Global Information Assurance Certification Paper

The Basic Steps to Securing Windows 2000 Terminal Services And Citrix MetaFrame XP

Abstract

In today's ever evolving business environment, Information Technology managers are continually looking for ways to improve user access, reduce costs and tighten security. Business requirements are fostering the need to provide a full anytime, anywhere access scenario. Additionally, in an effort to reduce equipment costs, companies are searching for ways to reuse old equipment, or to extend the life of existing end of life cycle technology. Many companies are turning to the thin client environment and Microsoft and Citrix MetaFrame software products. The focus of this paper will be on securing this environment from the ground up.

From the Ground Up

Before delving into ways to secure Terminal Services and Citrix MetaFrame, it is imperative to note an often-overlooked aspect of protecting this environment. You can encrypt all data and transmissions, provide the highest levels of authentication, physically lock away resources and tweak permissions and controls to harden the system, but if you have a user who logs onto your network from home, then leaves the session unattended, then all may be for naught. My point? Ensuring users are aware, educated and held accountable for their actions is extremely important. This can be the hardest variable to control, but a well thought out training strategy coupled with acceptable use agreements and a solid auditing program will go a long way in mitigating this risk.

Securing the Hardware

Obviously, it is important to physically secure the hardware housing your remote access implementation. All the hardware should be maintained in a controlled environment to ensure direct unauthorized access is not possible. Restricted access and distribution of access control can be effectively used to limit the extent of an individual's ability to damage valuable data resources. Ultimately, this control will be determined by the size of the organization and the willingness of management to support a distributed administration environment. Other steps that can and should be taken include locking server racks with each rack using a different key. Enforcing log out requirements on the servers as well as maintaining and managing change control logs are also valuable steps in protecting your environment.

Preparing for Citrix Installation

One key to successfully deploying a secure Citrix environment is to ensure the operating system is properly secured. There are basic steps in configuring

Windows 2000 systems that are crucial to ensuring a secure MetaFrame environment. A very important consideration in securing the environment is where to install the operating system. In the case of a Terminal Server and MetaFrame installation, it is extremely important that the solution is not installed on any type of domain controller. Domain controllers are critical to the operation of a Windows network and control how it operates. Installing Terminal Services and MetaFrame could jeopardize the network due to the fact that a user logging on is essentially logging onto the console. Even in a completely secure environment this is unadvisable.

Use NTFS

One of the strengths of the Windows 2000 security model is the ability to use NTFS file permissions. Ensure that during the operating system installation, the NTFS file format is selected. NTFS provides the necessary granularity to allow administrative control of system resources. Users logging onto a Terminal Server/MetaFrame environment log onto the console. Without the ability to lock down file and folder access permissions allowed by NTFS, users could potentially access and delete critical system files. Once the operating system is installed, a determination needs to be made as to what should be locked down. A good place to start is your system drive. Take a look at the program files in the system folder and restrict access to administrators and system. Occasionally files are needed to operate logon scripts and other tools, so be sure to test the system once the files are secured.

Arp.exe	ipconfig.exe	netstat.exe
At.exe	net.exe	ping.exe
Atsvc.exe	nslookup.exe	qbasic.exe
Cacls.exe	posix.exe	rdisk.exe
cmd.exe	rcp.exe	regedit32.exe
debug.exe	regedit.exe	route.exe
edit.exe	rexec.exe	runonce.exe
edlin.exe	rsh.exe	syskey.exe
finger.exe	secfixup.exe	tracert.exe
ftp.exe	telnet.exe	nbtstat.exe
xcopy.exe		

Table 1. Files recommended to be secured

To help keep track of what you've locked down and to simplify the procedure for future installations, take a look at the .inf configuration file and Terminal Services security guide provided by the National Security Agency. The file and security guide can be found at http://nsa1.www.conxion.com/win2k/download.htm. Be aware however, that it is not recommended that you apply any configuration file without first testing it. This file is a good starting point. The configuration file can be edited in two ways, you can open the file using a text editor such as notepad, or you can utilize the Microsoft Management Console (MMC)(See Figure 1).

Either way works, however it is much easier to use the MMC until you become familiar with the settings. Using the MMC you can open the configuration file and make the necessary changes to support the security level in your environment. The NSA configuration file is very locked down and may cause problems if it is not thoroughly tested prior to use. This file allows the configuration of Account policies such as the Password policy, Account lockout policy, and the Kerberos policy. It also can be used to configure local policies such as the Audit policy, User Rights Assignment and the Security Option, and the Event log policies. Additionally, System Services, Registry and File System permissions can be set up and maintained in this file. Once created, the file can then be reused to ease the rollout of additional MetaFrame servers.

Account policies

It is recommended that standard industry guidelines be followed in establishing lockout thresholds. Some of these include maximum password age 60-90 days, minimum password age at least 1 day, password length 6-8 characters, and the enabling of password complexity requirements. Account lockout threshold should be maintained at 3-5 attempts.

Local policies

Under local policies are all the settings for establishing audit requirements. As a minimum, auditing should be turned on and logon success and failure events should be monitored. There are a number of items under user rights assignment, but as a basic starting point the following should be managed: Access the computer from the network, load and unload device drivers, log on locally, manage audit and security logs, and shut down the system. Obviously accessing the computer and logging on locally would be required for all users, generally you would want to restrict loading and unloading of device drivers, managing audit logs and shutting down the system to administrators. The last area of consideration in local policies is the Security options. Under this tab some of the key items are additional restrictions for anonymous connections, disable CTRL+ALT+Del requirements for logon, Do Not Display Last user name in logon screen, the message text for users attempting to logon, message title for users attempting to logon, renaming the administrator account, and renaming the guest account. Some of these are just good security practices. Disabling CTRL+ALT+Del requirements for logon should be disabled. What you effectively want is that users are required to use the CTRL+ALT+Del combination to log on to the system. Disabling this function enforces this requirement. Do Not Display the last user logon name is important especially for users that are accessing your system remotely. Getting the user name is half the battle for someone trying to gain unauthorized access to your system. Additionally, text messages provided at logon are considered essential in informing users of their responsibility while accessing company resources and in many circles is considered the first step in providing some level of liability coverage.

