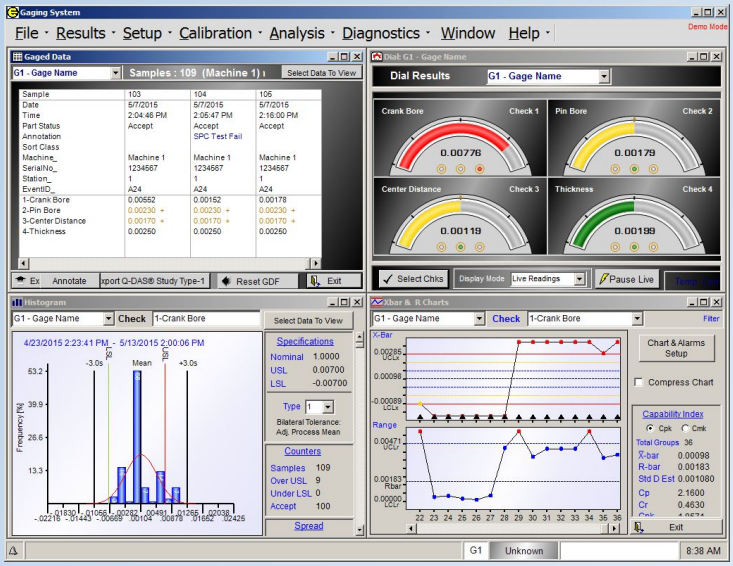
EPIC-CAG™ Administrators Guide

Windows Embedded Standard 7 (WES7)

Revision 1.0 02/24/16



Farmington, CT USA 06032
TEL: (860) 677-2813
info@edmundsgages.com
www.edmundsgages.com

Table of Contents

1. Introduction

The Edmunds Gages EPIC CAG™ is a multi-dimensional computer aided gaging system. The EPIC CAG™ runs Microsoft® Windows® Embedded Standard 7 (WES7) operating system that provides access to the EPIC gaging application and the full featured networking and maintenance resources. WES7 is a fully componentized operating system that provides a Windows 7 interface that has been tailored for a robust secure embedded system.

About this Guide

This guide is intended for IT administrators of EPIC CAG™ running Windows Embedded Standard 7. It provides information and detailed system configurations to help you connect and manage an EPIC CAG™ on facilities network. Depending on your hardware and software configurations, the figures you see may be different than the example figures shown in this guide. This guide supplements the standard Microsoft Windows Embedded Standard 7 documentation supplied by Microsoft Corporation. It explains the differences, enhancements, and additional features provided by in a EPIC CAG™. It does not attempt to describe the general networking concepts and standard features found in Microsoft Windows operating system. Windows Embedded Standard 7 help can be accessed from the Microsoft Help and Support Web site at: http://support.microsoft.com/default.aspx

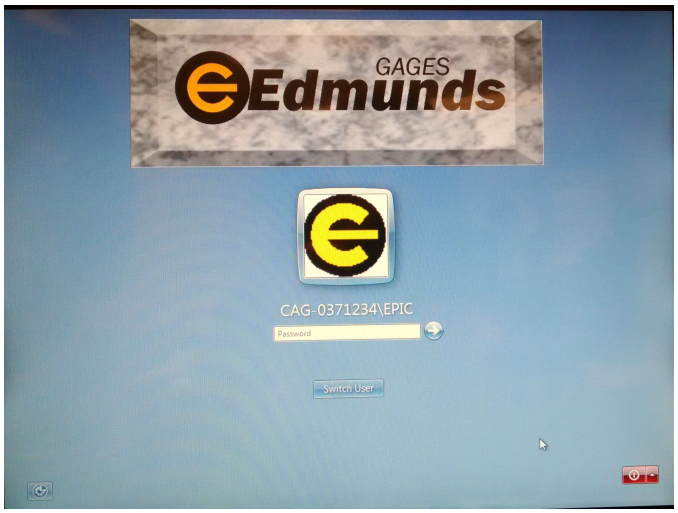
Default Logon

User Account

The default User Account is the account that will automatically log-in at initial power up. This User Account is setup before unit is shipped from the Edmunds Gages facility. This is the account that should be used for normal standalone gaging operation where no networking is required or special user accounts are required. There is no password associated with this account by default and the account has Administrator rights. This account should be used for network and system configuration because it has the required Administrator rights.

