



# Mercurion Systems, Inc.

**Information Technology Consulting and Support Services**

Phone: 919.266.5957 Fax: 919.217.5769  
<http://www.mercurionsystems.com>

## **SQUID AND SQUIDGUARD INTEGRATION IN A WINDOWS NETWORK**

*Products: Squid 2.5; SquidGuard 1.2*

### **Overview**

Many organizations choose to deploy proxy servers and web content filters to help control unwanted Internet bandwidth. The open source Squid is one such proxy server that provides caching and access control. With the addition of SquidGuard, organizations can also provide content filtering. Unfortunately, like most other solutions, Squid requires client-side settings to be made on each and every desktop computer. This may deter organizations from deploying Squid and SquidGuard and gaining the benefits these products offer.

This technical note describes the integration of the open source Squid proxy server and SquidGuard content filter into Windows-based networks.

### **More Information**

There are a few different ways in which Squid (and SquidGuard, since it operates as an extension to Squid) can be integrated into Windows-based networks. Each of these methods focuses on the automation of setting the client-side proxy settings for the users' web browser, as this is what will force users' traffic through the Squid proxy server (and thus through the SquidGuard content filter as well).

The easiest and most flexible method for integrating Squid into Windows-based networks is to use Group Policy. However, this option has some limitations. It is only available for those organizations running Active Directory on Windows 2000 Server or Windows Server 2003, and the policy changes can only be enforced for Internet Explorer (not other browsers). There is no provision for enforcing proxy settings for other browsers like Firefox or Mozilla.

As shown on the following page in Figure 1, a standard Group Policy Object in Active Directory includes settings for Internet Explorer, such as the proxy settings. By defining these proxy settings (as illustrated on the following page in Figure 2), administrators can centrally configure and enforce proxy settings for Internet Explorer on all domain members.

