Authentic8 Web Access

Web Access provides administrators with a collection of policies to control which sites users can access during their Silo session. These tools, located in the Admin Console, can be used to enforce HR policies and limit users' access to restricted and potentially dangerous web sites. Web Access is made up of four policies:

- Browser Configuration
  - Allows broad control over the open or closed nature of the Silo browser
- Category Filtering
  - Allow/Block categories to control users' web site access
- Domain Filtering
  - Whitelist/blacklist specific domains
- Block Content Notification
  - Customize the notification that users see when a block occurs

This document details the four policies that make up Web Access.

Browser Configuration

The Browser Configuration setting is used to configure Silo to either restrict access to provisioned web apps or allow broad web access. Open Browsing gives users the ability to navigate to any website as they would in a traditional web browser. Locked Down restricts users to only provisioned web apps. If a user tries to browse to a URL/domain that is not part of a provisioned web apps domain, they will be denied.

All apps, with the exception of admin provisioned apps and open browsing sessions are governed by filtering rules.

Category Filtering

With Category Filtering, administrators can choose to allow or block defined filter categories for users based on what is most appropriate for the organization. To take advantage of this feature, first enable Category Filtering. Once that selection has been made, admins will need to choose to blacklist or whitelist categories.

By choosing blacklist Categories in conjunction with an Open Browsing Configuration, access to selected filter categories will be blocked. This selection is intended for admins that want to allow their users the ability to access all websites except those sites that belong to selected filter categories. For example, a company may use this selection to give their employees' access to the Internet but block sites that would violate HR policies such as Questionable and Offensive, and Pornograhphc sites

By choosing whitelist Categories in conjunction with a Locked Down Browser Configuration, access to selected filter categories will be permitted. This selection will allow admins to limit users' Internet access to only provisioned web apps and sites that belong to the categories that have been selected. For example, a medical organization that is bound by HIPAA regulations may choose to only give their employees access to web sites that belong to the Health filter category.

Admins of sub-organizations can be granted the ability to override category filtering rules that were set at the parent organization level. Please note, that when Silo is configured this way, new rules that are implemented at the parent organization, will not propagate downstream to the relevant sub-organizations.

Filter Categories

Legal Liability

- Questionable and Offensive
    - Illegal and potentially offensive material including hate speech, racism, violence, pornography, illegal drugs and other questionable content.
- Adult and Pornographic
    - Sexually explicit material for the purpose of arousing a sexual or prurient interest. Includes the sale of adult products & services, online groups and forums that are sexually explicit in nature.

Security Threats

- Malicious Sites
    - Sites known to carry malicious content such as viruses, spyware, adware and sites associated with fraud, phishing, botnets and spam delivery.

Productivity Drains

- Social Networking
    - Social networking sites including interactive user communities and micro-blogging services.

    - e.g. facebook.com, linkedin.com, etc
- Shopping
    - Department stores, retail stores, company catalogs and other sites that allow online shopping for goods and services including auction sites.
    - e.g. amazon.com, ebay.com, etc
- Rich Media
    - Sites streaming audio or video content or delivering downloads or offering VOIP, messaging and internet telephony services.
    - e.g. youtube.com, etc
- Job Search
    - Assistance in finding employment, and tools for locating prospective employers, or employers looking for employees.
    - e.g. monster.com, indeed.com, etc

IT Impacting

- Network Hogs & Data Leaks
    - IT impacting services including streaming media, P2P, torrents, online storage services, internet communications, shareware/freeware and pay to surf sites.

Industry Verticals

- Finance
    - Financial sites including banks, mortgages, loans, insurance, facilitation of securities trading and investment management.
- Health
    - Healthcare and medical information including hospitals/doctors offices, specialities such as dentistry, psychiatry, optometry and medical insurance sites

Domain Filtering

Enabling Domain Filter Lists restricts or grants user browsing by domain name.

Administrators can specify domains to block and allow. The addition of whitelist or blacklist domains will always supercede other URL filtering rules. For example, if you were to both block social networking sites using Category Filtering and whitelist linkedin.com by way of the Domain Filtering setting, linkedin.com would be accessible to your end users.

Admins of sub-organizations can be granted the ability to override Domain Filtering rules that were set at the parent organization level. Please note, that when Silo is configured this way, new rules that are implemented at the parent organization, will not propagate downstream to the relevant sub-organizations.

Block Page Content

Administrators can define the message that users will see when they are denied access to a restricted site or domain. A custom block message of up to 500 characters can be entered. If a custom message is not provided, users will be presented with the following default message:

"Your organization does not allow access to this website based on policy. Please contact your admin if you think you have been blocked in error."

Admins of sub-organizations can be granted the ability to override this setting and provide their own custom message to the relevant sub-organizations.

Additional Notes

- All changes to Web Access policies do not impact users until their next session
- Toolbox users are bound by Web Access policies
- Filtering details are available through Log Extraction

Appendix

Enforcement logic for Web Access filtering policies