Default User Account (Administrator rights):

Computer Name: CAG-XXXXXXX (where XXXXXXX is the unit serial number, example CAG-0367123)
User Name: EPIC
Password: no password assigned
** assigned to automatically logon by default.*



Before Configuring the EPIC CAG™ for Networking

Before configuring the EPIC CAG™ for network connection, be aware that a Drive Protection utility is utilized to protect the unit and will prevent your EPIC CAG™ configurations from persisting after restart. Local Windows settings and profile configurations that are made are removed by the Drive Protection utility to prevent undesired flash memory writes and "clean-up" extraneous information from being stored on the local disk. Note that this does not pertain to changes made within the EPIC gaging application. While the Drive Protection utility protects EPIC CAG™ in important ways, there are instances where administrators need configuration changes to persist after logging off and restarting.

CAUTION: Before configuring the EPIC CAG™, see "Working with Drive Protection"

2. Drive Protection

Introduction to Drive Protection

The EPIC CAG™ has built in Drive Protection to insure absence of system failures due to operating system file corruption. The Drive Protection feature used on EPIC CAG™ utilizes the File Base Write Filters (FBWF) feature that has been incorporated into the Windows Embedded Standard 7 operating system. The Drive Protection allows the ability to protect the drive (compact flash) from write access. Instead of writing directly to a disk, disk writes are redirected into RAM cache called an overlay. The data that has been stored in the RAM overlay will not persist if the unit is powered down or power is lost. Some files and configuration such as the gaging results and setup of the EPIC gaging application are allowed to be written directly to disk for permanent storage.

The major benefit of Drive Protection is that changes to the operating system files are written to the RAM overlay and not to permanently stored to the disk. If the system files become corrupt, they are not written to the disk. Thus, upon next reboot, the system files will be restored. Drive Protection can also help protect against unintended or malicious changes to the system. If a virus or malware is installed, it will be written to the RAM overlay and not written to the disk. On next reboot, the malicious software will not persist. The features of Drive Protection are also beneficial in preventing accidental tampering of the EPIC CAG™ system. For instance, if a user alters some of the files or configuration data, the user could simply reboot the unit to return back to a original state. The Drive Protection also extends the life of compact flash media. Flash-based storage media has a finite number of erase cycles before erase blocks wear out. This means that there is a finite life span for a compact flash drive. Since Drive Protection redirects files writes into RAM this can decrease the amount of data being written to disk; thus, extending the life span of disk.

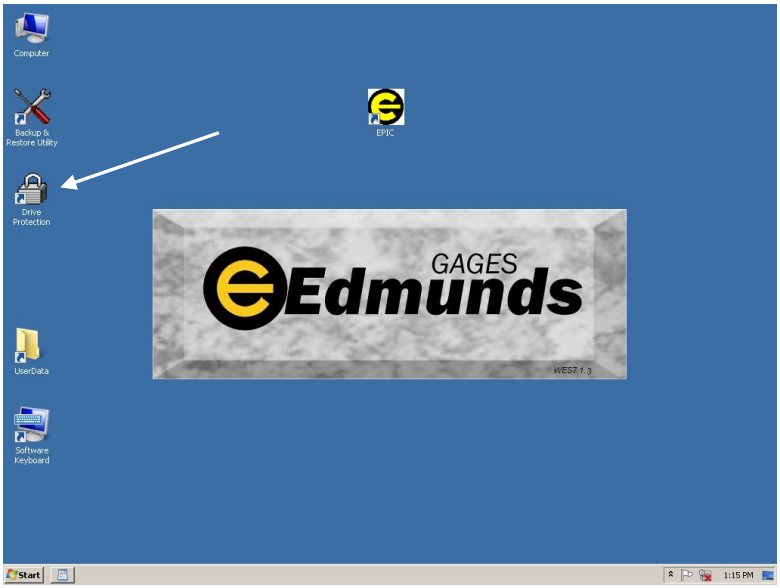
To make Windows configuration changes, such as changing Ethernet IP address or setting up the system to connect to a network, the Drive Protection will have to be disabled (see "Working with the Drive Protection Utility"). ***NOTE: The EPIC gaging application will not run if Drive Protection is disabled so it is important to re-enable Drive Protection as soon as the changes are complete.***