Registry

The registry is the heart and soul of any Windows environment. It can be used to tweak system settings and fix nagging issues that otherwise cause administrators headaches. By the same token, the registry, if not properly secured can be used to dismantle and cause problems for the MetaFrame environment. Locking down the registry can be tricky in the MetaFrame environment because users are logging on locally, and for many applications need permission to write to specific files and folders. As with many settings, complete testing is necessary to ensure full functionality. To exclude temporary Internet files from being saved in the user profiles open regedit32 and navigate to HKEY_CURRENT_USER\Software\Microsoft\WndowsNT\ CurrentVersion\Winlogon add the value ExcludeProfileDirs as a type REG_AZ and set the string data to the names of the folders you don't want saved, such as Temporary Internet Files. Because user profiles can get large, this change can be useful in saving space on your MetaFrame server. To stop things like Bonzai Buddy, Comet Cursor, etc…create a folder under program files with the name that they create and use security permissions to change the access to everyone none. This should effectively stop these installations from taking place. Keep in mind that the MetaFrame environment is global, these programs can cause huge resource hits against your server, and since they would be installed on the server, this affects all users logging into the system. Again, it cannot be stressed enough that all these changes should be well tested before implementing in a production environment.

Services

Once the operating system has been installed and locked down a review of services should be completed. Standard recommendations are to disable or uninstall unneeded services. Some that should be closely looked at include SMTP, Telnet, FTP, NNTP and www publishing. As always, if you don't need it, remove it as a potential threat to the system. Services configuration can also be managed through the .inf configuration file. Regardless of what services you disable or remove, all configurations should be well documented. The entire process should be written down from beginning to end. This will help in case a reinstallation is necessary, or if a new administrator comes on board. It also makes it easy to update the procedure if OS changes occur, when MetaFrame Feature Releases come out, and to use in trouble shooting the system.

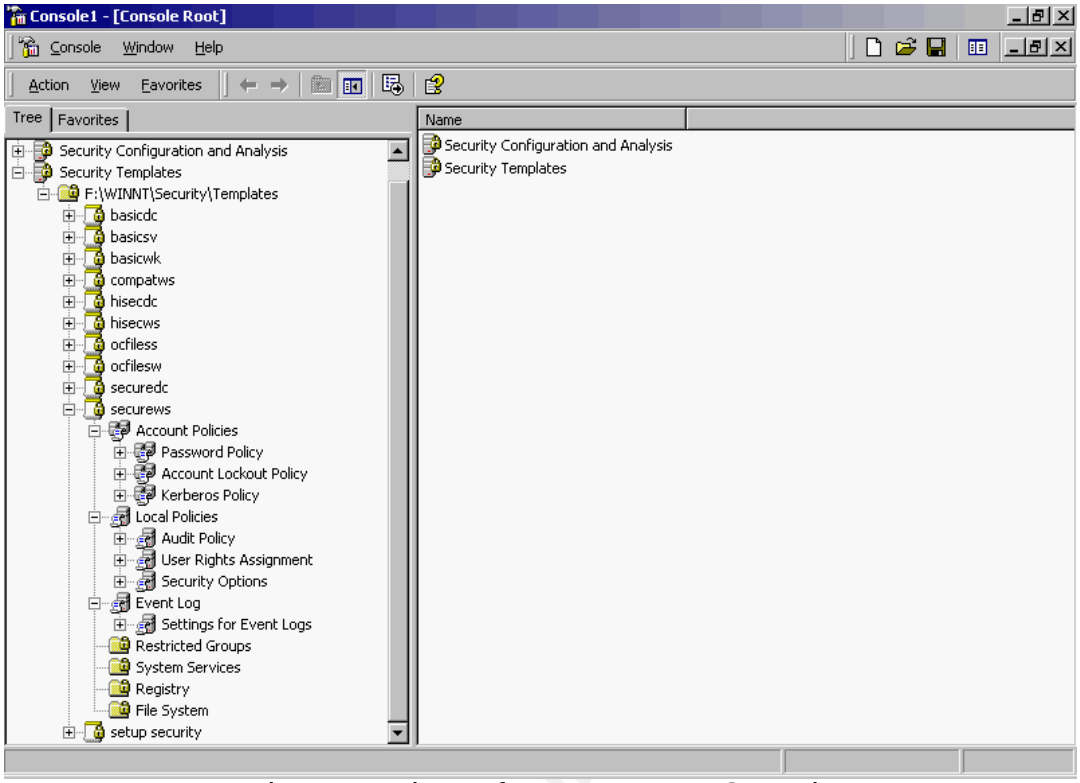

Figure 1. Microsoft Management Console

Hot Fixes, Security Patches and Service Packs.

Inherent to basic security is the upgrading and maintaining of the underlying operating system and the installed applications. Many attacks in recent years have grown from known vulnerabilities being exploited. In many cases these exploits not only have been identified, but software vendors and manufacturers have had patches available to fix the vulnerability. By not applying these fixes, administrators could leave the door open for disaster. Although it is recommended that hot fixes, security patches and service packs be installed, that doesn't mean it should be done without due caution. Testing should be done to ensure that upgrades will not adversely affect the production environment.

Group Policies

If the MetaFrame Farm resides in a Windows 2000 Active Directory environment, there is another tool that can make it much easier to manage security-group policies. Group policies simplify securing the users environment. They can be used to secure the browser (especially if allowing Internet access through the MetaFrame solution), as well as simplifying the lockdown of the users desktop. Depending on your environment and user competencies, it can be advisable to secure areas of the desktop from curious users. Some of the more important lockdowns to consider are the run, control panel access, system shutdown and believe it or not help files.

