

# Kerberos Security

June 18, 2012

# Kerberos Security

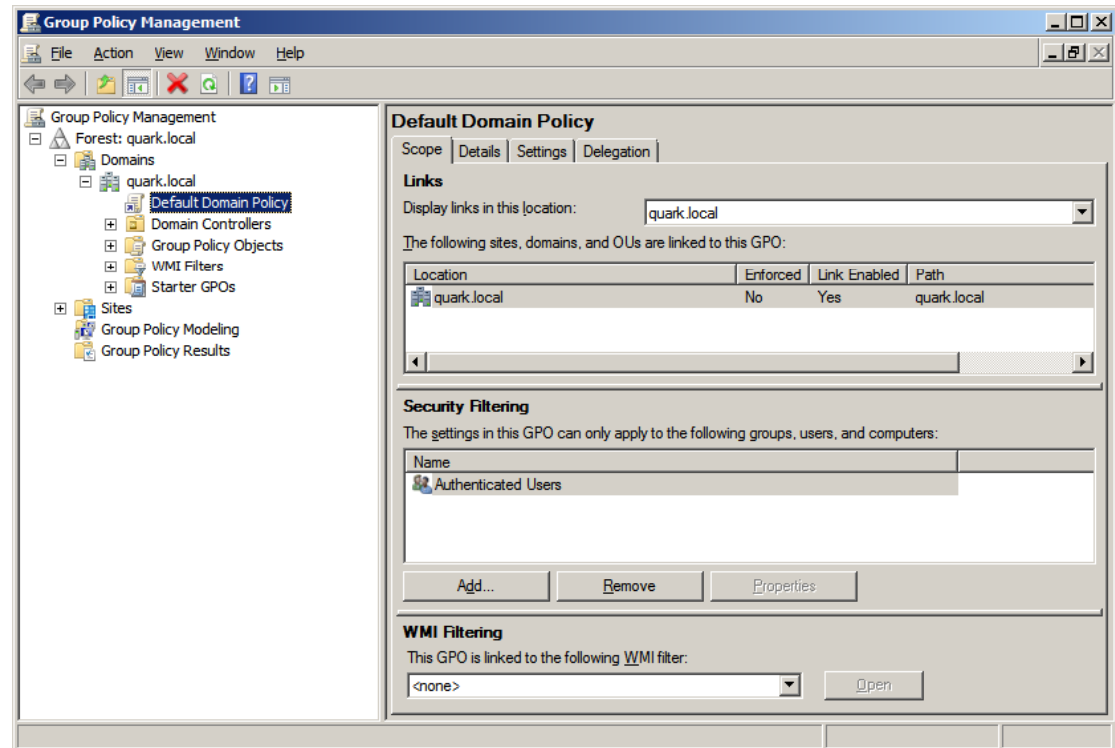
Kerberos is a client – server security system that uses tickets to authenticate that the user's computer is a valid member of the Domain. Tickets are issued when services are requested and the client computer and server clocks must be synchronized within the policy tolerance.



