



# Mercurion Systems, Inc.

**Information Technology Consulting and Support Services**

Phone: 919.266.5957

Fax: 919.217.5769

## Software Update Services (SUS) and Automatic Updates—An Overview

### The Need

New security vulnerabilities are discovered almost daily, and with each one comes a new security hotfix. Among all the hotfixes, patches, security rollups, and service packs, how do you keep track of them all? And how do you try to make sure that all your systems stay up to date?

With Windows XP, Microsoft introduced Automatic Updates, a system whereby client computers automatically update themselves with the latest patches from Microsoft. Windows 2000 adds this ability in Service Pack 3. With Automatic Updates, these fixes are deployed to client computers automatically.

The idea behind Automatic Updates is nice, but it only adds to the problem. Now you have all your client computers downloading the same set of patches over the Internet, increasing the traffic on your Internet connection and slowing everything else down. You have no way of testing the latest updates to make sure they don't cause problems with other applications in your environment. Users get confused when prompted about an update—do they download it or not?

No longer are you wondering how to keep your systems up to date; now you're wondering how to keep things under control, and how to keep your Internet connection from getting clogged up. Is there a better way?

### The Solution—Software Update Services

Software Update Services (SUS) is a solution. Not the only solution, to be sure, but a good one at the price point: free.

With SUS, a single server on your network downloads the latest security patches from Microsoft's public, live Windows Update servers. You, as the administrator, have the option to approve or re-

ject the update. If you reject the update, nothing happens. If you approve the update, that update is then advertised to your client computers, who will download the update across your high-speed local area network (LAN) *instead* of across your Internet connection.

The result? First, security patches are downloaded across your Internet connection only once, saving bandwidth for more important business purposes. Second, you retain control over which security patches are advertised to your client computers, allowing you to test the patches before approving them, if you desire. Third, because your systems are receiving the latest updates, your computers and your network stay secure.

### Only Part of the Puzzle

Although SUS and Automatic Updates are a large part of the puzzle that is referred to as "network security," they are still only a part. Your systems must be configured to be secure, and tools such as the Microsoft Baseline Security Advisor, IIS Lockdown and URLScan, and security templates can help get your systems into a more secure configuration.

### Mercurion Systems Can Help

Mercurion Systems has the experience and expertise in Windows NT/2000/XP networks to get them secure. And we have the experience with SUS to install it, configure it, and configure your clients appropriately. In addition, Mercurion Systems offers services to assist in project implementations, network design, server management and maintenance, and more.

### For More Information

If you want more information about SUS, Automatic Updates, or other services from Mercurion Systems, please call us at 919.266.5957. You can also e-mail us at [info@mercurionsystems.com](mailto:info@mercurionsystems.com).