Working with Drive Protection

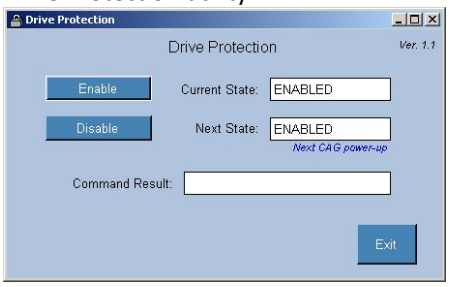
Drive Protection provides a secure environment for EPIC CAG™ by protecting the drive from undesired flash memory writes. Changes made to the EPIC CAG™ configurations are lost when the unit is restarted unless Drive Protection is disabled during the current system session. The Drive Protection utility can be used to disable, enable and view current status of the Drive Protection feature. Administrators right is required to use the Drive Protection utility.

Running the Drive Protection utility

1. Log on with Administrator rights (see "Default Logon").
2. If the unit is currently running EPIC gaging application, exit the application in order to get to the Windows desktop.
3. Open the Drive Protection utility by clicking on the “Lock” icon.



Drive Protection utility

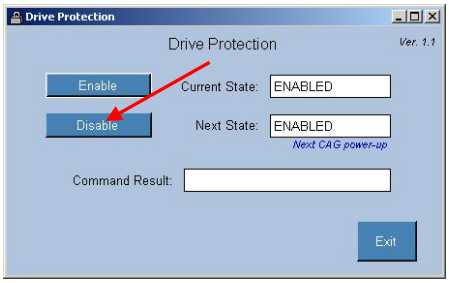


Drive Protection State

The “State” of drive protection is either “Enabled” or “Disabled”. The current state (Enabled/Disabled) can only be be changed by the operating system at power-up. The Drive Protection utility displays the “Current State” and the “Next State”. The “Current State” indicates if drive protection is Enabled or Disable on the running system at that point in time. The “Next State” indicates if drive protection will be Enabled or Disabled after the next reboot power-up.

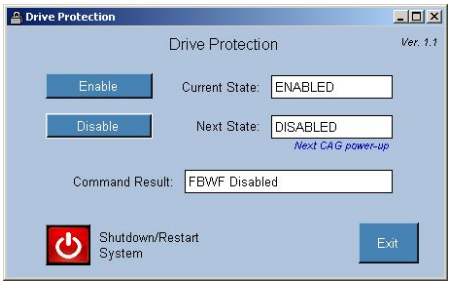
Disabling Protection Protection

1. Select the “Disable” button.



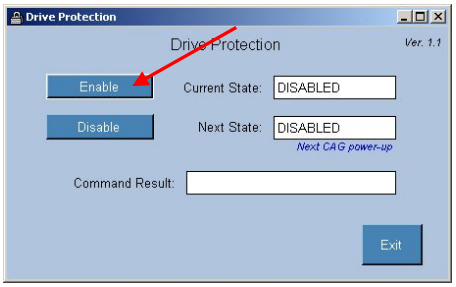
2. Select OK.

3. Drive protection will be disabled upon next power-up. The “Shutdow/Restart System” button can be used to restart the system.

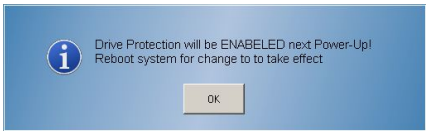


Enable Protection Protection

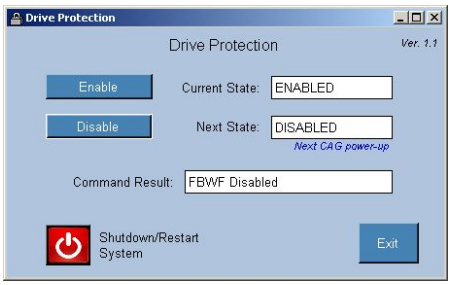
1. Select the “Enable” button.



