Data and Network Security

Configuring and Using Tektronix Products in Secure Environments

Global Operations, Quality and Compliance, Software Engineering
Tektronix, Inc.
November 12, 2010

Introduction

Tektronix recognizes the potential risks to our products when placing them onto a computer network and moving data from one computer to another through the use of removable memory media. We have taken precautions to assure instruments manufactured, calibrated, serviced, repaired, and demonstrated by Tektronix are free of malware and other computer based threats. However, when using Tektronix products in a secure networked or data sharing environment, further information measures should be taken.

This documents Tektronix recommendations for preserving data integrity while protecting Test and Measurement equipment from a wide variety of computer attacks.

The manner in which a security strategy is deployed will depend upon the Tektronix product type, network interfaces, information sharing methodologies, and operating systems.

This document provides security considerations for Tektronix products that implement the Microsoft Windows operating system. A few considerations are made regarding Tektronix products that did not implement an operating system, as well as for those products which implement VxWorks and Linux operating systems.

Due to the complex nature of Tektronix test and measurement instrumentation and the wide variety of possible operating system configurations this document makes no attempt to provide comprehensive coverage of computer and network security. However, this document may be used as a broad outline by computer security authorities in understanding, selecting, and implementing security measures on Tektronix instruments.

Please note: The following recommendations should not be used to supersede security authority requirements or directives. Rather, these recommendations may be used solely for the purpose to understand and enhance the security of Tektronix products, while working in support of secure installation requirements.

Common Attack Vectors

There are many tools and methods hackers use to perform an attack on a computer system. Software can be corrupted, information unknowingly or wrongly shared, computer performance can be reduced, service can be denied, or control over a computer gained. The following describes a few common methods of attack.

- Application vulnerabilities exploited through downloading of malicious programs – commonly used for data stealing or network compromises
- Website visits which exploit unpatched or as of yet unknown web browser vulnerabilities
- Documentation carrying malicious programs which attack document viewing, or corrupt systems through software application modification
- USB thumb drives carrying malicious programs which automatically launch when inserted into a USB port
- Malicious programs hidden in images, videos, or video streams
- Software application installations not supported by responsible security oversight functions, including computer security authorities
- Social Engineering where hackers attempt to extract private or sensitive information by attempting to manipulate computer operators

Protection Strategies

Protecting a computer from attack requires tools and knowledge in deploying effective defenses. While Tektronix takes strong measures to ensure virus free products are delivered to customers, there are several important steps that customers should take to protect their products from attack. Tektronix recommends the implementation of the following.

- Deploy virus scanners which run in the background during computer operation
- Allow only approved software applications to be executed by users
- Deploy firewall protections configured to the specific need
- Depending on which Tektronix product is deployed, do not allow users administrative privileges
- Enable User Access Controls
- Do not store data in folders or directories where software applications are executed from
- Disable “Autorun” features to prevent automatic virus transfer from hot-plugged external devices or downloaded materials.
- Where possible, use greater than minimum strength passwords

Microsoft Windows-based Product Protection

Viruses Protection

Tektronix Microsoft Windows® based products are not equipped with virus protection software. If these instruments are going to be placed on a network or you use external memory devices to share data, it is highly recommended that you add virus protection software.

Your computer security authority very likely already deploys a virus scanner. Tektronix encourages the installation and use of whichever virus scanner your computer security authority recommends. If a virus scanner is not readily available, there are several which may fit the need, including, but not limited to, Symantec, McAfee, and Microsoft Security Essentials.

Properly installed and configured, virus scanners consume no more than 1 to 3 percent of overall system resources. If, however, very strict performance requirements are specified, deferring virus scanning while making critical measurements is recommended. In all cases, periodic, if not active virus scanning, is strongly recommended.

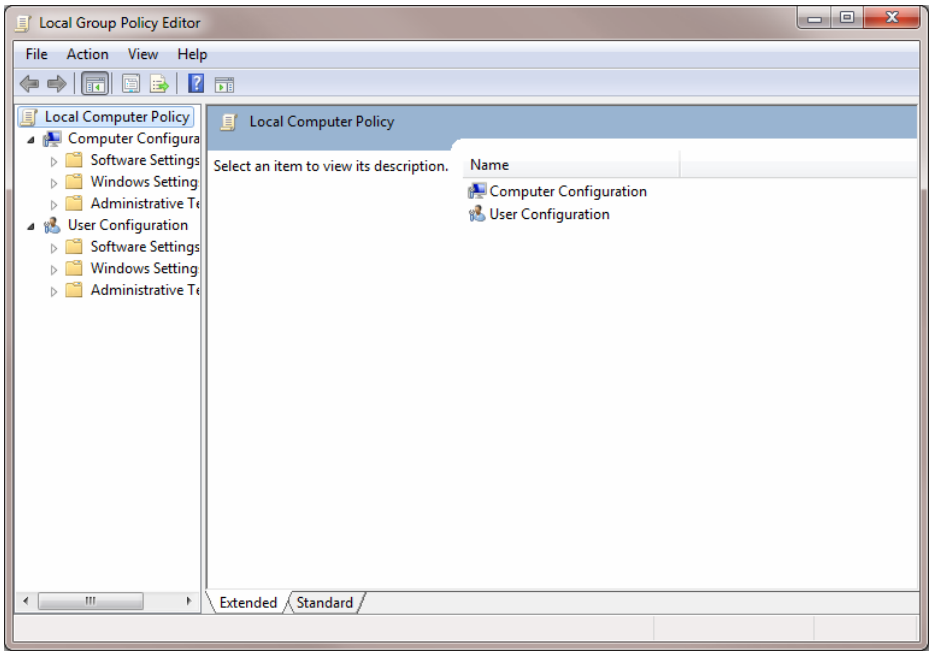
Once a virus scanner has been installed, additional security measures to prevent virus infection should be taken.

Example - How to configure the AutoPlay feature in Windows 7

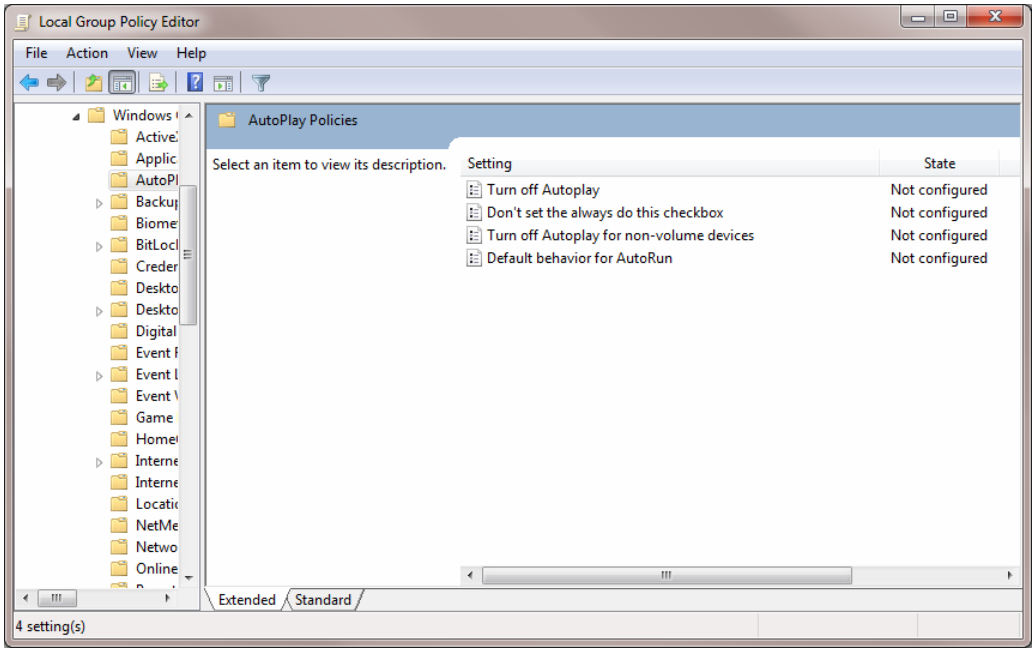
External memory devices connected to computers, such as through USB ports, are known vectors for virus attack. There is a class of virus that propagates through the “Autorun” feature of the Windows operating system. Here is a method for disabling “Autorun”.

You must run with administrator privileges to configure AutoPlay. In this example, we will turn off the AutoPlay feature.

