Title:
Extending the Functionality and Security of Shared Computers using GPO and Active Directory

Introduction

Shared computers in organisations offer a cost-effective means to provide users with access to computers, without supplying individual workstations. This is particularly important in education environments such as schools, colleges, or universities where the students increasingly demand access to IT systems.

Allowing users to log on to any available machine in an institution provides the university, college, or school with flexible teaching facilities so that students can work individually from any accessible desktop.

However, shared computers can create a host of problems for IT administrators. The first challenge of shared computers is that for the most part, it is impossible to predict which user will log on at any one time. With users connecting to a variety of external devices, and using removable storage such as pen drives, not to mention CDs and floppy disks, the challenge of keeping computers secure from virus threats, whether maliciously or unwittingly, is increasingly difficult.

Additionally, as computers become more accessible to users with a higher than average level of IT skills, it is not just viruses that pose a threat to the computers, but people. While firewalls can prevent external access to computing systems, a major peril to systems is the threat from within. How can an administrator stop an internal user, with an authenticated user logon, and who is behind the firewall, from causing damage to IT systems?

With all of these security considerations, IT administrators could probably do with a little help.

Summary of Solution

Based on feedback from its customers, Microsoft has produced a series of tools that complement the functionality already available in its software to help administrators secure the desktops in their complex shared resource environment. All of this software is free of charge or already supplied in Microsoft solutions. The aim of this article is to give you an insight into these tools and what they can do for you. The information below is based on research and experience of securing desktops in a shared computer environment.

The tools covered below will be the Shared Computer Toolkit for Windows and LimitLogin tool, both available from Microsoft. There will also be some discussion about securing desktops using Group Policies.

The Shared Computer Toolkit is a tool that can be applied to machines by administrators. Its purpose is to limit user access to files that are not theirs, as well as helping protect the integrity of data on computers from damage or corruption. This is achieved by using a trusted state and refreshing this when users log off.

The LimitLogin tool is a tool that monitors logon and logoff information from Active Directory, and, more importantly, can prevent concurrent users logging on. Preventing a single user

from logging on to more than one machine concurrently is a useful feature in itself, but it will also help to prevent other people in or outside of an organisation from gaining access to machines using compromised credentials. The tool can also be used to prevent students from sharing accounts by providing auditing information about logon activity.

Finally the paper will discuss the Group Policy settings, which can help administrators to further secure the desktop. By creating appropriate Group Policy settings, and applying them selectively to shared computers or roaming users in the environment, high levels of network security are achievable.

Solution Detail

Shared Computer Toolkit

The Shared Computer Toolkit, recently released by Microsoft, is a free toolset that contains a host of rich functionality for securing Windows XP SP2 shared computers. The toolkit stores details about a trusted state for the desktop. Once a user logs on, any changes made to the machine are logged and then reversed once the user logs off. This means that every time a user logs on to the shared machine, it is in a trusted state, free of viruses and changes made maliciously.

The three main features of the Shared Computer Toolkit are;

- Disk Protection—used to store the trusted state of a machine and restore it based on your criteria.
- User Restrictions—used to limit the access users have to the machine and its files in a similar way to group policy.
- Accessibility Tools—used to give your users access to all the accessibility controls of Windows without giving them access to the control panel.

The Shared Computer Toolkit console

In the case that you wanted the users to be able to make changes to the machine configuration, you can set the shared computer to allow changes to be retained for a specified number of restarts, or alternatively set the toolkit to allow changes indefinitely. The

same is true when administrative staff are applying patches and updates, where the toolkit can be set to retain changes for a restart. As soon as you decide that the information or changes to the machines are no longer required, the computer can be set to restart once again in its trusted state.

Another application of the Shared Computer Toolkit may be to store a trusted state on all machines, but then set those machines to retain all changes. This will allow users, particularly computing students, to make full use of the applications on the machines and keep their work when they log off. At the end of term, administrators can use the toolkit to clear all the machines without needing to restore from an image. Similarly, if a computer is attacked, the toolkit can be used to immediately refresh it to trusted state.

The toolkit can also be used to restrict users logging on to machines; limiting what applications can be accessed, what Web sites can be visited, and what functions of the machine can be accessed.

