Wavecrest has clients worldwide, including Canadian National Railway, Johns Hopkins, Goodyear, USPS Office of Inspector General, Chevron, Health Choice Network, and a growing list of enterprises and government agencies. For more information on our company, products, and partners, visit www. wavecrest.net.

Wavecrest Computing
904 East New Haven Avenue
Melbourne, FL 32901
toll-free: 877-442-9346
voice: 321-953-5351

www.wavecrest.net