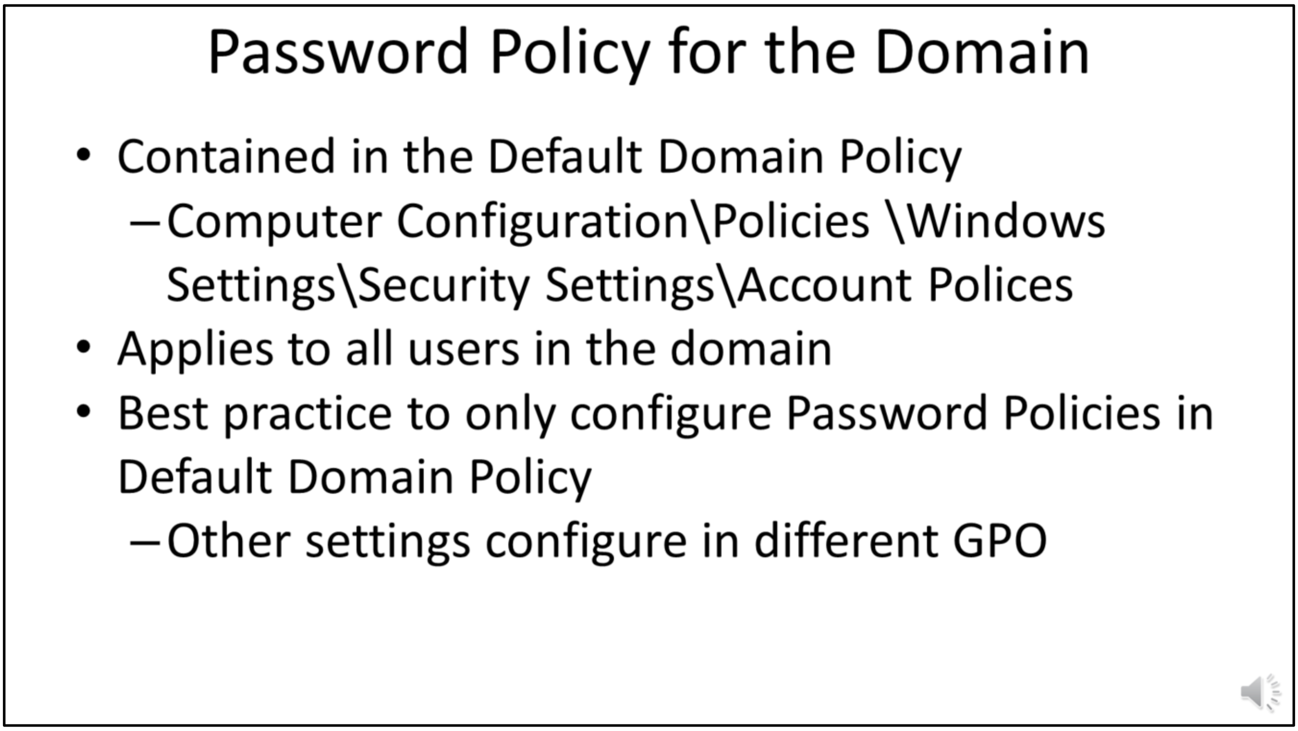
Password Policy

For the free video please see
http://itfreetraining.com/70-640/adpasswordpolices

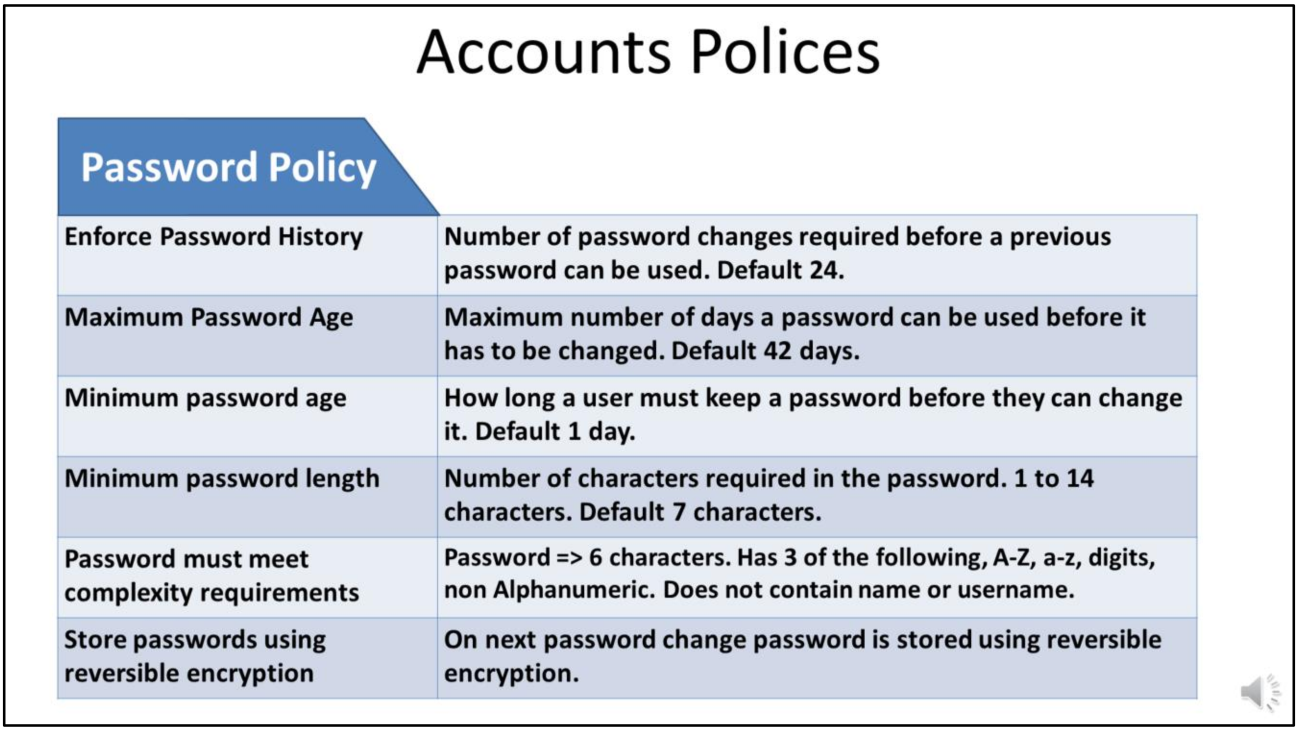
This video will look at configuring the default password policy in Active Directory. These setting determines setting like how long a user password will be, if the password needs to complex, and how many times a password needs to be changed before an old password can be used.



Password Policy for the Domain

- Contained in the Default Domain Policy
  - Computer Configuration\Policies \Windows Settings\Security Settings\Account Polices
- Applies to all users in the domain
- Best practice to only configure Password Policies in Default Domain Policy
  - Other settings configure in different GPO

Password Policy for the Domain
The password settings for the domain can only be edited in the Default Domain Policy. These are found in the following the location.
Computer Configuration\Polices\Windows Settings\Security Settings\Account Polices
These settings apply to all users in the domain. If you need to configure additional Group Policy settings in the domain it is considered best practice to create a new Group Policy Object for these settings rather than configure the settings in Default Domain Policy. To configure these settings, they can be done using Group Policy Management.



Accounts Polices

Password Policy	
Enforce Password History	Number of password changes required before a previous password can be used. Default 24.
Maximum Password Age	Maximum number of days a password can be used before it has to be changed. Default 42 days.
Minimum password age	How long a user must keep a password before they can change it. Default 1 day.
Minimum password length	Number of characters required in the password. 1 to 14 characters. Default 7 characters.
Password must meet complexity requirements	Password => 6 characters. Has 3 of the following, A-Z, a-z, digits, non Alphanumeric. Does not contain name or username.
Store passwords using reversible encryption	On next password change password is stored using reversible encryption.

Password Policy

Enforce password History: This setting stores the previous passwords used for that user preventing them from using that password again. The default setting is 24.