Run

Run on the start button menu list gives a knowledgeable user access to nearly the entire system. Even if you locked down program files and system directories, a lot of damage can be done from this location.

Control Panel Access

MetaFrame runs on a Windows Terminal Server. The users are logging on as if they are at the console. As such, it is not recommended that users be allowed access to the control panel. Users may try to make changes not realizing that their changes are affecting the entire operating environment for all users. They could also inadvertently damage or impair the capabilities of the system without realizing what harm they had caused.

System Shutdown

This can be a critical and disastrous component in a MetaFrame environment. When a user goes to log off from their session, if they are not aware of the fact that they are actually on the server, they could unintentionally shut down the server. Even an experienced administrator could mistakenly shut down the server instead of logging off. This in effect causes a denial of service situation, even though it done unintentionally.

Help Files

Help files can be useful in solving problems, and in helping users understand the computing environment. At the same time they can be used to access areas that have been removed from user access. Help files can allow access to the command line, to the control panel, and to other areas where system configuration can be accomplished. It is recommended that if help files are not going to be specifically used, that they be removed from the system.

All of the above listed items can be configured using Windows 2000 Group policies. Although it is much more useful in an Active Directory environment, group polices can still be used on the local Win2K/MetaFrame server if you are not currently operating in a native Windows 2000 environment. The biggest drawback is the lack of global control that is allowed through Active Directory. Using group policies in a non-active directory environment requires local management of each server. Although in a large farm this can be tedious, it still allows for a granular depth of security.

Securing Citrix MetaFrame XP

The tedious job of securing the operating system has been completed. Installation of the Citrix application is now in progress. There are several key issues that need to be addressed right up front during this installation. One of these will be shadowing. The shadowing function in Citrix allows someone with the correct access to literally watch another users actions while they are logged onto a session on the server. While this can be a great tool for troubleshooting user problems, it can also be a dangerous liability if not properly administered. "Due to the requirements of customers such as financial institutions, shadowing options selected here are permanent. Once they are chosen, reinstalling Citrix MetaFrame is the only method by which these options can be altered." (Crump, p.86) During the initial installation of MetaFrame, you are asked whether or not you want to use shadowing. If at this point you select no, shadowing will not be installed. Additionally, there is no way to install shadowing at a later date without completely reinstalling the application. Therefore it is imperative to determine before hand if you may want to use the feature in the future. If this is the case, make sure you select shadowing, and disable it in the application until such time that the feature is put into use.

During installation of the MetaFrame application you should have selected "permissions compatible with Windows 2000 users". If not, this can be set up through the terminal server configuration tool. This option is selected for the most secure configuration. If legacy systems are being supported, then the "Permissions Compatible with Terminal Services 4.0" must be selected. Please note that under this configuration all users will have full access to critical registry and file systems locations (see figure 2).

Another important aspect to consider during installation is whether or not you want to change the default drives. Since all your users are logging locally onto the server, it is highly recommended that user profiles and other public access files and folders such as program files, be moved from the default c: drive to another location. During installation, Citrix allows you to reassign drive letters. As a heads up, if you use Symantec Anti-Virus, you may have problems installing it once the drives have been reassigned. This is because by default Symantec installs to the c: drive. If the system is locked down, the install will fail. By using the subst command you can temporarily reassign the drive for the anti-virus installation.

