

Self Service Password Reset 4.1 Patch Update 3 Release Notes

May 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 \(https://forums.novell.com/forumdisplay.php/1343-Self-Service-Password-Reset\)](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.

- ◆ [Section 1, "What's New?," on page 1](#)
- ◆ [Section 2, "System Requirements," on page 4](#)
- ◆ [Section 3, "Installing Patch Update 3," on page 4](#)
- ◆ [Section 4, "Verifying the Installation," on page 4](#)
- ◆ [Section 5, "Known Issues," on page 5](#)
- ◆ [Section 6, "Contact Information," on page 5](#)
- ◆ [Section 7, "Legal Notice," on page 5](#)

1 What's New?

The following outlines the issues resolved in this release:

- ◆ [Section 1.1, "Security Updates," on page 1](#)
- ◆ [Section 1.2, "Enhancements and Software Fixes," on page 2](#)

1.1 Security Updates

Self Service Password Reset includes the following security updates:

- ◆ [Section 1.1.1, "Operating System Security Updates," on page 1](#)
- ◆ [Section 1.1.2, "Updated Java and Tomcat," on page 1](#)

1.1.1 Operating System Security Updates

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

1.1.2 Updated Java and Tomcat

For the appliance and Windows versions of Self Service Password Reset, Java and Tomcat have been updated to the latest versions. (Bug 1034697)

Java: JRE-8u131

1.2 Enhancements and Software Fixes

Self Service Password Reset 4.1 Patch Update 3 includes the following software enhancements and fixes for this release:

- ♦ [Section 1.2.1, “Contains all of the Updates in Patch Update 1 and Patch Update 2,” on page 2](#)
- ♦ [Section 1.2.2, “Randompasword REST API Requires profileID|userDN Syntax,” on page 2](#)
- ♦ [Section 1.2.3, “User Profile Confirmation Screen Not Honoring Display Settings,” on page 2](#)
- ♦ [Section 1.2.4, “Forgotten Password Module Returns Error 4033 Password Change Too Soon,” on page 3](#)
- ♦ [Section 1.2.5, “People Search Not Displaying Newly Added Attributes,” on page 3](#)
- ♦ [Section 1.2.6, “Unable to Edit HTML in the Email Templates,” on page 3](#)
- ♦ [Section 1.2.7, “Unable to Reset Users Passwords Using Forgotten Password if Password Minimum Age is Enabled,” on page 3](#)
- ♦ [Section 1.2.8, “Self Service Password Reset Allows Tokens to Be Used Multiple Times,” on page 3](#)
- ♦ [Section 1.2.9, “Token Database Table Is Not Properly Purged,” on page 3](#)
- ♦ [Section 1.2.10, “Password Change Agreement Page Cancel Results in 5043 Error,” on page 4](#)
- ♦ [Section 1.2.11, “A Log File on the Appliance Fills Up the Disk Space,” on page 4](#)

1.2.1 Contains all of the Updates in Patch Update 1 and Patch Update 2

Self Service Password Reset Patch Update 3 contains all of the security updates and fixes included in Patch Update 1. 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](#)

You can install Patch Update 3 without installing the previous patches it contains all of the fixes in the previous patches.

1.2.2 Randompasword REST API Requires profileID|userDN Syntax

Issue: The `randompasword` REST API requires a `profileID|userDN` syntax and this option should be optional. (Bug 1031161, 969643)

Solution: Patch Update 3 resolves this issue.

1.2.3 User Profile Confirmation Screen Not Honoring Display Settings

Issue: The User Profile confirmation screen displays the values of the attributes instead of the proper display information. For example, instead of displaying Enabled, the confirmation screen displays TRUE. (Bug 1030555)

Solution: Patch Update 3 resolves this issue.

1.2.4 Forgotten Password Module Returns Error 4033 Password Change Too Soon

Issue: The Forgotten Password module returns an error of 4033 Password change too soon. This happened because the Forgotten Password module initiates the check for minimum password lifetime by checking the last login time, not the last password modified use time. This caused the error to occur. (Bug1029209)

Solution: Patch Update 3 resolves this issue by having the Forgotten Password module use the last password modified use time to initiate the check for minimum password lifetime.

1.2.5 People Search Not Displaying Newly Added Attributes

Issue: After adding a new attribute to display in the People Search module, the People Search module does not display the new attributes. (Bug 1030943)

Solution: Patch Update 3 resolves this issue.

1.2.6 Unable to Edit HTML in the Email Templates

Issue: Unable to edit the HTML of the email templates in the Configuration Editor. (Bug 1030557)

Solution: Patch Update 3 resolves this issue for Firefox browsers. Chrome browsers cannot edit the HTML due to the HTML editor library Self Service Password Reset uses.

1.2.7 Unable to Reset Users Passwords Using Forgotten Password if Password Minimum Age is Enabled

Issue: Users are unable to reset their password using the Forgotten Password module, if the password minimum age option is enabled when using Oracle Directory Server as the LDAP user store. (Bug 1031390)

Solution: Patch Update 3 resolves this issue. Plus, ensure to add the following information in the Configuration Editor:

- 1 Log in to the Configuration Editor as an administrator.
- 2 Click **Settings > Application > Application > App Property Overrides**.
- 3 Click **Add Value**.
- 4 Specify the following exactly:

```
ldap.oracle.postTempPasswordUseCurrentTime=true
```

- 5 Click **Save changes**.

1.2.8 Self Service Password Reset Allows Tokens to Be Used Multiple Times

Issue: If you have select Token as an optional verification method, Self Service Password Reset allows the token to be used multiple times. (Bug 1034516)

Solution: Patch Update 3 resolves this issue.

1.2.9 Token Database Table Is Not Properly Purged

Issue: Self Service Password Reset does not properly purge the token database table over time. This leads to the tokens being reused when they should not be reused. (Bug 1034668)

Solution: Patch Update 3 resolves this issue.

1.2.10 Password Change Agreement Page Cancel Results in 5043 Error

Issue: With the **Password Change Agreement Message** enabled, a user clicks cancel on the password change agreement and receives a 5034 error. This only occurs if you enabled the **Settings > Security > Web Security > Enable Form** option. (Bug 1035028)

Solution: Patch Update 3 resolves this issue whether the option is set or not.

1.2.11 A Log File on the Appliance Fills Up the Disk Space

Issue: There was an internal file on the appliance that filled up all of the disk space. (Bug 1035527)

Solution: Patch Update 3 resolves this issue.

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 SP 2 or later (64-bit)
- ♦ SUSE Linux Enterprise Server 11 SP 4 (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

Self Service Password Reset also supports the Edge browser in this release.

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 Patch Update 3

Installing the Patch Update is different for each platform that Self Service Password Reset support. You must follow the step for your specific deployment to install the Patch Update 3. 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 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 the **SSPR Version** is v4.1.0.3 b321 r39084.

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 \(http://www.netiq.com/support\)](http://www.netiq.com/support).

- ♦ [Section 5.1, “Forgotten Password Module Error after Upgrading from Self Service Password Reset 3.2 or Prior Versions,”](#) on page 5

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.**

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 \(mailto:Documentation-Feedback@netiq.com\)](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 \(http://www.netiq.com/support/process.asp#phone\)](http://www.netiq.com/support/process.asp#phone).

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

For interactive conversations with your peers and NetIQ experts, become an active member of our [community \(https://www.netiq.com/communities/\)](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.

