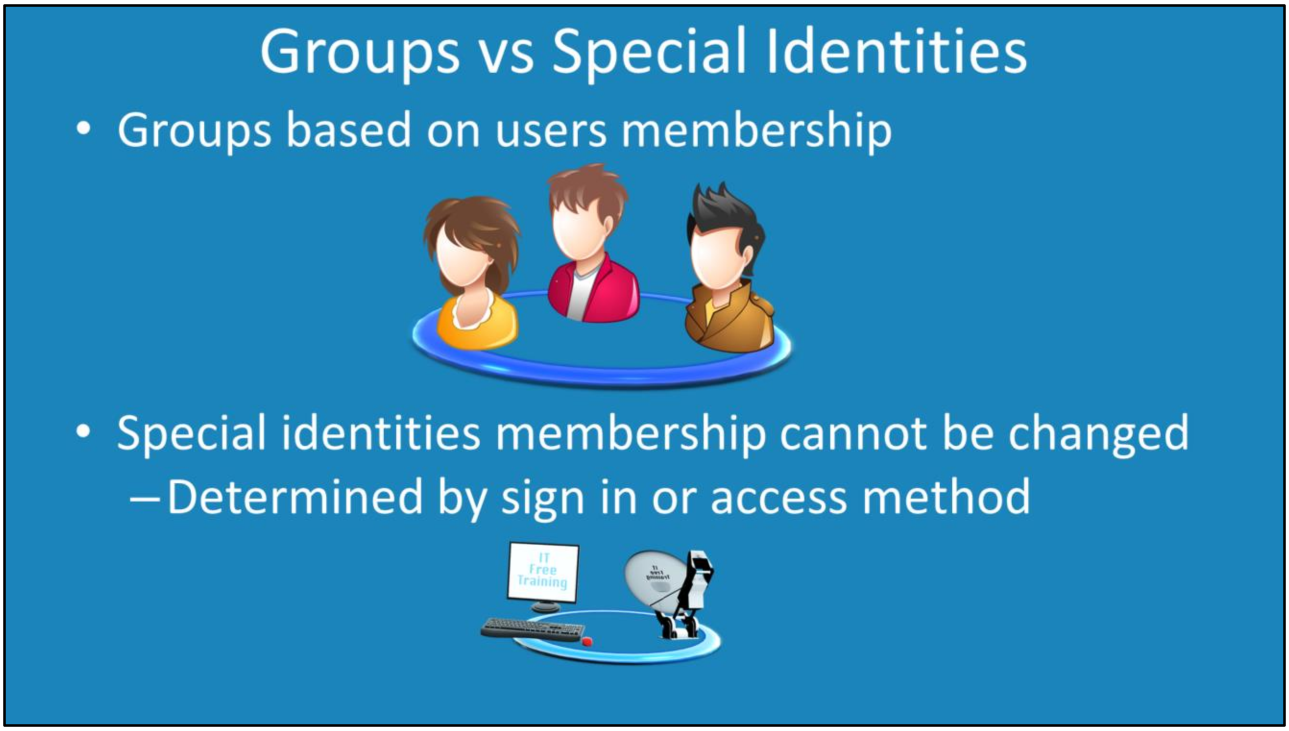
ITFreeTraining

Special Identities

For the free video please see
http://itfreetraining.com/server#/identities

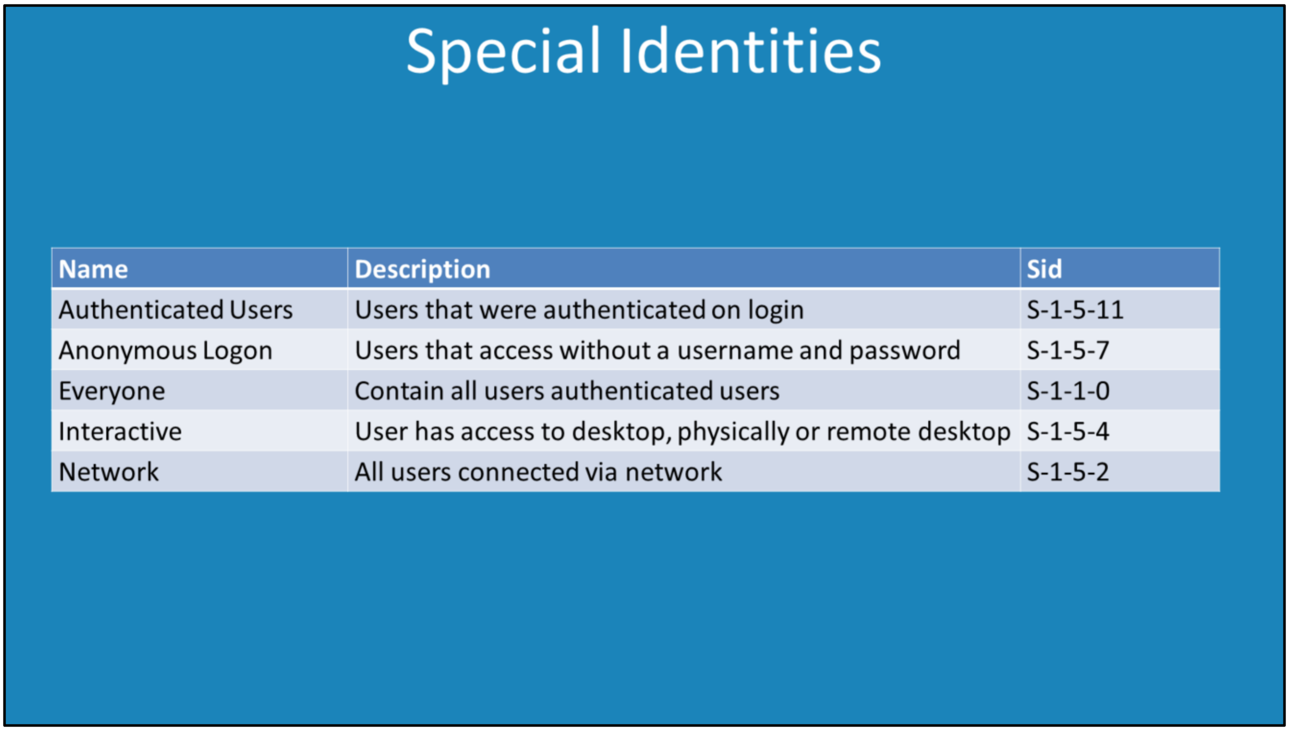
This video will look at special identities. These identities work like regular groups in Windows, however membership is configured automatically and allows the administrator to achieve results that are not possible with regular groups.



Groups vs Special Identities

