

Best Practices

The true benefit of Burstek's applications is in the customization designed to fit the needs of the individual user. Default best practice for everyone would negate that benefit.

Since we integrate with Microsoft, general guidelines on Active Directory and server configurations are sufficient for the Burstek applications.

For example, assume you are using a separate firewall with ISA acting as a proxy. With this you could setup WebFilter for ISA to provide content filtering functionality or remove ISA completely and use WebFilter Stand-alone to handle Proxy and filtering together. This choice is dependent on your organizational requirements.

In reference to the configuration of WebFilter's 'Custom Access Policies', this is based on the level of filtering and management that you are willing to undertake. You could for example create a custom access policy for each category with a corresponding active directory user group or create a single policy and apply it to the domain users group.

Depending on the departments in your organization, you may wish to have a permissions-based policy that only allows access to a specific group of URLs you have already specified while having additional policies for executives, middle managers, and employees.

When you add in quotas and schedules, the flexibility of the application, and its ease of use, it's easy to see what separates us from other filters in the marketplace.

Following are some links for your review:

ISA Server on Microsoft Technet

<http://technet.microsoft.com/en-us/library/bb794753.aspx>

Active Directory Best Practices on Microsoft Technet

[http://technet.microsoft.com/en-us/library/cc778219\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc778219(WS.10).aspx)

Burstek Document Resources

<http://www.burstek.com/products/burstek-resource-center/>