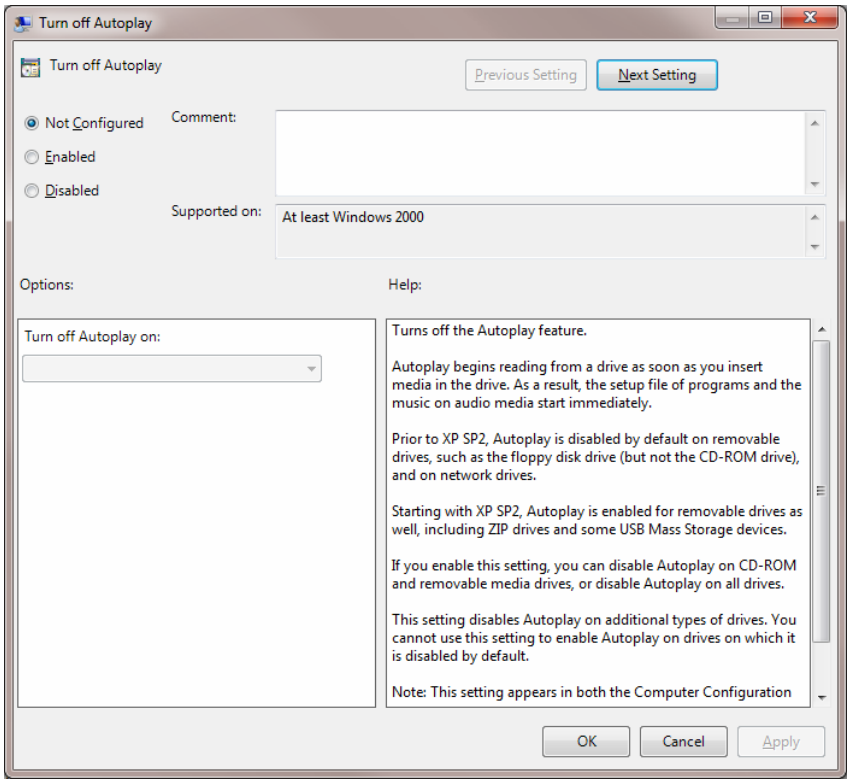
1) Type “gpedit.msc” in the Start-> Run text field and hit Enter. The Local Group Policy Editor appears:



2) Navigate to Computer Configuration > Administrative Templates > Windows Components > AutoPlay Policies. You should see this window:

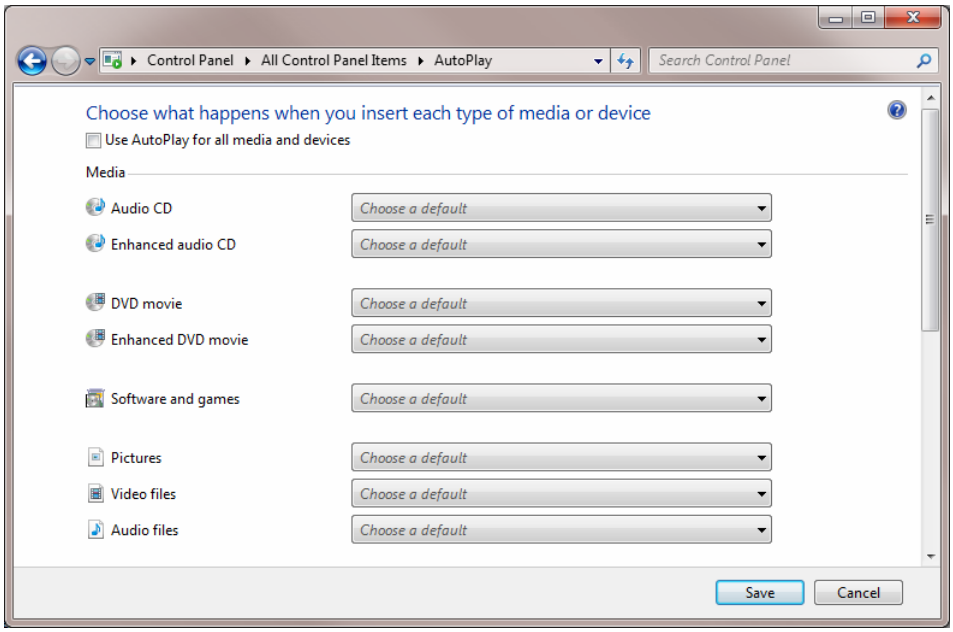


3) Double click the “Turn off AutoPlay” item in the right-hand pane. You should see the following window:



4) Select the “Enabled” radio button. Then click “Apply” and then “OK”.

5) Navigate to Start -> Control Panel -> AutoPlay. You should see the following window:



6) Uncheck the box labeled “Use AutoPlay for all media and devices” and then click the Save button.

Disabling USB Ports

To reiterate, external memory devices connected to computers, such as through USB ports, are known vectors of attack. USB memory sticks infected with virus or other malicious attack software can easily pass these attacks to Tektronix products.

While there are electronic means of disabling USB ports through BIOS settings management, certain Tektronix product functions and capabilities may be impacted if this USB port disabling method is chosen.

In situations where the use of USB ports is disallowed, Tektronix recommends physically disabling USB ports. This can be accomplished by filling USB ports with a non-electrically conductive material, such as through the use of certain epoxies.

Security Patch Updates

Keeping Tektronix products up to date with the latest Microsoft Windows security patches is an important means of combating attacks on these products. Microsoft makes security patch updates available every second Tuesday of the month. Occasionally Microsoft issues security patches more frequently that once a month.

Tektronix recommends the installation of "critical" and "important" Microsoft Security Patch Updates. Tektronix tests only “critical” and “important” security patches. Use the computer security authority’s processes and procedures for download, installation, and use of security patch updates.

In the event no guidance is given on how to download and install Microsoft security patch updates and if the Tektronix products in question are attached to a network capable of reaching Microsoft’s update center, follow these instructions.

- Click “Start”
- Find and click “Control Panel”
- Depending on the Control Panel view (Classic or Category), do one of the following
  - Click “System”, then find and click the tab “Automatic Updates”
  - Click “Performance and Maintenance”, find and click “System”, then find and click the tab “Automatic Updates”
- Tektronix recommends clicking “Automatic (recommended)” with an update/install period set to, minimally, once a month

Virus Protection for XP Embedded, Windows Embedded Standard

A small number of Tektronix products implement either Microsoft XP Embedded or Windows Embedded Standard. Windows Embedded operating systems may require special handling.

Security management strategies may need to accommodate for the fact these operating system images are not constructed by Microsoft. Original Windows components are provided by Microsoft. Windows OEM suppliers then use these components to build an operating system image that is tailored for embedded applications. For this reason, Microsoft does not support security patch updates in Microsoft’s standard desktop security patch update cycle.

There is a separate security patch update procedure implemented specifically for Windows Embedded. Additionally, due to the nature of Windows Embedded operating system image construction, security patch updates may need to be identified, downloaded, and applied manually to each instrument. Centralized distribution and installation of Microsoft security patch updates may not be available.

Contact Tektronix Customer Care Center for further information about how to protect products that use Windows Embedded operating system images.

Whitelist Protection

In addition to the standard Malware protection schemes, there is an important security measure which may be taken to insure unwelcome software does not execute or spread through systems under attack. It is called

application “Whitelisting”. Whitelisting uses Microsoft Windows Software Restriction Policies (SRP) to explicitly specify which applications are allowed to execute, and to disallow the execution of unauthorized software (such as viruses, “look alike” software installed in non-standard folder locations, or unauthorized software installations by users).

