

Configuring Windows 7 for a Limited User Account

Microsoft Windows Family of Operating Systems

Microsoft Corporation

Published: September 2009

Abstract

This document explains how to set up your Administrator accounts through User Account Control. User Account Control allows access to administrative rights, based on three account types: the built-in Administrator account; an account with administrative rights; and a standard, limited user account.



Copyright information

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, this document should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented. This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Microsoft may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. The furnishing of this document does not provide the reader any license to the patents, trademarks, copyrights, or other intellectual property rights except as expressly provided in any written license agreement from Microsoft.

Microsoft does not make any representation or warranty regarding specifications in this document or any product or item developed based on this document. Microsoft disclaims all express and implied warranties, including but not limited to the implied warranties or merchantability, fitness for a particular purpose, and freedom from infringement. Without limiting the generality of the foregoing, Microsoft does not make any warranty of any kind that any item developed based on these specifications, or any portion of a specification, will not infringe any copyright, patent, trade secret, or other intellectual property right of any person or entity in any country. It is your responsibility to seek licenses for such intellectual property rights where appropriate. Microsoft shall not be liable for any damages arising out of or in connection with the use of these specifications, including liability for lost profit, business interruption, or any other damages whatsoever. Some states do not allow the exclusion or limitation of liability or consequential or incidental damages; the above limitation may not apply to you.

© 2009 Microsoft Corp. All rights reserved.

Note

This blog was written by Steve Friedl (Unixwiz.net Tech Tips), and it originally published May 2009. He thanks Susan Bradley (Microsoft MVP) and Crispin Cowan, PhD for their assistance.

Windows® 7 has now been released and many are trying this new operating system. Those who skipped past Windows Vista® from Windows XP are finding a new experience and an entirely new security paradigm: User Account Control (UAC).

UAC was introduced with Windows Vista and was widely maligned due to its “in-your-faceness.” Although it's calmed down some as Windows Vista has been updated, it seems to have really hit its stride in Windows 7. I like UAC a lot.

But even in its imperfect form, it was a good idea, attempting to brighten the terribly blurry line between administrative tasks and user tasks that has plagued Windows since the early days.

Much of this is due to the early consumer operating systems Windows 95, Windows 98, and Windows ME, which maintained **no** technical distinction between these roles: everybody was always an administrator, and software developers had no way of even thinking about a separation of roles.

But even with the more modern Windows NT systems, Windows 2000, and Windows XP, it was so painful to really get your work done as a non-administrative user that most people simply gave up and ran with an Admin account. This was almost entirely due to poor habits by software developers: they themselves ran as Admins, and they simply wrote sloppy code that assumed everybody was one too.

Microsoft® has been trying very hard to counter this “everybody-is-an-admin” mentality, and UAC was their attempt at compromise—if you're going to run as an Admin, at least we can make you aware of the role differences. This is what UAC is attempting to do.

This Tech Tip was written exclusively for the Windows 7 experience, but most of it applies to Windows Vista as well. In addition, this paper describes workgroup or standalone computer setups only; it does not address the more complex enterprise environments for domain-joined computers.

Notes

For a complete view of Windows 7 resources, articles, demos, and guidance, please visit the [Springboard Series for Windows 7](http://go.microsoft.com/fwlink/?LinkId=147083) on the Windows Client TechCenter.

For a Web version of this document, see the [Configuring Windows 7 for a Limited User Account](http://go.microsoft.com/fwlink/?LinkId=165706) in the Microsoft Download Center (http://go.microsoft.com/fwlink/?LinkId=165706).

User Account Control explained

User Account Control works by guarding access to administrative rights, and this involves elevations of privilege: when attempting to perform admin tasks, the operating system either auto-elevates to Admin rights or requests some kind of consent or credentials to do so.

Windows 7 recognizes three broad classes of users:

The built-in "Administrator" account

This account is special for a number of reasons, and is disabled by default in Windows Vista and Windows 7. Because this account explicitly turns off some important security features (such as Internet Explorer® Protected Mode) as well as UAC, it's a really bad idea to use Administrator for anything.

I strongly urge leaving the Administrator account disabled!

Keeping this account disabled (which means you won't be tempted to actually use it) will help keep you safer!

