Global Information Assurance Certification Paper

Limiting Concurrent Logins in Windows NT/2000
Gene K. Burton

GIAC CSEC Practical Assignment Version 1.4b

Introduction

Network security is a critical issue for most companies today. As part of a Defense-In-Depth security infrastructure for a company, it is vital that an administrator be aware of what is happening on their network and what their users are doing. User logon consisting of a username and password is the basis for security on virtually all network operating systems in use today. Novell Netware has had the capability for years (since version 3.X) to limit concurrent user logins that will prevent a user from logging onto more that one workstation simultaneously. For unknown reasons, this capability has never been included with Windows NT Server or Windows 2000 Server. Windows NT/2000 does provide the capability to limit a users login to a specific workstation by defining a workstation restriction based on the workstations MAC address. This is done through the user account's properties in User Manager for Domains (Windows NT) and , but this restriction is very limiting in an Enterprise environment where a user would need the capability to login to any workstation. This document intends to research, evaluate and recommend solutions for overcoming the in-ability of Windows NT/2000 Server environments to limit concurrent user logins.

There are several security issues and administrative headaches that can occur when users are allowed to logon to several workstations simultaneously in a network environment. First and foremost would be the accountability problems that can arise from a user logging into several workstations at once. If the user deletes a critical file or somehow changes a configuration, how can they be held accountable if they were logged into 5 workstations at once? You could never be sure if the user actually committed the action or not. If a user is logged onto several workstations and an offensive e-mail is sent from his account, did that user send it or was it someone else that was using his account? Accessibility problems can also arise if the user is logged into several workstations and simply forgets to log off of all of them. Then you have a workstation with authorized access just sitting out in the open for anyone to sit down and start using. Administratively, the problems can be a nightmare. Have you ever dealt with a user that changed their password while logged onto 2 or more separate workstations? Their account will get locked out in a heartbeat if they change their password on one workstation and then try to access network resources on another workstation.

Methods

As stated previously, in Windows NT, a users account properties can be set in User Manager for Domains to restrict a users login to specific workstations. See

Figure 1 below. This may prove useful in a small LAN environment where the user only has a small number of workstations that they can login to, but in a large, Enterprise LAN setting with workstations spread out over a large geographical area, this could be very inconvenient and an administrative headache to try and maintain who has access to what workstations.

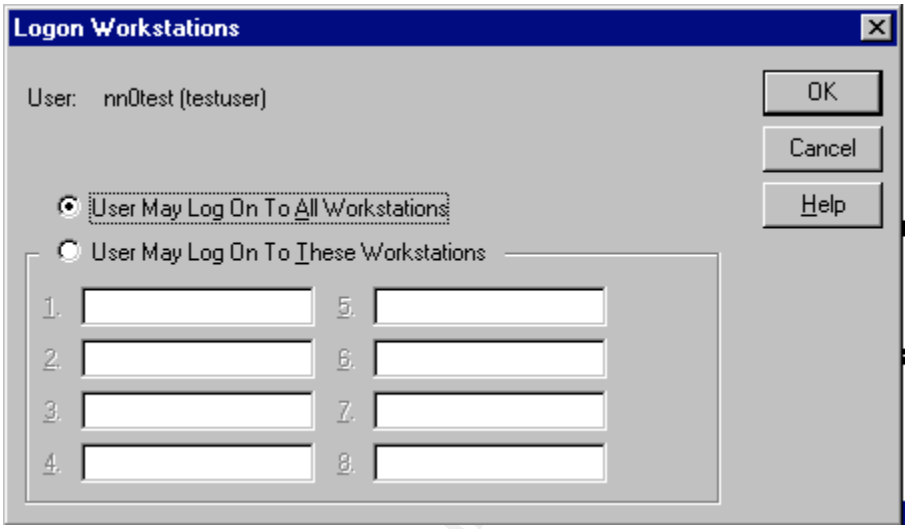

Figure 1: User Manager for Domains Workstation Logon Restriction Screen

Login Script Solutions:

Several methods exist that work to control/limit concurrent logins via a login script. These methods usually consist of various methods of checking if the user is logged on elsewhere via the login script. If they are, then an automatic logout utility is used to immediately log the user off of the system.

When you log on to NT or 2000, your PC adds a NetBIOS name consisting of your username plus Byte16=0x03 appended to the end with a maximum of 16 characters. This name is used to send you broadcast messages, such as print job completion notification messages. This name can be seen by running nbtstat –n which will show the local NetBIOS names on a workstation. See Figure 2 below for a sample output. This figure shows the nbtstat –n output when the user, nn065053a, is logged onto only one workstation on the network. Figure 3 shows the nbtstat –n output when the user is logged onto two or more workstations simultaneously. Please note that this output is taken from the second workstation that the user is logged onto. This shows that the NetBIOS name with Byte 16 = 0x03 is only assigned to the first workstation that you logon to and will not appear on the second or third workstations. Any broadcast messages sent to this user after they are logged onto multiple workstations will only show up on the first workstation that the user is logged onto. For example, if

this user prints from workstation # 2, then the print job completion message will show up only on workstation # 1.

Most of the login script methods for limiting concurrent logons will use this NetBIOS name. The script will look for the existence of this NetBIOS name on the workstation you are logging onto. If it does not find the name, then the system knows that you are logged on elsewhere and will then use another utility (such as logout.exe, a freeware utility available at http://www.jsiinc.com/SUBA/tip0100/rh0184.htm) or method to immediately log the user off, usually accompanied with a message box that alerts the user that they are logged on elsewhere and must logoff of the other workstation in order to log on to this one.

Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks website (http://www.jsiinc.com) contributor Nick Brown has made the NTNAME utility available for free download. NTNAME is a small utility that simply checks to see whether the given NetBIOS name is owned by the current PC. If so, it outputs nothing and returns errorlevel 0. If not, it outputs the name of the owning system to the standard output (so you can capture it in a file) and returns errorlevel 1. If you get this errorlevel, it generally means that you are already logged in on another PC. It's then up to you to write a logon script to detect this and log the user off. A sample logon script could look something like this:

```
NTNAME %USERNAME% >%TEMP%\OTHERPC.TXT
if not errorlevel 1 goto logon_ok

for /f %%f in ('TYPE %TEMP%\OTHERPC.TXT') do @echo Already logged onto
%%f %0\..\logout.exe
:logon_ok
```

Figure 2: NBTSTAT –n output when user (NN065053A) is logged onto only one workstation on the network.

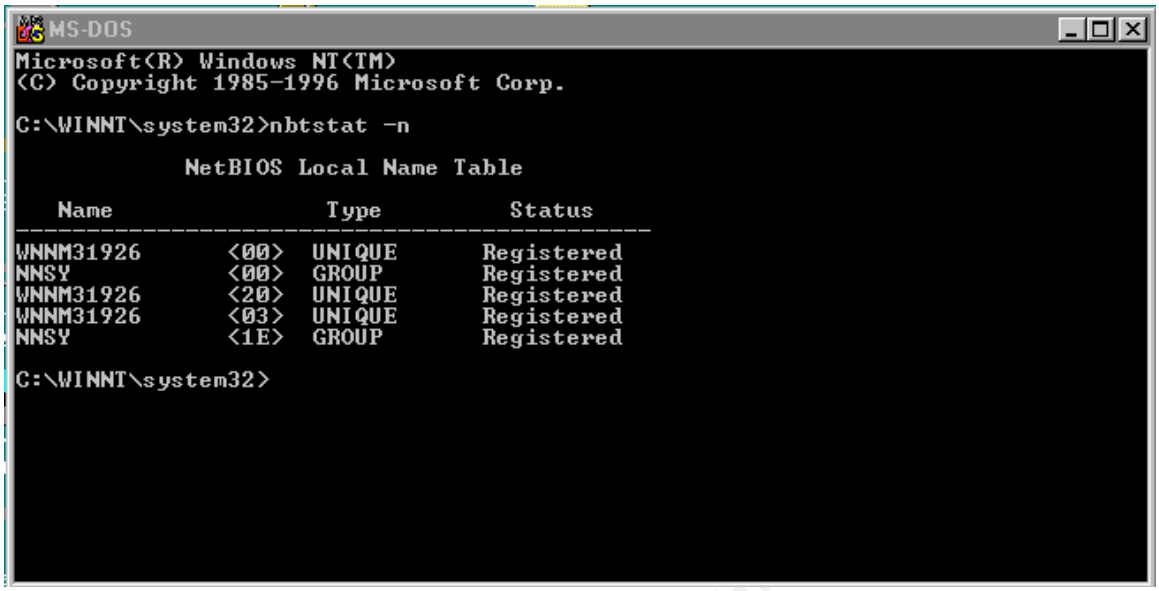

Figure 3: NBTSAT –n output when user (NN065053A) is logged onto two or more workstations (from second workstation). Note that the NN065053A NetBIOS name does not appear.

This method will work but there are several drawbacks involved. First, this method relies on a login script that can easily be interrupted by the user. As the login script is running, the user can easily hit Ctrl+C and interrupt/stop the login script. This weakness can be alleviated if you utilize Kixtart to generate your login scripts. KiXtart is a logon script processor and enhanced batch scripting language for computers running Windows XP, Windows 2000, Windows NT or Windows 9x in a Windows Networking environment and is available at http://kixtart.org. This utility can generate login scripts that cannot be interrupted by the user.

You can also run into problems if you have multiple domains and workgroups on your network with different people administering them. The possibility could arise where the same username exists on different domains. If this were to happen, user WJONES in one domain can fail to logon because user WJONES in another domain is already logged in.

Another login script method discussed on the Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks website at http://www.jsiinc.com/SUBA/tip0100/rh0175.htm is to assign a hidden share for each users home directory and then map this directory at logon. Once the hidden share is created, limit the share to one logon. This is done in the directory properties window under the Sharing tab. See Figure 4 below.

