

# **Command Control Access to Network Devices**

## **NetIQ Privileged User Manager**

**March 2014**



## Legal Notice

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.

**© 2014 NetIQ Corporation and its affiliates. All Rights Reserved.**

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

## Contents

1. Introduction .....	2
2. Creating Privileged Account.....	2
3. Creating Command Group.....	3
4. Creating Command Control Rule .....	4
5. Executing Rules.....	4

# 1. Introduction

SSH relay is a new feature in PUM that enables delegation of privileged credentials to those hosts where PUM agents are not installed. This feature makes use of the underlying SSH functionality of UNIX/Linux systems to provide privileged access and to monitor the activities after delegation. PUM has been designed to work with its own framework user management.

The document describes how to configure command control access for the network devices such as router and switch using PUM.

## 2. Creating Privileged Account

**Note:** The values used in this document are sample values.

To create the privileged accounts:

1. Before integrating PUM to use the authentication domain, you need to add account domain details to PUM. PUM supports creation of the account domain in the command control console installed as part of default manager installation. To add authentication account domain to PUM:
  - a) Go to **Home/Command Control console>Privileged Accounts**.
  - b) Select **Add Account Domain** to add a new account domain to PUM framework.
  - c) Provide information in all the fields in the Account Domain page, as shown in the following example screenshot. Name and SSH host should be network device IP address.

NetIQ Privileged User Manager

Account Domain

Name	192.178.1.254		
Type	SSH	Profile	Generic UNIX
SSH Host	192.178.1.254	22	
SSH Host Key	192.168.1.254 ssh-rsa AAAAAB3NzaC1yc2EAAAADAQABAAQgQCZ7gJgvPVG9wcEd7ZKfaFyq10KCqRqrkRptPS+		Lookup
Credential Type	Password		
Account	cisco		
Password	*****		

Now, an authentication domain for admin users has been created. You can add some more accounts to this authentication group

2. To add non-admin authentication accounts, go to **Home/Command Control console>Privileged**

**Accounts.** Select the privileged account that you created and click **Add Credential**.



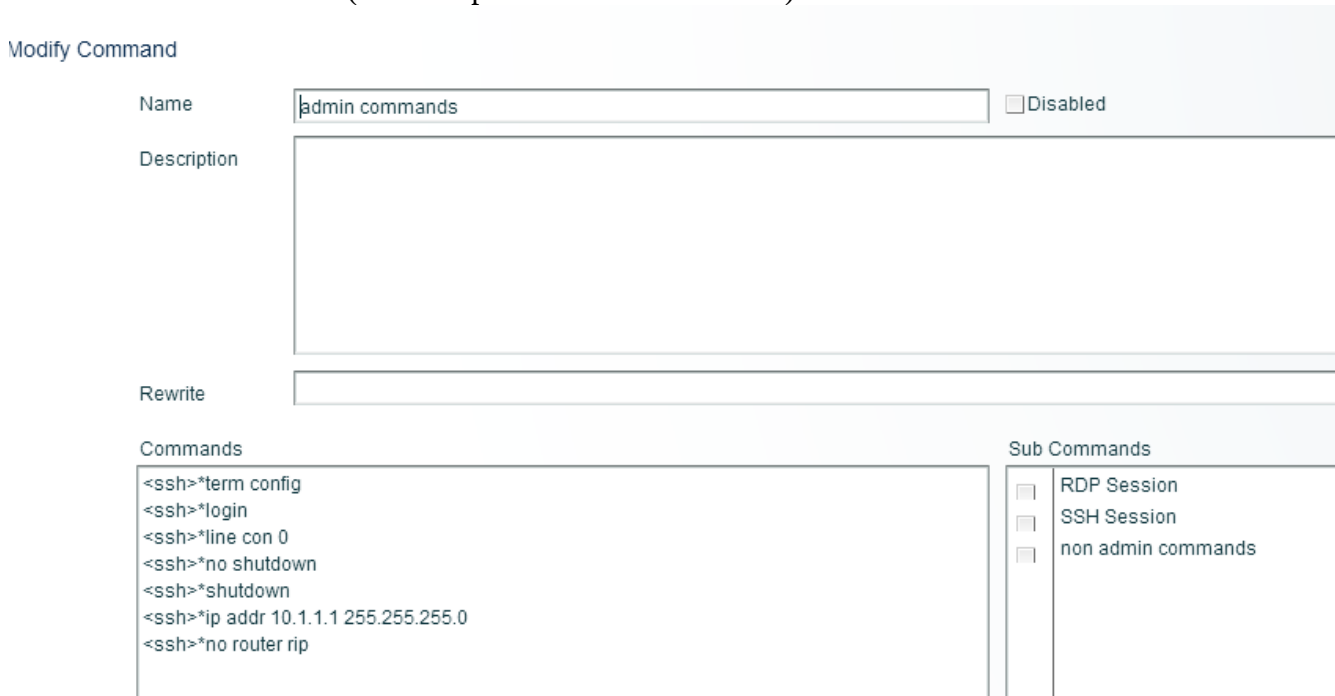
The screenshot shows the 'Privileged Credential' configuration page in NetIQ Privileged User Manager. The page has a dark blue header with the NetIQ logo and the text 'NetIQ Privileged User Manager'. Below the header, the title 'Privileged Credential' is displayed. The form contains three fields: 'Account' with the value 'nonadmin', 'Type' with a dropdown menu set to 'Password', and 'Password' with a masked field containing seven asterisks.

