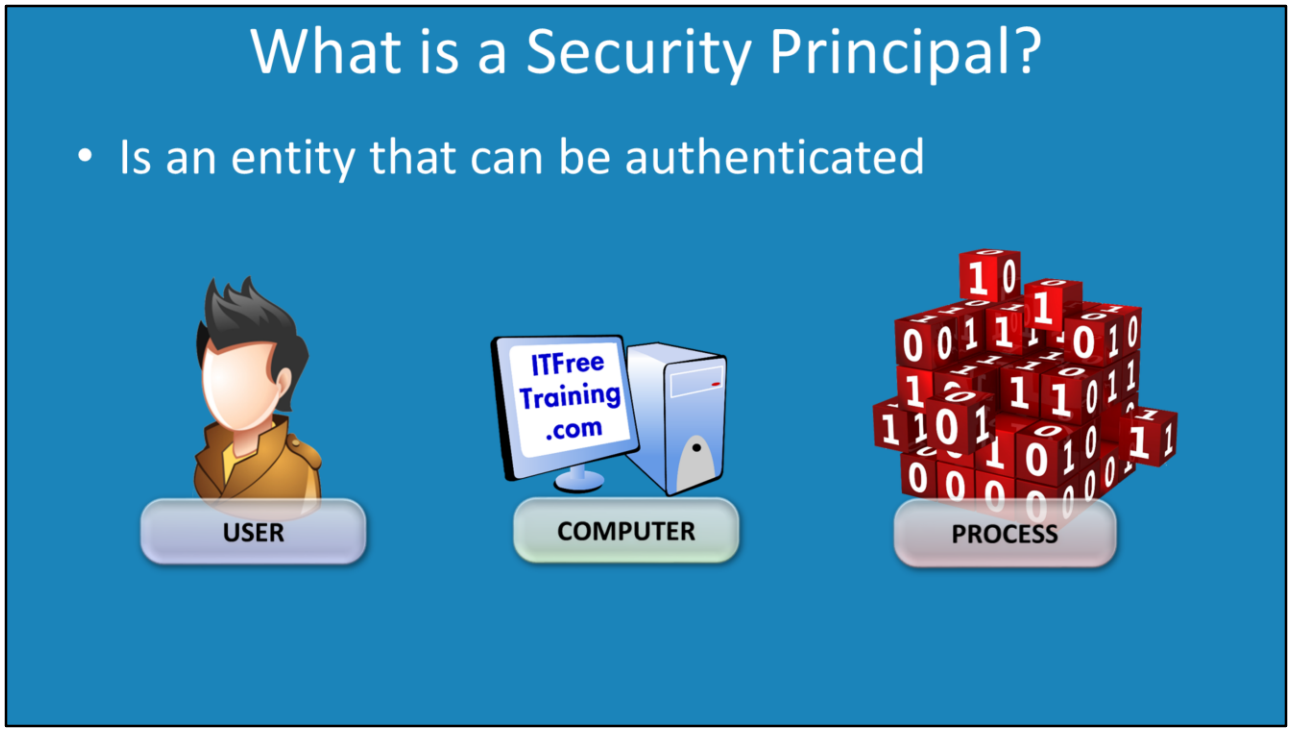
This video looks at all the basic parts that form the security model in Windows. Understanding this will give you a better understanding of how security works in Windows allowing you to better configure and secure Windows.