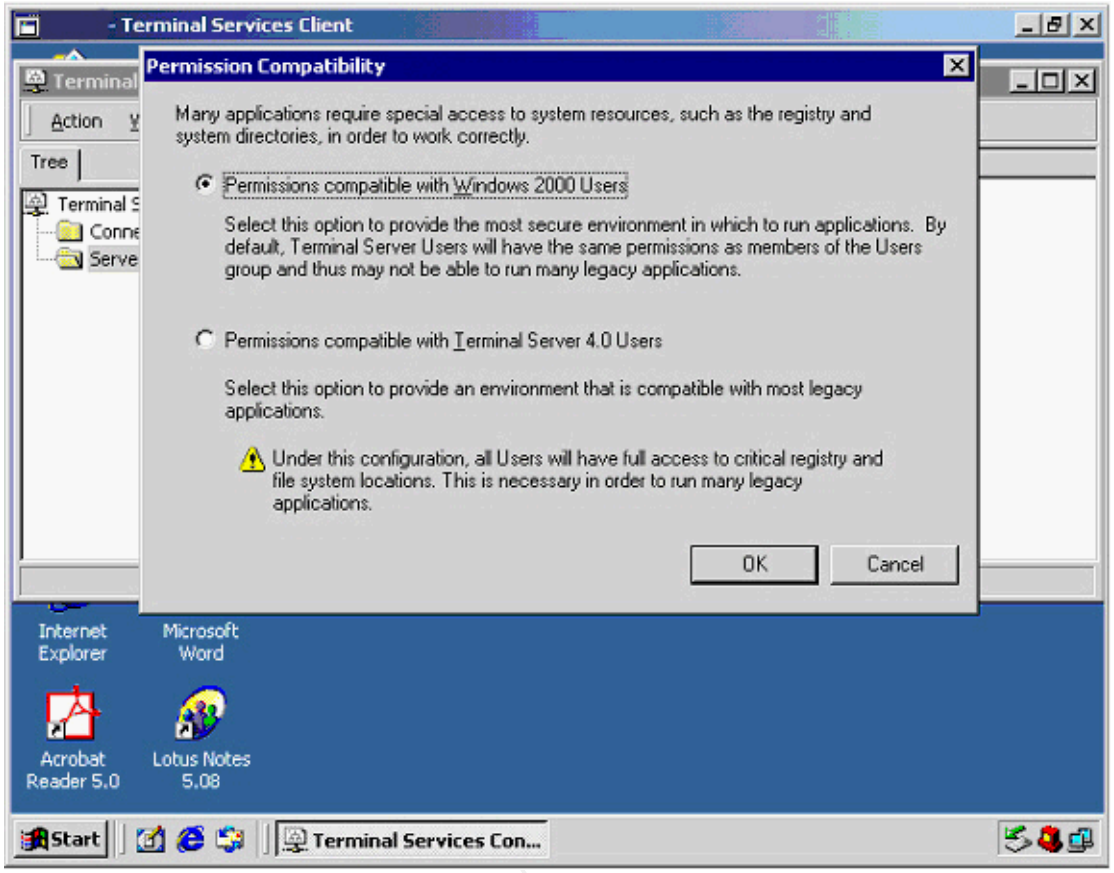

Figure 2. Compatibility Selection

Once you have MetaFrame installed, then comes the task of securing the environment. Depending on how you choose to deploy this could take several different paths. You could choose to publish applications, which then makes management of your server a little easier. You could also publish a desktop. Additionally, if you have a large number of remote users accessing your systems, you could provide access through the Citrix Nfuse web portal. This solution provides 128 bit, secure access through the use of session tickets.

Citrix functionality is provided through the use of the Citrix Independent Computing Architecture (ICA) client piece. This client piece does provide 128 bit protection provided the server side is properly configured. For that reason, this paper will focus on setting up the server environment. If the server is properly configured, the user will have to provide the correct settings to be able to logon to the network.

The first step in configuring your system is to secure the connections once they are established. To do this you need to access the Citrix Connection Manager (see figure 3). Open the connection manager, then right click on the ICA connection and select edit (see figure 4). This will allow you to make changes to the ICA access environment.