# Open Group Policy Management

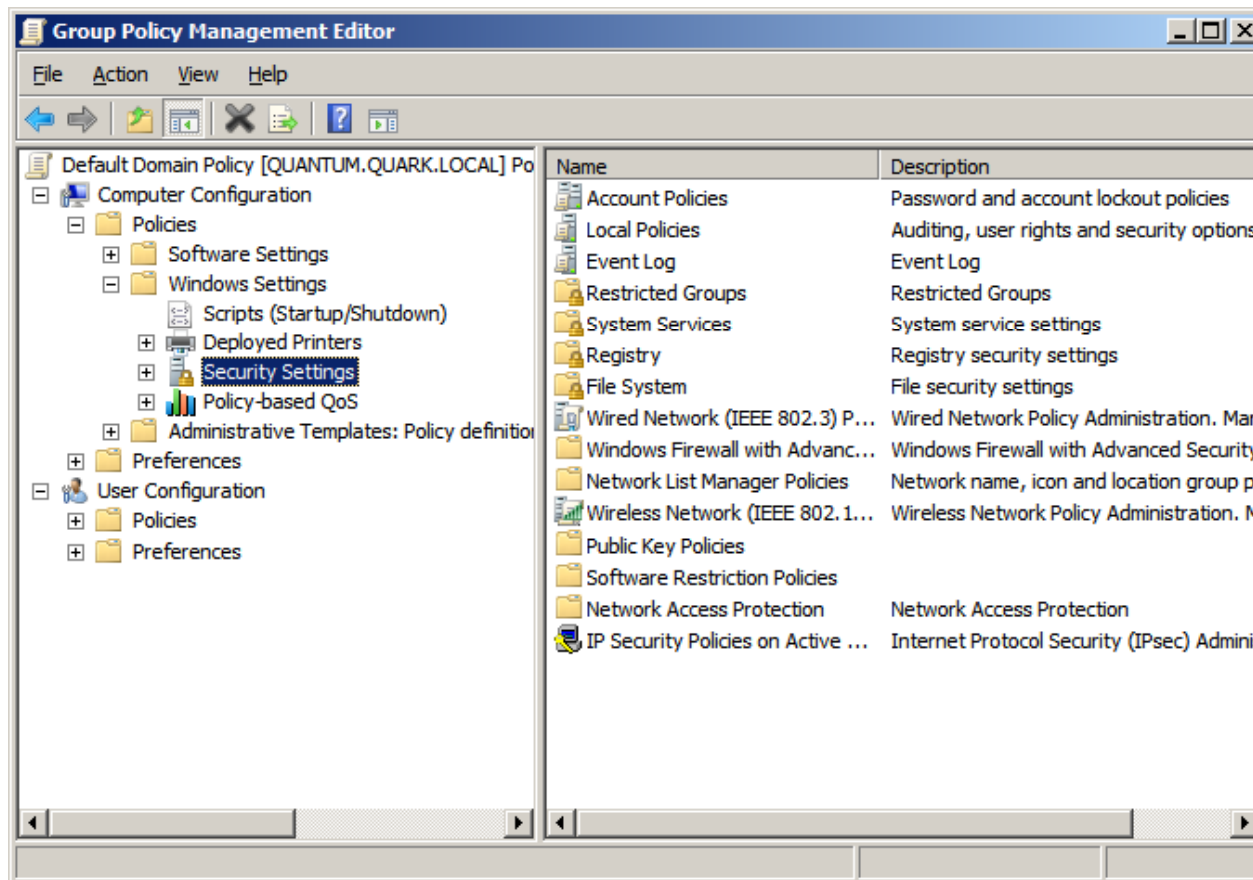
Kerberos can be enabled by going to the Start menu, selecting Administrative Tools and choosing Group Policy Management. The Group Policy Management window will appear.

We should right click on Default Domain Policy and select Edit from the menu.