- Groups based on users membership
- Special identities membership cannot be changed
  - Determined by sign in or access method

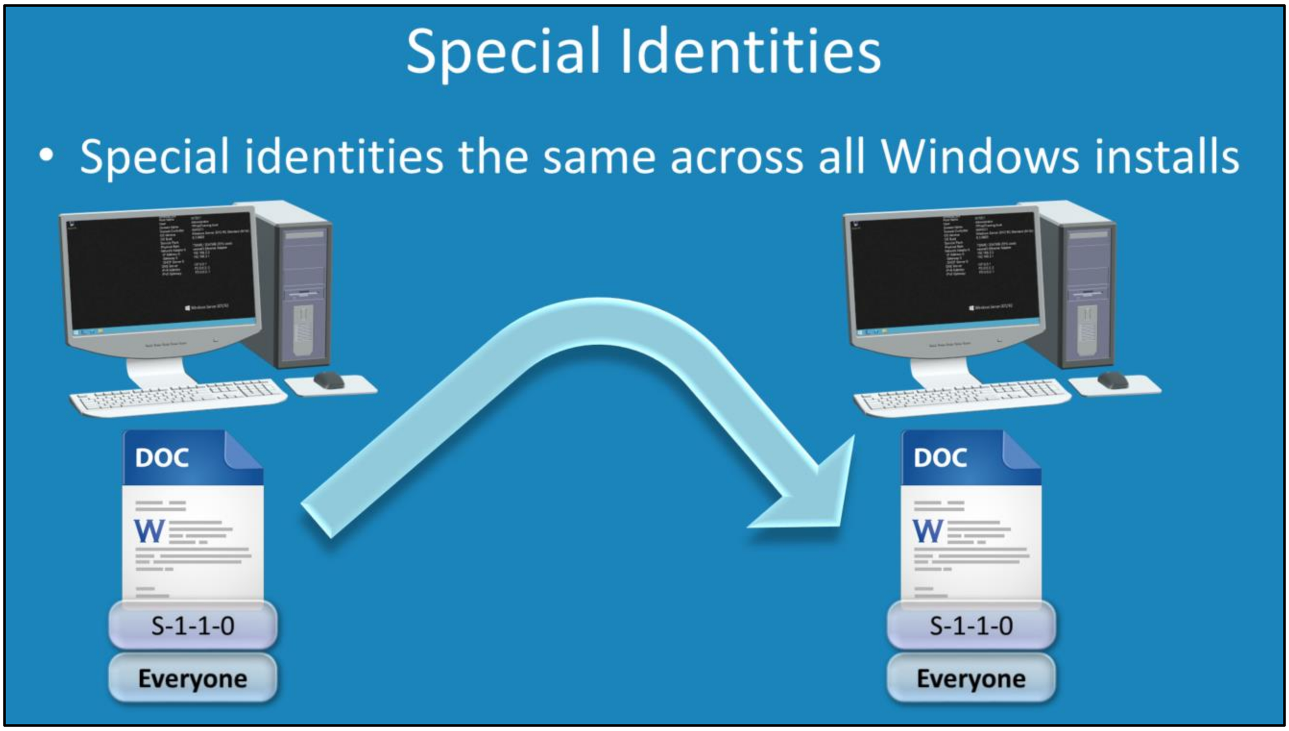
Users can be added or removed from a group. Special Identities in contrast cannot be modified by the administrator. A user is added or removed from a special identity based on conditions like which access method they used to sign in or how they are accessing the computer, for example wireless or wired.



