Self Service Password Reset 4.1 Patch Update 6 Release Notes

September 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 5

Self Service Password Reset 4.1 Patch Update 6 contains all of the security updates and fixes included in Patch Updates 1 through 5. 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*
- *Self Service Password Reset 4.1 Patch Update 5 Release Notes*

You can install Patch Update 6 without installing the previous patches.

1.2.2 Updated Version of Tomcat

With this patch update, for the appliance and Windows versions of Self Service Password Reset, Tomcat has been updated to version 8.0.46. The Java version (JRE-8u141) has not changed. (Bug 1057931)

1.2.3 SUSE Register Log Added to Appliance Bundle

With this patch update, the Self Service Password Reset appliance bundle includes the `/var/opt/novell/va/logs/suse_register.log` and `/var/opt/novell/va/logs/VAclientSetup4SMT.log` files to help troubleshoot registration issues. (Bug 1035542)

1.2.4 Unable to Apply Some SUSE Patch Updates

With this patch update, all patch updates can now be installed as expected. (Bug 1054145)

1.2.5 REST Get Profile Fails on 4.*x* Appliances

With this patch update, the Get Profile REST call now retrieves the user profile successfully and includes the correct information. The username must be included as a parameter in the REST call. (Bug 1038346)

1.2.6 Helpdesk Search Does Not Work Correctly in Internet Explorer

With this patch update, pressing **Enter** on the helpdesk page now submits a search as expected in Internet Explorer. (Bug 1037277)

1.2.7 REST /randompassword Requires Syntax That Should Be Optional

This patch update addresses an issue where the /randompassword REST call required profileID/userDN syntax for the username, which should have been optional. (Bug 1031161)

1.2.8 SMS and Email Maximum Queue Age Settings Are Not Working

This patch update addresses an issue where messages were stuck in the SMS queue and were not being cleared because the Maximum SMS Queue Age Setting and the Maximum Email Queue Age Setting were not working. Both settings are now working correctly. (Bug 1049335)

1.2.9 Incorrect Error: 5006 Multiple User Matches in Single Profile

This patch update addresses an issue where Self Service Password Reset was searching both the SAP and Default profiles and returned an error when the same user name was found in two different profiles. If the LDAP Contextless Login Roots option is just set to SAP, Self Service Password Reset now searches only that profile as expected. (Bug 1051971)

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 v4.1.0.6 b412 r39267.

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.

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.