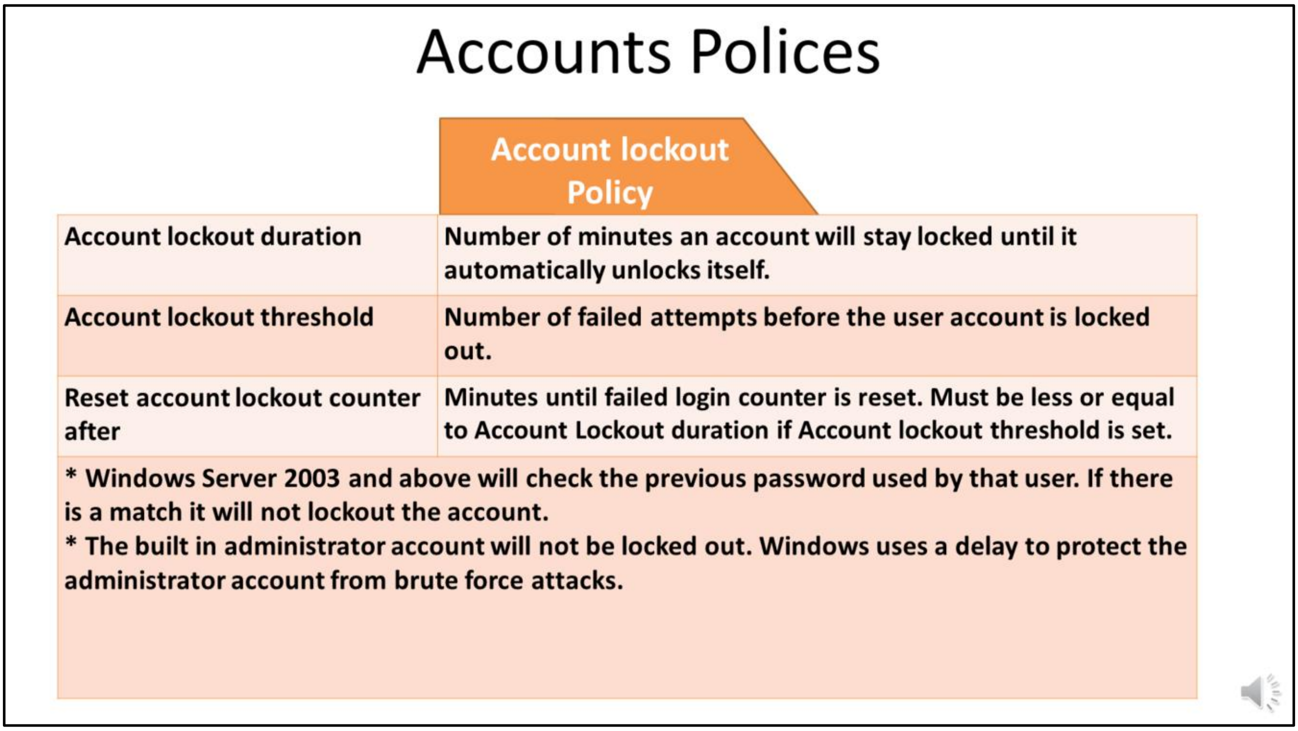
Maximum password Age: This determines how many days a user can use a password before it expires. When it expires the user will not be able to login or access resources on the network until the password is changed. If you want to prevent the password from expiring for a user, tick the tick box “Password never expires” in the properties for the user.

Minimum password Age: The minimum time a user must have a password before it is changed. This prevents a user changing the password repeatedly until they get to their old password.

Minimum password length: This setting determines the minimum length a password can be.

Password must meet complexity requirements: This means that a password must meet 3 of the following. Contain A-Z, a-z, digits, non- Alphanumeric. Also the password does not contain the username.

Store password using reversible encryption: This stores the password using reversible encryption and thus software is able to work out the password. The password is only reversible once it has been changed. Selecting this option will not grant software access to an existing password.