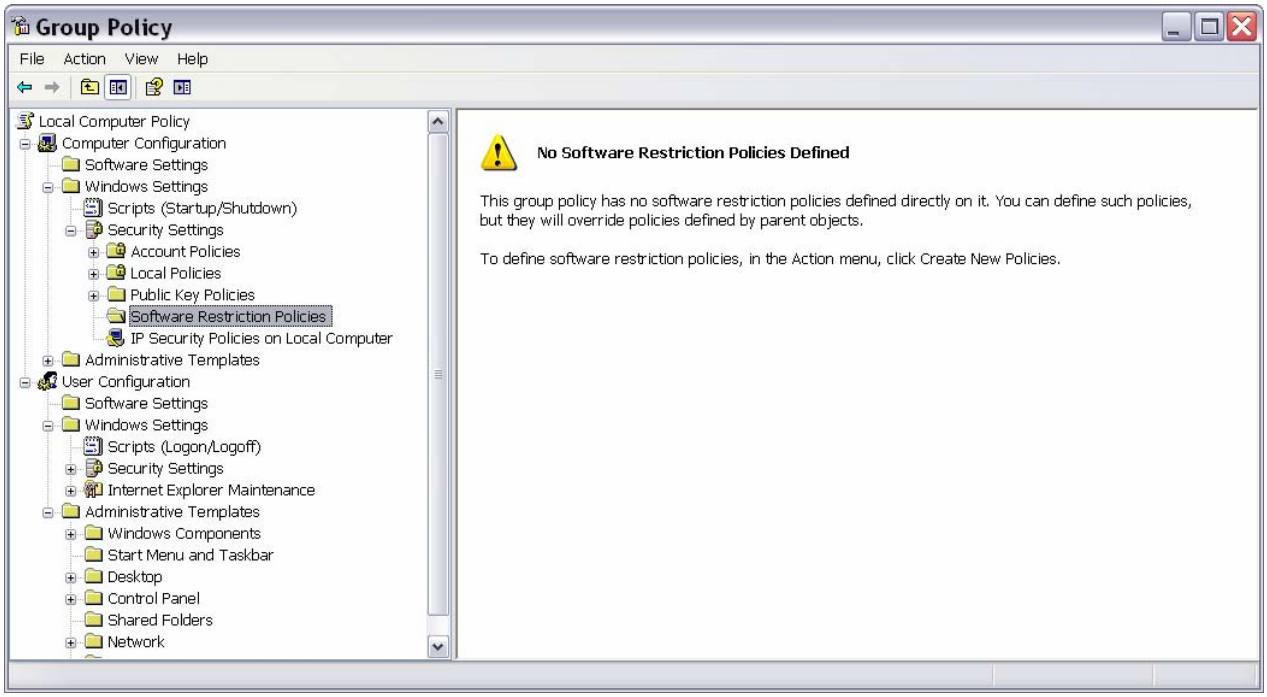
An SRP can be implemented and managed centrally (through Microsoft Windows Server 2003 or 2008 servers) or locally on a specific Windows computer. For Tektronix products which implement either a Windows XP Pro or Windows7 based operating systems, the following Whitelist SRP guidance is provided, assuming a centralized Microsoft Windows Server does not already provide SRP management.

When adding Tektronix Test and Measurement equipment to a Software Restriction Policies (SRP) environment, computer security authorities should be aware that SRP rules for allowing certain non-standard folder location Tektronix software will be required.

When implemented, SRP’s can may be monitored by viewing the Windows Event Log. Further adjustments to SRP “Path Rule” entries may be made, where appropriate.

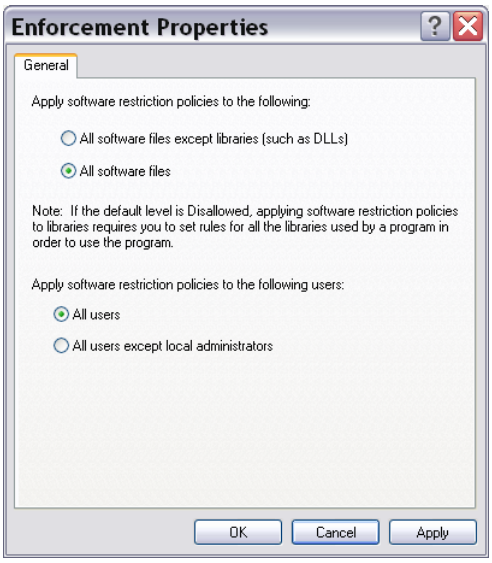
Example - Whitelist SRP settings for Windows XP Pro

To begin, log into an Administrator privileged account. Select “Start”, then “Run”, and type “gpedit.msc”. The Group Policy editor will start.

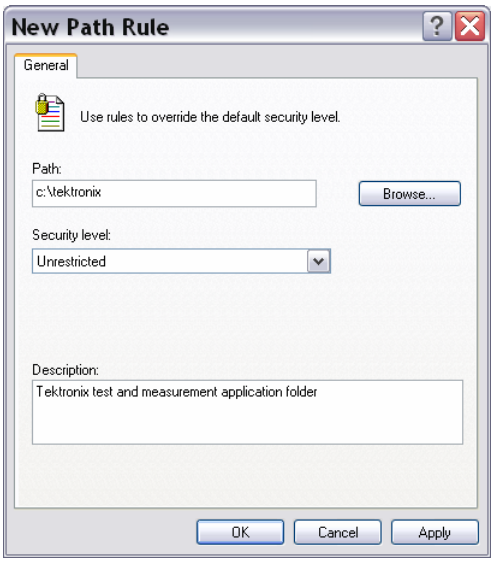


If a SRP does not already exist, right click “Software Protection Policies” and select “Create New Policies.” Then double click “Enforcement” found under “Object Type” in the right hand pane. Select “All Software Files” and “All Users”.

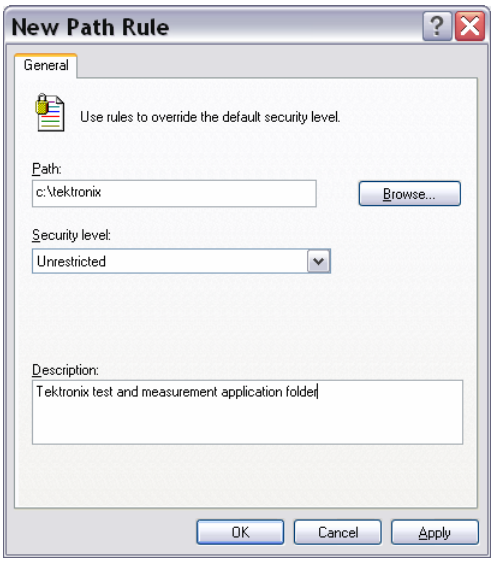
Otherwise, simply add a “New Path Rule” (information on how to do this is found below).



From the Group Policy Editor, select “Security Levels”. Double click on “Disallowed” as found in the right hand pane and “Set as Default” to enable Whitelist mode.



Minimally, add Tektronix specific folders by right clicking over “Additional Rules” and selecting “New Path Rule”. Add “c:\tektronix” to “Path:”. Set the “Security Level:” to “Unrestricted”. Add a description to the “Description:” field.



In the above example, “c:\tektronix” is being added to a SRP. Software found in this folder includes important installation and recovery applications. It will be important to implement this Path Rule in situations where clearing information may include reinstallation of certain software materials.

Normally, many important Tektronix software runtime materials will be located in “c:\Program Files\Tektronix. However, some Tektronix Test and Measurement products may implement additional important Windows folders not found under “c:\Program Files\Tektronix”. It is strongly recommended that the new or updated SRP configuration be tested prior to deployment. If software execution issues are uncovered, please contact Tektronix Customer Care Center for information on valid SRP configurations for Test and Measurement equipment.

Firewall Protections

Tektronix instruments running the Windows 7 OS come pre-loaded with the Firewall exceptions that will allow your Tektronix software to run appropriately. If new applications are introduced onto the OS, new Firewall exceptions rules may need to be added in order to allow the new software to run properly.

Example - Configure Windows Advanced Firewall exceptions list Windows 7

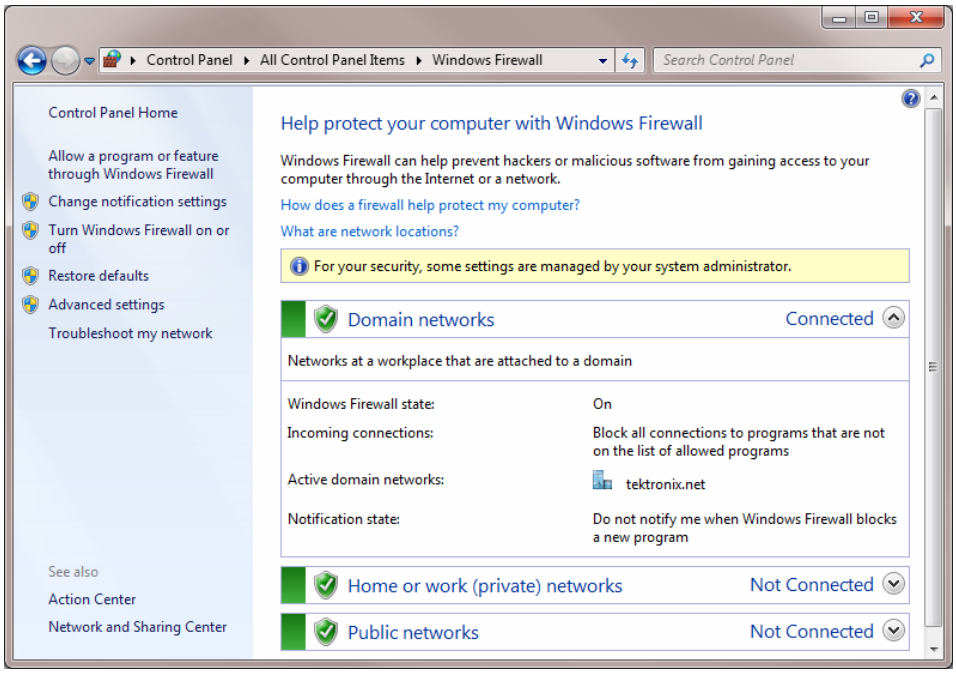
You must run with administrator privileges to configure the Firewall settings in Windows 7. There are 2 methods for adding exceptions to the Windows 7 Advanced Firewall.

