# BCTC Computer Admin Rights Tutorial

## Administrator Access to Bluegrass District Computing Resources

The purpose of this tutorial is to provide information to members of the Bluegrass Community & Technical College faculty and staff who need administrator access to workstations about the additional risks that are involved, as well as proper procedures to follow if administrator access is approved.

In addition to this material, you should also become familiar with the KCTCS Administrative Policy 4.2.5 that governs access to and use of KCTCS computing resources, as well as the BCTC ITS technology usage guidelines. The BCTC ITS department manages and is responsible for the institutional assets and security of the BCTC network.

At the end of this tutorial, there will be a mastery exam for you to demonstrate knowledge of this material, including the risks associated with administrator access and the proper procedures to follow to minimize them.

## Alternatives to Administrator Access

The main reason that most people require administrator access to their workstation is the need to install software applications, updates, patches, utilities, etc. Before you apply for administrator access you should consider three other alternatives that reduce the risk of exposure of your workstation to malicious acts.

The first option is to contact the ITS group and have them complete the installation or updates for you. This would reduce the amount of time that the workstation has an administrator logged on to it. ITS has the ability to complete these tasks after hours so that it would also minimize the amount of time that the workstation is unavailable for productive use.

The second option is to have ITS install VMWare or Virtual PC for you. These applications provide a virtual operating system environment that will allow you to install applications and updates at the Virtual Machine (VM) level without affecting or exposing the actual operating system on your workstation.

The third option is to request a temporary grant of administrator access to your workstation for a short period of time. This would allow you to apply the necessary updates, but reduce the exposure of your workstation in administrator mode for longer periods.

It is important that you consider these alternatives prior to pursuing a longer term administrator access to your workstation.

## Information about Administrator Access

Bluegrass Community & Technical College has local area networks installed in classrooms, offices, labs and other facilities that connect to the statewide KCTCS network, as well as the Internet. As you probably know, these networks are constantly being exposed to malware, which is a generic term for viruses, worms, spyware, trojan horses, and other forms of malicious programs. College campuses historically have been a prime target for these types of programs. The different categories of malware will be discussed later on in the presentation.

In order to protect the network from malware, a number of precautions have been taken at the KCTCS system level and at the BCTC level for security purposes. Additionally, each user has been assigned limited user account access, which is the access level recommended by Microsoft for its Windows XP users.

In certain circumstances, users may require a higher level of access in order to install new programs, add special utilities, or perform other tasks that are not available at the limited user account level. Along with that higher level of access comes a higher level of risk.

Access to an administrator account by a malevolent person or program can do considerably more damage than access through a limited user account. Therefore, it is important that all users with administrator access follow proper procedures to minimize this exposure.

## Use of the Administrator Account

The most important requirement is that you only use your administrator account when absolutely necessary.

You will be provided with a limited user account that should be your primary account for e-mail, web browsing, desktop applications, and other daily uses. You should only log on to your administrator account when you need to perform a task that is not permitted by your limited user account. You should then complete the necessary action, and immediately log off your administrator account.

It is important that you do not use your administrator account as your primary account since this exposes your computer and the network to more risk.

You should also make sure that the application or utility that you are installing is safe. There are a large number of shareware and freeware applications that are available on the Internet, and some of them contain malware. If you are not sure if the vendor of the application is a reputable one, please contact the ITS group for assistance.

The following pages contain more detailed information related to the use of a workstation in a networked environment. It is important that you familiarize yourself with this information before you use your administrator account. This information will also be covered in the mastery examination at the end of the presentation.

## The RUNAS Command (Run As)

The **RUNAS** command allows you to execute a program under a different user ID from the one currently logged into the workstation. This is particularly useful if you want to run a program or perform a task that requires administrative rights, but do not want to log out to do it.

The abbreviated syntax of the **RUNAS** command is as follows:

**RUNAS /user:***username ProgramName*

When run, it will prompt you for the password for the account you specify, and then execute the specified program with that account's privileges and access. Most common administrative functions can be performed with the **RUNAS** command, and it can greatly reduce the amount of time you might need to spend logged in as an administrator.

When using **RUNAS**, the *username* would be your administrator account name followed by the @ symbol and your workstation name. So for example, if your administrator account name was BLC-BSMITH and your workstation was BLC-BSMITH050, you would put use BLC-BMSITH@BLC-BSMITH050 as your username.