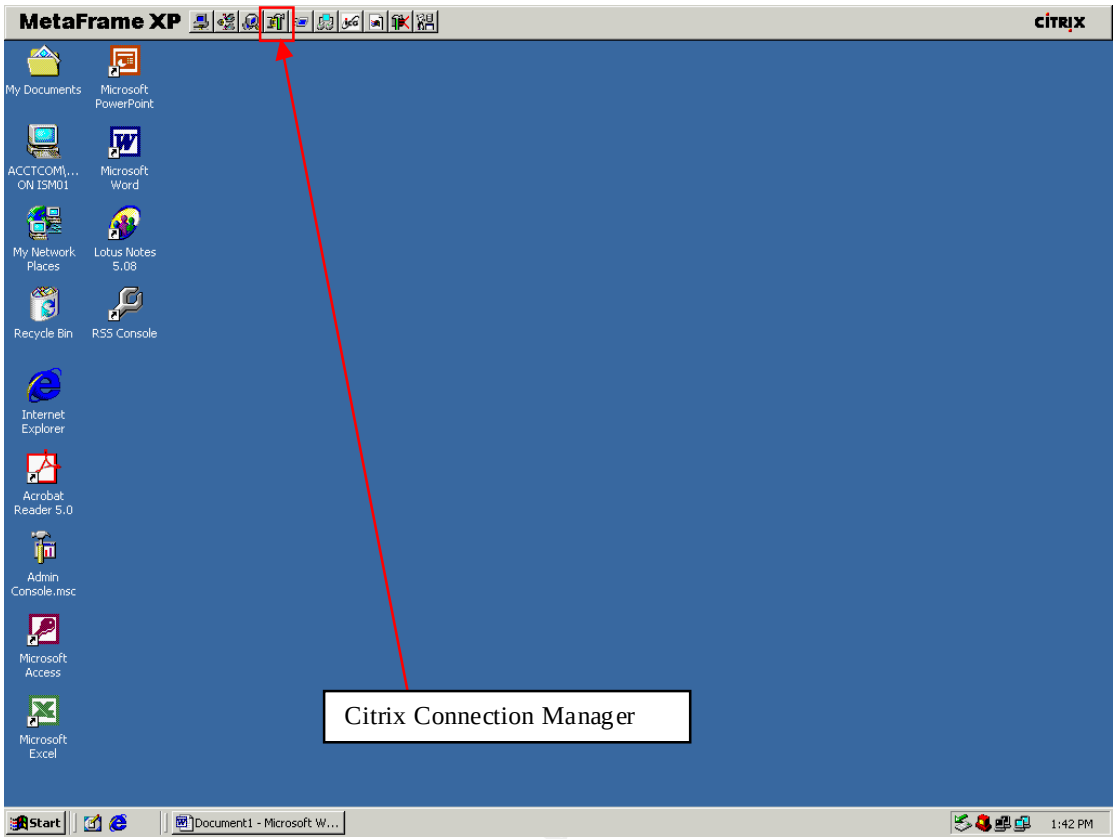

Figure 3. Citrix Connection Manager

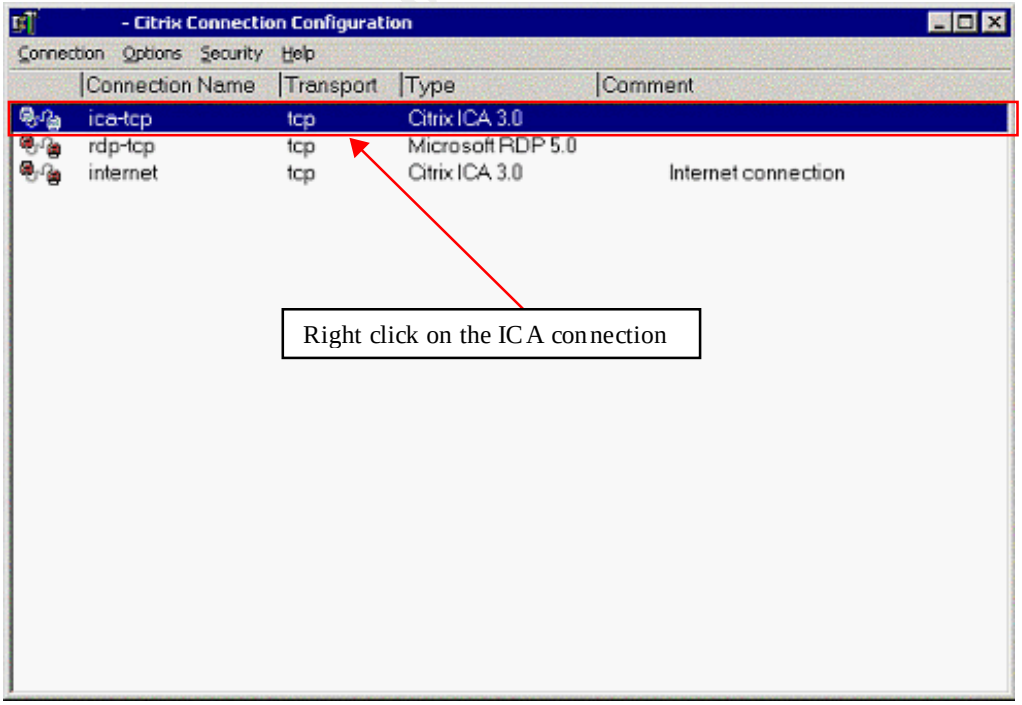

Figure 4. ICA Connector

When the edit connection screen is displayed (see figure 5) set maximum connection count to match your license allocation, and then select the advanced settings button to set the connection settings.

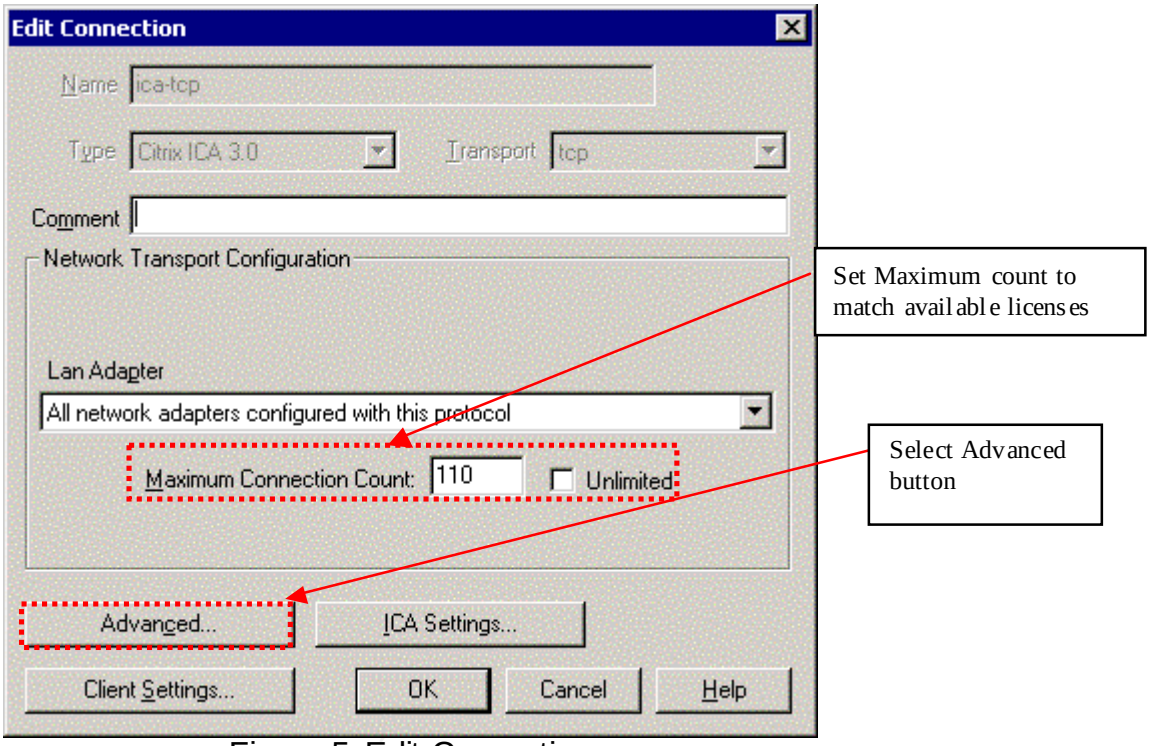

Figure 5. Edit Connection

Under Advanced Connections Settings the following should be set (see figure 6).

1. Logon >enabled –requires the user to logon to your network
2. Timeout settings
   a. Connection>-allows the administrator to control session timeout
   b. Disconnection (time disconnected sessions remain connected)>10 minutes
   c. Idle (time with no activity)>15 minutes
3. Security
   a. Required encryption>RC5(128 bit)-recommended 128 bit
   b. Use default NT authentication>not selected
4. On broken or time-out connection>reset
   a. Reconnect sessions disconnected>inherit user config
   b. Shadowing>is enabled, input on, notify ON-this will notify user if someone begins a shadow session
5. Auto Logon
   a. Prompt for password>selected
   b. Inherit client config>selected
6. Initial Program
   a. Inherit client/user config>selected
   b. Only run published applications>not selected (this will depend on your environment)