The Education Support Centre (ESC) recently received a call from a college seeking advice regarding management of its computer training suite. The college runs week-long training courses in various aspects of computer usage. However, students were altering the computer's settings and some were also installing new software. Over time, these changes were causing problems with the operation of the computers, causing crashes. To make matters worse, the computers were being used for online testing at the end of the course. As data was being added by certain students, this gave them an unfair advantage at testing time. The college approached the ESC to find out if there was any way they could protect their machines from malicious activity, with the aim of reducing their workload and reducing maintenance costs for the laboratory. The college considered imaging, but the process of re-imaging the machines after every use is quite laborious. To achieve the same result, the Shared Computer Toolkit simply requires a restart.

This example highlights the advantages of using the Shared Computer Toolkit. It can be installed on the client machines and provides a trusted state for easy maintenance. At the beginning of the course, the client machines can be set to retain changes on restart, so that the people on the course can save things they work on during the week. At the end of the week, rather than keeping all the changes that the students have made, or risking the machines failing at some point in the future through cumulative changes, the machines can simply be set to revert to the trusted state. Prior to online tests, the same operation can be undertaken. The machine can be configured to prevent students accessing the Internet or other resources and illicitly obtaining the test answers.

The ESC recommended this toolkit to the college for its desktops in the lab. Use of the toolkit has removed the large maintenance tasks associated with running the lab, and allowed strict control of the resources that users can access while undertaking online tests.

Based on the success our customers have seen, we recommend the trusted state capability of the Shared Computer Toolkit. If your client machines are configured in a domain environment, we would recommend also using Group Policy to secure the desktops further and restrict access to resources. If you are not using a network, then the access restriction functionality may be useful too.

Using the toolkit ensures that your IT staff will no longer need to constantly attend to machines that have been attacked, nor will staff need to remove viruses from infected machines. Of course, the toolkit is fully customisable so you can decide what tasks your

students are allowed to perform, or which drives they are allowed to access. The toolkit also allows important patches and updates to be installed, even if the users cannot install software.

There is some overlap between the functionality of the shared computer toolkit and some of the other tools that will be mentioned, depending on the environment in which the tool kit is deployed. These overlaps are fully explained in the toolkit documentation.

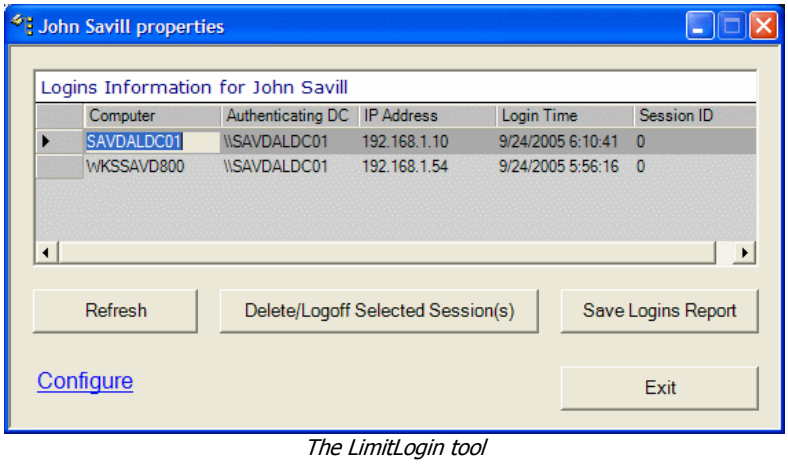
LimitLogin

The next tool we look at will be the LimitLogin tool. This feature—created by Microsoft—monitors logon information from Active Directory and prevents users from logging on to more than one machine simultaneously. It requires an Active Directory partition and is supported in line with other resource kit tools.

LimitLogin can be used simply as a reporting tool to measure how many people have been logging on and, more specifically, who has been logging on. This is useful information for administrators when trying to identify any unusual activity on the network. It can also prove a very useful tool for identifying who was logged on a particular machine, at a specific point, such as the point of a virus being released or an attack on the network. Educational establishments often use this tool to audit student logons, and identify which users regularly use the computing systems.

LimitLogin capabilities include:

- Limiting the number of logons per user from any machine in the domain, including Terminal Server sessions.
- Displaying the logon information of any user in the domain according to a specific criterion (e.g. all the logged on sessions to a specific client machine or Domain Controller, or all the machines on which a certain user is currently logged on).
- Easy management and configuration by integrating to the Active Directory MMC snap-ins.
- Ability to delete and log off user session remotely straight from the Active Directory Users and Computers MMC snap-in.
- Generating logon information reports in CSV (Excel) and XML formats.



The LimitLogin tool

The reporting features are very valuable, but only a secondary function to the main purpose of LimitLogin. The tool is primarily designed to prevent a single user logging on to more than one machine in a domain at any point.