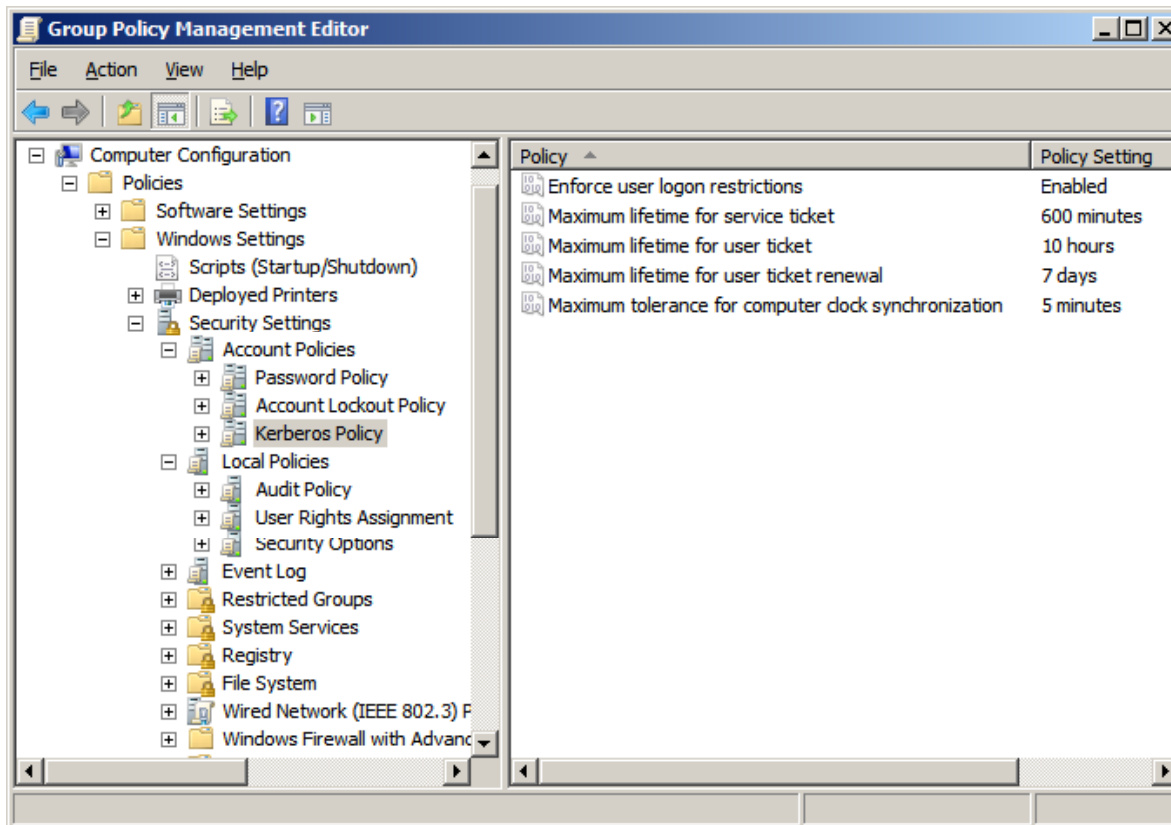
# Group Policy Management Editor

The Group Policy Management Editor window will open. Click on the Policy Folder and Windows Settings and then Security Settings.



# Kerberos Policy

When we open Security Settings and Account Policies as we did before to set the Password and Account Lockout Policy, we select Kerberos Policy.

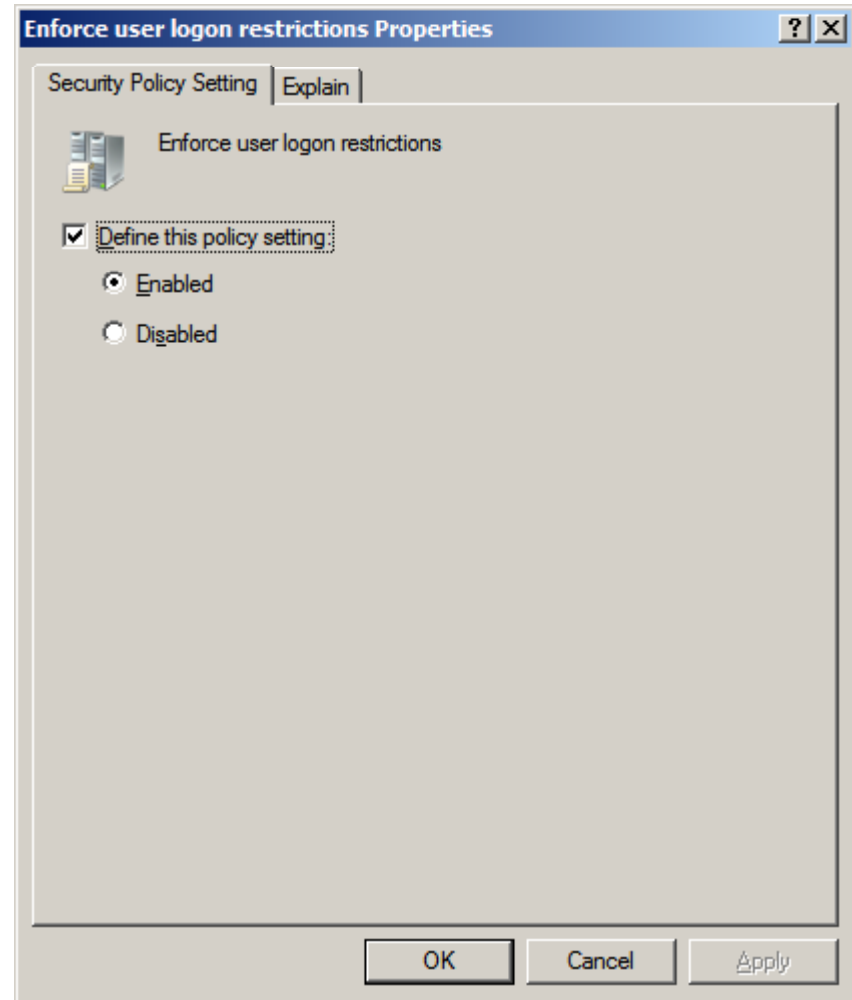


There are five policy settings for the Kerberos security setup.

# Enforce User Logon Restrictions

This security setting is enabled and controls whether the Kerberos V5 Key Distribution Center authenticates each request for a session ticket against the user rights policy of the user account.