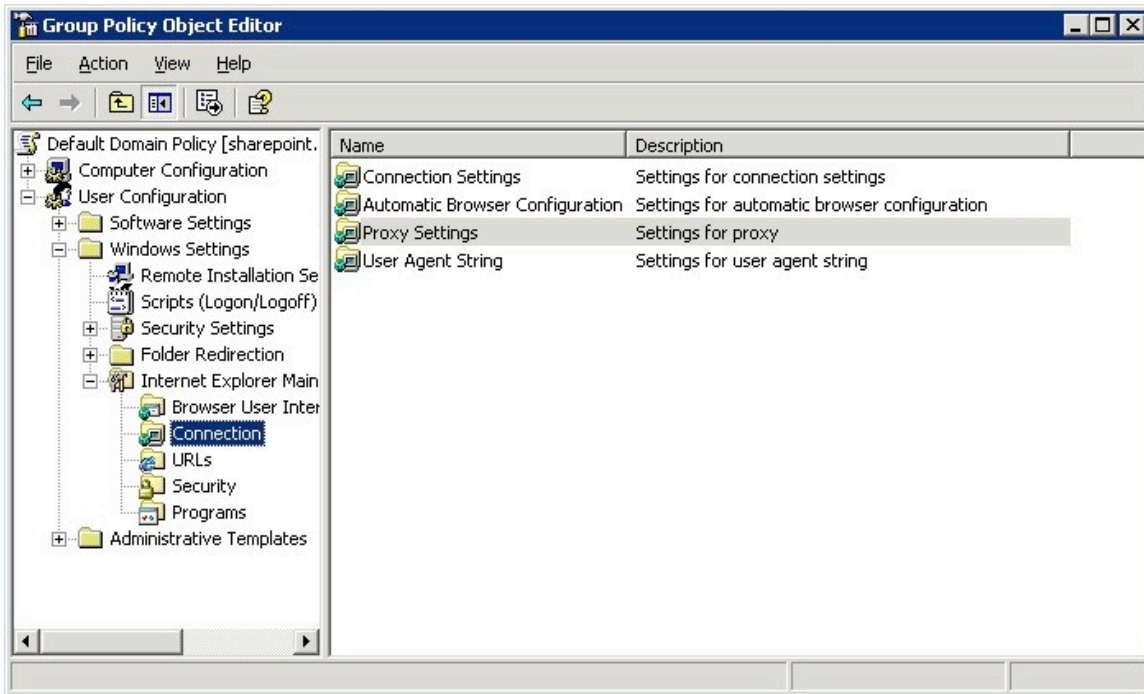


Figure 1. Location of IE's proxy settings in Group Policy Object Editor

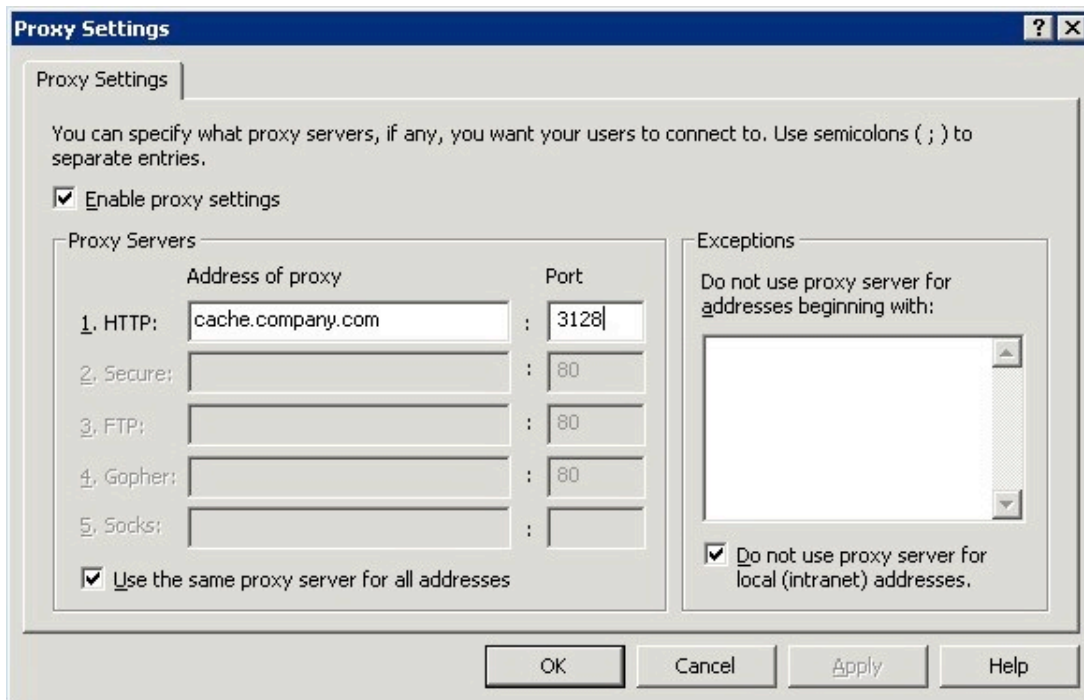


Figure 2. Setting IE's proxy settings via Group Policy

Note that port 3128 is the default port for Squid, so if the port has been changed that port will need to be accurately reflected in the Group Policy Object's settings. It is recommended that administrators configure a DNS CNAME (canonical name, or alias) record such as the generic

*cache.company.com* shown in Figure 2 on the previous page; this allows greater flexibility if the server running Squid ever needs to be replaced (the CNAME can then just be updated to point to the address of the new server, and no changes need to be made to Group Policy).

This is, by far, the easiest and most seamless way to enforce the use of a Squid-based proxy server for client computers running Internet Explorer and participating in an Active Directory domain. For other browsers, or for networks that have not or will not embrace Active Directory, it is not an available option.

To ensure that users do not remove the proxy settings and browse the Internet unchecked, firewall rules can be put into place that only allow web traffic from the proxy server itself. (Keep in mind, however, that Group Policy automatically refreshes itself every 90 minutes anyway, at which time the settings would be enforced again).

## **Other Notes**

Other versions of Squid (and SquidGuard) may work with the settings described in this document, but this document only tested Squid 2.5 with SquidGuard 1.2 on Red Hat Linux 9.0.

## **Related Articles/Resources**

None

## **Legal Information**

This document was created by Mercurion Systems, Inc., and may be freely distributed as long as it is distributed without modification and in its entirety. Mercurion Systems assumes no liability as a result of using the information contained in this document.