7. User Profile Overrides
    a. Disable wallpaper>selected (disabling frees up system resources)
8. Select OK

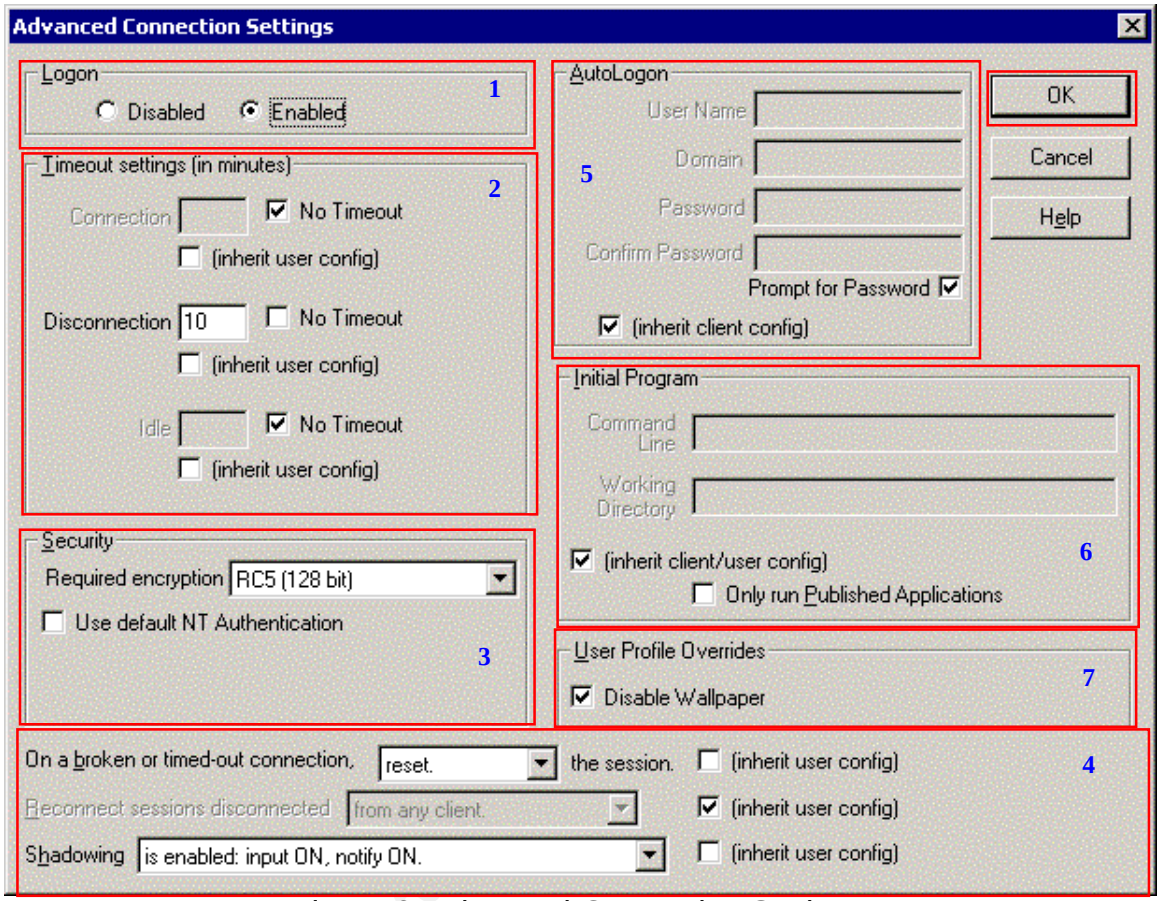

Figure 6. Advanced Connection Settings

Most of these settings will depend entirely on the environment and the discretion of the administrator. Citrix allows a high level of control of your environment. There are more settings under the client button that allow for disabling drive and printer mapping, and also allow for disabling or allowing port mapping and clipboard mapping. These settings should be set appropriate to the environment being supported.

The next consideration is whether or not to manage at the Farm level or at the server level. The advantage of using farm settings for overall settings is that once set all the servers in the farm adhere to the same settings. If there is a requirement for different settings at the server level, this can be accomplished and will only affect the server where the changes were made. To access these settings, you will need to log onto the Citrix Management Console (CMC). Select the CMC button on the Citrix toolbar. Once you get past the splash screen (figure 7), you will see the farm logon page (figure 8).

Figure 7. Citrix Management Console Splash Screen

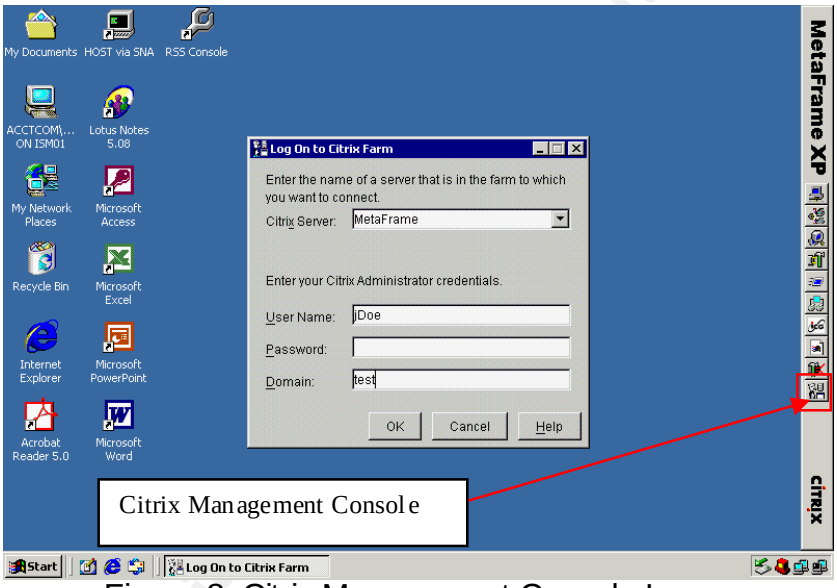

Figure 8. Citrix Management Console Logon

Logon to the farm and you will have access to all the administrative tools to manage farm and server settings. If you right click on the farm level setting ("Your farm" in figure 9) and select properties, you will be able change farm settings.

As seen in Figure 10, administrators can control ICA settings, SNMP, MetaFrame settings, Connection limits, Interoperability and Zones. These basic settings allow overall management of all servers within the farm. Particularly important here are the MetaFrame settings, which allow control of network broadcasting of ICA traffic, and Connection Limits which controls users ability to have more than one open session and allows for logging of over-the-limit denial attempts. In a limited resource environment, these settings will allow administrators to control resources so users have equal access to what is available.