2. Select OK.



3. Drive protection will be enabled upon next power-up. The “Shutdow/Restart System” button can be used to reboot the system.

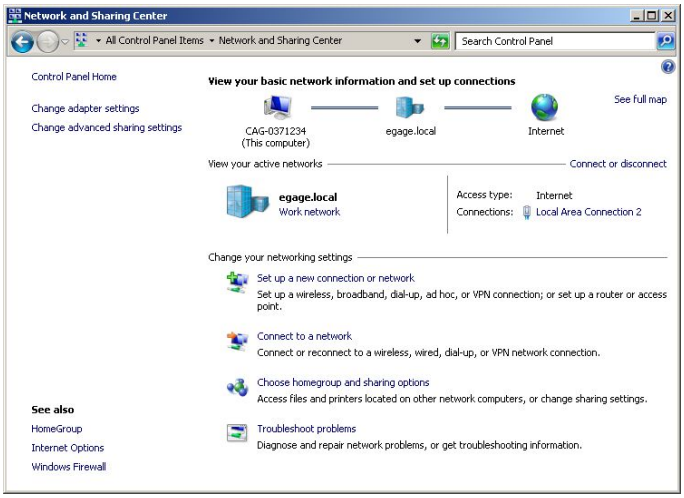


2. Networking

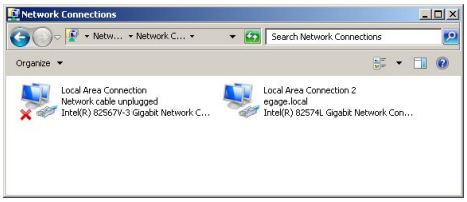
Setting Static/Dynamic IP Address

The EPIC CAG™ has two Ethernet adapter on board. Depending on the EPIC CAG™ hardware configuration and gage requirements one or two of Ethernet connectors will be available for network connection. In many cases one Ethernet connection (adapter) will be used for local connection to machine control (PLC) or other peripheral device and the other connection (adapter) used to connect to facilities network.

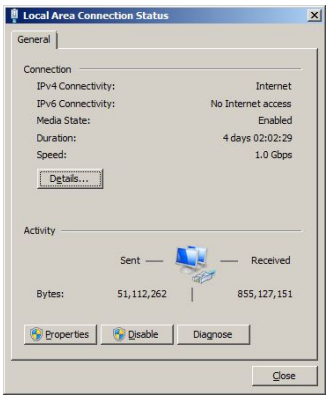
1. Logon with Administrator right (see "Default Logon").
2. Disable Drive Protection, reboot of system required. (see “Disabling Drive Protection”).
3. Select **Start->Control Panel** and open **Network and Sharing Center.**
4. Select “Change adapter settings”

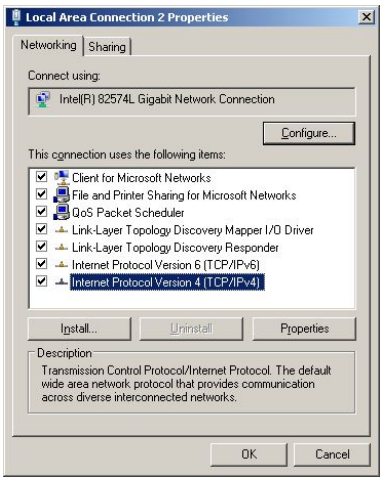


5. Double click on the “Local Area Connection” corresponding to the Ethernet adapter being used.
   NOTE: ***both “Local Area Connections” can not be on the same network (assigned the same first three set of IP address numbers).***