For instance, if a user's credentials were compromised, LimitLogin would go some way to preventing the credentials being used by another person. The LimitLogin tool will also give administrators the ability to delete and log off user sessions remotely straight from the Active Directory Users and Computers MMC snap-in. One major benefits of LimitLogin over alternative tools, is that it does not require an SQL Server database to store logon details. LimitLogin simply uses data from Active Directory.

The LimitLogin tool is commonly used to prevent a single user from being simultaneously logged on more than one machine at any one time. The importance of being able to audit who is logged on a specific machine at a specific time is vital in preventing misuse of computer systems. If a user were able to log on to more than one machine at any one time, it would be impossible to determine which computer he or she was using. The same would be true if a user's credentials were compromised.

An educational institute recently approached ESC for support after its network was repeatedly attacked. The institute was looking for a way to be able to identify who was causing the attacks. It was also experiencing incidents of user's credentials being compromised. ESC recommended the customer use the LimitLogin tool to enhance its ability to control its environment.

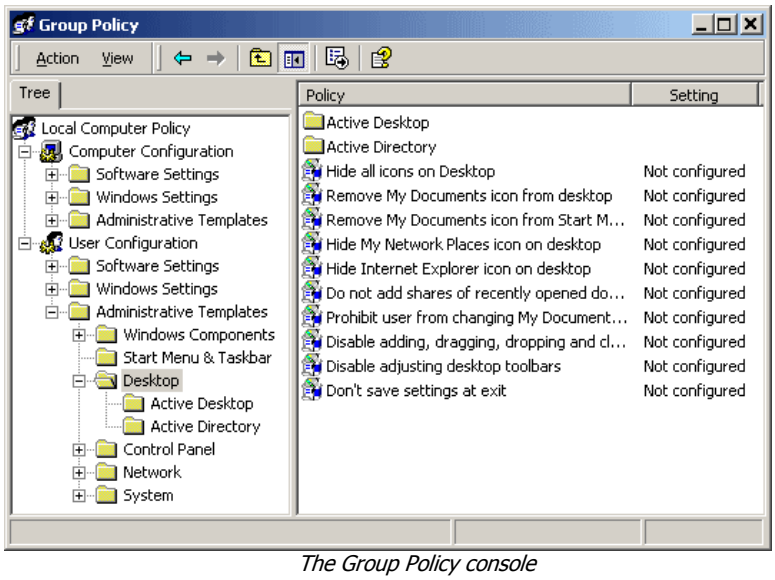
The college installed the LimitLogin tool, limiting student logons to one per user at any one time. This meant that the college was able to pinpoint exactly which computer a user had been using at any point. Alongside this, the reporting features of the LimitLogin tool also allowed the support teams to identify other users who had logged on each of the machines at other times. This allowed them to build a complete picture of network activity, helping to prevent misuse of computer systems and identify patterns and strange network activity that may suggest misuse.

Like the Shared Computer Toolkit, LimitLogin is a tool that can be used in a way which is appropriate to your department. It can be used to maintain rigid controls to prevent concurrent logons, or restrict a user's logon quota. Another application of it would be simply as a data gathering tool used to record all logon activity.

Securing with GPO

Group Policy is particularly useful in a large network environment with shared computing resources. Group Policy allows administrators to apply a series of settings to all machines that infer constraints on the use regarding what they can and cannot do with the machine.

Creating policy settings with the Group Policy tool allows you, as an administrator, to remotely enforce the ways in which you would like the users to use your machines, on a network-wide basis. Group policies can be used to enforce most aspects of system use, such as restricting access to parts of the system, restricting access to local or network drives, and a host of other things.



The Group Policy console

This could be used to prevent users accessing the C: drive, for example. There is some overlap between the functionality of Group Policy settings and the functionality of the Shared Computer Toolkit; for instance, restricting access to drives.

A university that managed a series of computer labs in its computer science department contacted the ESC wanting advice on how to set up some default file saving locations in some Microsoft applications. This would allow the university to point to network shares used by their users. The college also wanted to standardise the Start menu experience for all of the users in a particular user group, to ensure that they had access to the things that they needed, for example programming tools in the case of IT students.

The ESC suggested using Group Policy infrastructure to redirect the location of the users' My Documents folder to a location on a server when the users were using shared computers. Rather than having to navigate to a home directory on a server, the users could simply access the documents that they needed, thanks to the Group Policy feature.

