Content Filters & ClassView

Introduction

There has been a recent surge in the use of various content filter products in school environments. Content Filters may cause several different issues that have been identified when using ClassView. The following provides some insight for the district/school IT professional to help with tuning content filters so that impact on ClassView is mitigated.

What is content filtering? Content filtering, in the most general sense, involves using a program to prevent access to certain items, which may be harmful if opened or accessed. The most common items to filter are executables, emails and websites. Content filters can be implemented either as software or via a hardware-based solution within a school district's network.

Issues Using Content Filters

Issues that a content filter can cause with the ClassView product include:

- Needing to press the login button multiple times before the login process begins.
- Students who once received surveys, assignments, and broadcasts are no longer able to receive them. This may only affect a few students.
- Receiving the error "Please check your internet connection and try again" while using ClassView.
- Students are unable to submit assignments but receive no error messages about internet access.

Content filters have the ability to require users to login to the content filter before obtaining the internet access. Due to the robust configuration options that content filters offer, there are many ways to limit access to devices or users. Here are some examples of how content filters may restrict access to the internet:

- Per device, by using the device's IP address or MAC address.
    - Each device’s IP or MAC address is recorded into the content filter’s database. The administrator of the content will set what times or how long the device will have access to the internet.
        - They can set the timeout by minutes, hours, or days.
        - This is a fully automated system that requires no user input.
        - This requires a lot of configuration done by the admin and is not frequently used.

- Per device by using the school's network credentials.
    - When the user logins into the device it will login using the school's network credentials it will log into the content filter at the same time.
    - The session is still held on the device until the timeout period has expired. This means the next user that logs in does not refresh the session and has to wait for the first user's session to timeout.
        - This can cause issues because the 2nd user may get kicked out halfway through class due to a session timeout.
            - Example: The session timeout is set to 1.5hours. Student 1 logs into the device at 8am and class ends at 9am. Student 2 logs into the device at 9am however the session from Student 1 hasn't timed out yet. Student 2 has internet access for 30 minutes until Student 2 drops internet access because Student 1's session has just timed out on the device. Student 2 will now have to exit ClassView and log back into the content filter before continuing. This can cause data loss if the student is in the middle of an assignment.

- Per user account logging in with the content filters or schools credentials.
    - Users will sign into the content filter which will start an active session. Once the session times out the users are required to log back into the content filter.
    - If the user logs out of the device the session is closed until the next user logs in.
        - Lots of times the mobile device will have a logout icon on the desktop (iPad/Android) or as a bookmark/plugin (Browsers/Chromebooks).
        - If the student doesn't press logout the next student will stay on the active session until it times out.
        - This requires the student to manage their sessions with the content filter.

- Global session for all devices.
    - Content filter admins can set up the entire network and get access from specific times in the day.
        - This can be done for a block of time. Example 7am to 5pm.
        - Can be set up as a per user session timer. First user logs in and gets internet access until the user logs out or shuts down the device.
            - There is no timeout set. Users must login/logout each time they use the device.
        - Can be set up as a timer. If it is set to 1 hour when the first user logs in the device will stay connected for 1 hour. After the hour is up the device

will need to log back into the content filter to get internet access again regardless of what applications are using the internet.

- This can cause data loss if the student is in the middle of an assignment.

Solutions

The following are some known options for solving issues that impact ClassView and are caused by a content filter. These are general descriptions of options that may be implemented differently based on the content filtering product. Contact Support at **1-800-234-5832** if additional help is required.

- Per device by using the device's MAC address.
  - Adjust the device timeout session to match the school's hours of operation.
- Per device by using the school's network credentials.
  - Option 1: Adjust the device timeout session to match the school's hours of operation.
  - Option 2: Set the session timeout to begin when the student logs in and ends when they logout.
    - If students do not logout then the session never closes.
- Per user account logging in with the content filters or schools credentials
  - Option 1: Set the session timeout to begin when the student logs in and ends when they logout.
    - Note: If students do not logout then the session never closes.
  - Option 2: Adjust the device timeout session to match the school's hours of operation.
- Global session for all devices.
  - Adjust the global timeout session to match the school's hours of operation.
  - Adjust the user session timeout to match the school's hours of operation.

Universal Resource Links, (URL's)

When entering Universal Resource Links, (URL's) or domain names into the filter rules, please be sure to enter only the Top Level Domain, (TLD) and "allow all" subdomains under each TLD or root domain name. This technique will simplify the task of adding URLs to the filter table, reduce human error and ensure that all subdomains are allowed to pass.

Example:

- TLD: **pearson**api.com
- Sub Domain: **pearson**api.com/content/screen1/image1.png

In the example above, apply the filter rule only to **pearson.com** which will allow all subdomains to pass as well.

Caching

Some versions of content filters include the ability to cache frequently visited websites. Although enabling this feature may reduce the usage of bandwidth and improve local performance for some applications, it may interfere with ClassView. ClassView has already been optimized to use minimum bandwidth while providing the most current content available. ClassView content is only downloaded on demand and includes intelligent caching on both the server and client apps.