Control Access to Privileged User Manager Service

Privileged User Manager

June 2013

Legal Notice

Control Access to Privileged User Manager Service

This document lists the steps to be followed to control access to Privileged User Manager service.

Assumptions:

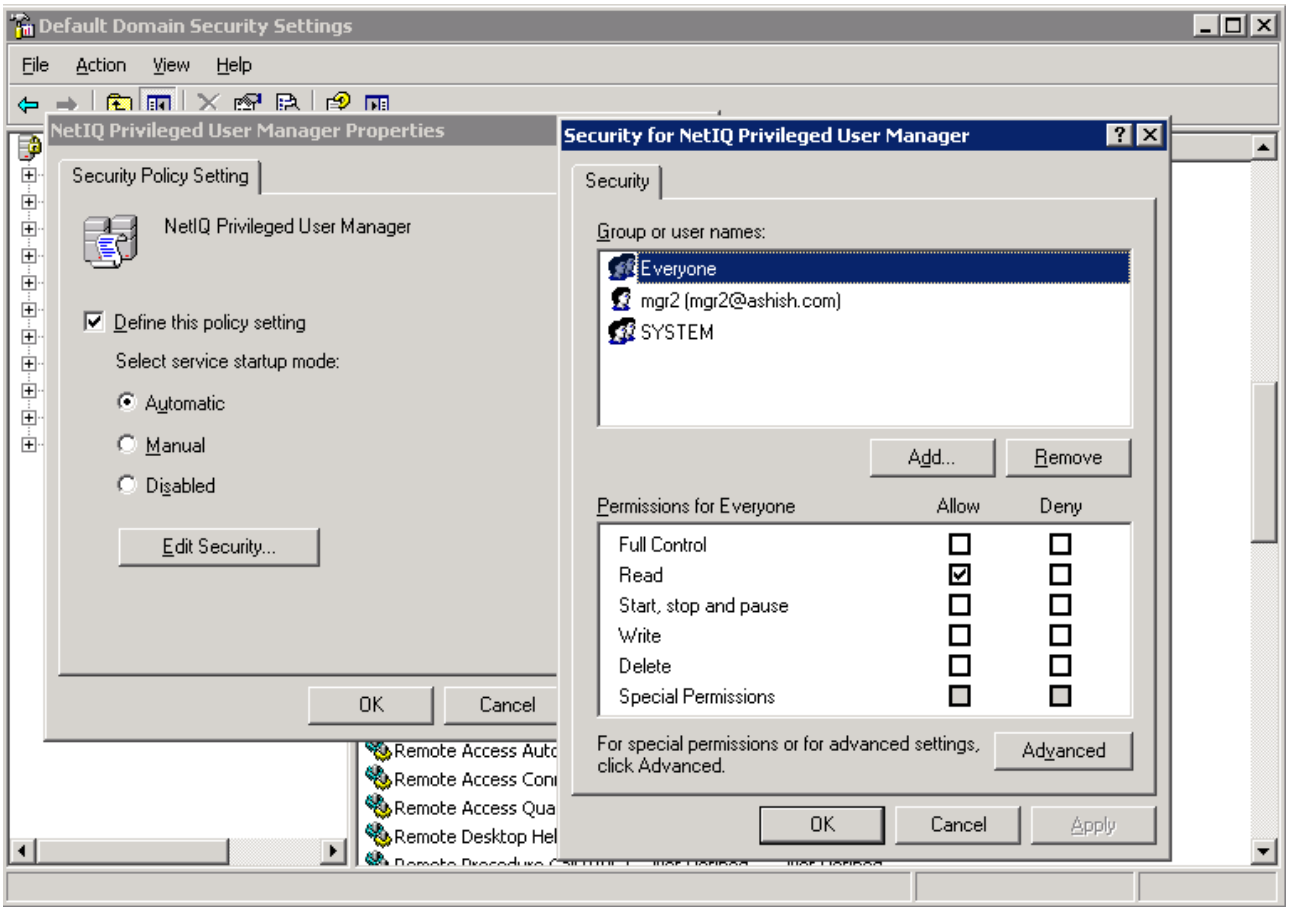
1. It is assumed that the Windows computer where PUM is installed is added to a Windows domain.
2. The privileged credential used in PUM is a domain user.

Steps:

Following steps need to be followed by a domain admin when at least one instance of PUM is installed on a Windows system in the domain:

a) Open the Domain Security Policy tool on domain controller machine. This tool displays the default domain security.
b) Traverse to 'System Services-> NetIQ Privileged User Manager'.
c) By default, it shows ‘not defined’. Go to properties and define a policy.
d) Select ‘Automatic’' startup mode.
e) In security, do following:
    i. REMOVE – Administrators group if any.
    ii. REMOVE – INTERACTIVE group.
    iii. ADD – Everyone group and give only READ access to it.
    iv. ADD – A domain admin, and give FULL access to it. This user can uninstall the PUM software or start/stop the service.

For example, check following screen shot:



Here, ‘mgr2’ and ‘SYSTEM’ has FULL control, whereas ‘Everyone’ has only READ access.

Usually, Group Policies update themselves to individual computers in the domain at some time interval. If you want to update immediately, go to the computer where PUM is installed and perform GPUPDATE at the command prompt.