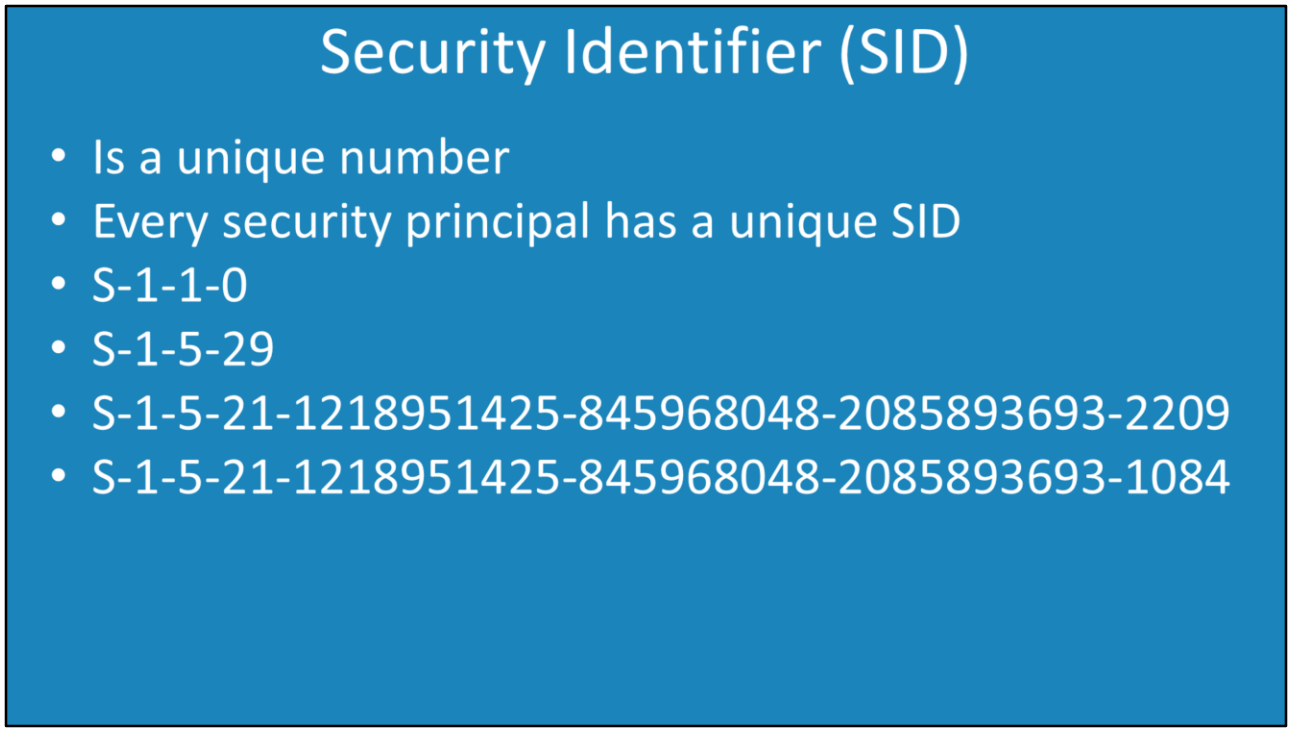
What's in this video

This video will look at the core parts of Windows security which are as follows: "Security Principal", "Security Identifier", "Access Control Entry/Access Control List" and "Access Tokens". This will give you a better understanding of how security in Windows works which will assist you later on when you work on configuring security.