An account with administrative rights

Though a user has the ability to elevate to admin rights due to membership in the local Administrators group, UAC interposes itself at key times with prompts that confirm your intentions:

This is the Prompt-for-Consent mode, and upon clicking Yes, it will elevate the task and run as an Administrator.

For performing administrative tasks, always use this kind of custom admin account instead of the built-in Administrator.

Windows 7 introduces a slider to the UAC settings that allows for changing the level of UAC prompts, including a setting to disable it entirely (Admin-approval mode).

A standard, limited user

UNIX and Linux systems have never had the confusion between what's an administrative task and what's a user task—it was simply always apparent which was which.

What's more, the culture of this role distinction is best illustrated by behavior in the newsgroups in the eighties. If a user posted messages from his root account (the computer's administrator), he would be chastised: "Don't run as root!"

These accounts simply do not have the power to perform administrative tasks directly, nor do they have the ability to elevate with a mere confirmation. They instead require **credentials** such as a password or a smartcard. This is requested through the following prompt to the user:

This is informally known as Over-the-Shoulder mode (where somebody can lean over the user's shoulder to type a password and elevate an approved task).

I strongly believe in limited user accounts!

I've been doing so since Windows XP Service Pack 2, including my laptop and my main software-development workstation. It's been painful at times, but it's dramatically lowered the attack surface of my system, and it has contributed to my Windows computers never suffering a compromise.

Stepping into Windows 7, I of course, wanted to run as a limited user, but because I didn't know how it worked (in Windows 7 or in Windows Vista), I essentially locked myself out of my own computer (see [Securing yourself out of your own computer](#BKMK_Secure) later in this document).

So after figuring it out (and reinstalling a couple of times), I created this Tech Tip to assist a security-minded user to do the safe thing.

This paper presents two procedures: one for a first-time installation of the operating system and one for retrofitting an already-installed system where the main user is a custom admin.

Method 1: Configuring a new installation

A new installation is the easiest to get right because there's no prior setup to work around. This illustration uses two Windows accounts:

* SteveAdmin: The first account created during installation; it should be used solely for administrative tasks.
* Steve: The second account created as a standard user; this limited account is used for day-to-day work.

The built-in Administrator account will not be used in any way, and it will remain disabled.

Follow these steps to set up Windows 7:

Install Windows 7, creating an initial user named "SteveAdmin"

This should be the usual “install-from-DVD” process. The initial parts take some time (and at least one reboot) before asking any questions related to setting up users.

When prompted, name the first user SteveAdmin. It's automatically created as an Administrative account.

If you choose to give the account a password, be sure to remember it—it will be required for all administrative duties on your computer.

Complete the Windows 7 installation

This includes configuring Automatic Updates, addition of required drivers, configuring the network, and the like. This is all done as the Administrative user SteveAdmin.

Create a new account named "Steve" as a standard user

While logged in as SteveAdmin, navigate to the Control Panel:

* Click the Start icon.
* Click Control Panel.
* Click Add or remove user accounts under User Accounts and Family Safety.
* Click Create a new account under the list of current accounts.
* Populate the dialog box with the new user name—Steve—and then click Standard User.
* Click Create Account to make it so.

Assign a password to the new user "Steve" (if desired)

When the account has been created, a list of current users appears with the caption, "Choose the account you would like to change." Click the icon for the newly created Steve account, which should be listed as a Standard User.

Click Create a password, and enter a password (twice!), along with a password hint if you like.

Because you're changing the password for a different user than yourself (Steve versus SteveAdmin), the following ominous message appears, which can be disregarded: “If you do this, Steve will lose all EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.” Because this user was freshly created, there is no private data to lose, so we can ignore this message and proceed.

Dismiss the Control Panel dialogs, log out, and log on as Steve

At this point, Steve is a standard user. Now that we're a standard user, attempts to perform admin tasks are greeted with a UAC prompt for SteveAdmin's password.

Method 2: Convert an already installed Admin user

This method is used if Windows 7 has been already set up, where the installer user (here, Steve) was automatically created with administrative rights. Though one could technically rename the account to SteveAdmin and make a new account for Steve as a limited user, this would play havoc with the user profiles, the desktop, and other personal configurations. It's possible to copy profiles, but it's easier to create a new Admin account and demote this one.