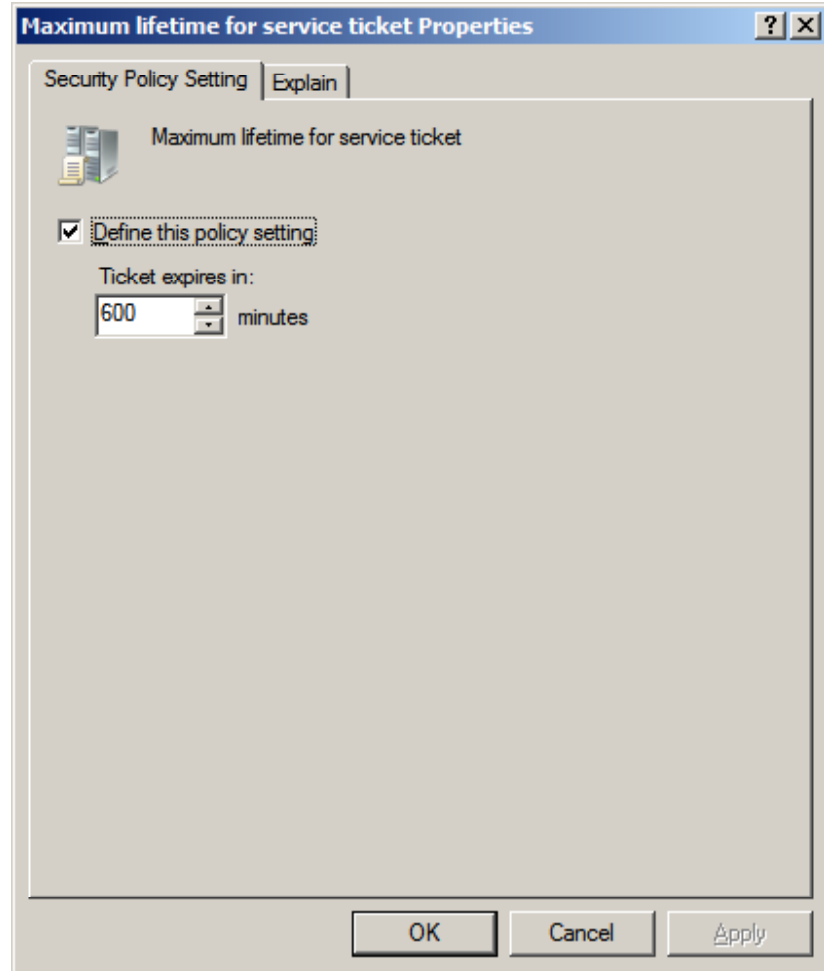
This policy is enabled by default.



# Maximum Lifetime for Service Ticket

Maximum Lifetime for Service Ticket determines the maximum time in minutes that a granted session ticket can be used to access a service.

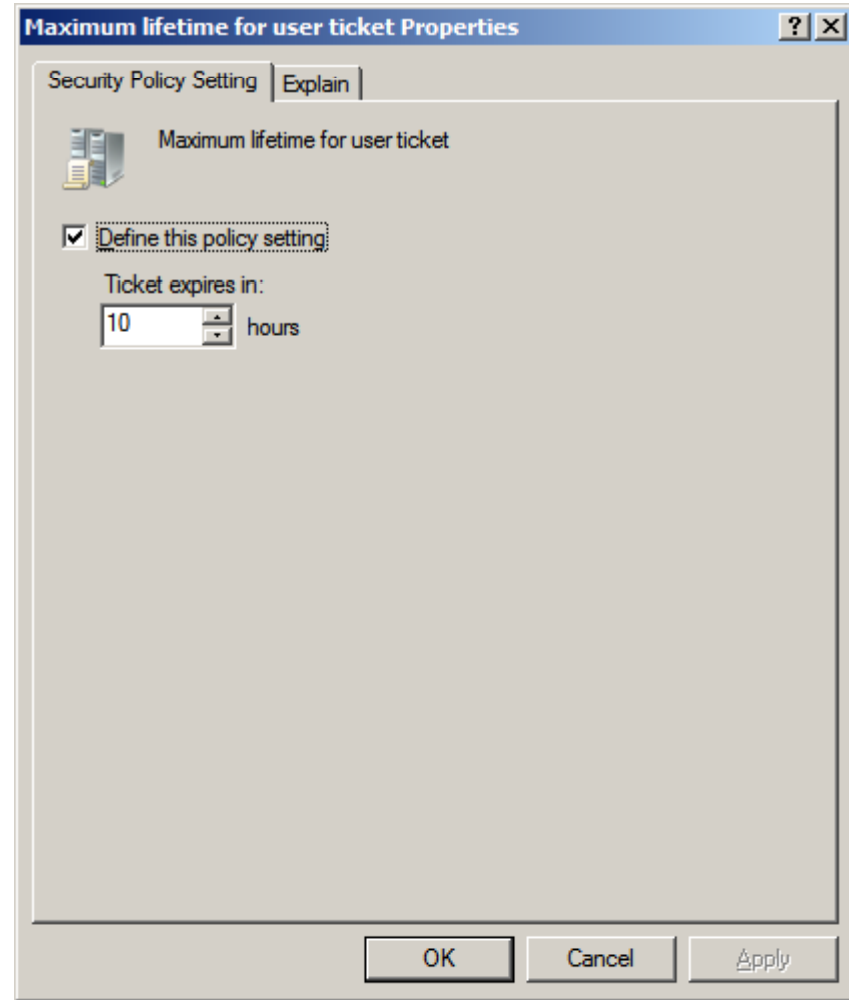
The default setting is 600 minutes and must be greater than 10 minutes. The time setting must be greater or equal to the time setting for Maximum lifetime for user ticket.