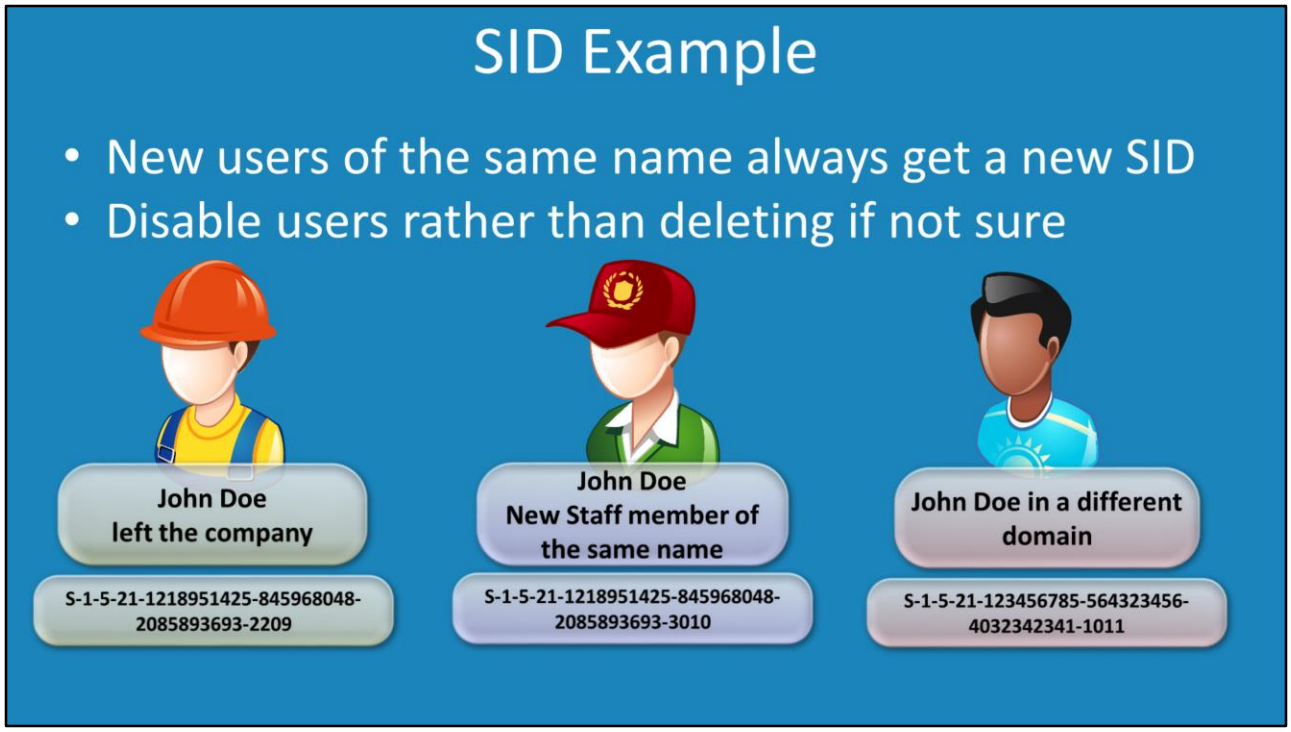


What is a Security Principal

A security principal is essentially the name given to an entity. For example a user, computer or process. This security principal is generally a friendly name to make it easier to identify the entity. For example, it is easier to identify a user by a name rather than a long number. A security principal will always map to one entity, but it is possible to have to entities with the same name. For example two users with the same name. Perhaps one has been deleted and replaced by the other. In order for an entity to always be able to be uniquely identified, it needs a unique value assigned to it.