1) Use the GUI interface through the Control Panel.

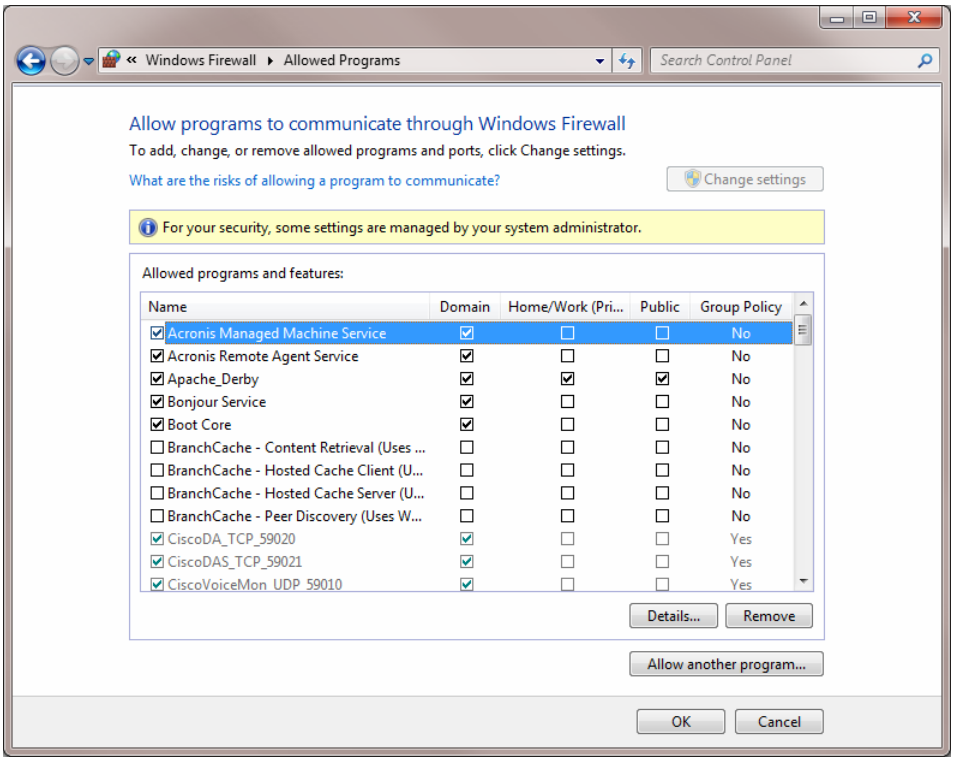
2) Use command line arguments.

This documents how an administrator may add a new application to the Windows 7 Advanced Firewall exceptions list using the GUI.

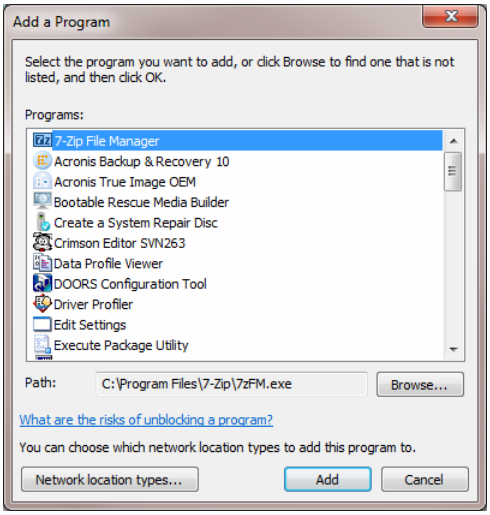
1) Navigate to Start->Control Panel->Windows Firewall. You should see the following window:



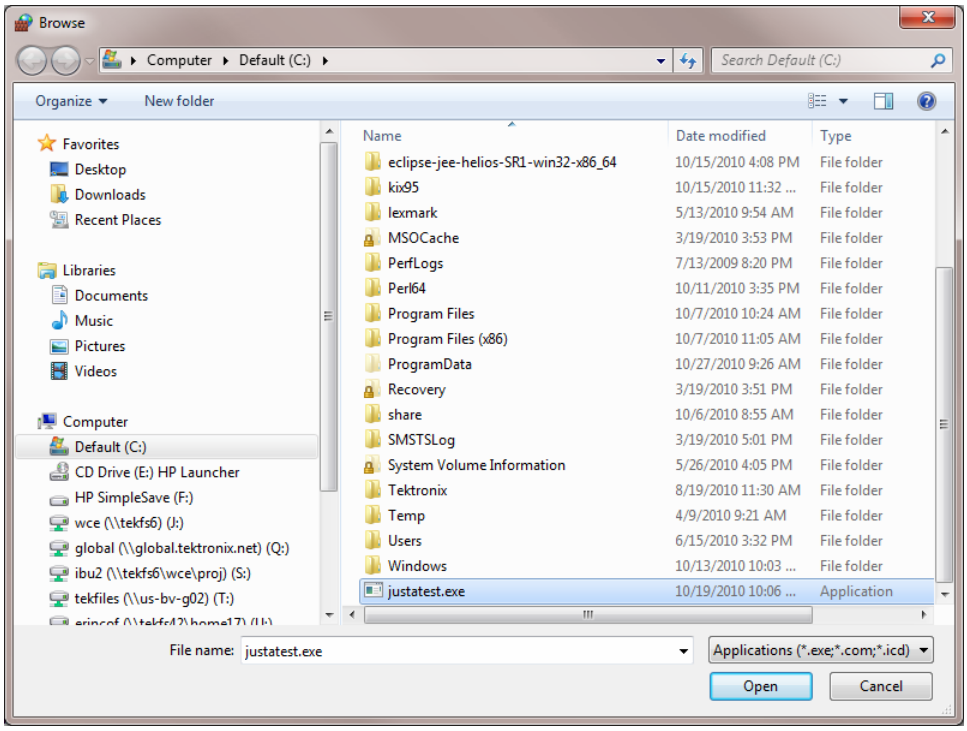
1) Click on “Allow a program or feature through Windows Firewall”. You should see the following window:



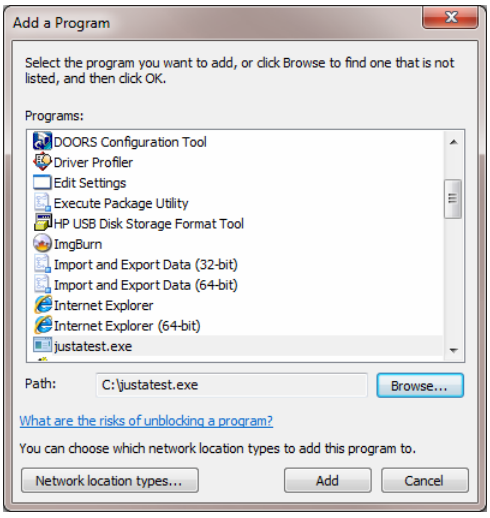
2) Click on the “Allow another program” button. You should see the “Add a Program” window. Browse to the location of the application that you want to add to the exceptions list and, click the “Add” button.



3) Click on the “Browse” button to select the executable that you need to add to the exceptions list and, click “open”.



4) Now that the application has been selected, click on the “Add” button to add the application to the Firewall exceptions list.



Managing Account Privileges

Many secure installations require that administrative privilege accounts be strictly limited to computer security authorities only. Further, normal users should have access to only user privileged accounts accessed through strong password logins (for more information on passwords, please see Password Protection below).

Please Note: Many performance oscilloscopes require administrative privilege level accounts for the proper execution of the oscilloscope application. Tektronix real time spectrum analyzers, logic analyzers, and signal sources are not restrictive in this manner. The following should only apply to specific performance oscilloscope products from Tektronix.

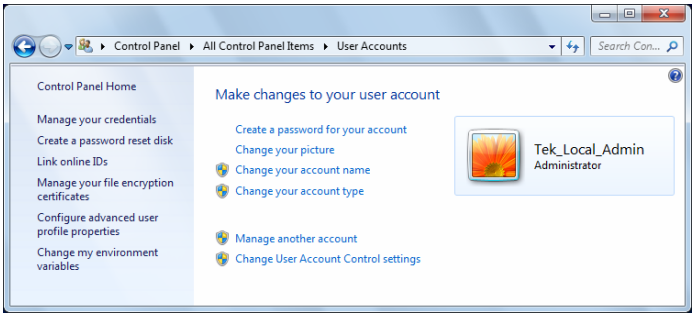
In security applications where administrative level accounts are strictly controlled, Tektronix recommends taking one of two approaches.