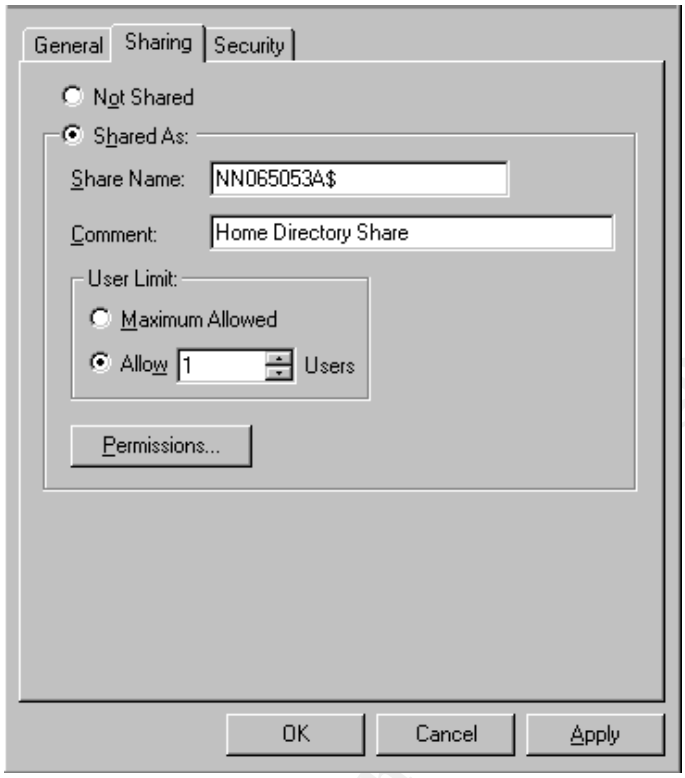

Figure 4: Setting the Share Limit to one User

You should also give only the user Full Control of their home directory as well. Once the proper permissions and user limits have been set on the user home directory, a text file is then created on each users home directory with their username as the file name, such as username.txt, with read permissions assigned only for that user. Then a simple check (if exist) for the existence of the text file can be done in the login script. How does this method work? Since only one user is allowed to connect to the user's share, the net use command in the logon script will fail to map a drive letter to the users home directory share if one connection to that share already exists. The logon script will be unable to locate the username text file and can then be directed to immediately log the user off of the system. A sample logon script using this method is provided below:

```
; map users home directory to J:\
NET USE J: \\Servername\%Username%$

If exist J:\%username%.txt
Goto continue
Endif

CLS
ECHO YOU ARE ALREADY LOGGED ONTO THE NETWORK
ECHO SYSTEM POLICY DOES NOT ALLOW MULTIPLE LOGINS
ECHO YOU WILL BE IMMEDIATELY LOGGED OFF OF THIS PC
```

PAUSE
LOGOUT.EXE

:CONTINUE
Continue logon script command processing

Using this approach, we once again run into the login script vulnerabilities as discussed earlier. You will also run into problems if the home directory share's server is down. If the home share server is down, then the login script will \never find the text file on the users home share, and thus, prevent the user from logging on at all.

Microsoft's Solution – Cconnect:

As stated earlier, in Windows NT/2000 environments, you can limit a users login to a specific workstation by defining a workstation restriction on the user account's properties in User Manager for Domains. All this does is limit a user to logging into one or more workstations instead of limiting concurrent logins. If you set the number of workstations to 2 or more, the user can still logon concurrently. Plus this is an administrative nightmare to keep track of and to implement.

The Windows 2000 Server Resource Kit contains several useful tools for the system administrator, including the Concurrent Connection Limiter (Cconnect) utility that lets you limit concurrent logons in Windows 2000 and Windows NT networks. The drawback to the Windows 2000 Server Resource Kit is that it is not free (current cost is $209.99 at http://www.amazon.com). Cconnect contains two components: Cconnect Administrator lets you view current logons across you entire domain and forcibly logoff users when necessary. Cconnect Client runs on each workstation and enforces the concurrent logon restriction. Cconnect client must be installed on each workstation. When a user logs on to a workstation, Cconnect client counts the number of currently active logons for that user in Microsoft SQL Serve database, then compares this number to the maximum number you have allowed for that user. If the user has exceeded their limit, Cconnect immediately logs the user off of the network.

Cconnect has the following features: It is completely hidden from the end user. It keeps track of all computers that users are logged into. It allows concurrent connection limitations to be set on a per-user or per-group basis. All information is kept in a Microsoft SQL Server database assigned by the administrator. It also tracks the last known user of a computer and monitors what logon servers are being logged into.

To use Cconnect, you must first set up a new database and user account on a SQL server machine. Microsoft SQL Server 6.5 or higher is required. In order for Cconnect to work, each install of Cconnect must be given certain rights via a Server Name, Username and password to the appropriate SQL server. These

rights are Database Creation, Table Creation, Field Creation and Field Update and Delete. These rights are very similar to the SQL Server SA user account rights. It is never a good idea to use the SA user account because of its all-powerful SQL capabilities. Therefore, it is suggested to create a new SQL User account with Full rights to the SQL Server. Assign the new account the Cconnect database as its default database. If this is not done, Cconnect will use the SA user defined default database which is MASTER.

To setup Cconnect, create a new Cconnect database using SQL Manager on your SQL server. Microsoft recommends using a single SQL Server specifically designated for the Cconnect database. Configure the database with the default settings for a new database. Cconnect.exe will automatically configure the database the first time that it is run. After the database is setup, then create a SQL Login for the database (Microsoft recommends that you create a SQL Specific login and not a Windows NT/2000 login). Use SQL Manager to create the login as follows:

1) Select the Security Folder.
2) Select Logins.
3) Right-click Login and select New Login.
4) Name the new Login CCLogin.
5) Select SQL server authentication and place a password.
6) Under Defaults, select Cconnect as the default database.
7) Under the Database Access tab, check Cconnect Database.
8) Under Database Roles, select All Roles.
9) Under the Server Roles tab, select All Roles.

The CCLogin account will now be equivalent to the SA account, yet its default database will be Cconnect. This new user's credentials can be assigned to every computer through the Cconnect group policy ADM file. If the credentials do not exist, the user will be prompted to enter the credentials the first time Cconnect is run (See Figure 5). Once they are supplied, they will not be prompted again.

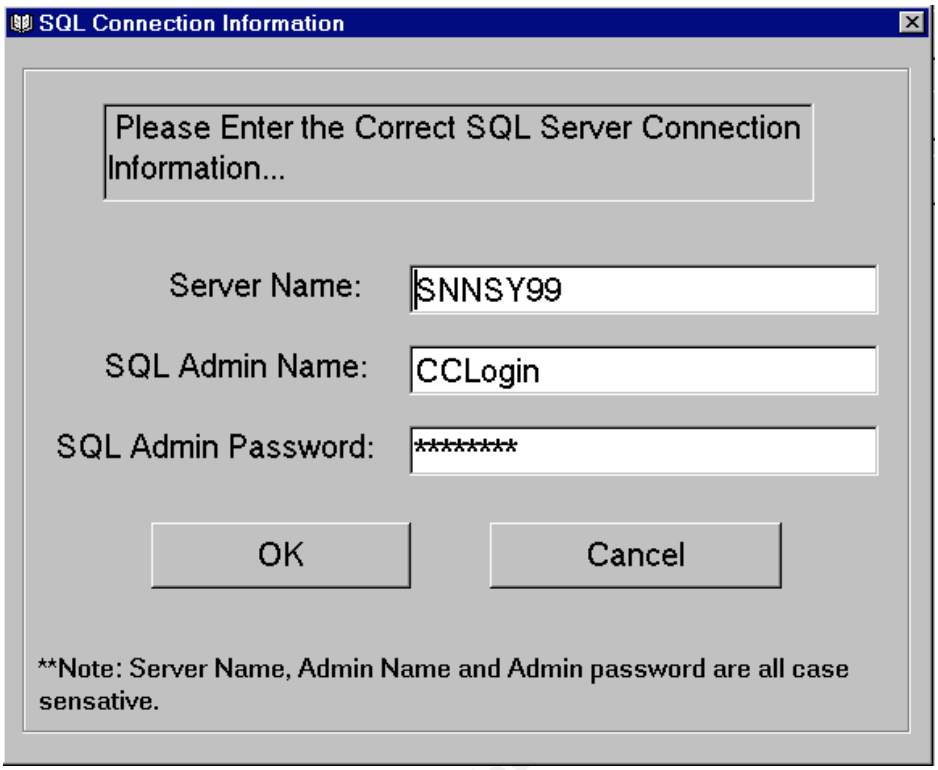

Figure 5: SQL Connection Information Prompt

Once the database and login have been created, Cconnect can be easily installed by running the \Cconnect\Admin\setup.exe program on your SQL Server. This will populate the SQL Server database.

Then, to centrally manage all the Cconnect clients, you need to import the Windows 2000 Group Policies or Windows NT system policies that are included in the cconnect.adm file included on the Resource Kit CD-ROM. These policies define registry values under the HKEY_CURRENT_USER\Software\Microsoft\Cconnect subkey. These registry values point the Cconnect client to the SQL server database mentioned above and define the user's concurrent logon limit. See Figure 6 below. After you import the cconnect.adm file, you can configure Cconnect's policy and SQL server connection data and then configure your network's workstations to import this policy. An explanation of utilizing Windows NT System Policies and Windows 2000 Group Policies is beyond the scope of this article. Please refer to Microsoft Knowledge Base Articles 168579 and 318753 for more information. Cconnects Policy settings are explained below (taken directly from Cconnect.doc available on the Windows 2000 Server Resource Kit CD-ROM):

Track Last User - Enables more Windows 2000 security. If "track last user" is enabled, and the computer was not properly shut down, CConnect will not remove the user/computer entry from the database. No other use except the last

known user will be able to log in to the computer. If the last known user does log in, then the database is updated with the new information.