## RUNAS command examples

If you wanted to invoke the Add/Remove Programs control panel item with your administrator account, you would run:

```
RUNAS /user:BLC-BMSITH@BLC-BSMITH050 appwiz.cpl
```

On the other hand, if you wanted a command prompt instead, you would run:

```
RUNAS /user:BLC-BMSITH@BLC-BSMITH050 cmd
```

This will give you a command prompt on the screen, and anything run from it will execute with administrative privileges. This can be supremely handy if you have several operations you need to perform in a row, but it can also be hazardous if you type a command meant for a regular command prompt. It's best if you do something to distinguish this command prompt as special, if not dangerous. Fortunately, the CMD command allows you to specify a title and background color when you run it. For example, this set of options for the CMD command:

```
"cmd.exe /k Title ***Administrator Prompt*** && cd c: && color 4F"
```

will give you a command prompt titled ***Administrator Prompt***, sitting at the root of C: with a red background. In actual practice, the full command you would type then would be:

```
RUNAS /user:BLC-BMSITH@BLC-BSMITH050  "cmd.exe /k Title ***Administrator Prompt*** && cd c: && color 4F"
```

Obviously, when you reach this point, it's a good candidate for a batch file.

## Things you can do, but should not. Ever.

Capability does not imply permission. There are several things you can do with your administrator account that you should not do. This includes, but is in no shape or fashion limited to:

- Uninstalling or disabling the anti-virus software on the workstation

- Uninstalling or disabling any component of the system management software, including the Altiris Agent, Altiris Client and CarbonCopy.

- Modifying the password of the local Administrator account on the workstation.
- Creating additional accounts on the workstation.
- Creating or modifying shared folder settings on the workstation.
- Installing or running any sort of network surveillance or monitoring tool.
- Installing or running any sort of server service.

This is by no means a comprehensive list. If you aren't sure what you are about to do is permissible or not, ask an ITS representative.

## What is Malware?

Malware is short for malicious software and is typically used as a catch-all term to refer to any software designed to cause damage to a single workstation, server, or computer network, whether it's a virus, spyware, or other malicious software application. Malware typically performs one of several unwanted functions. It either destroys or modifies data on the workstation's hard drive or a network drive, or it attempts to find information such as passwords, credit card numbers, and other confidential data and transfer it back across the network to its creator.

Since the workstations and servers in the Bluegrass Community and Technical College contain sensitive data, it is important that we protect that data from being destroyed or compromised.

## What about SPAM?

Other types of malicious programs generate spam, which are unwanted e-mails. These programs accomplish this by obtaining e-mail addresses from your e-mail directory and sending out one or more e-mails periodically in order to propagate themselves or just to annoy the recipient. In most cases, the sender is unaware that they are transmitting spam unless they are notified by the recipients.

Although most spam is annoying, it can also be used to inadvertently disclose sensitive data. This type of spam typically represents a legitimate e-mail from a business or organization that needs to verify certain account or password information in order to make sure their data is correct. This process is called phishing. If you respond with the information that they need, it can compromise the security of that business or organization.

When in doubt, contact the business or organization through another method, such as telephone or regular mail, to confirm that they did send the e-mail to you requesting information. Most businesses do not request sensitive data via e-mail.

## Are There Other Forms of Malware?

Other types of malicious programs create what we refer to as denial-of-service attacks. These programs attempt to either flood the network with additional traffic, or to disrupt connections between two or more machines on a segment of the network. When the network becomes saturated with traffic, you will notice that access to file servers, network printers or other shared devices will slow down considerably or, in a worse case scenario, stop altogether. This can also affect your ability to access the Internet, since we use our local area networks as a primary method to get to a point of presence on the Internet.

Unfortunately, these types of programs do not typically exhibit symptoms on the infected workstation. Therefore, you will probably not be aware that your workstation is causing these problems. Later on in the tutorial, we will address how to determine if you are infected with these types of viruses, and how to protect your workstation from becoming infected.

## How Does a Virus on my Workstation Affect the Network?

Bluegrass Community and Technical College has a number of ways that our workstations are connected. Most campus locations use a wired local area network in and between buildings for the purpose of sharing files, printers, and other resources. In some cases, there is also a wireless network installed to allow portable devices with wireless network adapters to interface with the network. The most common protocol for local area networks is called Ethernet, and your workstation is, in most cases, configured to support an Ethernet local area network.

The main campuses in the district are also connected to a wide area network that allows us to share resources with other campuses. This wide area network is typically leased from various telecommunications companies, and allows us to connect to the KCTCS statewide network system. This current standard software for sharing resources within KCTCS is Microsoft Server (either NT, 2000 or 2003). Your workstation is normally configured with the Client for Microsoft Networks software in order to allow you to log on to the district domain, and share resources. You are assigned a user ID and password for this domain.

This network also provides us with a connection to the Internet, so that any workstation on the KCTCS network can access the Internet without having to use an Internet service provider. Most workstations in the district are configured with TCP/IP, which is the protocol required to allow you to access the Internet. Additionally, the network is configured to assign your workstation a unique TCP/IP address, which identifies you on the Internet.