The first approach would be to write a waver requesting the allowance of specific Tektronix instrumentation to be deployed into the secure environment.

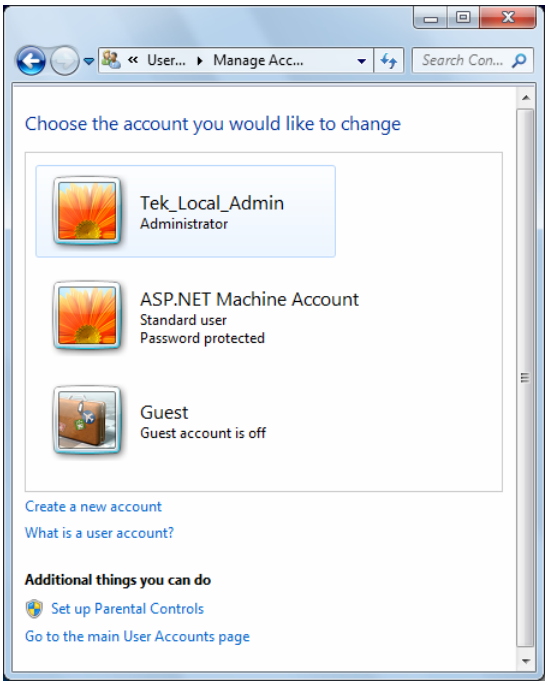
If wavers cannot be granted, a second approach should be considered. Tektronix recommends the use and deployment of Microsoft Windows SteadyState software. This software may be used by computer security authorities to protect against unauthorized changes to persistent storage devices (such as hard drives), and restricts users from accessing system settings and information. For further information regarding SteadyState, please contact Microsoft.

Example - How to add a standard user account and make the user login – Windows 7

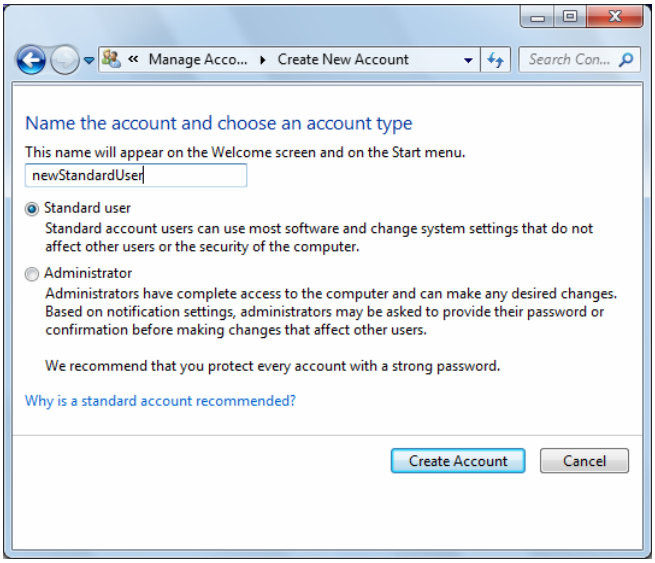
Navigate to Start -> Control Panel -> User Accounts to see the following:



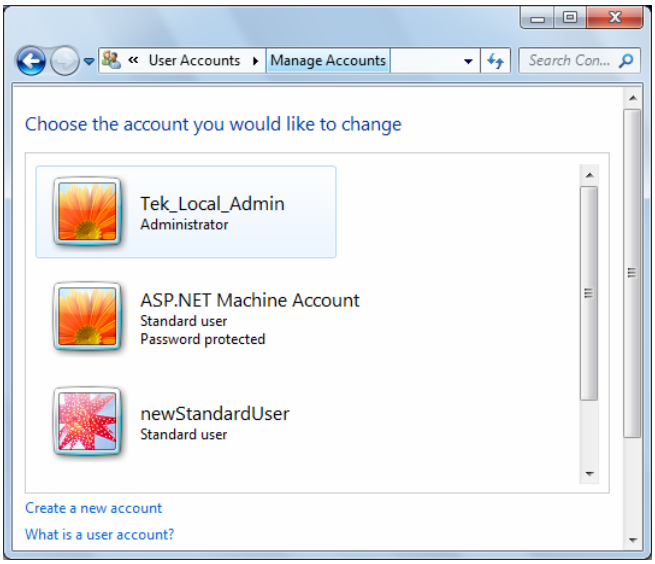
Click on Manage another account to see the following:



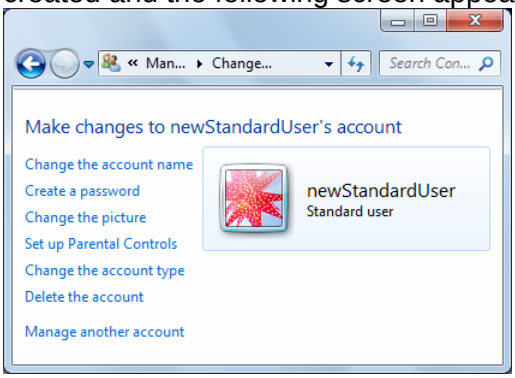
Click on Create a new account and you should see the following:



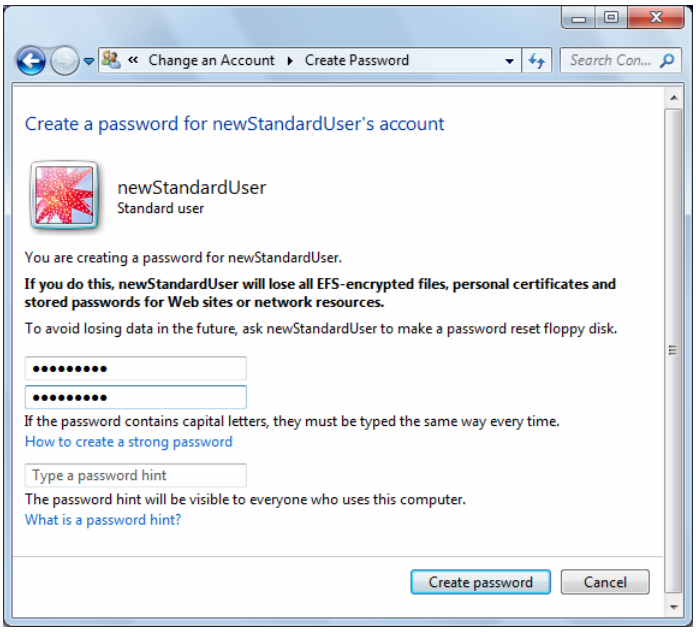
Enter the name of the new account and make sure that the standard user radio button is selected, and then click Create account. Verify that the new account is added to the user accounts list:



In order to make the new account login, you need to add a password. Click on the new account that was just created and the following screen appears:



Click on Create a password and the following screen appears:



Enter the password for the new account and then confirm the password. A password hint may be added. Now click Create password.

The new user will have to login using the password in order to gain access to the Tektronix product.

User Account Control (UAC) Protections – Windows 7

The **User Account Control** (**UAC**) is a security feature of the Windows 7 Operating System. It is intended to be used by the end user to limit applications to run in standard user space with standard user privileges. Limiting applications to run as a standard user limits their ability to read from or write to sensitive or secure directories.

There are 4 possible settings for the UAC:

Setting 1) "Never notify"

This is how Tektronix has configured your Windows 7 Operating System. This setting allows Tektronix proprietary applications to run in Administrator user space. This setting also allows all other applications to run in Administrator user space creating potential security risks. You won't be notified before any changes are made to your computer by any applications running on it.

Setting 2) "Notify me only when programs try to make changes to my computer but, don't notify me through the secure desktop mode"

This setting will notify you before programs make changes to your computer that require Administrator privileges. However, since the notification is made outside of the secure desktop environment, malicious software running on your computer can actually modify the notification window itself.

Setting 3) "Notify me only when programs try to make changes to my computer"

This is the default setting recommended by Microsoft. This setting will notify you, in a secure desktop environment, before programs make changes to your computer that require Administrator privileges. This setting is a balance between security and usability. You won't be notified if you try to make changes to Windows that require Administrator privileges while you are logged into an account with Administrative privileges.