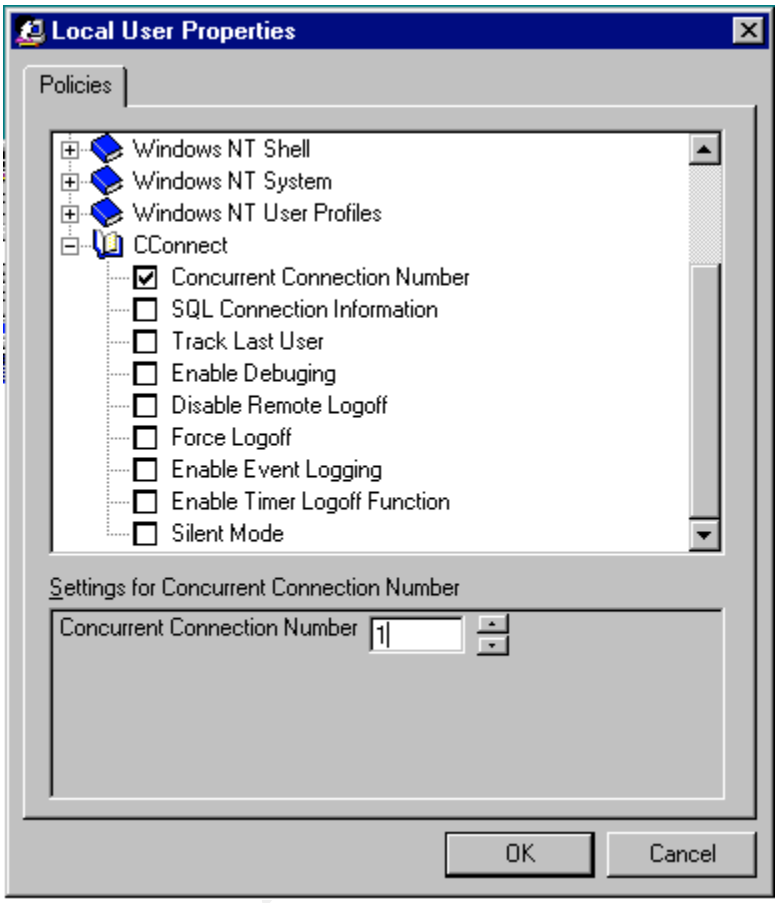

Figure 6: Cconnect Policy Settings

Enable Debugging – Enables the debug output of both the client and the administrative tool. The output will be on the %SystemDrive%\CConnect.txt for the client tool. And %SystemDrive%\CCAdmin.txt for the administrator tool.

Disable Remote Logoff - Gives the administrator the ability to allow the user to see which computers their account is logged into. But it does not allow them to remotely log off the computer. This can be used for companies that wish to provide a mechanism for users to know where their account is logged in, but the users are not administrators of the local computer. Being an administrator of the local computer is a system requirement to remotely log off a computer.

Enable Force Logoff - Gives the administrator the ability to forcibly log off a user from the local computer when their Con Current Connection Limitation is reached. When this is enabled, the user will not be prompted for anything, they will simply be logged off the current computer.

Enable Event Logging - Gives greater error logging to CConnect. The CConnect Client will now, log events for all errors it encounters. It will also log events for any successful acts that occur. Such as proper loading and unloading as well as all logoff attempts. Whether successful or not. Event Logging will log events to the local computer unless otherwise specified. In which case you can specify a specific Event Server to use in the Group Policy. CConnect will write events to that server's application log.

Enable Time Logoff - Forces the user to log off the local computer if they do not make a choice when the user is presented with the logoff choice. Example would be when the user is presented with the choice to be logged off the local computer or logoff one of the remote computers they are logged into. If the Enable Time Logoff feature is enabled. You can limit the amount of time they have to choose. When the timer expires, whether or not they made a choice it will log them off the local computer. See Figure 7 below for the prompt the user will see. If Yes is selected, the user is presented with a listing of the computers they are currently logged on to and can select which one they want to log off. See Figure 8.

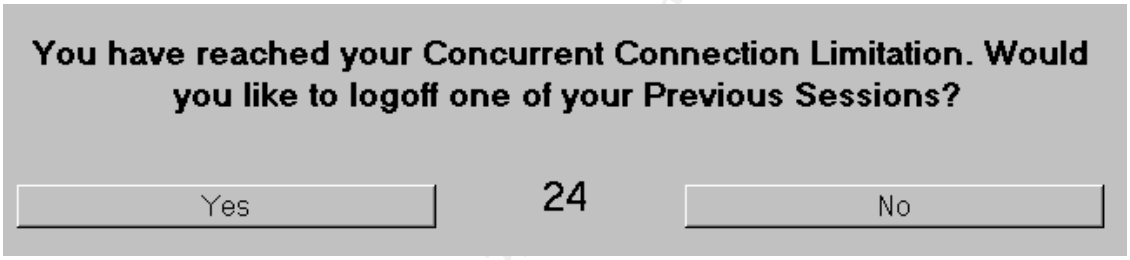

Figure 7: Cconnect Logoff Choice Prompt

Figure 8: Selecting a Computer to Logoff From.

Enabling Silent Mode - Will not prompt the end user when the CConnect Client receives an error. Meaning that if CConnect experiences any connection problems or update problems the end user will not be notified. It is recommended that you enable Event Logging or Debug mode, so that the administrator can track success or failure of CConnect Client.

Next, you must install the Cconnect client on each workstation (run setup.exe from the Cconnect\Client directory on the Resource Kit CD-ROM). After the Cconnect client has been installed on each workstation, you must then configure the cconnect client program (cconnect.exe) to run at startup by either placing the program in the All Users Startup program folder or by setting up the Cconnect client to run as a service using the Windows NT Resource Kit tool SRVANY (Please reference the Windows NT Resource Kit SRVANY instructions on how to use this tool). If the Cconnect client is not run as each user logs in, then the functionality of Cconnect is lost.

There are some important points to consider if you decide to implement Cconnect on your network. First, because the SQL Server Cconnect database deletes active logon records when a user logs off in a normal manner (i.e. a user initiated logout such as Start..Programs..Log Off or Ctr+Alt+Del then Logout), Cconnect can sometimes deny logons improperly. For example if a power outage occurs or a user's workstation freezes up and requires a hard reboot (power turned off then back on), the database will not delete the users logon record. If the user uses the same workstation to log back in to the network, the database will delete the orphaned logon record and let the user logon. However, if the user tries to logon to a different workstation, Cconnect will think the user is trying to exceed the logon limit and deny them access to the workstation. To fix this problem, you will have to use Cconnect Administrator to manually delete the existing/orphaned logon record.

Another drawback to Cconnect is that a knowledgeable user can easily defeat its measures on the workstation. Cconnect uses SQL server only to store current logon data for users. Other configuration and policy settings for Cconnect are stored in the workstation registry HKEY_CURRENT_USERS\Software\Microsoft\Cconnect subkey (see Figure 9). A knowledgeable user could disable Cconnect by simply pointing the tool to a bogus SQL Server, increase their concurrent logon limit or by deleting the subkey itself. To minimize this risk, you can use Group Policy in Windows 2000 or System Policy to disable registry editors. More powerful methods would be to limit access to registry editors (regedit.exe and regedt32.exe) only to system administrators, and to limit user permissions on this subkey to read access only by using regedt32.exe.

Another weakness of Cconnect is that the client stores the SQL server user and password data in the workstations registry in clear text (See Figure 9). If you have not restricted the Cconnect SQL Server user account's access only to the

Cconnect database as mentioned earlier, then you will have a SQL Server accounts' username and password in plain text on every workstation that has all the capabilities and authority of SQL Server's built-in administrator account. This would allow any user to utilize that account to attach to and attack any other database you have installed on your network.

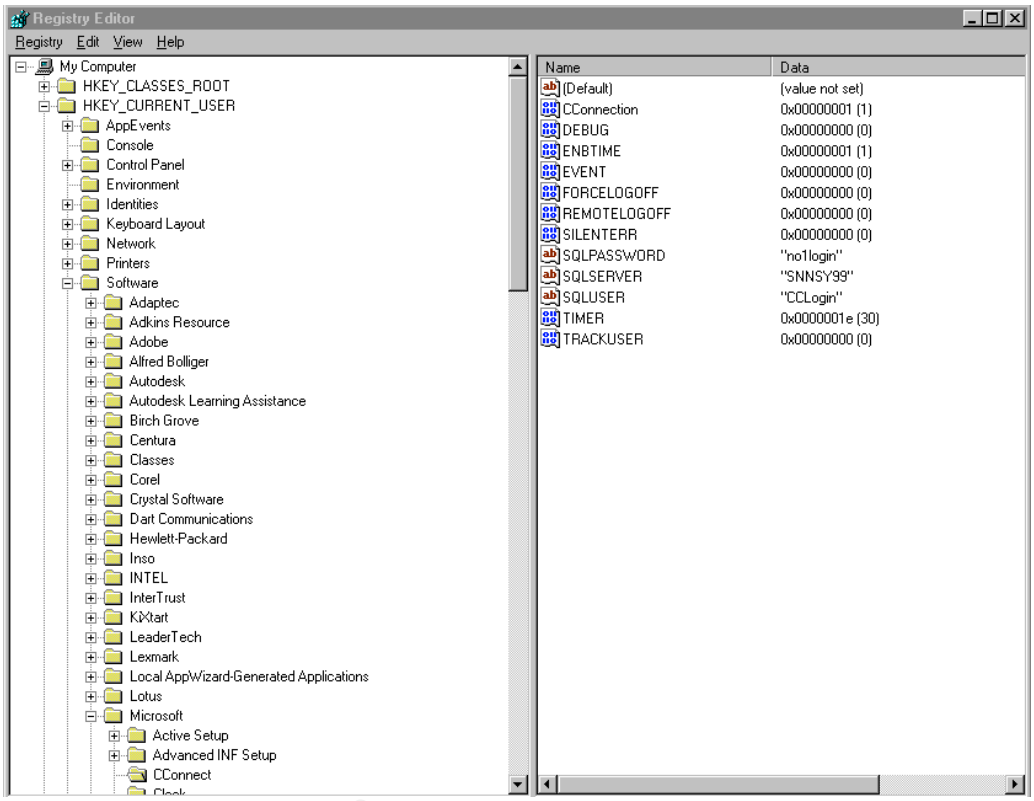

Figure 9: Cconnect Registry Settings

Another weakness exists on the users workstation running the Cconnect client. In order for Cconnect to work correctly, the cconnect client must be running on each workstation. Once it is running, it gives no outward indications that it is active. However, if a user runs Task Manager, he or she can see that it is running (see Figure 10) and has the capability to remove the program from memory. This can cause the Users information to be removed from the database without a proper logoff or it can leave the Users information in the database, which will increase the number of concurrent logins that user has. This can cause problems with Cconnects administration as it could allow a user to bypass their concurrent login limit or it could prevent a user from logging in when they have not exceeded their limit. It is recommended that access to the Task Manager application be restricted via Windows NT/2000 Group Policy to prevent this problem.