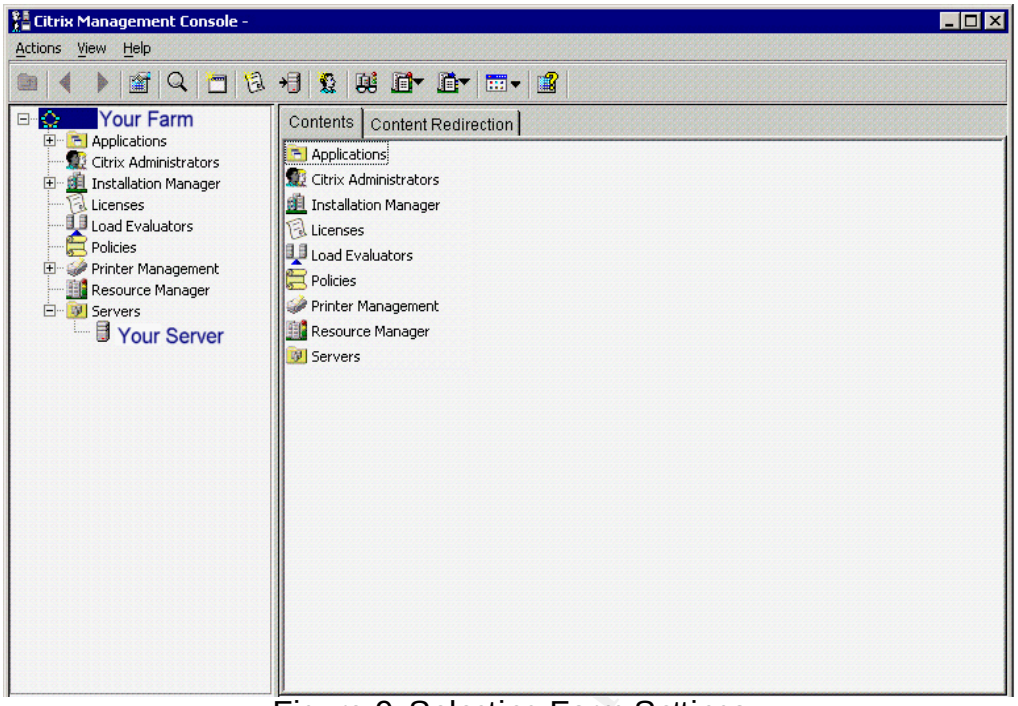

Figure 9. Selecting Farm Settings

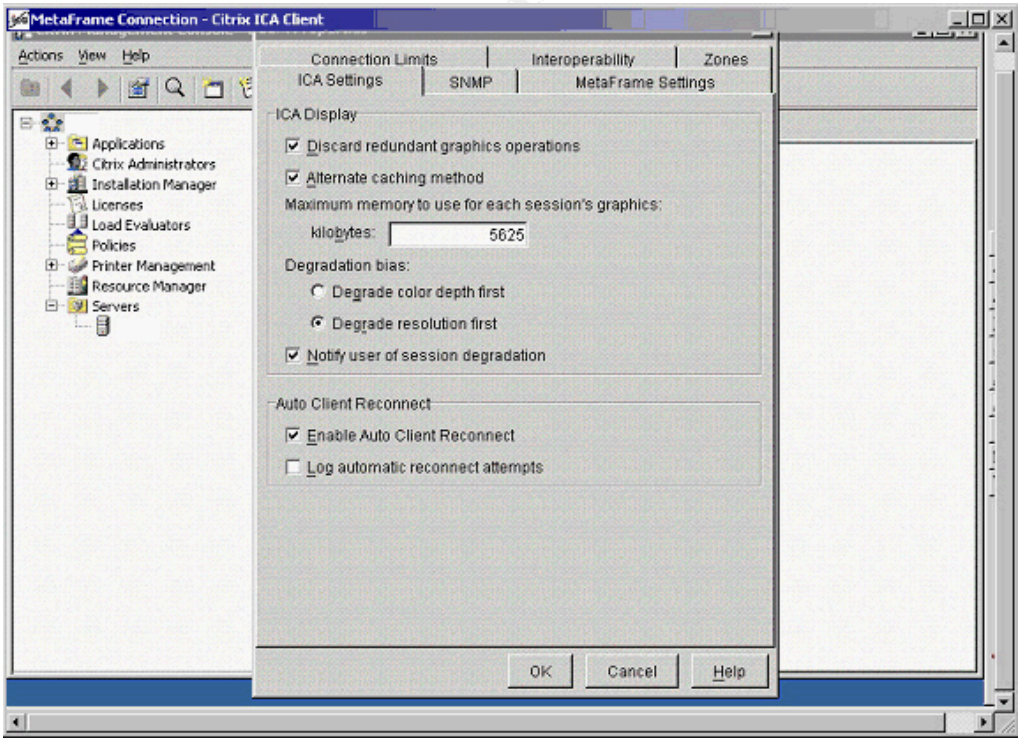

Figure 10. Farm Settings

By selecting a server, right clicking and choosing properties, you have access to similar controls, but are given much more granularity (see figure 11). As can be seen in the picture, the information tab gives particular information about the

selected server. Additional tabs not included at the farm level are Hotfixes, Published Applications, Printer Bandwidth, Metric Summary Schedule, Ignored Processes, Reboot Schedule, and Resource Manager Alerts Recipients. The important ones from a security standpoint are the Hotfixes tab which keeps track of all the Citrix hotfixes installed on the selected server, and the MetaFrame Settings tab which allows or disallows broadcasting, enables logging onto the server, and controls how MetaFrame servers will talk to each other.