Viruses on your workstation have potential access to a large number of other workstations.

## How Does My Workstation Get Infected With Malware?

The most common method of propagating malware is through e-mail. Most people would guess that surfing the web is the most popular use of the Internet; actually, e-mail is by far the most used application on the Internet. Attachments to e-mail provide the easiest way to propagate malware.

The best method of combating these malicious programs is with a good antivirus program. This software is installed on every workstation by the ITS group and needs to be active and up to date in order to effectively deal with malware. Antivirus software, such as McAfee, contains virus definition files that are regularly downloaded to your workstation via the network. It is important that you do not deactivate or modify the automatic update feature.

In addition to e-mail, using a web browser such as Internet Explorer, Firefox or Opera can expose your workstation to malicious programs. Internet hackers are constantly looking for ways to exploit potential weaknesses in web browsers. Since Internet Explorer is currently the most popular web browser in the Windows environment, it is the biggest target for hackers. For that reason, ITS has installed Firefox on all workstations, and recommends using it as your primary browser to minimize risk from hackers.

## What Other Ways Can My Workstation Get Infected?

When using your web browser, you may encounter a web site that needs a special plug-in in order to process certain text, images or sounds. A plug-in is a special web application that provides additional functionality not available in the basic web browser. An example of this would be Adobe's Acrobat Reader. This plug-in is designed to process Adobe's PDF file format. The installation of plug-ins is another way your workstation can become infected. There are a large number of legitimate plug-ins that are available on the Internet. However, some of these plug-ins are infected with viruses and can cause serious problems. If you are not familiar with the company providing the plug-in that is needed by your browser, it is important that you contact the ITS group to verify that it is legitimate.

Another potential area for problems while using your web browser to access the web is the availability of free programs that can be downloaded from the Internet. Free downloads should be treated like plug-ins. Unless you are sure that the program is legitimate and is being made available by a reputable web site, you should check with the ITS group before downloading and installing it.

## What Can I Do To Protect My Workstation?

Aside from the antivirus program previously mentioned, Windows XP has a built-in firewall that is available to block unauthorized access from the network to your workstation. The firewall is designed to recognize network traffic that are responses to legitimate programs like Internet Explorer and Outlook, but it will block traffic that it does not recognize, and prompt you to let you know that there is a potential threat to your computer.

Similarly, programs that are installed on your workstation may try to transfer data from your workstation across the network to other workstations. If the firewall detects this, it will also prompt you to let you know that this is occurring. It is important that you do not allow programs that are not legitimate network applications to gain access through the firewall, or transmit data from your workstation back across the network. If you are unsure of the legitimacy of programs that are identified by the firewall as needing access to the network, please contact the ITS group.

Lastly, it is important to keep your workstation's operating system and application software up to date. The ITS group uses software called Altiris to download the latest upgrades to your workstation. You should always insure that this process is active and the updates are being applied. The Altiris client should appear as an icon in the Windows XP system tray. If this is not the case, you need to contact the ITS group. Also, if you install applications that require periodic updates, it is important that you check regularly for updates and install them as soon as possible.

## What Other Workstation Issues Should Be Addressed?

Aside from programs that contain viruses, there are also programs that do not work well with key applications used within the Bluegrass Community and Technical College District. One example of this is the Yahoo Instant Messenger product. Although this is a very good product for providing communications between individuals on the Internet, we have unfortunately identified potential conflicts with the Peoplesoft application. Since we use a wide variety of applications in our district, there is a significant possibility that two or more applications may interfere with each other.

## Updating Antivirus Software

McAfee antivirus software is provided for each workstation on the KCTCS network, and is installed, and enabled by default. Normally, each workstation receives .dat file updates on a daily basis on some sort of schedule which varies from campus to campus depending on the schedules setup by the local administrators. Updating .dat files allows the McAfee software to continue to provide protection against the latest virus' and malware threats that continue to pop up from time to time from the outside world. These .dat files may also be applied in other ways. When this software is installed, it is configured to pull .dat files first from a local server, and then from a repository at NAI.com. When you right click on the virus-scan shield on the lower right hand side of your screen and select "update now", from the menu, this will force the software to pull the latest .dat file from one of these configured sources.

There is yet another way to manually update your McAfee antivirus .dat files. COT, or the Commonwealth Office of Technology, hosts an ftp site that holds a repository of files containing the latest releases of .dat files and another type of file called an Sdat file. An Sdat file is an executable file that allows for upgrades to both the antivirus dat files and the McAfee antivirus software itself. To install an Sdat file, all you have to do is copy it to a known location on your computer, double click the file, sdat4717.exe for example, and follow the prompts. This will force the antivirus software to perform an update regardless of its current .dat file level. The link to the COT .dat file and Sdat file repository is ftp://sunset.state.ky.us/pub/virus/ , and this site is updated on an almost daily basis. Members of the KCTCS technology contacts who are responsible for updating and/or maintaining the antivirus repositories on our district servers receive email notifications whenever updates are made to this site.