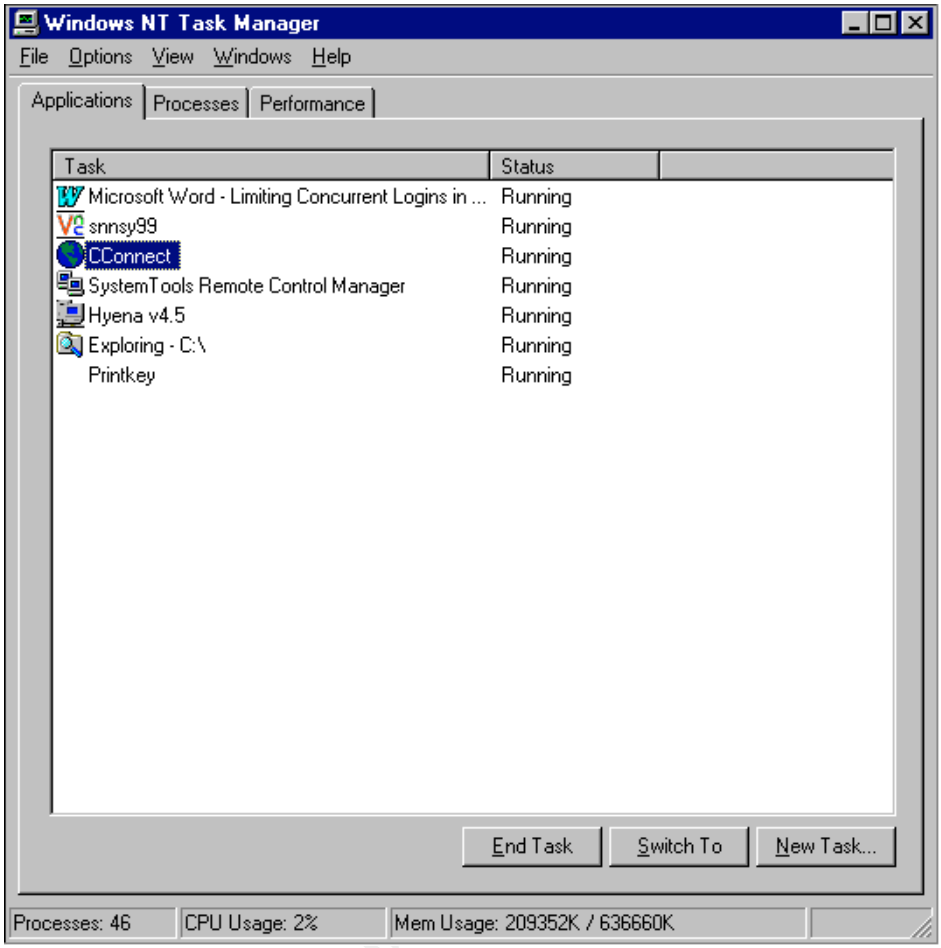

Figure 10: Task Manager showing Cconnect Running

Finally, if you plan to user Cconnect in a Windows NT environment, there are special requirements that must be met for each workstation. Each NT workstation must have Service Pack 4 (SP4) or later installed with the Windows Scripting Host (WSH), Web-Based Enterprise Management (WBEM) and Microsoft Data Access Components (MDAC) 2.0 or later. Without the WBEM installed, forced remote logoffs cannot occur. All of these components are available for download at http://www.microsoft.com. Also, please note that Cconnect will not work for Windows 9X systems.

3rd Party Commercial Product Solutions:

UserLock:

IS Decisions (http://www.isdecisions.com) offers the product UserLock to provide the addon capability of limiting concurrent logons to a Windows NT/2000 network. EngageNT (http://www.engagent.com) is the United States distributor of the UserLock software. Detailed information on the UserLock software may be found at either web-site listed above. UserLock solves the problem by preventing users from

opening several sessions at the same time and provides the following functionality:

- UserLock limits the number of simultaneous logons for each user on the entire Windows NT / 2000 / XP network.
- Limit logons by group or by user.
- Limit users to a specific group of workstations, or limit by IP range.
- 100% compatible with all existing systems, UserLock restrains simultaneous connections on any Windows computer.
- Functions on all networks...LAN or WAN.
- Thanks to the snap-in MMC (Microsoft Management Console) included with UserLock, the administrator can choose to limit certain users and not others.
- Customizable user notifications.
- Manages single or multiple domain networks.
- Uses GINA extension for maximum security.
- Automatically deploys GINA extension to workstations.
  (Engagent UserLock Product Information Page - http://www.enagent.com/products/productsinfo.asp?product =UserLock)

UserLock also contains built-in reports for showing current status of the users including when they last logged on and off, as well as their current status.

UserLock installs as a service on a Windows NT/2000 server and is based on a customized Graphical Identification and Authentication (GINA). The GINA is a dynamic load library (DLL) component loaded by the WinLogon process that implements the authentication policy of the interactive logon model. It performs all user identification and authentication interactions. Msgina.dll, the standard GINA provided by Microsoft and loaded by Winlogon, can be replaced by a GINA that is custom-built by a third party, such as UserLock. A good discussion of Microsoft's GINA and the WinLogon process can be found in the Microsoft white paper "The Essentials of Replacing the Microsoft Graphical Identification and Authentication Dynamic Link Library" at http://www.microsoft.com.

UserLock's customized GINA ensures that UserLock is allowing a logon to occur and notifies the UserLock server of logoffs. It is compatible with other GINA extensions by forwarding all GINA procedure calls to any existing GINA extension. This enhancement (the UserLock Agent) must be installed on every protected workstation on your network. The installation of the UserLock Agent can be performed using the Agent Deployer on the UserLock primary server, which constantly looks for GINA installation status and can install them without any user intervention.

UserLock servers are administered using the Microsoft Management Console (MMC) and run as a standard Windows NT/2000 service (See Figure 11). The Agent Deployer mentioned above is included in the UserLock MMC Console. Installation consists of installing the server component first, defining the

restrictions and notifications using the UserLock Console MMC and then using Agent Deployer to install the UserLock Agent on your workstations. UserLock can place restrictions on concurrent logons based on specific Users or User Groups, it can provide notifications of successful or failed logons/logoffs (See Figure 12) and can prevent users from logging onto specific computers (See Figure 13).

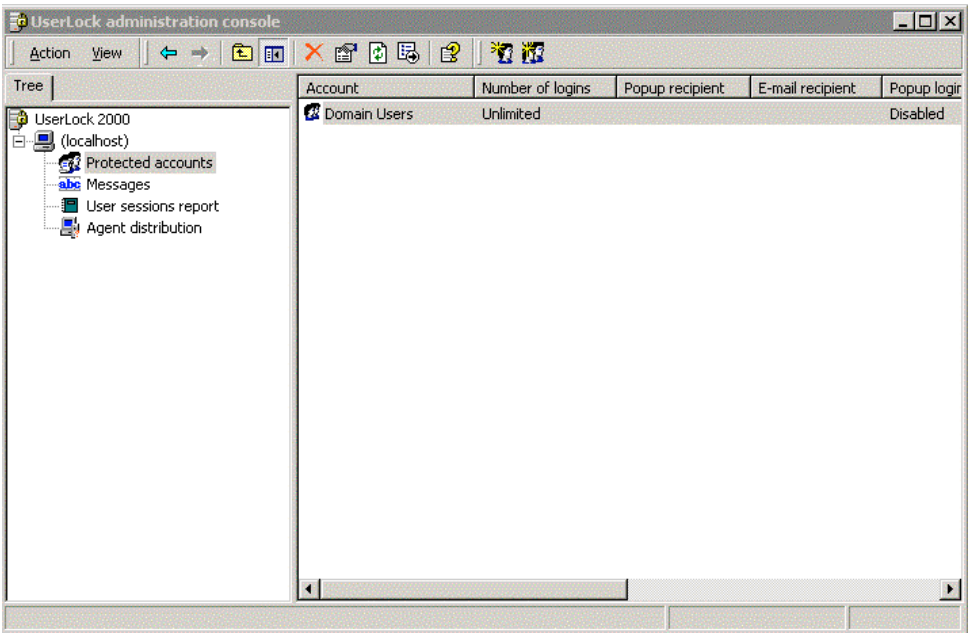

Figure 11: UserLock MMC Console

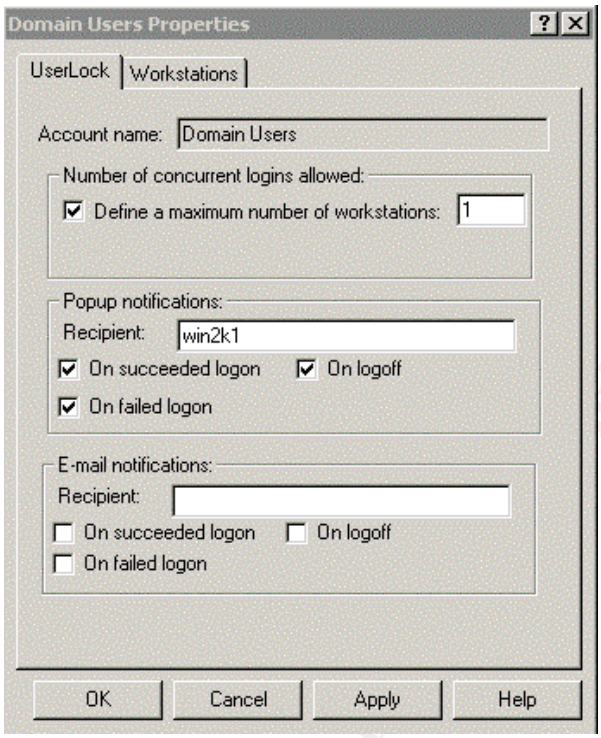

Figure 12: UserLock User or Group Restriction Settings

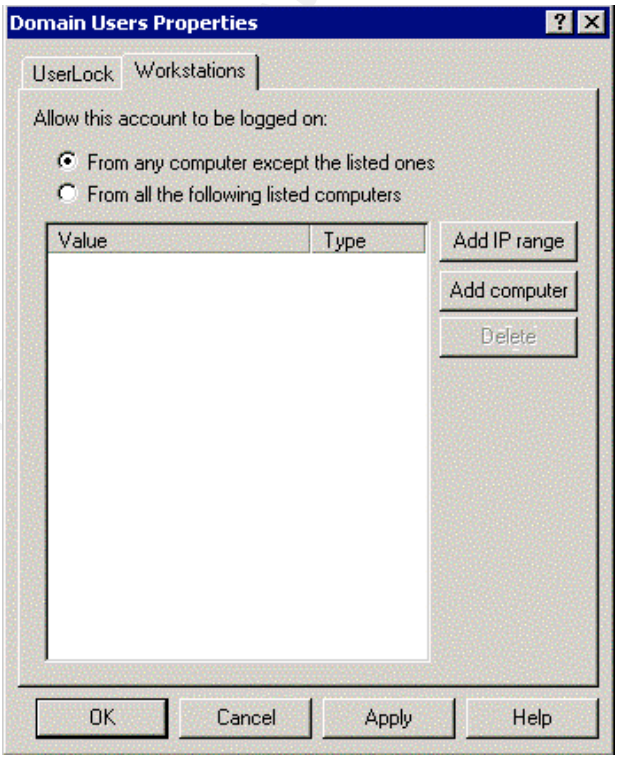

Figure 13: UserLock Workstation Restriction Settings

UserLock can also be configured to provide custom messages to inform users of its actions (See Figure 14).