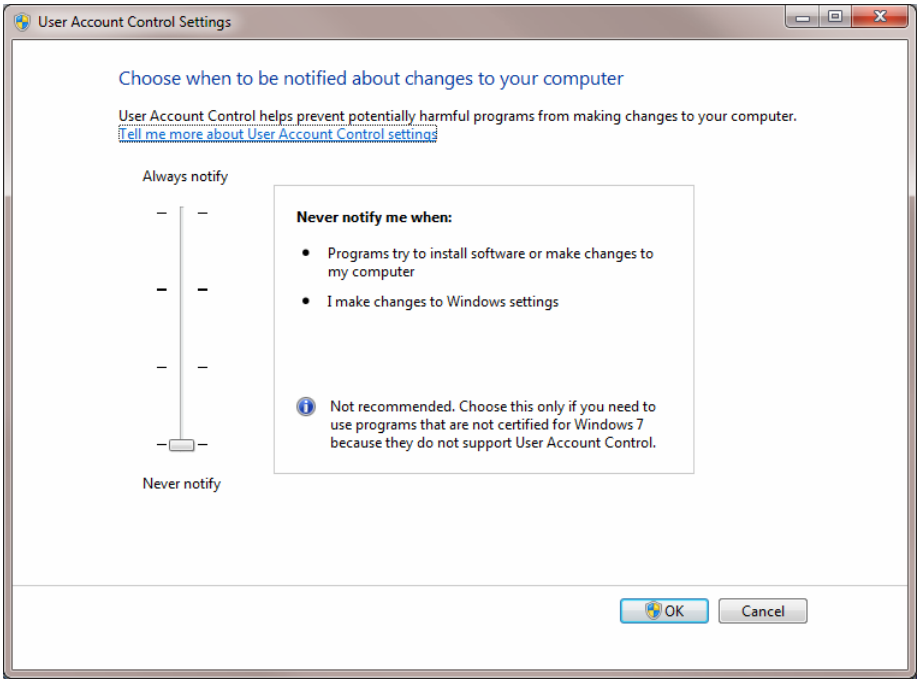
Setting 4) “Always notify me”

This is the most secure setting. You are always notified before programs make changes that require Administrator privileges. The notification occurs within the secure desktop environment which prevents programs from running until you respond. You will be notified every time you try to make a change to Windows that requires Administrator privileges regardless of whether or not you are logged into an account with Administrative privileges.

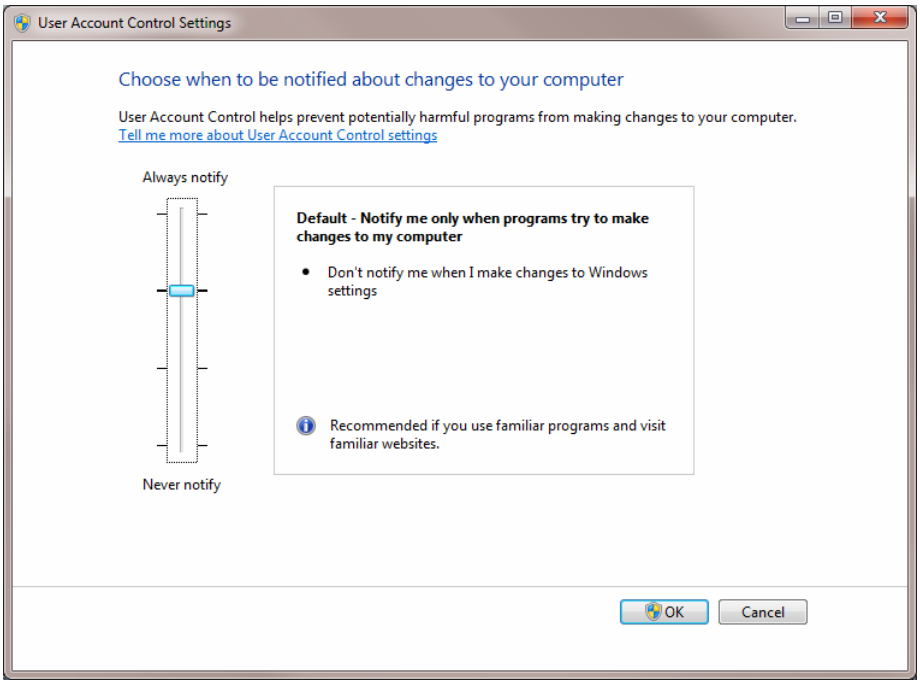
To configure the UAC, you must be running with Administrator privileges.

Example - Configure User Account Controls

1. Select **Start**, open the “Run” window and type “UAC”. Then select the “Enter” key to bring up the User Account Control window. On Windows 7 Operating Systems released by Tektronix, Inc., the UAC may be set to “Never Notify.”



2. To change the setting to the Microsoft recommended default, slide the bar up to “Notify me only when programs try to make changes to my computer” Select “OK”.



3. Restart the computer to enable the new UAC configuration.

Social Engineering Protections

Social engineering attacks attempt to coerce a computer operator into revealing something that should or would normally not be revealed. A successful attack could gain control over a computer system or a network of computers. This kind of attack is also known as a "confidence trick."

While social engineering attacks are typically non-technical, there are a few precautions to consider taking. Common vectors of attack include –

- Email phishing (emails embedded with hyperlinks)
- Application pop-ups and Dialog boxes
- Web browser hyperlink phishing
- Instant messaging spoofing

In the unlikely event that precautions have not yet been made by computer security authorities, and in the unlikely event that Tektronix products (due to the implementation of desktop Microsoft Window operating system images) are called upon to provide social engineering protections, Tektronix makes the following recommendations.

To prevent –

- Email phishing - Limit email access to securely configured computers. If this includes the installation and operation of email readers on Tektronix products, Tektronix recommends computer security authorities configure and test email systems prior to deploying an instrument.
- Application pop-up or dialog box attacks - Limit the execution of software application which run on test and measurement products. One way (perhaps the best way) to accomplish this is through the configuration and use of Whitelisted applications (for further information, please see the prior section on Whitelist Protection).
- Web browser hyperlink phishing - Restrict web browser use. When web browsing is required, Tektronix recommends computer security authorities use Tektronix default entries and carefully selecting additional firewall entries that specifically meet security requirements. For further information, please see the prior section on Firewall Protection.
- Instant messaging spoofing – Tektronix products do not ship with non-web browser based instant messaging applications pre-installed. If an instant messaging application has been installed, Tektronix

recommends un-installing the application. Further, limiting browser based instant messaging is recommended.

Password Protection

Tektronix Windows based products typically boot straight to a test and measurement application, by-passing the need for a user to log into a system. For secure applications, this is not sufficient protection where specific users may or may not be granted access to certain test and measurement systems.

When password protection is required, Tektronix recommends creating a restricted user account on the instrument and then setting the user's minimal password strength as follows. User privilege passwords should contain –

- At least 8 characters
- Character mix of at least –
  - 2 upper case characters
  - 2 lower case characters
  - 2 numbers
  - 2 special characters

Since many Tektronix products ship instruments that boot straight to the test and measurement application, administrators are strongly encouraged to create passwords for Administrative privileged accounts. Administrative privilege passwords should contain –

- At least 15 characters

- At least 4 character sets including –
  - upper case characters
  - lower case characters
  - numbers
  - special characters

In the unlikely event that computer security authorities do not provide guidance or policies, Tektronix recommends changing passwords every 30 days in situations where security is of utmost concern. In all cases, passwords should be changed every 90 days, if not sooner.

Example - How to change or set a password in Windows 7

To change or create a password for the account that is currently logged on:

You are able to change the password for the account that is currently logged on to the computer. You will be prompted to enter the existing password and, enter and confirm the new password.

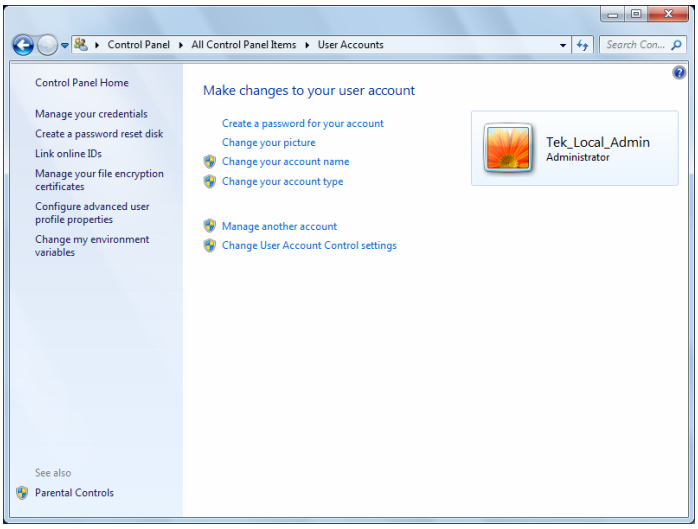
1) type control + alt + delete

2) click on change a password.