In this way, Group Policy allowed users to save files using the same method as they would when saving a file on their computers at home. This also solved the university's initial dilemma; rather than altering the default file save locations in applications such as Word or Excel, the existing 'My Documents' default location can be used simply.

To give the users a standardised Start menu, the ESC recommended creating a standard Start folder and then assigning this to all of the users in a particular group. As Group Policy can be applied to different user groups, the college could simply create a different version of the Start menu suited to the needs of each separate user group. For example, faculty staff can access different applications than computer students.

Group Policy also provides massive advantages for administrators trying to secure the network. Group Policy can be used to quickly distribute a network-wide security template that locks down user desktops. In terms of shared computing, the kiosk template from Microsoft is particularly useful.

Extra Resources

Shared Computer Toolkit

This link is the main Microsoft Web site regarding the toolkit, which provides support, tutorials, and an excellent interactive introduction about what the tool can do for you. User documentation and the tool itself are available to download from this site. We would recommend this as a first port of call for anyone wishing to learn about or use the toolkit.
http://www.microsoft.com/windowsxp/sharedaccess/default.mspx

This link provides an independent overview of the tool as well as a pictorial step-by-step guide to setting up the toolkit and using it once installed. If you are going to deploy the tool, we would recommend reviewing this first.
http://www.windowsecurity.com/articles/Microsoft-Shared-Computer-Toolkit.html

This case study by Microsoft gives details of how a school district in the U.S. tested and deployed the Shared Computer Toolkit in its environment to reduce demand on its information systems department and save on maintenance costs. This is a particularly handy link as it relates to an academic environment.
http://download.microsoft.com/download/3/1/3/3139BBF1-DFD4-49C7-9CEA-A31EEB0078FD/CuracaoCaseStudy.pdf

LimitLogin tool

This article from the Microsoft TechNet Magazine gives a snappy overview of what the tool can do for you, along with a diagram and technical description of how the tool operates and integrates with currently installed applications.
http://www.microsoft.com/technet/technetmag/issues/2005/05/UtilitySpotlight/default.aspx

The LimitLogin tool can be downloaded by clicking the following link. We would recommend downloading and saving the tool locally before installing.
http://download.microsoft.com/download/f/d/0/fd05def7-68a1-4f71-8546-25c359cc0842/limitlogin.exe

The following blogs give a little more detail about the specifics of the tool and also contain some of the questions that have previously been asked about the tool in the past. The first of the blogs is by Yossi Sa'aron, one of the Microsoft engineers who created the tool.
http://blogs.msdn.com/yossis/default.aspx
http://blogs.technet.com/jhoward/archive/2005/03/14/395135.aspx

Group Policy Methods to secure the desktop

The following link is to the Microsoft Group Policy Centre. This link provides an excellent resource for all aspects of Group Policy, giving details about how to set up and use the tool to secure the desktop. It has an excellent FAQ section, and also provides some examples of setting up Group Policy in common scenarios.
http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/default.mspx

This independent link provides a very handy overview of using Group Policy settings, including a quick reference guide to some of the more common Group Policy settings. This article relates to Windows Server 2000 though much of it is relevant to Server 2003.
http://www.geocities.com/explore_windows/gp_pol.htm

The whitepaper at the following link describes and details how the Group Policy Management Console can be used to implement common desktop management scenarios using group policy. This whitepaper will be particularly handy if you are new to Group Policy and will show you how to get started easily.
http://technet2.microsoft.com/WindowsServer/en/Library/7b33dcd6-0ad2-44e8-82f8-962425b6cf8e1033.mspx?mfr=true

Summary

The sections above highlight a few of the different methods and tools that can be used to secure the shared computers in your departments. These tools and techniques are all free of charge, and can help to reduce the time required to maintain and repair shared machines.

They can also help secure the computers against corruption, virus attack, and other threats—both accidental or with malicious intent—from users.

The LimitLogin tool can be used to manage users' access to computers, with the aim of preventing unauthorised access to machines in your domain. Once the user logs on, Group Policy settings can be used to limit their access to the machine in an appropriate way.

Behind all of this, the Shared Computer Toolkit will be keeping a log of any unauthorised changes to the hard drive and will reverse these once a user logs off.

The best method to secure your computers in a shared resource environment, and enjoy the benefits that this brings, is by using an appropriate combination of the above methods. What's more, all of these tools can be adapted to suit your specific needs and environment. There is extensive documentation on how to do this on the Internet to help you through the process.