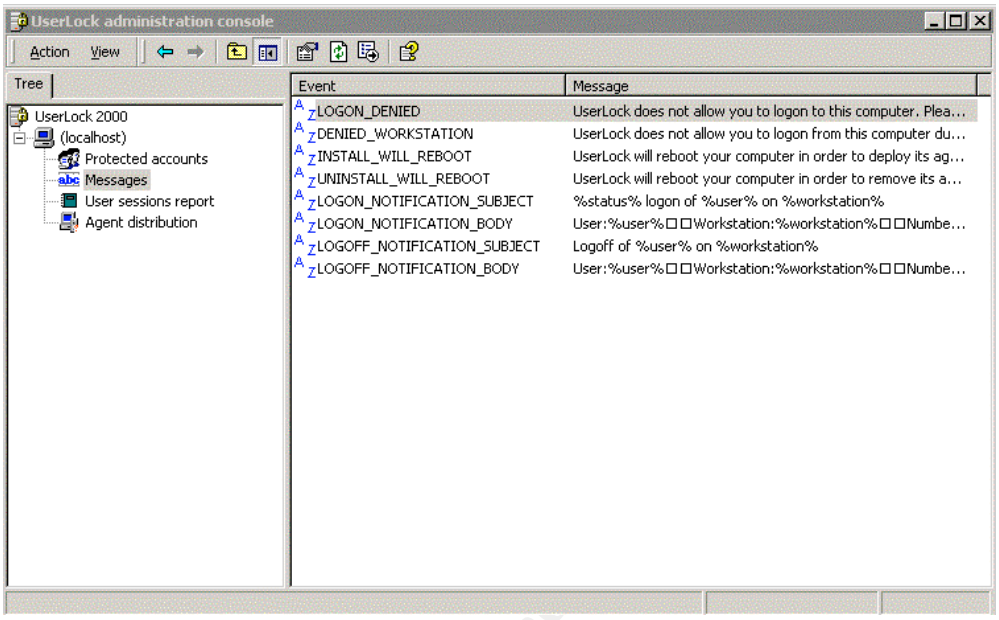

Figure 14: UserLock Console Messages Settings

Userlock's installation is fairly straightforward. The only caveat is to ensure that you specify a domain administrator account when choosing the UserLock Service Account (See Figure 15). You may want to setup a unique administrative account such as userlock_admin that will only be used for this purpose.

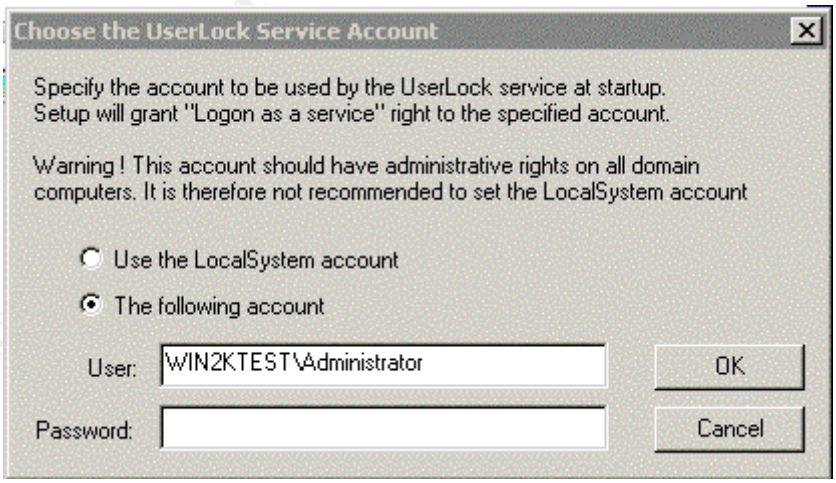

Figure 15: Specifying the UserLock Service Account

Once UserLock is installed on the server, you can activate the Agent Distribution installation to all workstations in your domain by starting the Agent Deployer.

This will automatically detect workstations in your domain and install the agent on each one. At each workstation, the users will be prompted that the agent has been installed and then an automatic reboot is performed. UserLock agent installation on the workstation is transparent to the user. The UserLock agent installation on each workstation modifies the registry at the HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon key and replaces the standard GinaDLL value of msgina.dll with the UserLock Gina ULAGENT.DLL (See Figure 16). UserLock also adds the following values for communications with the UserLock server: UserLockServer, UserLockServerIp and UserLockServerLastUsed (See Figure 16).

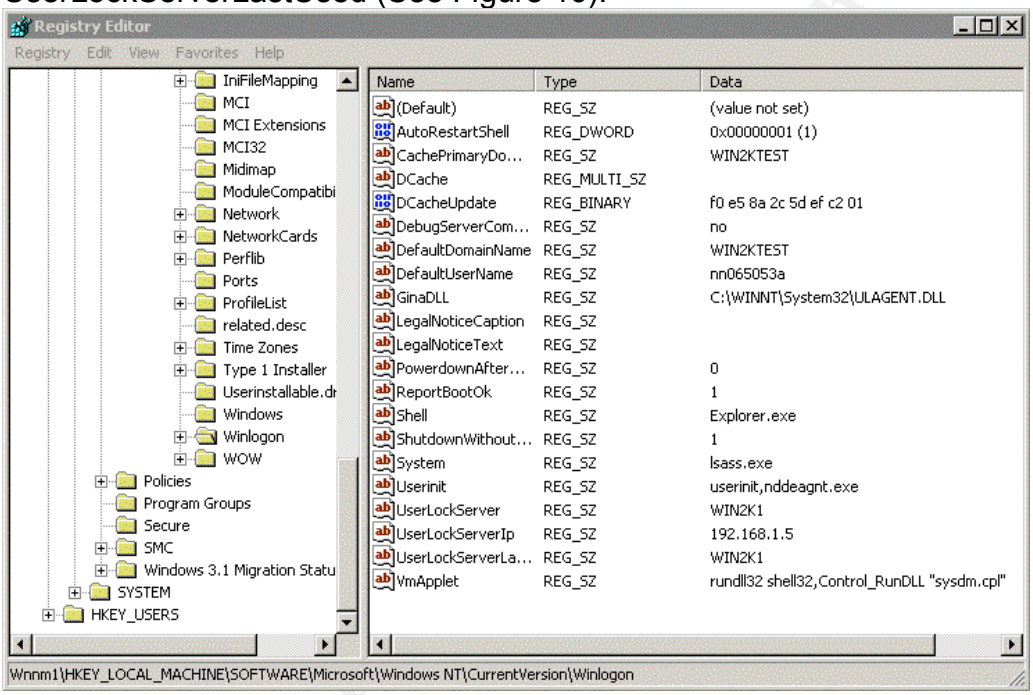

Figure 16: UserLock workstation registry settings

After you have the UserLock agent installed on your workstations, the concurrent login restrictions take affect immediately. If a user is logged onto a workstation and attempts to logon to a second workstation without logging off of the first workstation, they are shown the prompt in Figure 17 below. Clicking on the OK button immediately takes the user back to the Windows Logon prompt. The user will be unable to logon to another workstation until they logoff of the workstation they are currently logged on.

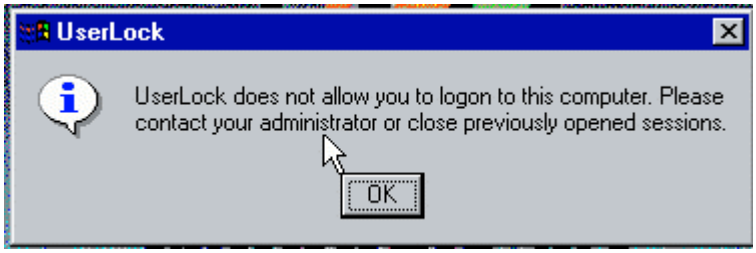

Figure 17: UserLock Warning Prompt

Successful and un-successful logon notification messages can be configured to notify an Administrator of such actions. (See Figures 18 and 19). You can also setup e-mail notifications of such events. However, this could become very cumbersome on an Enterprise network with a large number of users.

Overall, UserLock is a well-designed product that is very easy to install and get up and running on your network. The specific registry entries for UserLock are located in the HKLM\Software\Microsoft\WindowsNT\CurrentVersion\Winlogon key, which by default has stringent access rights assigned (only administrators can modify the registry values in this key. Therefore, the weakness that exists with Cconnect of a knowledgeable user editing the registry to defeat the product does not exist. The program also deals with improper logoffs (such as power failures) very easily (recall that Cconnect did not). To clear the user logon session from the UserLock Console, simply go to the User Sessions Report section, select the affected user and then reset their user sessions back to 0. A user can also clear this error by logging back into the workstation that was affected by the power failure and then logging back out. This action will reset the UserLock session count to 0 sessions, thus allowing logon to the system again. Another inconvenience of UserLock is that it does not prompt the user with the workstation that they are currently logged onto if their logon is denied. This information is always helpful so that the user can locate the workstation an log out. (Author's Note: This inconvenience has been corrected with the latest release of the UserLock software v2.63).