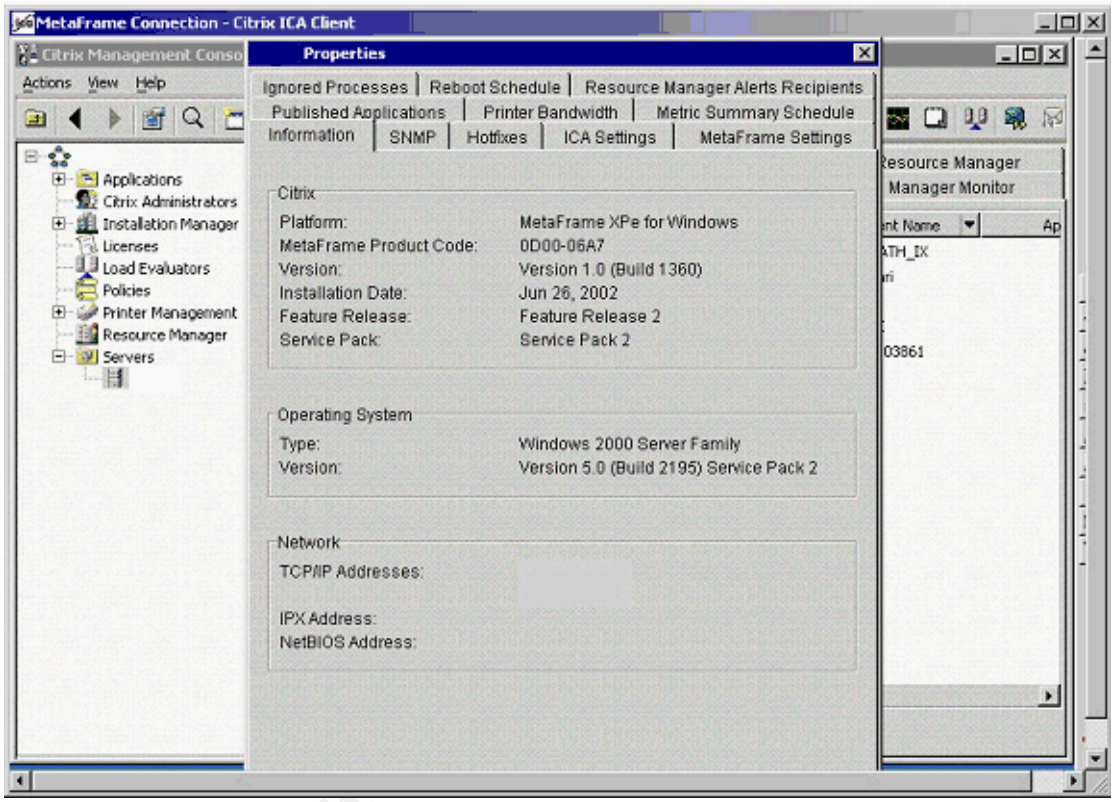

Figure 11. Server Properties

With the release of Feature Release 1 and 2, Citrix has increased options for providing security within the Citrix MetaFrame environment. Specific control of administrators access as well as Resource Manager allow for logging and auditing of all actions taken on the server. Resource Manager will actually track programs opened, who opened them, and when. This can be used to determine when and how problems occur. It will also allow an administrator to monitor what applications users are trying to access.

Other Security Options

Some administrators consider publishing applications as a security measure. Publishing provides no particular security advantage, however, it does help ease management of resources. Access to applications can be published to a particular user and controlled that way.

Citrix also allows for the ability to apply policies within the MetaFrame farm. This allows an administrator to create rules and apply them to specific users and groups of users adding control to the environment. Some of the policies that can be applied include requiring some users to use high encryption, allowing a group of trainees to shadow a supervisor, limit users from performing functions that burden the network, or controlling a specific groups drive and printer mappings. All these policies increase the ability of the administrator to better manage and secure resources.

Conclusion

Although there are many, many more settings and tips on securing a MetaFrame environment, the goal of this paper was to give a basic starting point. The complete lock down of any environment will depend upon what is being supported, and what the corporate environment requires. The primary concern of any administrator should be trying to balance user support and functionality with security and resource management. The Windows 2000 Terminal Server and Citrix MetaFrame environment help provide that secure functional environment while providing administrators a flexible way to manage resources, and at the same time giving users a productive working situation..

References

Madden, Brian S. Citrix MetaFrame XP Advanced Technical Design Guide. Washington DC: BrianMadden.com Publishing, November 2002, Pg 632

Dimaria, Vincent J., Barnes James F., Birdsong, Jerry L., Merenyi, Kathryn A. Guide to Securing Microsoft Windows 2000 Terminal Services Report Number C4-023R-01 July 2001, http://nsa1.www.conxion.com/win2k/guides/w2k-19.pdf January 2003.

Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice. "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations." July 2002. URL: http://www.cybercrime.gov/s&smanual2002.htm#toc. Jan 2003

Smith, Randy F. "Dangerous Services Part 2." December 21, 2000. URL: http://www.secadministrator.com/Articles/Index.cfm?ArticleID=16363 December 2002.

Niser, Paul "Managing Security Hotfixes." June 24, 2002. URL: http://www.winnetmag.com/Articles/Index.cfm?ArticleID=25316

Harwood, Ted. Inside Citrix MetaFrame XP. Boston: Addison-Wesley, July 2002, Pg 440-442

"Citrix Expands the Capabilities of MetaFrame XP for Windows with Key Performance and Security Enhancements." May 20, 2002. URL: http://www.citrix.com/press/news/releases/20020520_expands.asp December 2002

Crump, Ralph. Guinn, Travis. Luchtefeld, Craig. Et. Al Citrix MetaFrame XP for Windows Administrator Study Guide. California: Osborne McGraw-Hill, 2001, Pg 86

Last Updated: July 27th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event