Now you have created a credential domain for non-admin users.

### 3. Creating Command Group

To create a command group:

1. Go to **Home/Command Control>Command Group** and add two Command groups (for example: Admin command group and Non-admin command group).
2. Modify the **admin commands** command group. Select the group, click **Modify Command**, and add admin commands (for example: <ssh>\*no shutdown) in the **Commands** field.



The screenshot shows the 'Modify Command' form for the 'admin commands' group. The form has a light blue header with the title 'Modify Command'. The 'Name' field contains 'admin commands' and there is a 'Disabled' checkbox. The 'Description' field is empty. The 'Rewrite' field is empty. The 'Commands' field contains a list of commands: <ssh>\*term config, <ssh>\*login, <ssh>\*line con 0, <ssh>\*no shutdown, <ssh>\*shutdown, <ssh>\*ip addr 10.1.1.1 255.255.255.0, and <ssh>\*no router rip. The 'Sub Commands' field contains a list of sub-commands: RDP Session, SSH Session, and non admin commands, each with a checkbox.

3. Modify the **non admin commands** command group. Select the group, click **Modify Command**,

and add non-admin commands (for example: <ssh>\* show version) in the **Commands** field.

NetIQ Privileged User Manager

Modify Command

Name: non admin commands  Disabled

Description:

Rewrite:

Commands:

- <ssh>\*show version
- <ssh>\*show running-config
- <ssh>\*show interfaces
- <ssh>\*show logging
- <ssh>\*show tech-support
- <ssh>\*show interfaces description

Sub Commands:

- RDP Session
- SSH Session
- admin commands

## 4. Creating Command Control Rule

After creating privileged account and user group, the next step is to create rules in Command Control, so that authorization to access the SSH relay host is given based on the rule.

To create command control rules:

1. Go to **Home/Command Control>Rules**. Click **Add rule** in the left panel and add two rules - “Admin Rule for Router” and “Non Admin Rule for Router”
2. Modify **Admin Rule for Router** rule. Set Session capture to On and Authorize to Yes and Stop, Select credential as cisco@192.178.1.254 and run user as cisco.
3. Modify **Non Admin Rule for Router** rule. Set Session capture to On and Authorize to Yes and Stop, Select credential as nonadmin@192.178.1.254 and run user as nonadmin.

## 5. Executing Rules

To execute rules:

1. Connect to the router through the SSH client and log in as admin user “cisco”.
2. For admin commands:
  - a) In the shell prompt, run the following command:  
ssh -t -p 2222 admin@<PUM Manager IP address> <cisco@Router IP address> <any command which is part of admin command group>  
Provide the PUM Manager console password when prompted and press enter. You will see that

the command will be executed.

- b) In the shell prompt, run the following command:

```
ssh -t -p 2222 admin@<PUM Manager IP address> <cisco@Router IP address> <any command which is not part of admin command group>
```

Provide the PUM Manager console password when prompted and press enter. You will see that the command will not be executed a permission denied error message is displayed.

3. For non-admin commands:

- a) In the shell prompt, run the following command:

```
ssh -t -p 2222 admin@<PUM Manager IP address> <nonadmin@Router IP address> <any command which is part of nonadmin command group>
```

Provide the PUM Manager console password when prompted and press enter. You will see that the command will be executed.

- b) In the shell prompt, run the following command:

```
ssh -t -p 2222 admin@<PUM Manager IP address> <nonadmin@Router IP address> <any command which is not part of non admin command group>
```

Provide the PUM Manager console password when prompted and press enter. You will see that the command will not be executed a permission denied error message is displayed.