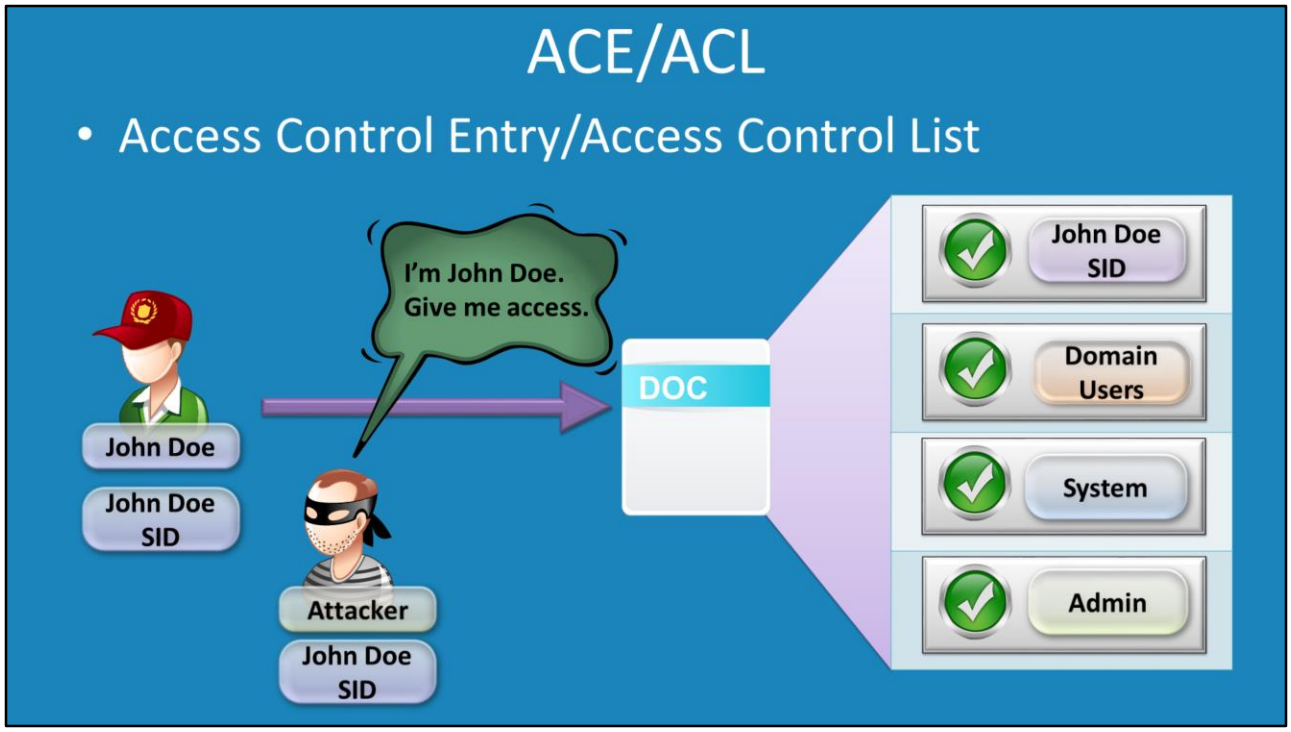


Security Identifier (SID)
Every object in Windows has a SID assigned to it. A SID is a unique number like a serial number. They always start with S. The short SID's are local SID's and are only used on the local computer. The longer SID's are domain SID's and are issued by a Domain Controller.
The list of profiles currently in use can be found in Regedit at the following location HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList
The containers in this location are called after the SID of that user. This means that if the username of that user were to change, this would not affect Windows being able to find the profile for that user as the SID for that user has not changed.



SID Example

Whenever a user is created, a unique SID is assigned to them. This SID is then used with objects to give the user access. Since a unique SID is assigned to every user that is created, it is possible to have multiple users with the same SID at different times or in different domains. It should be remembered that once a user is deleted the SID associated with that user is lost. For this reason, many administrators will disable a user rather than deleting them and thus keeping the SID. If later on the access that was given to that user is required, the user can be re-enabled and the access reused.