Pricing for UserLock is based on the total number of users in a domain as shown below:

10 Users - $45.00
50 Users - $182.00
200 Users - $596.00
1000 Users - $2432.00
5000 Users - $9927.00
(EngageNT web site
http://www.engagent.com/Products/productsinfo.asp?product=Userlock&link=Standard+Pricing.)

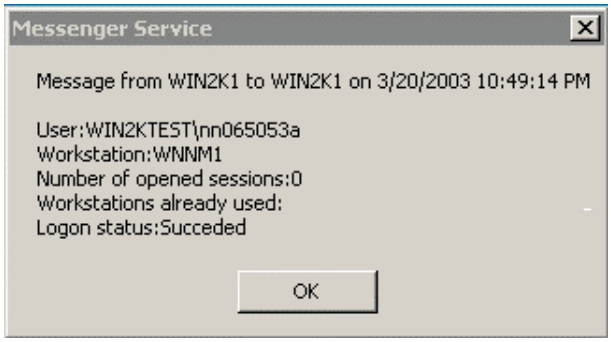

Figure 18: UserLock logon success message.

Figure 19: UserLock logon failure message.

ServerBoss:

ServerBoss, available for download from http://www.serverboss.com, is another 3rd party solution for restricting concurrent logons in Windows 2000/NT. ServerBoss provides the following extensive features:

- Restrict concurrent user and group logons to a single or user definable number of logons.
- Restrict concurrent user and group execution of applications to a single or user definable number of executions.
- Restrict user logons by IP Address (ICA and RDP logons)
- Full Application Metering Capability on Citrix and Terminal Server platforms.
- Restrict concurrent NT® RAS connections to a single or user definable number of remote connections.
- Restrict concurrent NT RADIUS connections to a single or user definable number of remote connections.
- Modular Design allows you to select and pay for only those capabilities you need.
- In most cases you can set restrictions by user, by group, by application, by server, by IP address...very flexible.
  (ServerBoss Home Page – http://www.ServerBoss.com.)

ServerBoss also supports the following Windows based 32-bit platforms: Microsoft NT4 Terminal Server Edition, Microsoft NT 3.51, Microsoft NT 4, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Citrix WinFrame, Citrix MetaFrame, Citrix MetaFrame XP, NT RAS Routing and RADIUS in NT 4, Windows 2000 and Windows 2000 Advanced Server. ServerBoss is a very flexible and capable product. In our testing, we will look at its LAN Server checking capabilities.

ServerBoss installation is very straightforward, in fact the product can be installed on a workstation as long as the workstation is stable and always visible to all workstations on the network. To install ServerBoss, save the downloaded installation file on the server/workstation that will be the ServerBoss server in a temporary folder, un-zip the file and then run setup.exe from the temporary folder. Follow the prompts to install the software onto your server/workstation. After installation is complete, share the installation folder (C:\ServerBoss) and assign change rights for users to both the folder and the network share. Users need change access to ServerBoss.lic license file and .log files only. Users do not need any access to the ServerBoss.exe or SBSetup.exe. Read/Execute access should be given to all other ServerBoss programs and DLLs. Users also require Read/Execute access to the machnm1.exe and the keylib32.dll files which are located in the winnt\system32 folder on the ServerBoss server.

After ServerBoss is installed on your server and all the rights have been setup properly, run ServerBoss.exe to setup your managed servers and workstations. Under Manage → Servers, add each server that you want to authorize logons to (See Figure 20). Generally, these servers will be member servers or servers that provide the types of sessions that you want to control, such as RAS, RAS RADIUS or LAN servers. For the purpose of our testing, we want to control/authorize LAN sessions, therefore we will have to identify all managed workstations under Manage → Workstations (See Figure 21). Note that you only need to install ServerBoss on the workstation or server that you have designated as your ServerBoss Server. SBSetup.exe located in the ServerBoss share folder

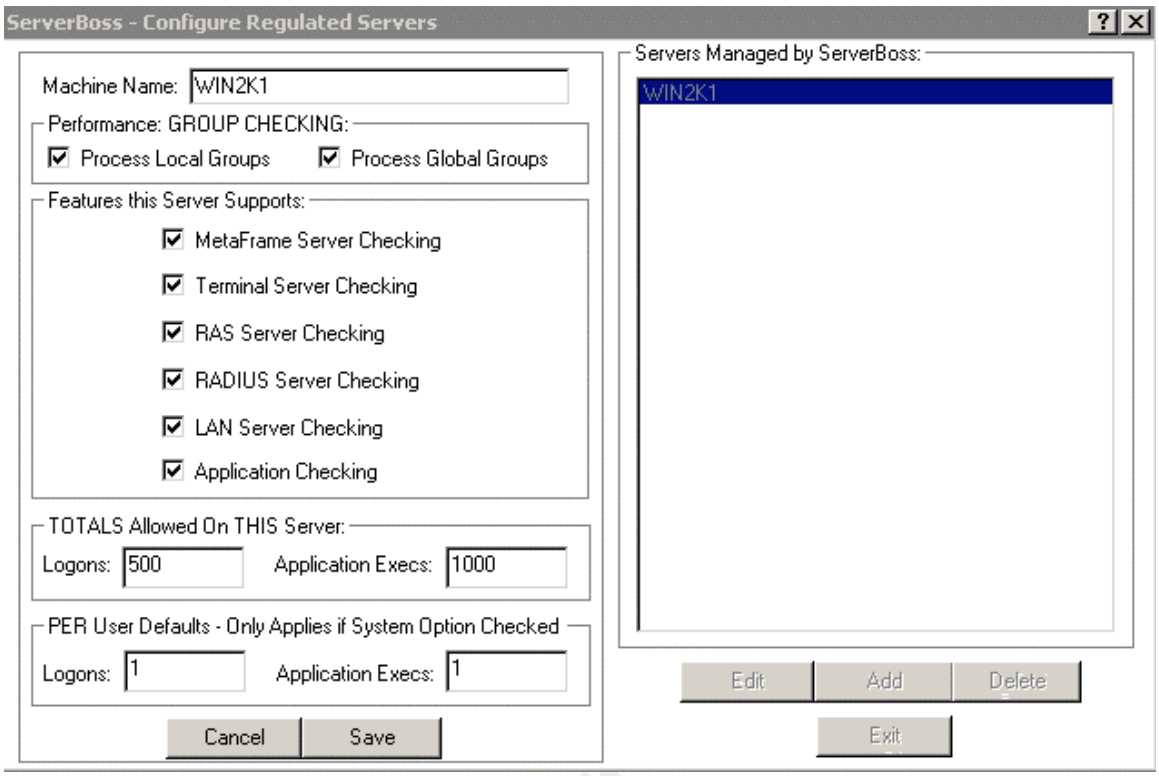

Figure 20: ServerBoss Server Configuration Options

on your ServerBoss Server is used to configure the servers and workstations that you want to restrict concurrent logons. The ServerBoss server must be a Windows 2000/NT server or workstation and all data is accessed and stored in this central location for ease of management. ServerBoss automatically defaults to one concurrent logon on all regulated servers. See Figure 22 to see a listing of the ServerBoss default System Options. You can also set user authorization rules that will allow specific users to have more than one concurrent logon if necessary (See Figure 23), such as administrators.