# Maximum Lifetime for User Ticket

The Maximum Lifetime for User Ticket determines the maximum time in hours that a user's ticket-granting ticket may be used. A new ticket must be requested or the current ticket renewed when the old ticket expires.

The default setting is 10 hours.

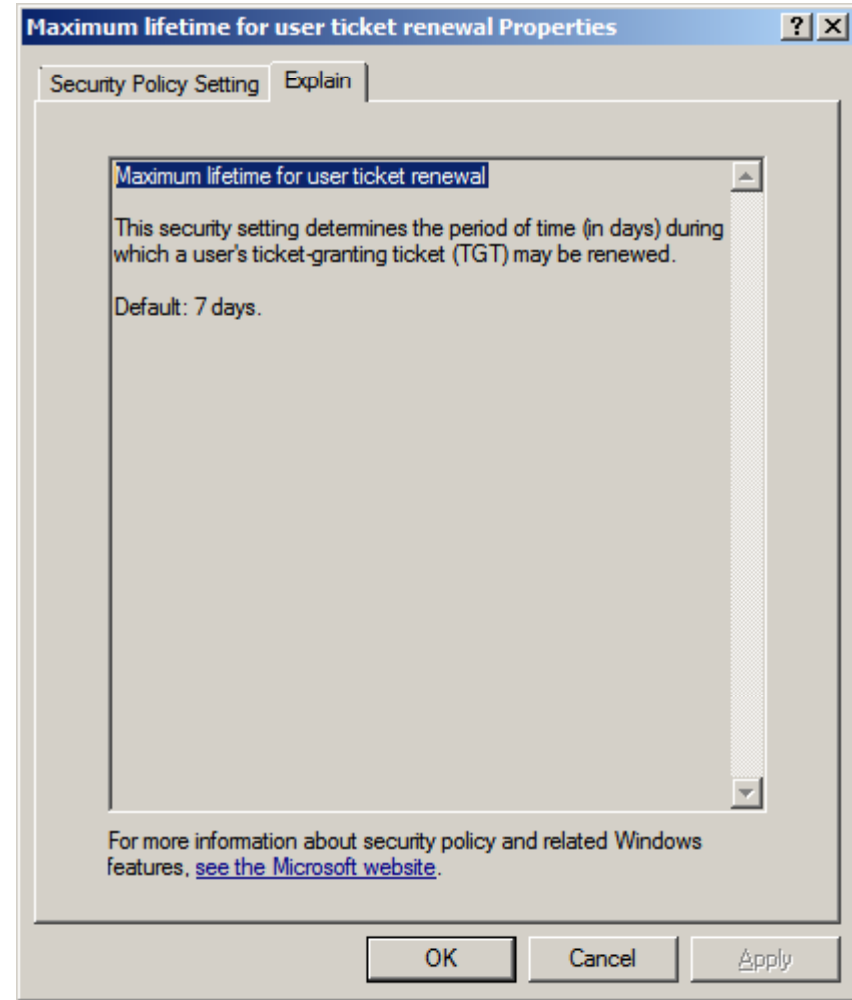




# Maximum Lifetime for User Ticket Renewal

Maximum Lifetime for User Ticket Renewal determines the time in days in which a user's ticket-granting ticket may be renewed.

The default setting is 7 days.



# Maximum Tolerance for Computer Clock Synchronization

Maximum tolerance for computer clock synchronization determines the maximum time difference in minutes that Kerberos permits between the time on the client clock and the time on the Domain Controller machine.

Kerberos uses time stamps as part of its operation so the client computer and the Domain Controller's time clocks need to be synchronized as close as possible. The default for this policy is 5 minutes, so the client and server cannot deviate more than that amount.