Special Identities

Name	Description	Sid
Authenticated Users	Users that were authenticated on login	S-1-5-11
Anonymous Logon	Users that access without a username and password	S-1-5-7
Everyone	Contain all users authenticated users	S-1-1-0
Interactive	User has access to desktop, physically or remote desktop	S-1-5-4
Network	All users connected via network	S-1-5-2

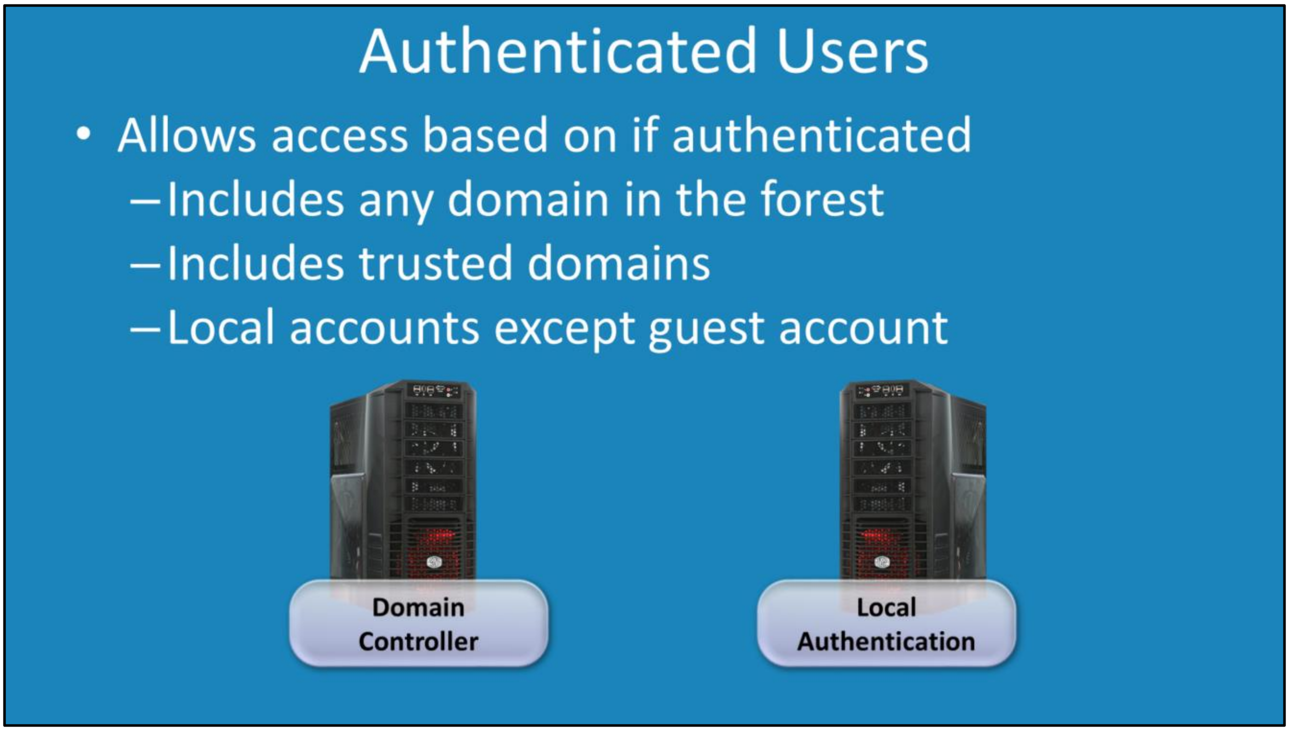
There are a lot of special identities in Windows. Additional special identities are generally added to later operating systems. This video will look at 5 commonly used special identities “Authenticated Users”, “Anonymous Logon”, “Everyone”, “Interactive” and “Network”.