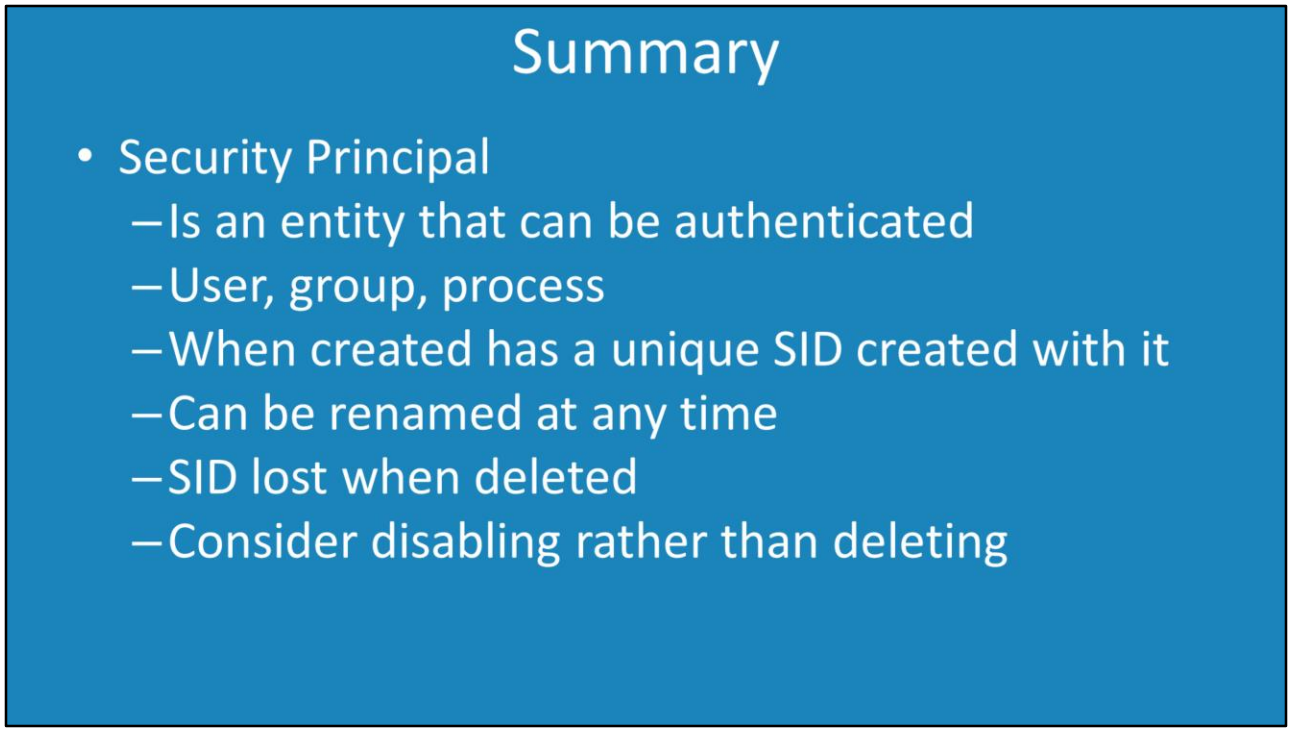


ACE/ACL

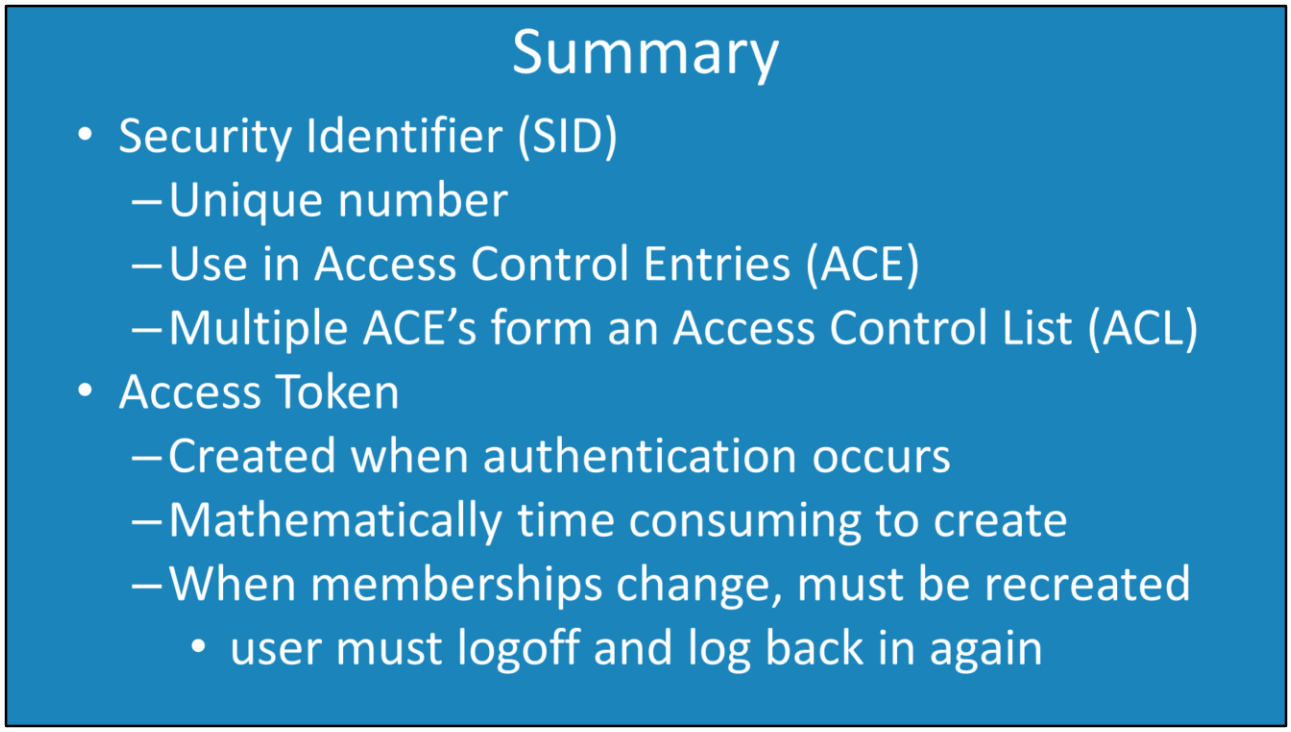
In order to determine who can access an entity, ACE's and ACL's are used. An ACL or Access Control List is a list of permissions. For example who can read the entity, those that can write to the entity. An ACE or Access Control Entry is simply an entry in that list. For example, if you had a document on the file system, this document would have an Access Control List associated with it. This Access Control List would contain Access Control Entries which determine who has access. For example, it is common for files to be allowed access by administrators and the system user. If additional access is required, it is just a matter of adding an ACE to the ACL with the required permissions and the entity that requires access. The access is determined by using the entities SID. Thus to determine if someone is allowed access, the SID of that user is looked at and then checked against the ACL to see if there is a match. If there is a match the user is allowed access.

