

Control Access to Privileged User Manager Service

Privileged User Manager

June 2013



Legal Notice

NetIQ Product Name is protected by United States Patent No(s): nnnnnnnn, nnnnnnnn, nnnnnnnn.

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2013 NetIQ Corporation and its affiliates. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Control Access to Privileged User Manager Service

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

Assumptions:

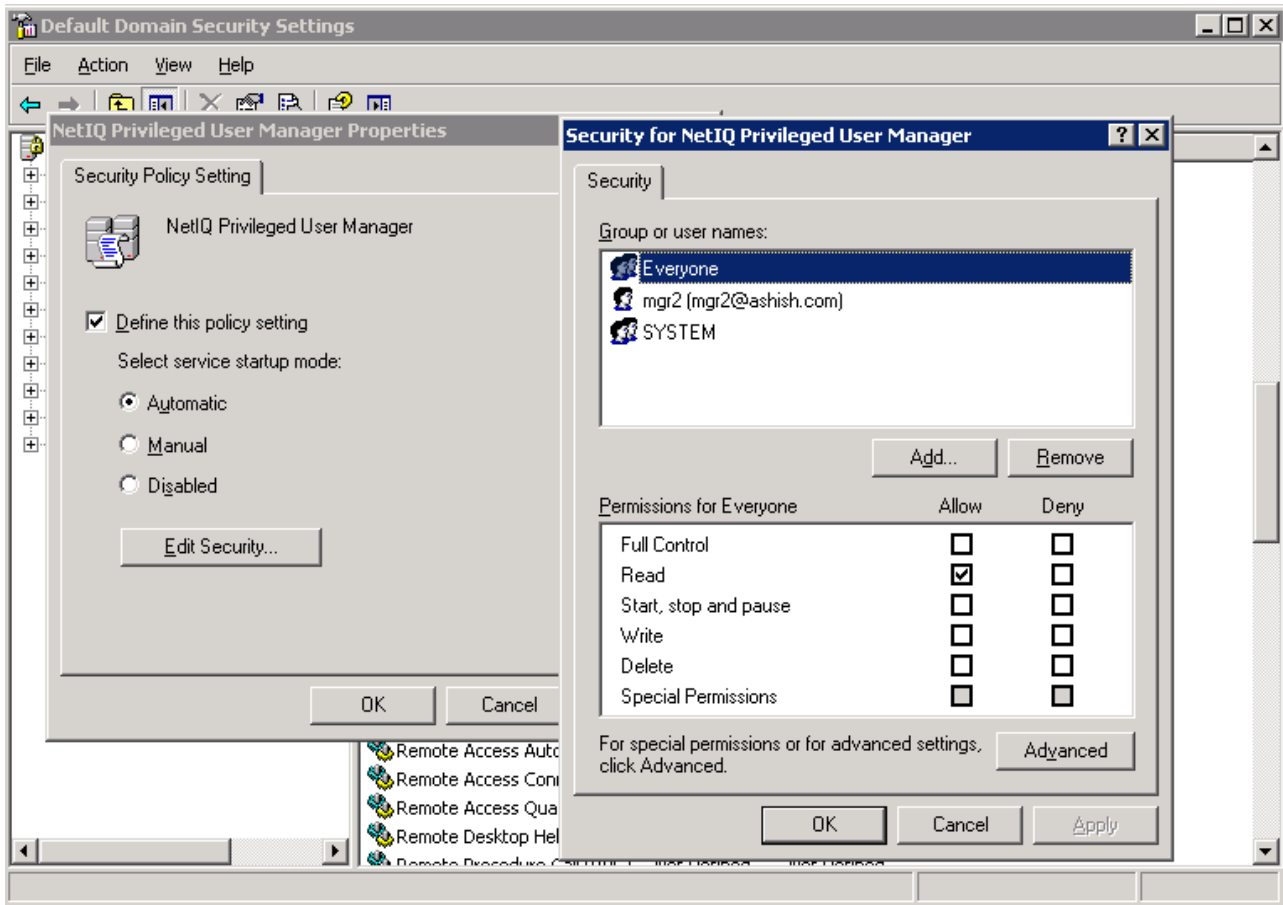
1. It is assumed that the Windows computer where PUM is installed is added to a Windows domain.
2. The privileged credential used in PUM is a domain user.

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.