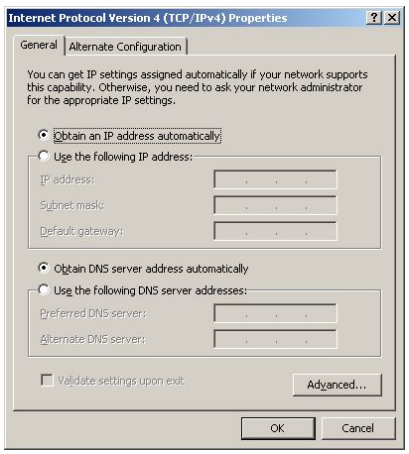


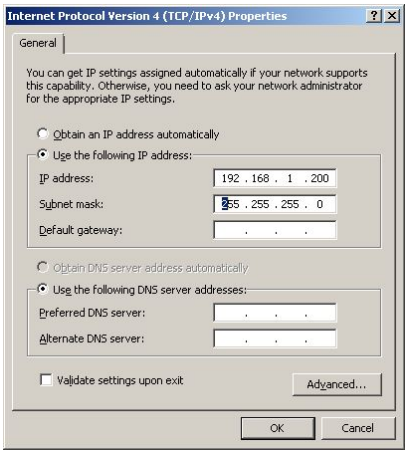
6. Select Properties and and select “Internet Protocol Version4(TCP/IPv4). Select properties.





7. If IP address is to be assigned automatically by DHCP then select “Obtain an IP address automatically”. If the IP address is to be static then select “Use the following IP address” and enter the IP address and Subnet mask.

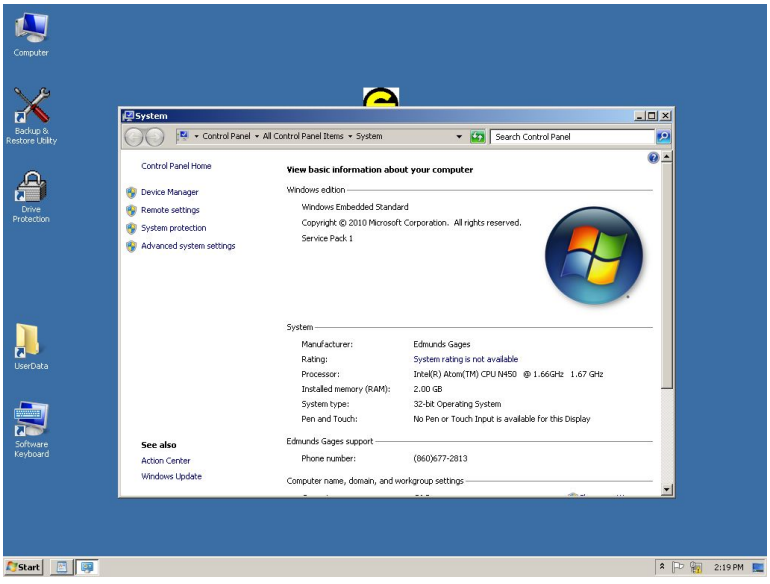




8. Enable Drive Protection, reboot of system required. (see “Enable Drive Protection”).

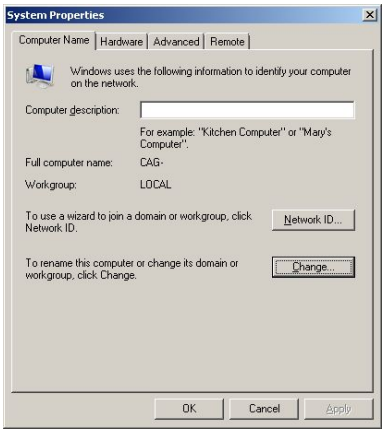
Changing Computer Name EPIC CAG™

1. Logon with Administrator right (see "Default Logon").
2. Disable Drive Protection, reboot of system required. (see “Disabling Drive Protection”).
3. Right click on the “Compute” icon on desktop and select properties.

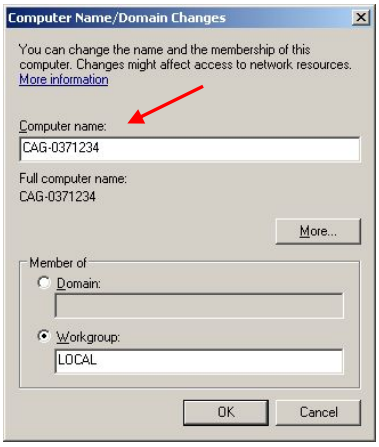


4. Select “Advanced system settings”.

5. Select “Computer Name” tab and select “Change” button.



6. Enter new computer name.

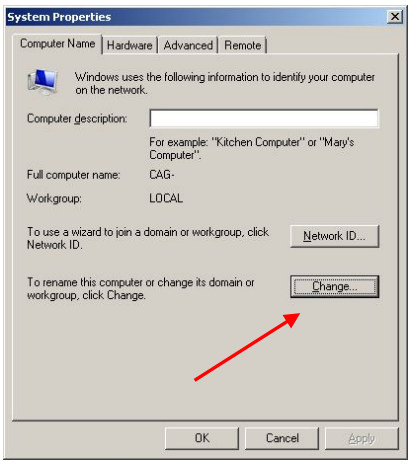


7. Restart the system.
8. Logon with Administrator right (see "Default Logon").
9. Enable Drive Protection, reboot of system required. (see “Enable Drive Protection”).

