Soroban Support Guide

Why you SHOULD always create TWO Windows accounts

Summary

Provides an explanation as to why you should always have at east TWO Windows accounts to make your system safe:

- One will be an Administrator Account that permits you to make changes to your system
- The account that you use for normal day to day tasks should be a Standard User Account.
  - Using this account for all your work prevents you, **or any malware**, from directly making changes to your system
  - To make significant changes you need to enter the Administrator Account password and this greatly reduces the chances of malware silently infecting your computer

Original Author: John Steele
Revised by: John Steele
Version: 2.00
Date: 16 Nov 2023

Copyright Notice

Revisions

Version	Date	Changed by	Summary of change
1.0	9 Aug 2022	John Steele	Transferred from the Gerrards Cross Computer Club site and copyright updated to Soroban Systems
1.01	12 Dec 2022	John Steele	Minor changes to layout of title page
1.02	18 Jan 2023	John Steele	Revised document template – changed layout slightly
1.03	11 Aug 2023	John Steele	Minor typo
2.00	16 Nov 2023	John Steele	Further clarification about Admin and User accounts

Table of Contents

1 OVERVIEW

1.1 The Problem

Microsoft have produces a VERY secure Operating System in Windows 10 and 11. They have always recommended a method of of using it securely but regrettably I have never seen a computer manufacturer supply a new computer with instructions on how to set this up.

If this is not done correctly your computer is FAR more vulnerable to being compromised than it was intended to be. Adding anti-malware software, **and ensuring it is up to date** goes some way to mitigating the additional **and unnecessary** risk but does not replace the security that you already have, but are not using.

1.2 An analogy

An approximate analogy of the security using a real world scenario might go as follows.

- You are the owner of a company with employees and the data the employees process is confidential and hence must not be shared with other staff.
  - You, as the company owner, are permitted to see the information that each employee holds on a “need to know” basis.
- Each staff member has an office with a locked filing cabinet for all of their current and historical work
  - Each has their own physical key to access their own filing cabinet but nobody elses.
- You, as the company owner, have a Master Key that can open any of their filing cabinets.
  - This would be used in case of an emergency where the data was needed but the staff member was unavailable.

If anyone, whether another employee or an intruder, tried to gain access to the private data they would have to either break into the filing cabinet, or obtain a copy of that individuals key or the Master Key. If they were able to obtain a copy of the master key they could then access ALL the information held by everyone. If they only obtain a user key they could only access that user’s data thus the data loss would be minimal.

1.3 User Accounts

Microsoft, in common with all current Operating Systems, manages security by having “User Accounts”. Each account has associated **privileges** which determine what the user is allowed to do.

There must be at least one **Account** created on your Windows computer for you to be able to access it. When you run a manufacturer's initial set up program an initial account is created during this process.

There are two types of User account which are intended for different purposes.

1. An **Administrator Account** is intended (and required) to be used for updating and maintaining the computer and the FIRST account created when initially setting up a new computer has to be an Administrator account
   - This account is a member of the **Administrator Group**

- There must always be at least one Administrator Account on each computer
    - This deliberately bypasses many of constraints imposed on Standard User accounts such as preventing installion of new programs.
    - When attempting to install programs using the User account the installer will typically pop up a dialogue box asking for the Administrator Account password to continue. **This is NOT a nuisance – it is your major defensive measure!**
- An Administrator Account is TRUSTED by Windows.
    - That is why you MUST NOT use it for general day to day work.
    - For home users there is typically only one Administrator account.

2. A **Standard User Account** is intended for day to day use.
    - This account is a member of the **User Group**
    - There SHOULD always be at least ONE User Account on each computer
    - There can be more than one User Account on a computer if there are two or more people sharing a computer.
        - Unless one user deliberately allows it one Standard user does not have permission to access another Standard user’s data.

Almost every aspect of Windows operation is regulated by **Permissions**.

All Standard User accounts belong to a Users Group and membership of that Group sets the Permissions which control what that user is permitted to do.

All Administrator accounts belong to an Administrators Group which grants far more extensive Permissions to members of that group of accounts.

1.3.1 Permissions

Permissions control whether an attempted operation is permitted, or not, on a resource such as a file. An example is an attempt to access file:

- If a file has Read Only permission any attempt to write to that file will be rejected.
- If a file belongs to another User then access will be denied unless explicitly granted by the owner
- If a file is marked as being a program (an executable file) it needs Administrator Permissions to install it or make changes to it.

Permissions may be granted at a Group or individual account level.

It should be evident that changing a permission is only possible if the account attempting to change that permission actually has the permission to do so.

