Self Service Password Reset 4.1 Patch Update 5 Release Notes

August 2017

This patch update resolves specific previous issues. This document outlines why you should install this patch update.

Many of these improvements were made in direct response to suggestions from our customers. We thank you for your time and valuable input. We hope you continue to help us ensure that our products meet all your needs. You can post feedback in the Self Service Password Reset forum (https://forums.novell.com/forumdisplay.php/1343-Self-Service-Password-Reset) on Micro Focus Forums, our online community that also includes product information, blogs, and links to helpful resources.

1 What's New?

The following sections outline the issues resolved in this release:

1.1 Security Updates

If you are running the Self Service Password Reset Appliance, this patch update contains operating system and security updates.

1.2 Enhancements and Software Fixes

This version includes the following software enhancements and fixes:

1.2.1 Contains all of the Updates in Patch Updates 1 through 4

Self Service Password Reset 4.1 Patch Update 5 contains all of the security updates and fixes included in Patch Updates 1 through 4. For more information, see:

- *Self Service Password Reset 4.1 Patch Update 1 Release Notes*
- *Self Service Password Reset 4.1 Patch Update 2 Release Notes*
- *Self Service Password Reset 4.1 Patch Update 3 Release Notes*
- *Self Service Password Reset 4.1 Patch Update 4 Release Notes*

You can install Patch Update 5 without installing the previous patches.

1.2.2 Added a Registration Log for the Appliance in the Support Download Bundle

With this patch update, the file `/var/opt/novell/va/logs/suse_register.log` is part of the appliance download bundle. For more information, see "Sending Information to Support" in the *Self Service Password Reset 4.1 Administration Guide*. (Bug 1035542)

1.2.3 Random Passwords in the Help Desk Module Do Not Conform to the Maximum Length Policy

With this patch update, the random passwords in the Help Desk module now conform to the maximum length policy. (Bug 1043967)

1.2.4 Regular Expressions and Placeholders Work for the LDAP Attributes for the Forgotten Password Module

With this patch update, the regular expressions and placeholders work for the LDAP attribute in the Forgotten Password module. (Bug 1037480)

1.2.5 Unable To Read NMAS Responses If XML Does Not Have 16 Character Prefix

With this patch update, Self Service Password Reset can now read the NMAS responses even if the XML does not have the 16 character prefix. (Bug 1034281)

1.2.6 SMS Verification Button Not Displayed When Configured for Only SMS

With this patch update, the SMS verification button appears when you configure verifications for only SMS. (Bug 1049511)

1.2.7 Update Profile Module Email Verification Setting Not Sending Correct Template

With this patch update, the Update Profile module sends the correct email template to users for verification of their accounts. (Bug 1048776)

1.2.8 REST Call for Profiles Fails on the Appliance

With this patch update, the REST call for profiles works for the Self Service Password Reset appliance. (Bug 1038346)

1.2.9 Themes Show System Status Icons Prior to Login and to Non-Administrator Users

With this patch update, the NetIQ, NetIQ (SSPR3.2), and IDM themes no longer show system status icons prior to login or to non-administrator users. (Bug 1033309)

1.2.10 Unable to Add Logos to NetIQ Theme

With this patch update, logos can again be added to the NetIQ theme. (Bug 1021497)

1.2.11 SkipCaptcha Fails on Forgotten Password Page

With this patch update, adding the "skipCaptcha" parameter to the URL works as expected and reCAPTCHA is not displayed. (Bug 1045432)

1.2.12 Passwords With Ampersand Generated at Help Desk by Random Password Generator Do Not Work

With this patch update, if a Help Desk administrator changes a password using the Random Password Generator, new passwords containing an ampersand (&) character now work as expected. (Bug 1043222)

2 System Requirements

Self Service Password Reset includes support for the following operating system versions:

- Red Hat Enterprise Linux Server 7.3 or later (64-bit)
- SUSE Linux Enterprise Server 12 SP2 or later (64-bit)
- SUSE Linux Enterprise Server 11 SP4 (64-bit)
- Windows Server 2012 R2 (64-bit)

Self Service Password Reset is also available as an appliance since the 4.0 release. The appliance runs on the following virtual systems:

- Hyper-V 4.0 and 3.0
- VMware 5.5 or later

For detailed information on system requirements, supported operating systems, and browsers, see "Installing Self Service Password Reset" in the *Self Service Password Reset 4.1 Administration Guide*.