These are the steps:

Create a new SteveAdmin user

Login as Steve, who is still an Administrative user, and navigate to the Control Panel to create a new user:

* Click the Start icon, and then click Control Panel.
* Click Add or remove user accounts under User Accounts and Family Safety.
* Click Create a new account under the list of current accounts.
* Populate the dialog box with the new user name—SteveAdmin—and then click Administrator.
* Click Create Account to make it so.
* Now we have a new SteveAdmin account without a password yet! And this system now has two Admin users.

Assign a password to the new user, SteveAdmin (if desired)

When the account has been created, a list of current users appears with the caption, "Choose the account you would like to change." Click the icon for the new SteveAdmin user, which should be listed as an Administrator.

Click Create a password, and enter a password (twice!), along with a password hint if desired.

Because you're changing the password for a different user than yourself (SteveAdmin versus your logged-in Steve account), the following ominous message appears, which can be disregarded: “If you do this, SteveAdmin will lose all EFS-encrypted files, personal certificates, and stored passwords for Web sites or network resources.” Because this user was freshly created, there is no private data to lose, so we can ignore this message and proceed.

This completes the creation of the SteveAdmin account, leaving two accounts on the computer with Admin rights.

*Do not dismiss the dialog yet!* We'll be getting right into the next step from here.

Demote the user "Steve"

With the SteveAdmin account in good shape, it's time to demote the original installation user Steve from an administrator to a standard user. Since we're still in the Control Panel, we can easily pick up where we left off:

* Click Manage another account.
* Click the icon on the Steve account.
* Click Change the account type.
* Click Standard User.
* Click Change Account Type.
* Dismiss the Control Panel dialogs.

The next time user Steve logs on, he'll have strictly standard user powers.

Log out as "Steve," then right back on

Logging out destroys the session token that still has Admin rights, so the next logon gets the new set of limited rights.

After you are logged on as a limited user, attempts to perform Admin tasks are greeted with a UAC prompt asking for credentials for the SteveAdmin user.

Disabling the Administrator account

At this point, one of the two procedures has set up a limited user Steve and a proper administrative account SteveAdmin, but some users might have previously enabled the built-in Administrator account as well.

I believe this is a bad idea, and I recommend that the account be disabled. This won't be required if you've freshly installed Windows 7, or if Administrator does not appear on the logon page as an icon for a user who can log on.

If you're not sure, the steps to check and disable are almost the same:

Open the “Manage Users” applet

Enabling and disabling accounts is not done in the same place where you created a new user, so it requires navigating to a new place.

* Click the Start icon.
* Right-click Computer, and then select Manage**.**
* Navigate to Users.
* Double-click Administrator.
* Insure that Account is disabled is checked (if it was already checked, you're done).
* Dismiss the dialog boxes.

At this point, the Administrator account is disabled, and it cannot be used to log on or to approve UAC elevations. It's not necessary to change the account's password because disabling the account overrides any password (even a blank one).

Picking a password

Curiously enough, it's not always necessary to have a password on an account. Since an account with a **blank** password cannot be accessed over the network, you can substantially reduce the attack surface of a computer this way.

But this requires that you have good control of physical security over the computer. If there are users on the computer (or in the environment) who are not allowed to perform administrative duties, it would be a poor idea to have a blank password because it would allow anybody to walk up to the computer and go to town.

In addition, a laptop that leaves the house is probably not a good candidate for a blank password because physical security is seriously problematic.

For most home users, it probably doesn't really matter that much how you choose your password schemes, but if you have any questions about this, please present your scenario to a trusted security adviser for guidance.

Securing yourself out of your own computer

As noted earlier, I had not set up Windows Vista before, so I was unaware that the Administrator account was disabled by default. This lead to an uncomfortable surprise after demoting the installation account Steve.

After configuring our computer, I'd gone into the Control Panel to downgrade the Steve account to a Standard User account. I had unknowingly removed the only remaining Admin account, so after logging out and logging back on (to allow the account change to take effect in our session), the next UAC operation provided the following prompt:

The careful reader will note that ***there is no place to enter a password!*** To say that this was maddening would be an understatement. Depending on your computer's configuration, there may be an invitation to use a smartcard, but that won't likely do much good on a computer that has not had smartcards configured.

It seems like a poor user experience, even though technically it was my own fault.