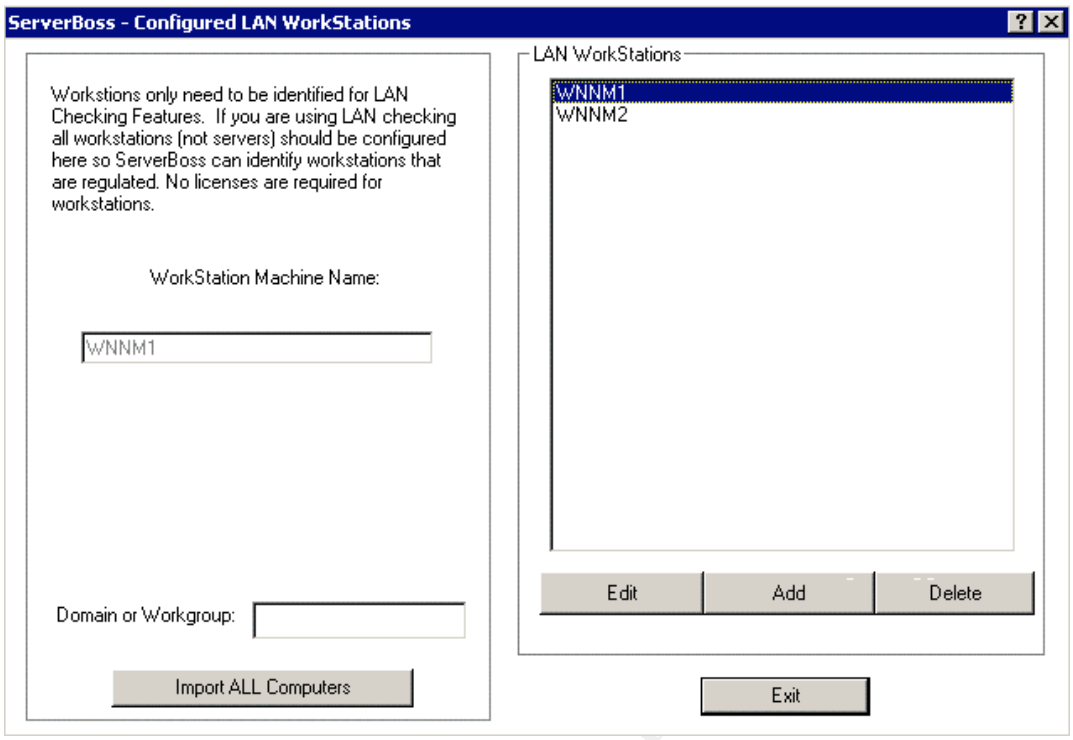

Figure 21: ServerBoss Managed Workstations Screen

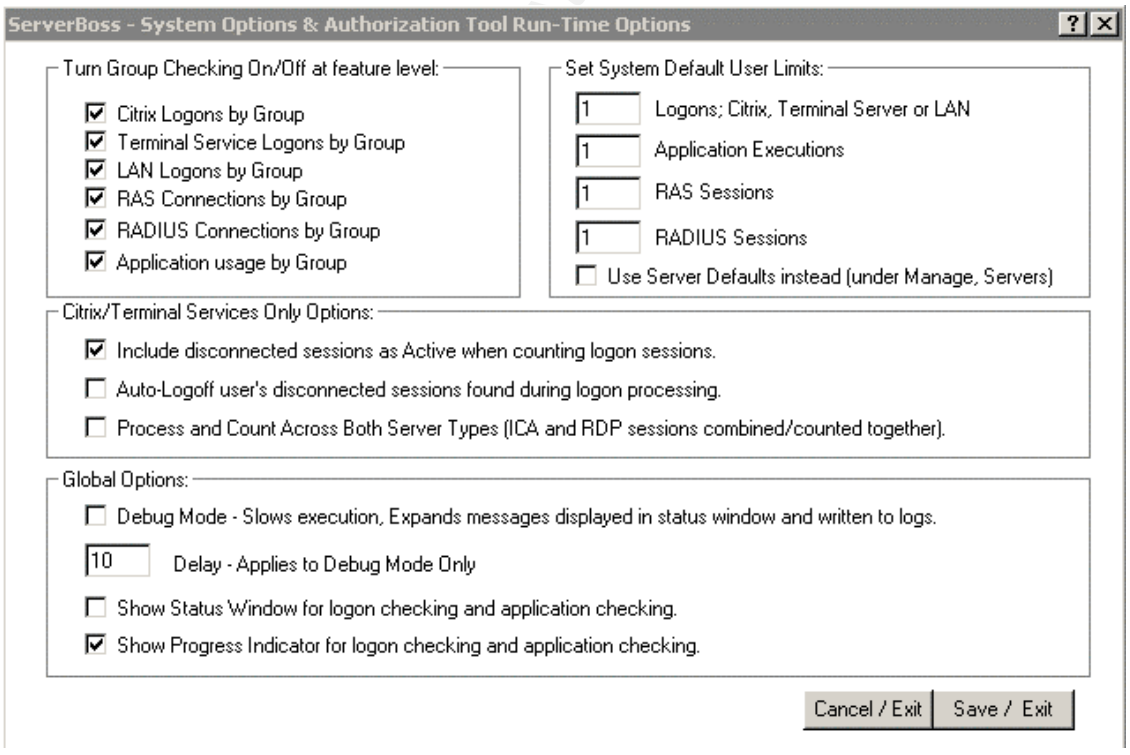

Figure 22: ServerBoss Default System Options.

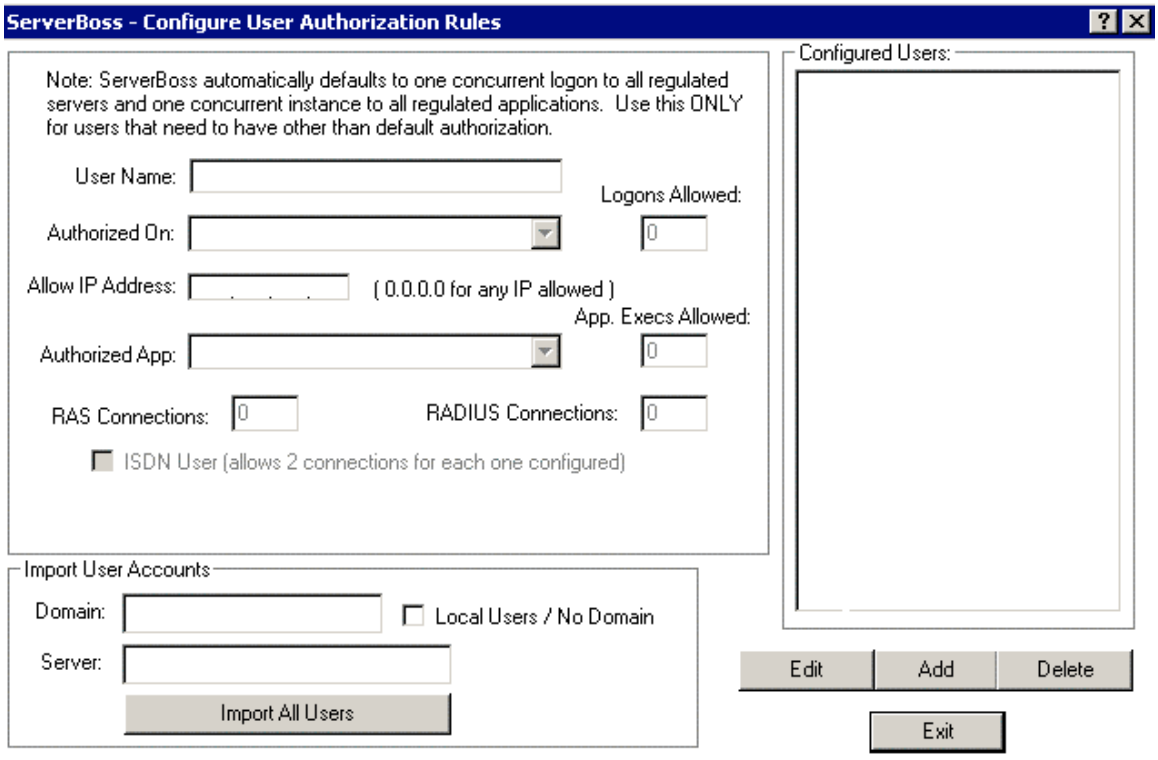

Figure 23: Configure User Authorization Rules Screen

The option to manage LAN Checking, requires installation and configuration of the SBSetup.exe on each managed workstation. ServerBoss authorizes users in the following order:

1. Total sessions for the server.
2. IP address restrictions (Citrix and Terminal Services only).
3. User restrictions (counts user sessions on all managed servers).
4. Group restrictions (counts group sessions on all managed servers).

On each managed workstation, you must run SBSetup.exe from the ServerBoss share folder on the ServerBoss server. Check the box next to the feature sets you wish to support (See Figure 24) on the workstation and click Add/Update Support to add the feature set. If you are authorizing logons to Windows NT/2000/XP based workstations, you need not be concerned with LAN sessions to the servers and no further configuration is required.

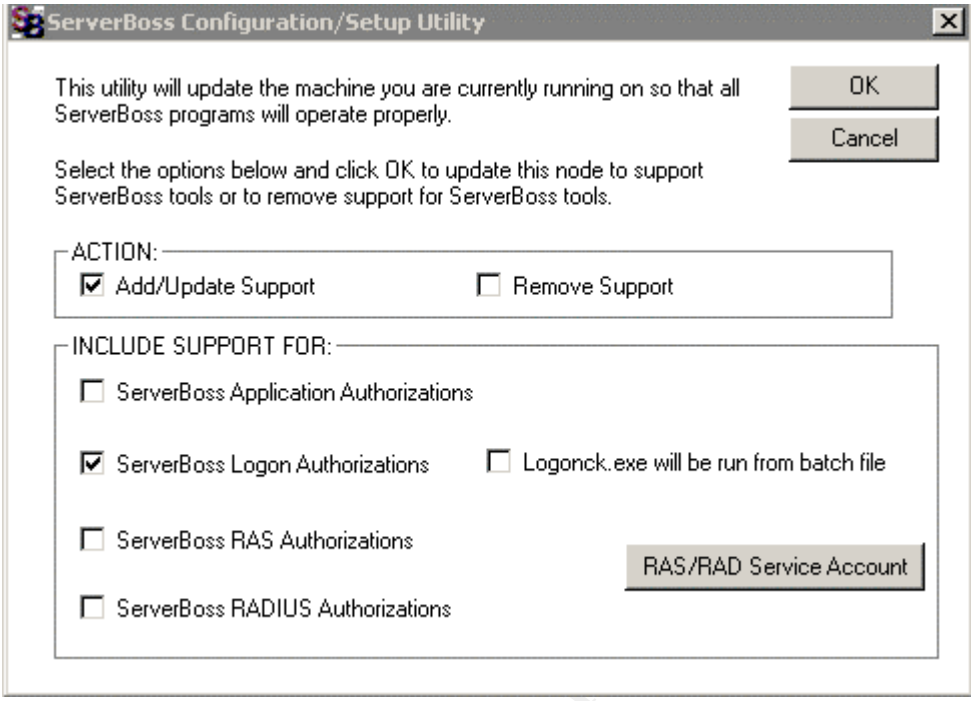

Figure 24: SBSetup.exe Configuration Screen

When SBSetup.exe is run on an NT/2000/XP based workstation, it automatically configures the workstation to run logonck.exe after authentication and before any login scripts are run (unless you check the Logonck.exe will be run from a batch file checkbox when running SBSetup.exe → this is required to support Windows 95/98/Me workstations – for our purposes, Windows 95/98/Me workstations will not be considered due to their inherent lack of security). This is done by adding the logonck.exe program to the Userinit value of workstations registry at the HKLM/Software/Microsoft/WindowsNT/CurrentVersion/Winlogon key. This allows the program to run before the Windows NT/2000 shell loads. Once SBSetup.exe is installed on a workstation, ServerBoss immediately begins logon restrictions based on the configurations you have setup. If a user tries to logon to multiple workstations, they are prompted as shown in Figure 25 and immediately taken back to the Windows Ctrl+Alt+Del logon screen.

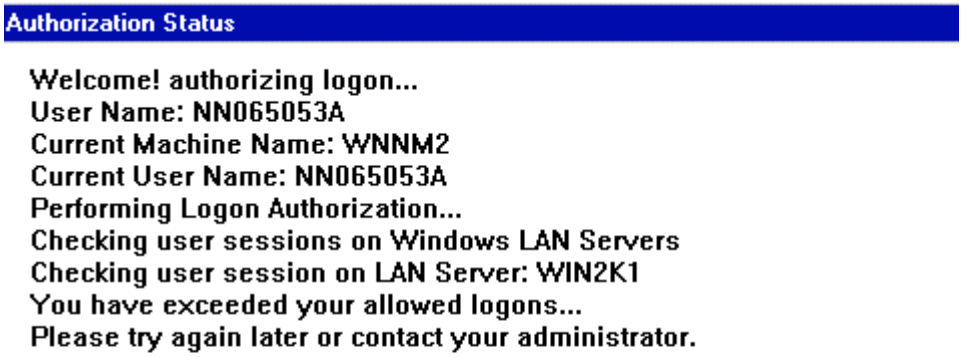

Figure 25: ServerBoss Logon Denied Message

Overall, ServerBoss is a very capable product. However, an important area of concern exists with using ServerBoss and LAN Checking. The LAN Checking in ServerBoss is based on User sessions on the network. In many cases, there are multiple LAN sessions for one user under normal use of a LAN workstation, especially on domain controllers. In Windows 2000, to check what sessions are in use on a server during a normal user logon, right-click on My computer, then select Manage, go to System Tools.. Shared Folders..Sessions and there will be a listing of all LAN sessions for users connected to the server. In Windows NT, run Server Manager and double-click on the appropriate server and then click on the Users button to see a list of all the sessions in use. As shown in Figure 26 below, it is normal for one workstation to use 2 or more legitimate LAN sessions on a server. If you set the ServerBoss restrictions to one concurrent session on the server, you could severely impact a user's abilities to connect to the appropriate resources that they need. Therefore it is recommended that you not set the Sessions restrictions on your servers and just enforce it through workstation restrictions.