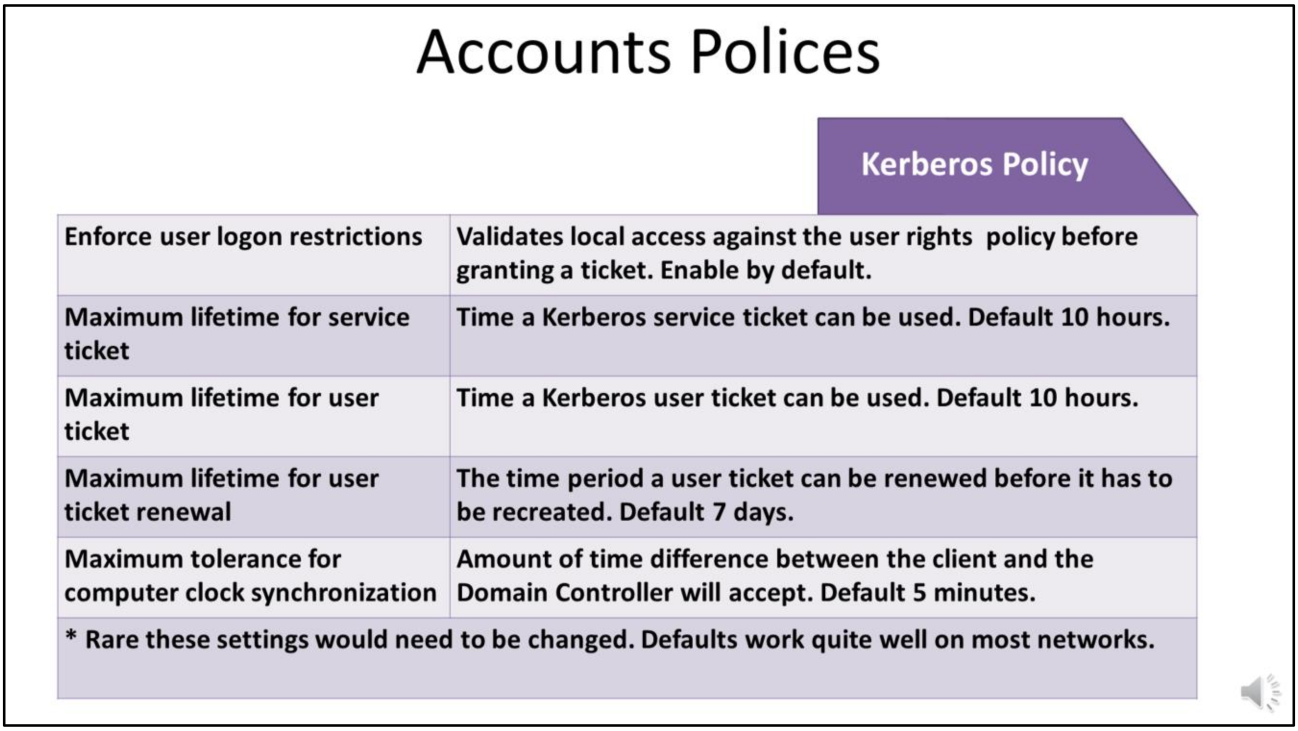


Accounts Polices

	Account lockout Policy
Account lockout duration	Number of minutes an account will stay locked until it automatically unlocks itself.
Account lockout threshold	Number of failed attempts before the user account is locked out.
Reset account lockout counter after	Minutes until failed login counter is reset. Must be less or equal to Account Lockout duration if Account lockout threshold is set.

* Windows Server 2003 and above will check the previous password used by that user. If there is a match it will not lockout the account.
* The built in administrator account will not be locked out. Windows uses a delay to protect the administrator account from brute force attacks.

Account Lockout Policy
When an account is locked, a tick box called unlock account will be ticked in the properties for that user. To unlock the account, clear this tickbox. When the account is locked, the user will not be able to login or make new connections to servers if already logged in.
Account lockout duration: This setting will determine how long a locked account will remain locked before the system will automatically unlock it. If this is set to zero, the administrator must physically unlock the account.
Account lockout threshold: This is the number of failed password attempts until the account is locked. This must occur within the time period contained in the next setting.
Reset account lockout counter after: When the time period set in this setting expires, the timer for account lock out is reset. This means that if the user puts in another wrong password, effectively the counter starts from 0 again.