3 Installing this Patch Update

Installing the patch update is different for each platform that Self Service Password Reset supports. You must follow the steps for your specific deployment to install this patch update. For more information, see "Adding a Patch Update" in the *Self Service Password Reset 4.1 Administration Guide*.

4 Verifying the Installation

Complete the following steps to verify that the installation was successful.

To check the installed version:

1 Log in to the Self Service Password Reset administration console as an administrator.

2 In the toolbar, click your name, then click **Administration**.

3 Click the **About** tab, then verify that the **SSPR Version** is v4.1.0.5 b389 r39182.

5 Known Issues

NetIQ Corporation strives to ensure our products provide quality solutions for your enterprise software needs. The following issues are currently being researched. If you need further assistance with any issue, please contact Technical Support (http://www.netiq.com/support).

5.1 Forgotten Password Module Error after Upgrading from Self Service Password Reset 3.2 or Prior Versions

Issue: Self Service Password Reset 3.3 and above contains a new configuration option for forgotten password verification methods. If you upgrade without reviewing these new options, when you access the Forgotten Password Module it returns an error of `SSPR Error 5006 - The username is not valid or is not eligible to use this feature.` (Bug 979153)

Solution: To fix the error, you must review the forgotten password verification methods and change these options for your environment.

To review the forgotten password verification methods:

1 Log in to Self Service Password Reset at `https://dns-name/sspr` as an administrator.

2 In the toolbar, click your name.

3 Click **Configuration Editor** > **Modules** > **> Forgotten Password** > **Forgotten Password Profiles** > **default** > **Verification Methods**.

If you have created a different profile, select that name instead of **default**.

4 Review the verification methods and change these options for your environment.

5 Click **Save changes**.

5.2   Cannot Log In to Appliance Administration Console

Issue: Due to a security update for the operating system, the most recent versions of certain browsers cannot access the administration console of the Self Service Password Reset appliance. If you have not already encountered this issue, you can apply this patch update as usual and it addresses this issue. (Bugs 1042079, 1027746)

Solution: If you have already encountered this issue and are unable to log in to the administration console for the appliance at `https://mycompany.example.com:9443`, follow these steps:

1 On the appliance, access the command line as root and enter the following commands:

   `zypper refresh`

   `zypper patch`

2 Restart the appliance.

These commands download and apply the most recent patch update for the appliance that contains the fix for this issue.

5.3   Helpdesk Search Does Not Work Correctly in Internet Explorer

Issue: With Firefox and Chrome after you navigate to the helpdesk page, the cursor is in the search field. Typing characters causes the page to search for matches, and pressing **Enter** submits the search. With Internet Explorer, pressing **Enter** opens the locale selection dialog instead of submitting the search. (Bug 1037277)

Workaround: This is a browser issue in Internet Explorer. To work around this issue, use Firefox or Chrome instead.

6   Contact Information

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com (mailto:Documentation-Feedback@netiq.com). We value your input and look forward to hearing from you.

For detailed contact information, see the Support Contact Information website (http://www.netiq.com/support/process.asp#phone).

For general corporate and product information, see the NetIQ Corporate website (http://www.netiq.com/).

For interactive conversations with your peers and NetIQ experts, become an active member of our community (https://www.netiq.com/communities/). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

7   Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see https://www.netiq.com/company/legal/.

Copyright © 2017 NetIQ Corporation. All Rights Reserved.