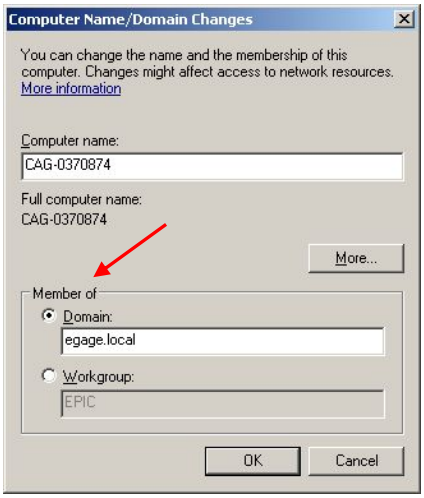
Joining a Domain

A domain is a collection of computers on a network with common rules and procedures that are administered as a unit. Each domain has a unique name. Typically, domains are used for workplace networks. To connect your computer to a domain, you'll need to know the name of the domain and have a valid user account on the domain. **CAUTION**: **To save the settings so that they persist after reboot, be sure disable Drive Protection (see "Disabling Drive Protection").**

1. Logon with Administrator right (see "Default Logon").
2. Disable Drive Protection, reboot of system required. (see "Disabling Drive Protection").
3. Set the EPIC CAG™ IP Address as required to join the domain (see "Setting IP Address").
4. Right click on "Compute" icon on desktop and select properties.
5. Select "Advanced system settings".
6. Select "Computer Name" tab and select "Change" button.

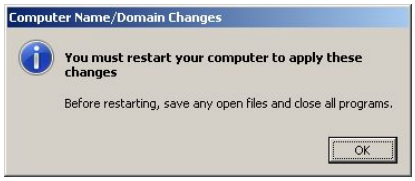


7. Select "Domain" and enter the domain name.



8. Enter a valid user name and password.

9. If successful will get the following message.



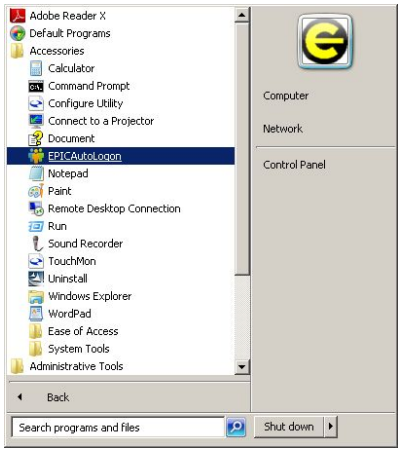
10. When system restarts logon with administrator right in order to enable drive protection. (see "Default Logon").
11. Enable Drive Protection, reboot of system required. (see “Enable Drive Protection”).

3. EPIC Auto Logon utility

The EPIC Auto Logon is a utility than can be used to enable or disable Auto Logon, and to change the default user logon User name, Password, and Domain for EPIC CAG™. ***CAUTION: Drive Protection must be disabled to to use the EPIC Auto Logon utility (see "Disabling Drive Protection").***

Starting the EPIC Auto Logon utility

1. Log on with Administrator rights (see "Default Logon").
2. Disable Drive Protection, reboot of system required. (see "Disabling Drive Protection").
3. Select ***Start > Accessories > EPICAutoLogon***.



EPIC Auto Logon Settings

Default Logon User: If this option is selected the user account specified in the "User Name" field will be assigned as the default user when system powers-up (prompt for password).

Auto Logon: If this option is selected the user account specified in the "User Name" field will automatically attempt to logon at power-up using the information provided in the "Domain Name", "User Name" and "Password" fields.