Access Token

When a user authenticates with a Domain Controller an access token is created. This access token contains the SID of the user and also any SID's for any groups that user is a member of. The access token uses digital signatures in order to secure the token. This means that an attacker cannot change the token or create their own token. When the user has a token, they can present this token to a file server and the file server will check the token to make sure it is valid. Once this done, the file server will look in the token and determine what SID's that user has. To grant access, it is just a matter of comparing the SID's that the user has with the SID's that are in the Access Control List. If there is a match the user is granted access, if there is no match, the user is denied access. When a file or folder is opened in Windows, Windows will obtain the friendly name for that SID. If the SID is a local SID, this will be obtained from the local computer. If the SID is a domain SID, this will be obtained from a Domain Controller.



Summary
A security principal is essentially an entity that can be authenticated. In a lot of cases this will be a user, group or process. When any object in Windows is created, a unique SID is created for that object. Since the SID is used in security, this means that the friendly name and any other attributes can be changed without effecting the security this entity was used on. This also means that when a user is deleted the SID is lost and thus with it any access that user had. For this reason it is recommended to disable a user rather than deleting a user in case the user's access is required later on.



Summary
A security identifier is essentially a unique number. This is used in an Access Control Entry (ACE). Multiple ACE's form an Access Control List (ACL). This is used to determine if access is granted or denied. In order to make the system secure, an access token is created when the user logs in. This access token contains all the SID's for all the groups that user is a member of and the user's SID. This access token is presented to a resource to determine access. The access token uses digital signatures so that it cannot be modified and is very difficult to fake, however it is a very simple and fast process to prove that the access token is authentic.

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
"Installing and Configuring Windows Server 2012 Exam Ref 70-410" pg 83
"Principal (computer security)" http://en.wikipedia.org/wiki/Principal_(computer_security)
"Security Identifier" http://en.wikipedia.org/wiki/Security_Identifier
"Access Control Entries" http://msdn.microsoft.com/en-us/library/windows/desktop/aa374868(v=vs.85).aspx
"Access Tokens" http://msdn.microsoft.com/en-us/library/windows/desktop/aa374909(v=vs.85).aspx