Special Identities

- Special identities the same across all Windows installs

A special identity is always given the same SID. For example, the SID S-1-1-0 is for the special identity everyone. If a file is given this special identity, Windows will look up in its local database what the special identity is. If the file is copied to a different Windows computer, that computer will look up in its database to work out what that special identity is. Since later versions of Windows have more special identities, it is possible to copy a file to a different computer and Windows may not have that special identity in its database.



Authenticated Users

- Allows access based on if authenticated
  - Includes any domain in the forest
  - Includes trusted domains
  - Local accounts except guest account

Domain Controller

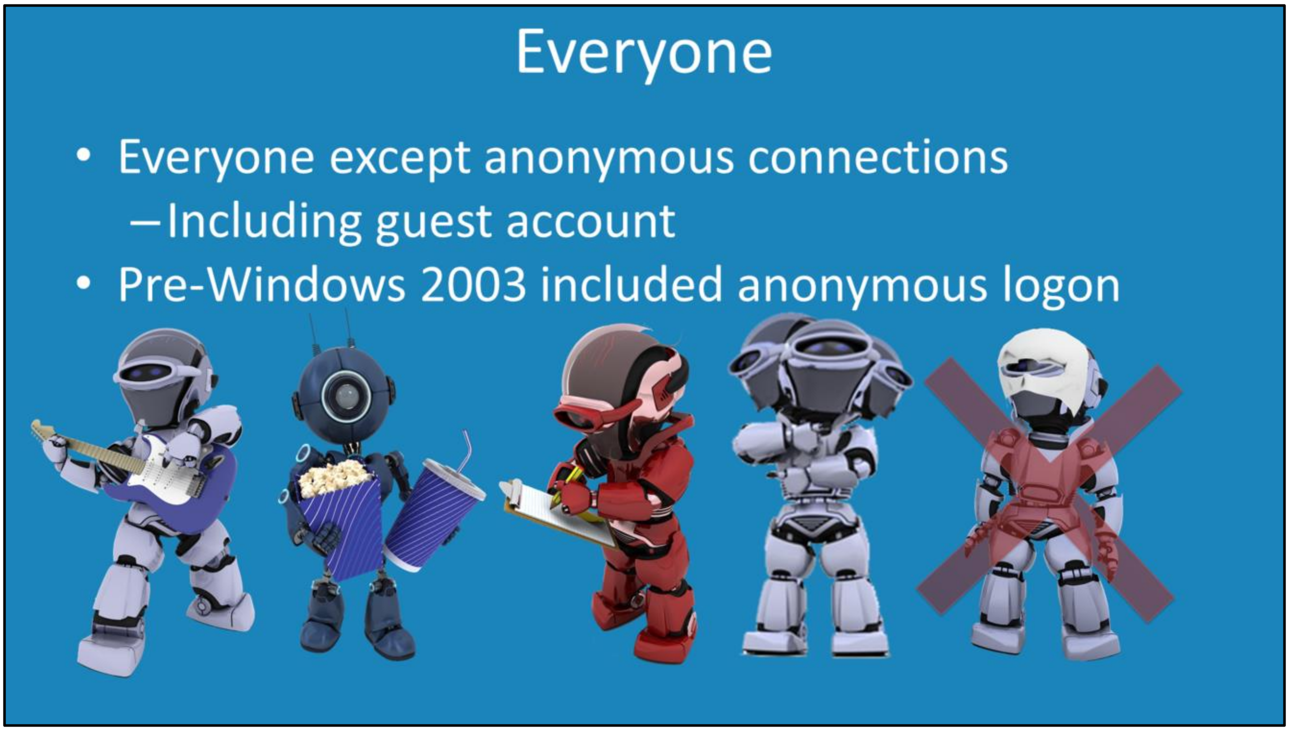
Local Authentication

Generally when a user is authenticated they will be added to the special identity. The authentication can happen in a number of different ways. The user may be part of a domain, a trusted domain or a local user account. As long as they are authenticated, for example using a username and password, they will be part of the authenticated users special identity. Anonymous and guest users are not included in the authenticated users special identity.