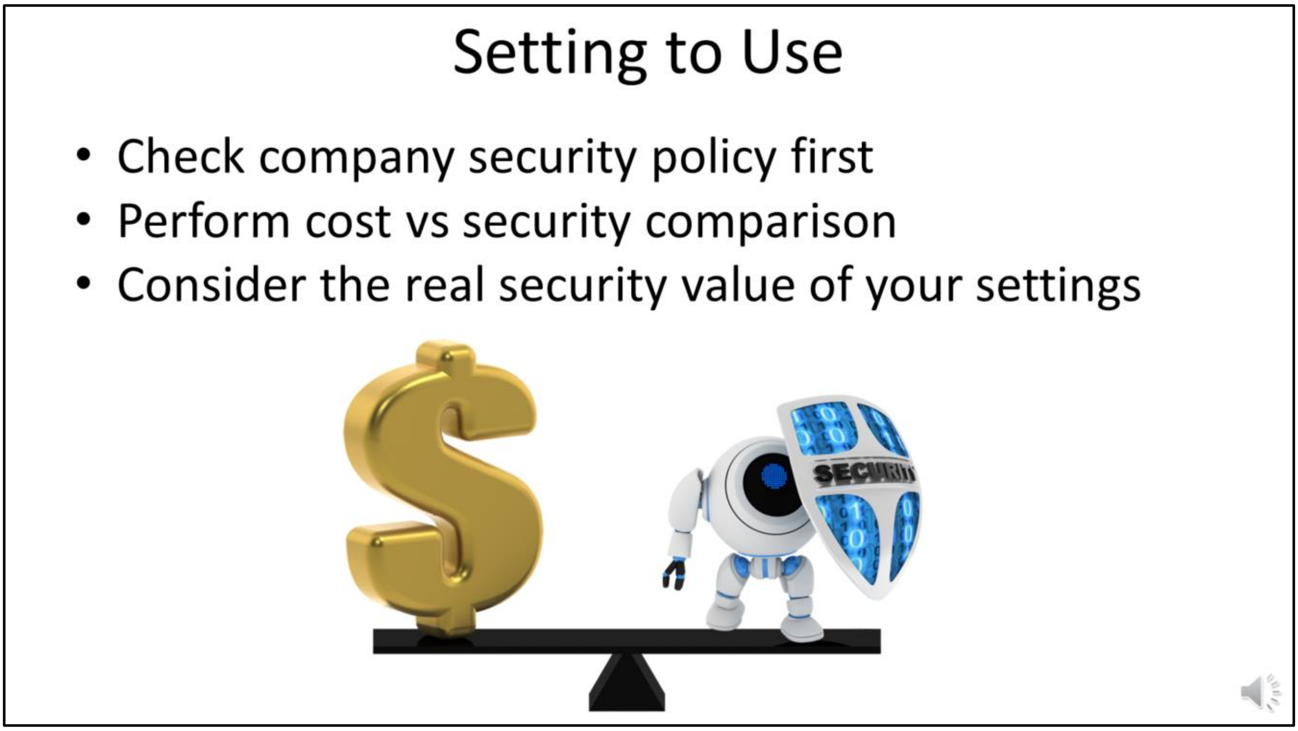


Accounts Polices

Kerberos Policy

Enforce user logon restrictions	Validates local access against the user rights policy before granting a ticket. Enable by default.
Maximum lifetime for service ticket	Time a Kerberos service ticket can be used. Default 10 hours.
Maximum lifetime for user ticket	Time a Kerberos user ticket can be used. Default 10 hours.
Maximum lifetime for user ticket renewal	The time period a user ticket can be renewed before it has to be recreated. Default 7 days.
Maximum tolerance for computer clock synchronization	Amount of time difference between the client and the Domain Controller will accept. Default 5 minutes.
* Rare these settings would need to be changed. Defaults work quite well on most networks.	

Kerberos Policy
Unless you have good reason to, these settings should be left on the defaults.
Enforce user logon restrictions: This will check that a user has the required rights before issuing a ticket for access. It is generally quicker to check if the user has the required rights first rather than issue the ticket as the ticket takes a lot of computing power to generate unless you have very slow network connections.
Maximum lifetime for service ticket: Determines how long a service ticket can be used before it has to be recreated.
Maximum lifetime for user ticket: Determines how long a user ticket can be used before it has to be recreated.
Maximum lifetime for user ticket renewal: The time period a ticket can be renewed before it has to be recreated.
Maximum tolerance for computer clock synchronization: How many minutes Kerberos will allow in time difference before the ticket will be rejected.



Setting to Use

- Check company security policy first
- Perform cost vs security comparison
- Consider the real security value of your settings

Cost VS Security
When determining which password settings to use, you should consider the cost that using these settings will have on the organization. Changing user passwords too often will result in more calls to the helpdesk and also users tend to write their passwords down rather than remembering them. Before putting in security settings, perform a cost verses security comparison to determine if the settings should be put in or not.

References
"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 392