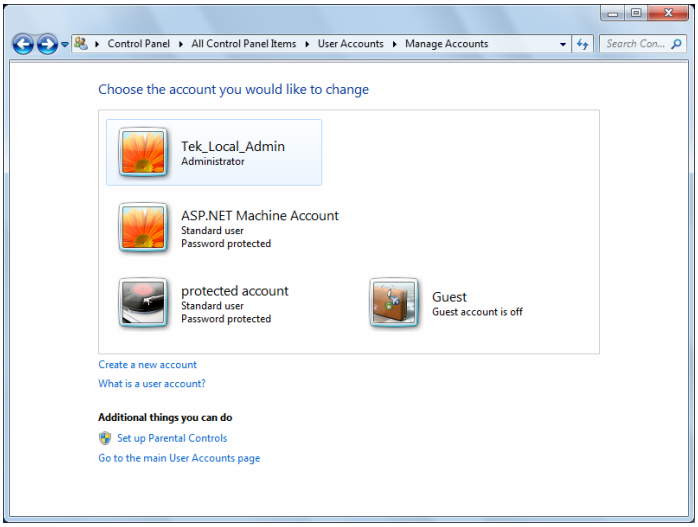
To create or change a password for an account that is not currently logged on:

In order to modify a password for an account that is not currently logged on, you need to have administrator privileges on the computer.

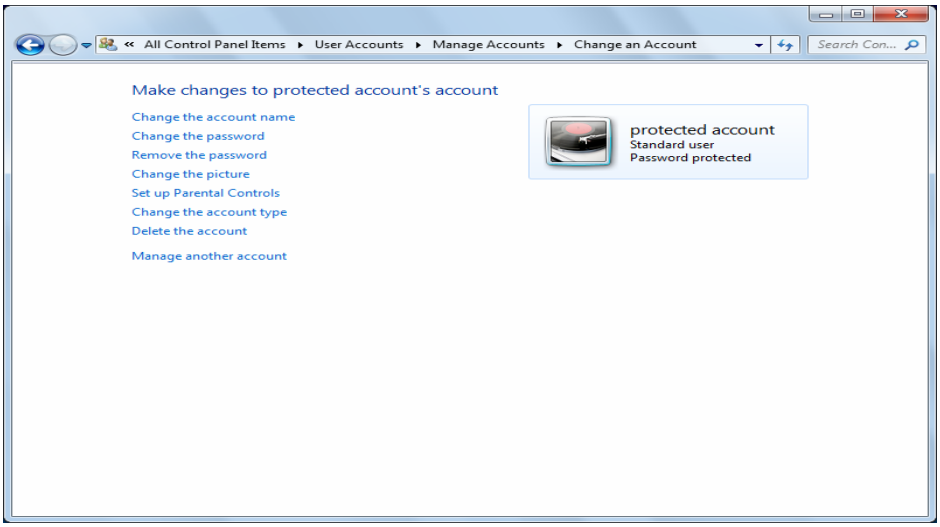
1) Navigate to Start->Control Panel->User Accounts



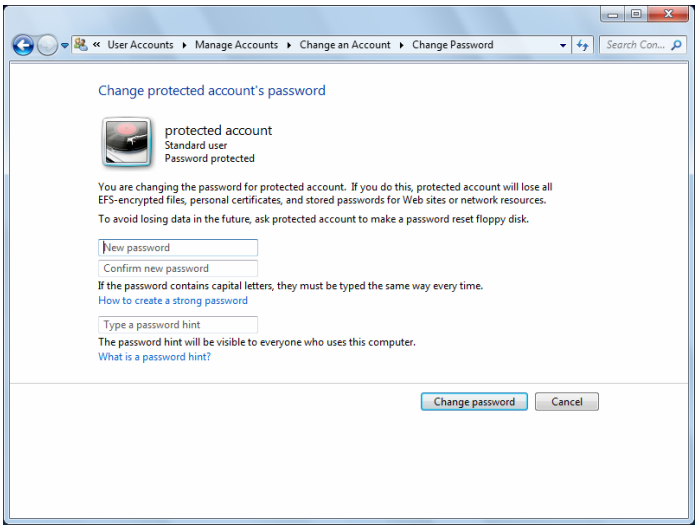
2) Click on “Manage another account”



3) Select the account you want to manage. In this example we select the “protected account”



4) Click on “Change the password”



Enter and confirm the new password. Enter a hint if you like. Click on the “Change Password” button and, you are done.

Example - How to configure BIOS-level password protection on Tektronix instruments

Some BIOS in Tektronix products allow a password to be set that limits access to BIOS functions. If specific BIOS settings are required and if computer security authorities are required to limit access to the BIOS, passwords should be used.

Please NOTE: If BIOS settings are used to limit access to ports, such as USB, please confirm valid product configurations with Tektronix Customer Service Center. Some Tektronix products require USB capability to provide vital instrument functionality. Electronically disabling USB ports through the modification of BIOS settings may impact performance, and in extreme cases, the ability of a product to reboot and operate correctly.

Example - AIMB-5786 and AIMB-562 Motherboard Products:

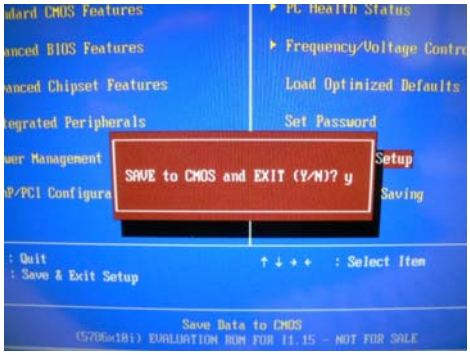
1. When restarting the instrument wait for the Tektronix logo to appear and then begin hitting the Delete key until you enter the BIOS.

2. Once the BIOS comes up, use the arrow keys to scroll over to the SET PASSWORD option:

3. When you select Enter you will be asked to enter a password. Your password can be letters and numbers (no symbols such as @#$%^) and up to seven characters in length.

4. After you have entered the password you will be asked to reenter the password. If you reenter it incorrectly the entire process will have to be restarted.

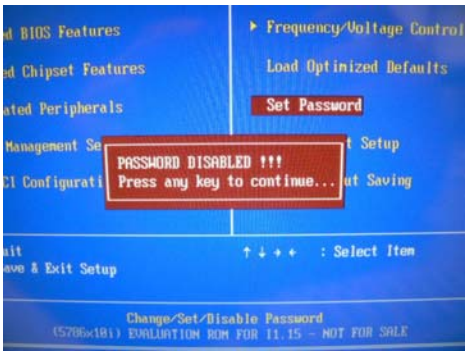
5. Once your password has been confirmed scroll to the “Save & Exit Setup” option. Press “Y” when asked and select Enter. The instrument will reboot.



6. To verify that the password has been successfully entered repeat Step 1 to get back into BIOS. If the password was configured properly you should be immediately asked to enter the password.

Resetting the password to blank:

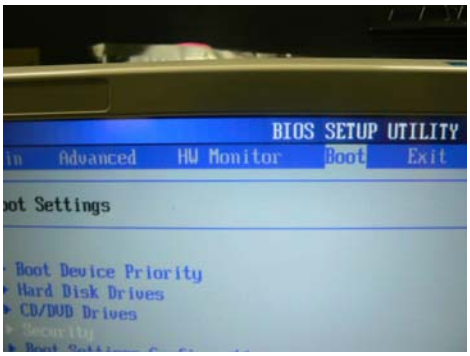
In the event that you want to remove the password from the BIOS on the instrument in the future, simply repeat Steps 1 through 3 but instead of entering a password leave the input text box empty and select the Enter key.



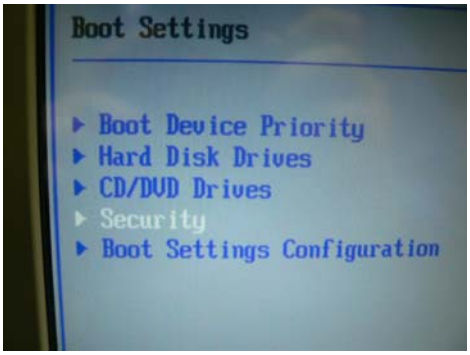
Example - AIMB-256 and AIMB-566 Motherboard Products:

1. When restarting the instrument wait for the Tektronix logo to appear and then begin hitting the Delete key until you enter the BIOS.

2. Once in the BIOS, use the left and right arrow keys to scroll over to the Boot tab at the top of the screen.



3. Once there you will see a “Security” option further down the screen. Use the up and down arrows to navigate to this option and hit Enter.