If you experience problems with applications working together, it is important that you notify the ITS group as soon as possible.

## Setting Permissions Levels for Other Users

When you are logged on to your workstation with administrative rights, you now have the ability to modify a whole slew of settings in the control panel, including those in the User Accounts area. It is imperative that you do not modify the permissions to the local workstation for other users – that is to say – do not give administrative rights to other users on your workstation. This can cause a great deal of administrative burden, not only to you, but to ITS and other faculty and staff as well due to the increased threats brought about by security threats imposed by machines logged on with administrator access. This also allows other users to modify settings, install programs, change passwords, and do any number of modifications to your systems without your knowledge, be it malicious or otherwise. Even with administrator rights accounts in your possession, it is common knowledge among IT professionals that you should do the majority of your computer work while logged in with a non-administrative account, and only log in as an administrator when you absolutely have to.

From more of a wide area network perspective, administrative rights on workstations can potentially bring a campus network to a complete halt. In the recent past, there were a few users within the KCTCS system who had administrator rights on their workstations, and chose to abuse the privilege by installing some unapproved and untested software. This software caused a great burden to be placed on the network link to the outside world from that campus. Within less than one day, KCTCS systems office quarantined that campus from the network for a period of 3 days (which meant no email or internet access period for anyone). This was a drastic measure, but it has been proven time and time again that these measures will be quickly taken in the event that the network is compromised by a system that is slowing down the links between our sites. This is yet another reason to be very cautious about how and what is done with administrative privileges on local computers within the district.

## Backing Up Your Computer

There are many options available to you for backing up the files on your computer. On the Cooper, Regency, and Leestown campuses, if you save your files to the "My Documents" folder, your files are essentially backed up to a server at that point. The "My Documents" folders on these campuses reside on a file server which is also backed up on a regular schedule.

In Danville and Lawrenceburg, the "My Documents, Favorites, and Desktop" folders are backed up daily to a folder on your campus' local file server, which is also backed up nightly to another file server. Even so, with all the redundant backups going on behind the scenes, there are still plenty of opportunities to lose files. Either they get saved to the wrong location, are not saved at all, or are over written to a different location with the originals being lost, not to mention the chances of hard drive failure, fire, flood, to name a few. With all this, backups should be a number one priority for your important files. Those of you with Administrator rights are no exception.

Many IT professionals rely exclusively on IT shops to take care of their backup needs, and in most cases this does the trick.  There is a lot more that can be done, however, to safeguard your data and piece of mind.

Most – if not all – faculty and staff workstations within the district are equipped with CD/RW or DVD/RW drives.  These provide an excellent option for backing up critical files.  Often, users can make copies of those all important files to a CD or DVD and store them at home, in a file cabinet, or some other cool, dark, dry place.  This method is often overlooked, but with the speed of today's "burners", it may be a good way to get those extra copies you may be thankful for later on.  Also, within the district, ITS has made several other backup options available to you.  There is the H drive on the server – which is the fastest and quickest way to ensure file safety at the Cooper, Leestown, and Regency campuses.  In Lawrenceburg and Danville, each faculty and staff member has a similar feature – their own folder on a file server – that they are free to use to store what ever files they want to place there.  Theses folders are backed up in several places 7 days per week.

Also, media backups such as CD/ DVD are still options, and don't forget our newest option – the USB drive.  These small hard drives come in sizes ranging from 128kb up to 30GB!!! – enough to backup the entire contents of a hard drive!  Just don't forget BACK UP YOUR FILES!!!!!!!!!!!!!!!

I'll say it again – and it doesn't really matter which method you choose – just do it… BACK UP YOUR FILES!!!!!!!!!

## Mastery Exam

Now that you are familiar with the capabilities of administrator rights, and have become familiar with the KCTCS Administrative Policy 4.2.5 that governs access to and use of KCTCS computing resources, as well as the Bluegrass Community & Technical College ITS technology usage guidelines, it is time to demonstrate that knowledge. The next step is the administration of a Mastery Examination on this material. Contact Connie Rine to schedule a time for the exam. Upon successful completion of this examination, you will need to print the final results. After printing the results, you will need to complete a section on the form justifying the need for administrator rights. This form will then be approved by your Assistant Dean or Department Director, and submitted to the campus ITS liaison.

Upon approval by the campus ITS liaison, your administrator account will be set up and activated. If for any reason, the request is not approved, it may be appealed to the District Technology Committee for resolution.