An Administrator Account usually has permission to change, or override, any permissions on a resource whether they own the resource or not.

The administrator account will also typically need, and will have, fewer restrictions than a user account.

For example a program running with Administrator privileges can install software on the computer and can even install it so that it runs silently when the computer is rebooted.

This is what malware does.

You are totally reliant on having anti-malware software to prevent this happening if you always use an Administrator account.

A User Account can only change permissions on a resource that they own.

A program running with User Account privileges **cannot directly install** any software as the installation folders are protected from writing by their permissions so Malware is prevented from installing any persistent software. **This is without any anti-malware software being present.**

Attempts at installation will usually result in a prompt to enter the Administration account credentials. In other (now rare) cases you will need to logon to Windows with your administrator account

This is not a nuisance – it is essential protection

Note that programs can still be run but cannot be persistent.

This is the key to understanding the purpose of have two User Accounts and using them correctly.

2 HOW TO SET UP A NEW MACHINE CORRECTLY

When running the initial set up on a new computer be aware that it is the **Administrator Account** you are creating and NOT the one you should normally use. It is all too tempting to use your own name i.e. the one you plan to use for all your work. Ideally you should create a new name for this account e.g. John-Admin whereas you actually want your account name to be John. You just need create this account later!

This is exactly what all computer manufacturers initial setup will initially create without telling you the risks and without encouraging you to set up a second account as a Standard User.

If you have done this already using your intended normal user name – don't panic. It is possible to correct it later – see Section 3.

The setup process typically wants you to use, or create, a login to a Microsoft account so you are actually logging into Microsoft every time you use your computer. **I don't have too much of an issue with this, although I choose not to do it.** This applies especially as you are creating your Administrator account first. Why would you want to use a Microsoft account here? This however is a personal decision.

Recent updates have made the option to AVOID using a Microsoft account increasingly difficult to find. I have not (yet) had to set up a new computer since the most recent updates but the reports on the Internet suggest that the only way available now is to avoid connecting to the Internet when initially prompted to do so. It will eventually allow you to continue with a Local Account. You can connect to the Internet later.

Once you have created this first account you will need to login to Windows to complete the setup. I recommend that you connect to the Internet and let all the updates happen before you go onto the next stage.

The final stage is to use Settings/Accounts to create your user account. This must be a **Standard User**

2.1 Multiple user Accounts

If the computer is going to be used by more than one person then it is probably preferable to set up more than one User Account, one for each user.

All the accounts will share the same set of programs. It is very difficult (not impossible) to make some programs available to one user and to prevent the other one being able to use it.

It is however easy to customise the Start Menu panel for each user so they have easy access to their own preferred set.

Unless explicitly allowed User Accounts are unable to access another User's data. If data needs to be shared a special set of folders called **Public** are accessible to all User and Administrator account(s).

3 CHANGING THE INITIAL USER FROM ADMIN TO STANDARD USER

If you have made the very common error of creating the first user account with the name and password you really want to use as your normal user account but has been created as an Administrator Account **all is not lost.**

You will need to perform a number of simple steps. These will make your computer as secure as it is intended to be.

1. Logon to your computer using the account that was initially created as Administrator and you now want to make into a Standard User Account.
2. Create a new Administrator account that you will in future use to make changes to your computer.
   a) Follow the steps given in this link Create a new User Account to create a new user account that will become the new Administrator account
      i You will need to choose
         - a name for the new Administrator account
         - a password for the new account – your security depends on this being a “good” password (a mix of letters and numbers and punctuation)
            - You will need this password to install any new software
         - Select suitable security questions from the list and invent appropriate answers that you can remember in case you forget this all important password. You will need to select 3 questions!
         - This will create a new Standard User account
      ii You now need to convert this account from Standard User to Administrator.
         - This is described in this link change account type to Administrator
3. You now need to sign out from your existing User Account and sign in with your new Administrator Account so you can change your initial account from Administrator to Standard User
   a) This time however use the link change account from Admin to User to see the steps to take
4. You will then logout from your Administrator account and login as your original account but now it only has Standard User privileges
   a) **You will now be MUCH safer**

4 PREVIOUS DOCUMENT HISTORY AND COPYRIGHT

A version of this document was written by myself and published on the Gerrards Cross Computer Club site using their logo.

When the club web site was being updated I was instructed, by the committee, to move it to my own Soroban Systems domain site, remove the GXCC logo, and remove all direct references to GXCC.

Permission was received to revert the copyright from GXCC back to the author, John Steele, and the document was rebranded and published on https://soroban.co.uk/ as a "Soroban Support Guide".