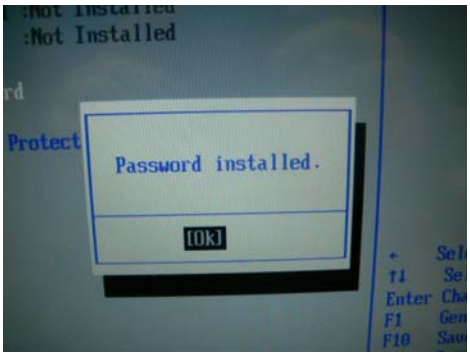


4. Once inside the Security page you’ll see an option for “Change User Password”.

5. Press the Enter key when the “Change User Password” option is selected and you will be prompted to create a password. Your password can be letters and numbers (no symbols such as @#$%^) and up to seven characters in length.

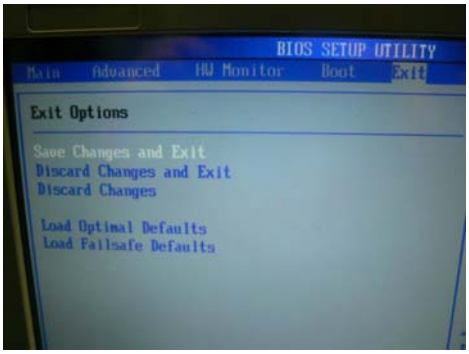
6. Once you have entered a password and select Enter you will be prompted to confirm the password.

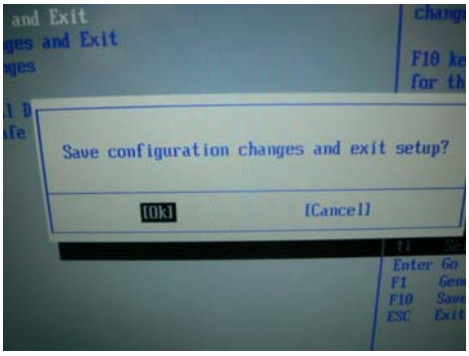
7. When the password have been entered and confirmed, the BIOS will prompt you letting you know that the password has been installed.



NOTE: There will now be more options on the Security screen. The “Password Check” option has two selections which configures when the user will be prompted for the password during the course of the instrument’s operation.

8. Using the left and right arrow keys highlight the Exit tab and select “Save Changes and Exit”.



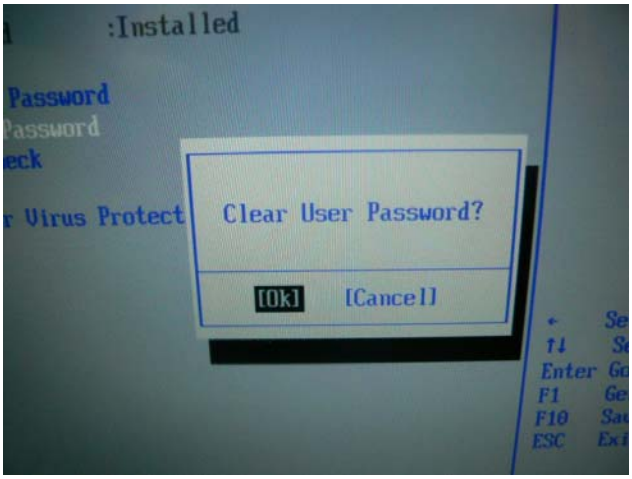


- Setup: The user will only be prompted for a password when entering the BIOS itself.
- Always: The user will be prompted for the password each time the instrument is rebooted. The instrument will not finish POST until the password has been entered.

9. To ensure the password has been configured properly repeat Step 1. The BIOS should prompt for a password before letting the user view any details about the system.

Resetting the password to blank:

In the event that the password must be removed or reset from the BIOS simply repeat Steps 1 through 3, highlight the “Clear User Password”, press the Enter key and select the Enter key again when prompted to remove the password.



VxWorks, Linux-based Products

Computer and network security considerations and configurations previously discussed for Tektronix products that implement the Microsoft Window operating system do not apply to Tektronix embedded test and measurement instrumentation.

Login Privileges

Tektronix implementing embedded VxWorks and Linux operating systems do not include an ability to log into a product. This class of products simply boot from power-on straight into the test and measurement application. Computer management capabilities are strictly limited.

Virus Protection

VxWorks and Linux based products are largely immune to direct virus attack. There are currently no known virus attacks which would affect the performance of embedded VxWorks or embedded Linux-based Tektronix products. In general, this class of instrumentation may be treated from computer security authority perspective as embedded systems.

For VxWorks based products user access to kernel level functions is strictly limited. Similarly, for embedded Linux products, there is no customer accessible administrative privilege level access to these systems. Furthermore, product test and measurement applications are constructed to utilize user level privileges and do not implement direct user access to core operating system kernel functions.

To date, Tektronix has not tested nor currently recommends the implementation of Linux virus scanners. In the case of embedded systems, there is no administrator privilege accessible means for installing or implementing virus scanner.

Please Note: For Linux server class products, the operating system may be administered per existing computer security authority standards previously defined for managing UNIX operating systems.

Legacy Products

Tektronix long history of test and measurement product development includes a wide range of products which have no operating system. In these cases, the concept of administrative and user privilege accounts or control was not implemented and access to an operating system is unavailable.

In the case of a Tektronix product that does not implement an operating system, two considerations may be made. The first is for that class of products which do not implement a network interface. These products are largely safe from storing or passing virus infected materials.

The second is for that class of products which implement some form of limited network interface. In Tektronix products, this was typically a General Purpose Interface Bus (GPIB IEEE 488.2) with perhaps a Com/DCom interface that users could write software applications to communicate through. GPIB itself is currently considered safe from virus attack.

Please NOTE: Customer software written to implement Com/DCom software interfaces (included in certain legacy Tektronix products) should take special precautions. If a customer software application has been written to implement Com/DCom, Tektronix recommends systems deploying the software not be connected to a network, including through a GPIB to Ethernet converter. Microsoft reports that Com/DCom is vulnerable to attack through various means of exploitation.

Testing Security Changes

When making changes to the Microsoft Windows operating system in Tektronix products, it is important to test to ensure instrument performance meets deployment requirements. Tektronix Test and Measurement equipment implements a wide variety of configurations with and even wider variety of possible operating system settings. While Tektronix makes every attempt to ensure product performance across numerous configurations, it is possible that instrument performance may significantly change as security precautions are implemented.

Tektronix recommends taking a step by step approach to implementing security measures. That is to say, make a handful of security changes and test an instrument's performance against security requirements. Make another series of security changes and test again. Do this until the full set of security requirements have been met.

Questions may arise regarding valid security configurations on Tektronix products. When this happens, please call Tektronix Customer Care Center for direction on how best to proceed.

If you have any questions regarding Tektronix product security, network security, security applications or technical questions, you can contact the Tektronix Technical Support Center by either phone or e-mail:

- Inside US: 1-800-TEK-WIDE (1-800-835-9433, ext. 2400) (6AM-5PM PST)
- Outside US: (503) 627-2400 (6AM-5PM PST)
- E-mail: support@tek.com

References

Chairman of the Joint Chiefs of Staff Instruction – Defense Information System Network (DISN): Policy and Responsibilities, CJCSI 6211.02C, 9 July 2008

Chairman of the Joint Chiefs of Staff Instruction – Directive current as of 12 August 2008, CJCSI 6510.01E, 15 August 2007, Information Assurance (IS) and Computer Network Defense (CND)

Defense Information Systems Agency, Application Security and Development, Security Technical Implementation Guide, Version 2, Release 1, 24 July 2008

Defense Security Service, Office of the Designated Approving Authority, Standardization of Baseline Technical Security Configurations, March 2009, Version 2.2

Defense Security Service, NISPOM Chapter 8 with Annotated Q&A's from DSS Industrial Security Letter, 2007-01, April 2008, Version 1.0

Department of Defense, Instruction, Number 8510.1, November 28, 2007, Subject: DoD Information Assurance Certification and Accreditation Process (DIACAP)

Department of Defense, Instruction, Number 8551.1, August 13, 2004, Subject: Ports, Protocols, and Services Management

Memorandum for Secretaries of th4e Military Departments, Subject: Federal Desktop Core Configuration (FDCC), Aug 15, 2008

Microsoft Solutions for Security and Compliance, Windows XP Security Guide

Microsoft, TechNet, Windows Client TechCenter, User Account Control Step-by-Step Guide, Updated: May 11, 2010

Microsoft, TechNet – How to Protect Insiders from Social Engineering Threats, published: August 18, 2006

National Security Agency, Information Assurance Directorate, Vulnerability Analysis and Operations, Systems and Network Analysis Center – Application Whitelisting using Software Restriction Policies

Solutions for Security and Compliance, Threats and Countermeasures: Security Settings in Windows Server 2003 and Windows XP, Version 2.0, Published: December 2005

Tektronix®