Anonymous Logon

- Allows access without a username and password

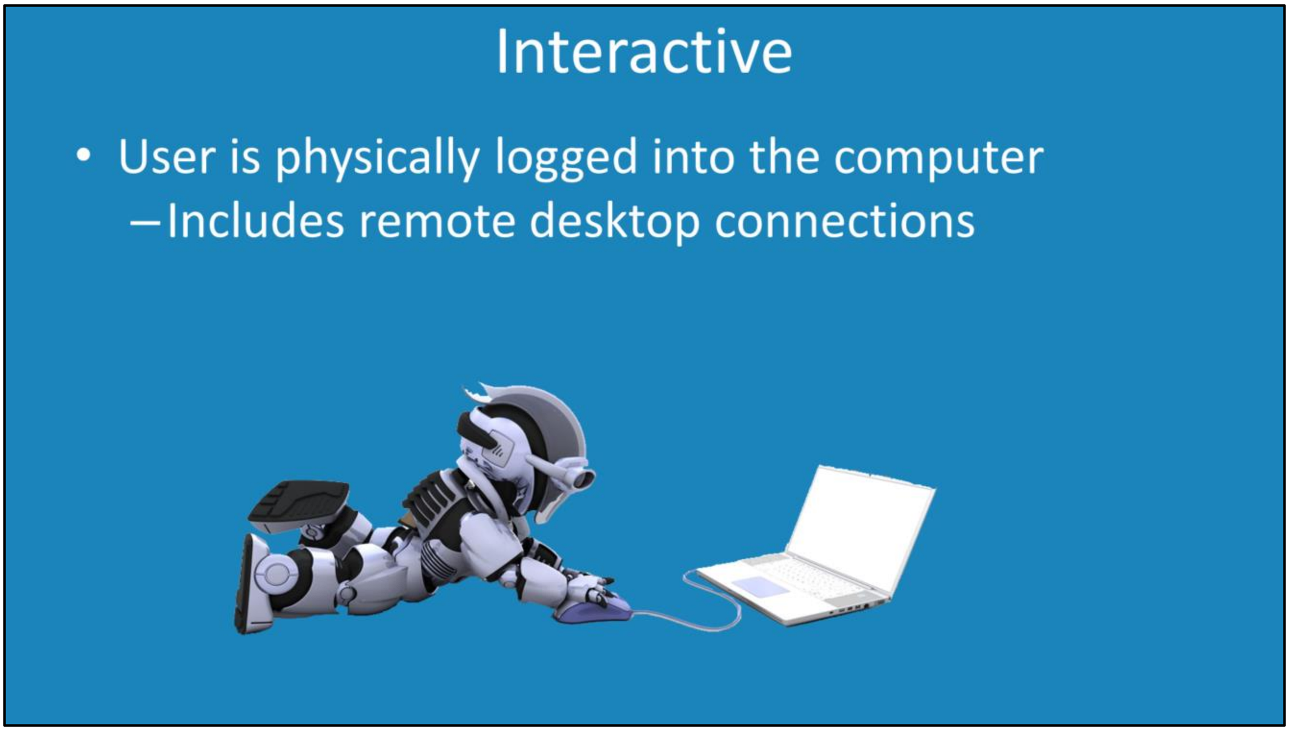
Membership of this special identity is determined by if the user is accessing the computer without at username and password. This is commonly used for public access servers. For example, if the user is accessing a web server then it is common for the anonymous logon special identity to be used. If the user is authenticated in any way, they will not be included in this group.



Everyone

- Everyone except anonymous connections
  - Including guest account
- Pre-Windows 2003 included anonymous logon

This includes also user authentication including the guest account except for the anonymous logon. The simple way to think of it is as any authenticated user. Anonymous user does not require any authentication. Pre Windows 2003 included the anonymous logon as part of the special identity everyone.



Interactive

- User is physically logged into the computer
  - Includes remote desktop connections

A user is included in this special identity if there are physically logged into the computer. This also includes remote desktop connections.