Multiple session connections to the server also affect how ServerBoss administers improper logoffs (such as a power failure). If a workstation loses power while a user is logged on, the server sessions eventually time out and are removed from the server. However, the user will not be able to logon to another workstation until those sessions timeout. This usually takes a minute or two. Once the sessions time out, then the user will be able to log back onto the network. ServerBoss does not have a method to reset a users session count back to zero to allow a user to log back in quickly. In an emergency, the ServerBoss admin console could be used to increase the users logon session so that they can logon, but this has the drawback of affecting all users on the network.

ServerBoss also suffers from the same problem that Cconnect has whereby a knowledgeable user could edit the registry and disable the product. As always, access to registry editing tools should be restricted to administrators only. Also, please note that ServerBoss contains a myriad of different options for the administrator to choose from and that setup can be confusing. The first test install I performed, I managed to lock myself out of logging onto my domain controller as an administrator. I was able to correct the situation by logging into a workstation and running the ServerBoss.exe from the network share. Administrators are suggested to fully read the installation instructions and options available on ServerBoss's web site and the Help files available with the product. Pricing for ServerBoss is based on a ServerBoss Base License fee of $345.00, with additional charges for options (LAN Checking - $245.00) and number of servers (1-10 Servers - $245/server with discounts for more) and number of workstations (1 – 50 workstations - $25/workstation with discounts for more) (ServerBoss web site – http://www.serverboss.com/orders/secure/order.asp)

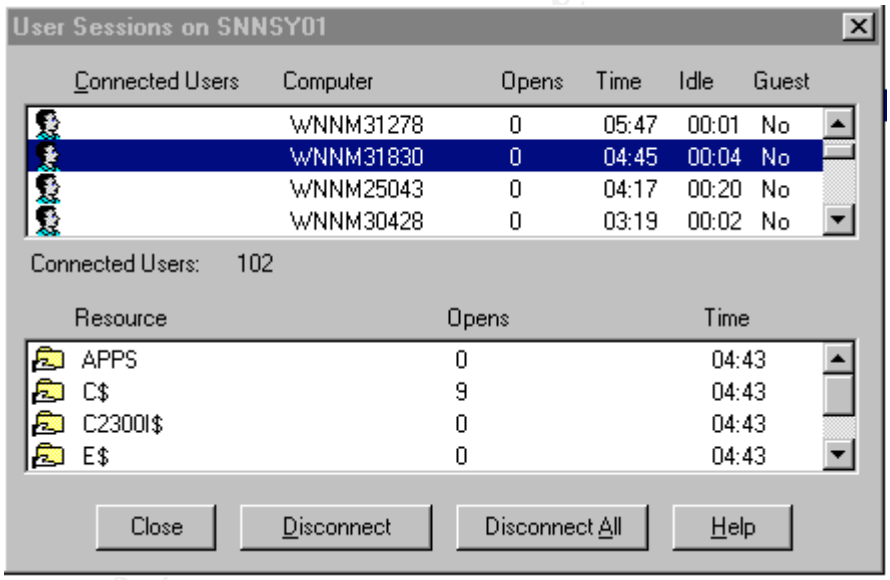

Figure 26: Multiple User Sessions on a Server

Conclusions:

We have looked at several different methods for implementing concurrent logon restrictions in a Windows NT/2000 network. All the methods included in our evaluations are capable of implementing a concurrent logon policy for your network. Logon Script methods, although the least expensive method evaluated, will work, but will require extensive preparation and testing on the part of the administrator and are not always foolproof. Cconnect, Microsoft's solution to the concurrent logon problem, is a capable product, but it has some severe security

flaws in its design. Namely the SQL Server account and password storage in clear text on each workstations registry. It also does not handle improper logoffs (such as a power failure) very well and requires administrator intervention to correct. UserLock and ServerBoss, the two 3rd party products reviewed are both very capable and elegant solutions the concurrent logon problem. Based on the installation and testing of these products, I would have to give my vote to UserLock as the preferred product for implementing concurrent logon restrictions on my network. The program installs very easily and automatically installs on workstations without administrator intervention (ServerBoss installations is complicated and requires its agents to be installed manually on each workstation on a network). However, as always, the choice is up to you, the administrator. I hope the evaluations performed here can help you in your decision to choose a method to implement a concurrent logon policy on your network.

References:

1. Brown, Nick, " A Better Way to Prevent a User From Logging on More Than Once." Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks – Tip 296. URL: http://www.jsiinc.com/SUBA/tip0200/rh0296.htm.

2. Brown, Nick, "NTNAME – A program to enforce one-logon-per-user." NTNAME.txt download from Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks. URL: http://www.jsiinc.com/SUBA/tip0100/rh0175.htm.

3. Engagent Corporation, "Enforcing Concurrent Logon Policies with UserLock." Engangent Web Site, URL: http://www.engagent.com/products/userlock/userlock_presentation.ppt.

4. Engagent Corporation, "UserLock – Details." Engagent UserLock Product Information Web Page, URL: http://www.enagent.com/products/productsinfo.asp?product=UserLock.

5. Engagent Corporation. "UserLock 2000 Technology Presentation." EngageNT Web Site, URL: http://www.engagent.com/Products/productsinfo.asp?product=Userlock&link=Technology+Presentation

6. "How can I build a file of all currently logged on UserNames?." Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks – Tip 595. URL: http://www.jsiinc.com/subb/tip0500/rh0595.htm.

7. Microsoft Corporation, "Cconnect.exe Version 1.2 Con-Current Connection Limiter Client and Administrator." Microsoft Windows 2000 Resource Kit CD-ROM, Cconnect folder.

8. Microsoft Corporation, “How To: Create a System Policy Setting in Windows 2000.” Microsoft Knowledge Base Article – 318753, October 26, 2002, URL: http://support .microsoft.com/default.aspx?scid=kb;en-us;318753.

9. Microsoft Corporation, “How to Determine from Which Computer a User Logged On.” Microsoft Knowledge Base Article – 175062, August 9, 2001, URL: http://support .microsoft.com/default.aspx?scid=kb%3Ben-us%3B175062.

10. Microsoft Corporation, “How to Set Up Locally-Based System Policies.” Microsoft Knowledge Base Article – 168579, August 9, 2001, URL: http://support .microsoft.com/default.aspx?scid=kb;EN-US;168579.

11. Microsoft Corporation, “Local Logon Process for Windows 2000.” Microsoft Knowledge Base Article – 231789, October 10 , 2002, URL: http://support .microsoft.com/default.aspx?scid=kb;EN-US;231789.

12. Microsoft Corporation, “SMB Traffic During Windows NT Domain Logon.” Microsoft Knowledge Base Article – 139608, February 6, 2002, URL: http://support .microsoft.com/default.aspx?scid=kb;EN-US;139608.

13. Microsoft Corporation, “Whitepaper - The Essentials of Replacing the Microsoft Graphical Identification and Authentication Dynamic Link Library.” Microsoft Knowledge Base Article – 810756, December 6, 2002, URL: http:// support .microsoft.com/default.aspx?scid=kb%3Ben-us%3B810756.

14. “NT Admin Tip #331: Restricting Concurrent Logins.” Wayne’s Windows Administrator Support Site for Windows NT/Windows 2000/Windows XP/Penetration Testing/Firewalls. URL: http://is-it-true.org/nt/atips/atips331.shtml.

15. “Prevent Simultaneous Logins in Windows 2000.” ExpertsXexchange. May 24 2002. URL: http://www.experts-exchange.com/Operating_Systems/Win2000/Q_20304249.html.

16. “Prevent Users From Logging on More Than Once.” Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks – Tip 175. URL: http://www.jsiinc.com/SUBA/tip0100/rh0175.htm.

17. “PsLoggedOn freeware tells you who is logged onto a computer, or it can locate a user.” Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks – Tip 4712. URL: http://www.jsiinc.com/subj/tip4700/rh4712.htm.

18. ServerBoss, “Installation for Logon Authorization on Citrix MetaFrame/WinFrame Servers, Windows Terminal Servers and LAN Servers.” ServerBoss Web Page, URL: http://www.serverboss.com/installation/logon.htm.

19. ServerBoss, “Logon Checking – Citrix MetaFrame and WinFrame Servers, Microsoft Windows Terminal Servers and LAN Servers.” ServerBoss Web Page, URL: http://www.serverboss.com/features/logon.htm.

20. ServerBoss, “ServerBoss Installation Overview.” ServerBoss Web Page, URL: http://www.serverboss.com/installation/overview.htm.

21. ServerBoss, “ServerBoss Tips and Info on Common Issues.” ServerBoss Web Page, URL: http://www.serverboss.com/support.htm.

22. Smith, Randy Franklin, “Access Denied.” Security Administator. May 2001. URL: http://www.ntsecurity.net/Articles/Print.cfm?ArticleID=2055.

23. Smith, Randy Franklin, “Top 10 Security Tools in the Win2K Server Resource Kit.” Windows 2000 Magazine December 2000 (2000): 85 –91.

24. “Where is UserName logged on from?.” Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks – Tip 981. URL: http://www.jsiinc.com/subb/tip0900/rh0981.htm.

25. “Where is <UserName>?.” Windows NT/Windows 2000/Windows XP/Windows .Net Tips and Tricks – Tip 3438. URL: http://www.jsiinc.com/subg/tip3400/rh3438.htm.

Last Updated: September 22nd, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive