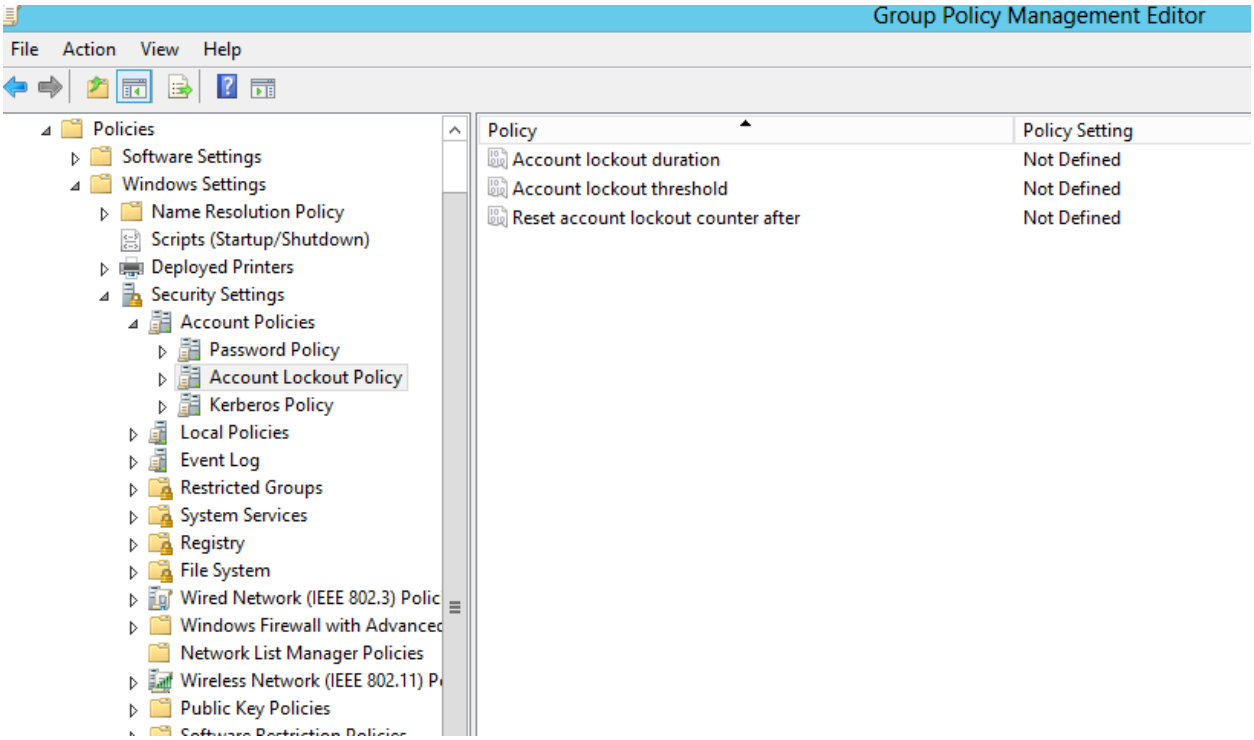
Account lockout policy settings

Kerberos policy settings



Accounts lockout duration

This security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is from 0 minutes through 99,999 minutes. If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it.

If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.

Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.

Account lockout threshold

This security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 0 and 999 failed logon attempts. If you set the value to 0, the account will never be locked out.

Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password-protected screen savers count as failed logon attempts.

Default: 0.

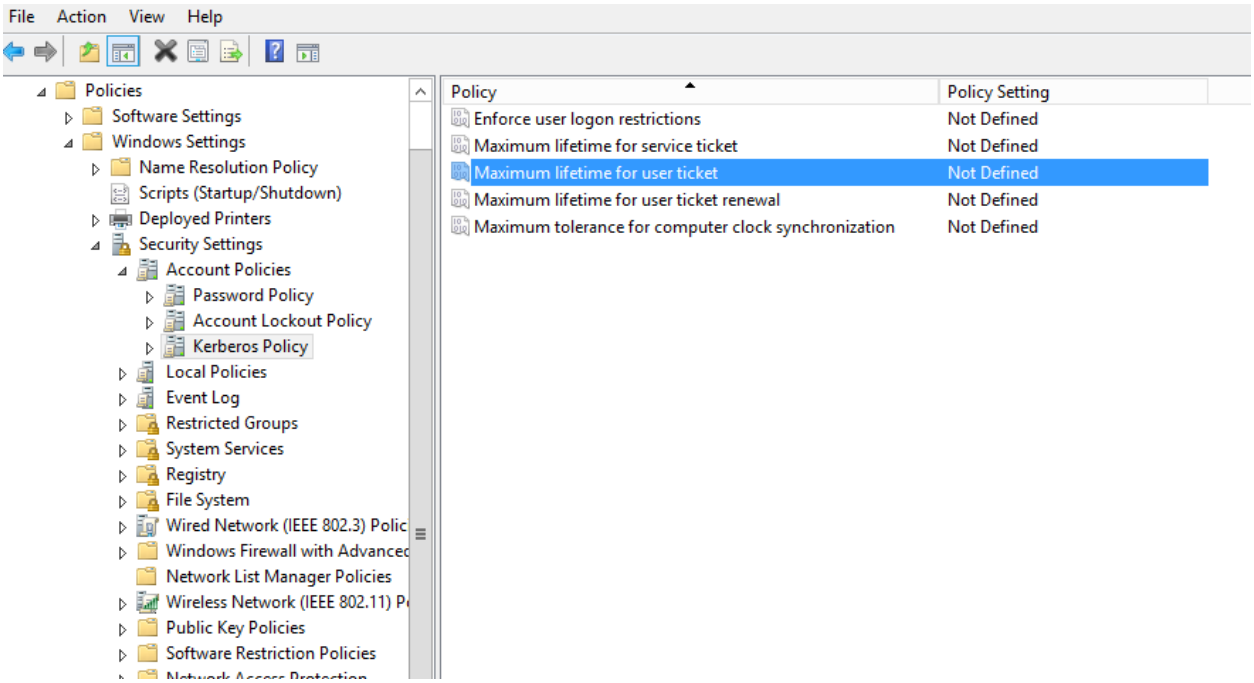
Reset account lockout counter after

This security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes.

If an account lockout threshold is defined, this reset time must be less than or equal to the Account lockout duration.

Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.

Kerberos Policy Settings (see understanding Kerberos concepts)



Enforce user logon restrictions

This security setting determines whether the Kerberos V5 Key Distribution Center (KDC) validates every request for a session ticket against the user rights policy of the user account. Validation of each request for a session ticket is optional, because the extra step takes time and it may slow network access to services.

Default: Enabled.

Maximum lifetime for service ticket

This security setting determines the maximum amount of time (in minutes) that a granted session ticket can be used to access a particular service. The setting must be greater than 10 minutes and less than or equal to the setting for Maximum lifetime for user ticket.

If a client presents an expired session ticket when it requests a connection to a server, the server returns an error message. The client must request a new session ticket from the Kerberos V5 Key Distribution Center (KDC). Once a connection is authenticated, however, it no longer matters whether the session ticket remains valid. Session tickets are used only to authenticate new connections with servers.

Ongoing operations are not interrupted if the session ticket that is used to authenticate the connection expires during the connection.

Default: 600 minutes (10 hours).