Network

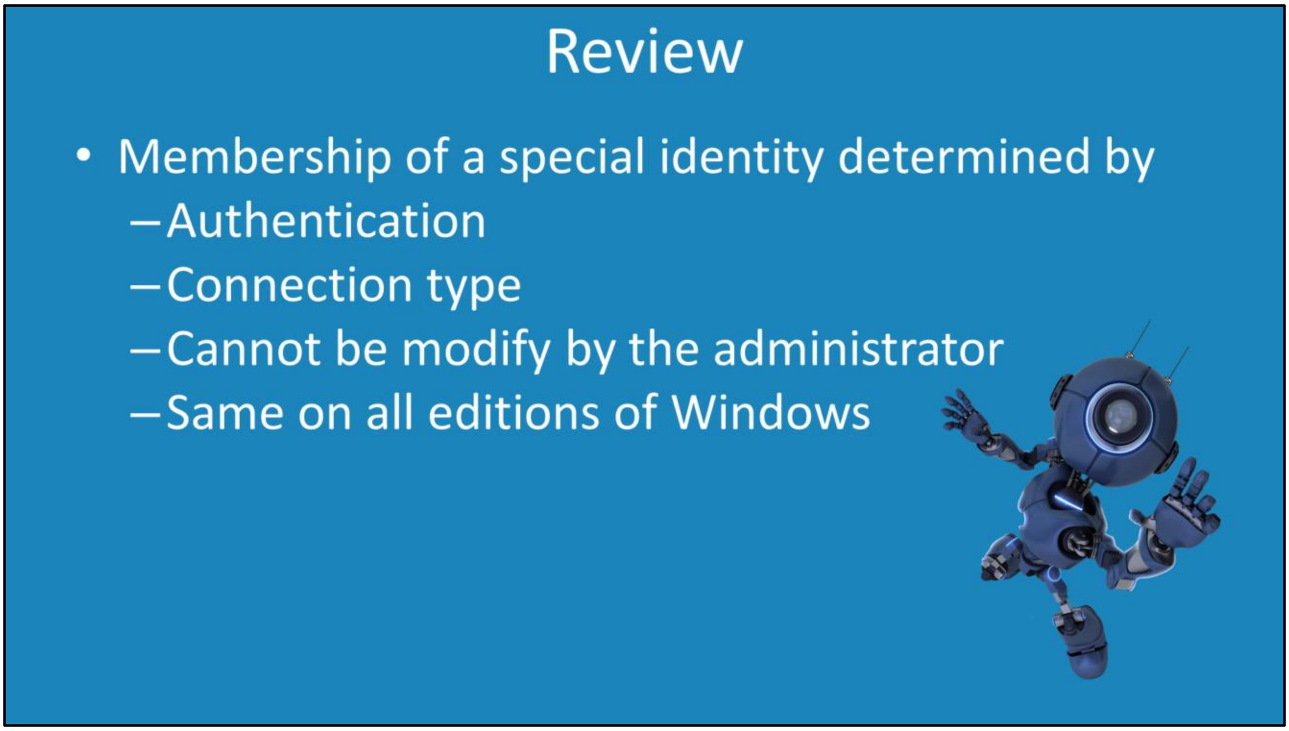
- Access any resource via the network
  - E.g. File and printing

A user is added to this special identity when they access a computer via the network. Examples would be file and print sharing, however remote desktop users are not part of that group. This is because remote desktop users are considered to be interactive users rather than network users. The user can connect by any type of network connection, e.g. wired, wireless or VPN.

Demonstration

In this demonstration, a folder will be created that can only be accessed by a user that is physically logged in the computer or over a remote desktop connection.

1) Open Windows Explorer and create a folder called Data.
2) Right click the Data folder and select the option properties.
3) Select the security tab.
4) The folder data is inheriting the permissions from the folder above. To switch inheritance off, press the advanced button and then press the button change permissions.
5) On the permissions dialog, untick the tickbox “Include inheritable permissions from this object’s parent”.
6) When prompted, press the add button so the previously used permissions will be used.
7) Remove authenticated users, and users group.
8) Add the user interactive and make sure location is set to the local computer.



Review

- Membership of a special identity determined by
  - Authentication
  - Connection type
  - Cannot be modify by the administrator
  - Same on all editions of Windows

Membership of a special identity is determined by authentication and connection type. The administrator cannot decide who is a member of a special identity as membership is determined automatically. Generally special identities work the same way on all editions of Windows so if a file is copied from one Windows system to another the file permissions should work the same.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"Special identities" http://technet.microsoft.com/en-us/library/cc778060(v=ws.10).aspx
"Well-known security identifiers in Windows operating systems" http://support.microsoft.com/kb/243330