Self Service Password Reset 4.2 Release Notes

August 2017

Self Service Password Reset 4.2 includes new features, improves usability, and resolves several previous issues.

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.

The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at the Self Service Password Reset Documentation (https://www.netiq.com/documentation/self-service-password-reset/) page. To download this product, see the NetIQ Downloads (https://dl.netiq.com/index.jsp) website.

1 What’s New?

The following sections outline the key features and functions provided by this version, as well as issues resolved in this release:

1.1 Security Improvements

Self Service Password Reset includes the following security improvements:

1.1.1 Operating System Security Updates

If you are running the Self Service Password Reset appliance, this release contains operating system and security updates.

1.1.2 Updated Versions of 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 1048735, 1049463)

Java: JRE-8u141

Tomcat: 8.5.16

1.1.3 Default Hashing Method for Challenge-Response Answers Changed

With this release, the default hashing method for the Challenge-Response answers has been changed from PBKDF2WithHmacSHA1 to PBKDF2WithHmacSHA512. This increases the security of your users' Challenge-Response answers. For more information, see "Understanding Challenge-Response Storage Methods" in the *Self Service Password Reset 4.2 Installation Guide*. (Bug 1051382)

1.2 Oracle Directory Services as an LDAP User Store Is Deprecated

Self Service Password Reset 4.2 and later versions will no longer support Oracle Directory Services as an LDAP user store. Active Directory and eDirectory are the only supported LDAP directories for user stores. For more information, see "Deployment Requirements of Self Service Password Reset" in the *Self Service Password Reset 4.2 Installation Guide*.

1.3 Options to be Deprecated in a Future Release

To facilitate future enhancements to SMS and email tokens, certain options for the following settings will be deprecated in a future release:

- **Modules** > **Public** > **User Activation** > **Token Send Method**
- **Modules** > **Public** > **Forgotten Password** > **Profiles** > *profile* > **Definition** > **Token Send Method**

For each of those settings, the following options will be deprecated:

- **Both** (Send token to both email and SMS)
- **SMS First** (Try to send token via SMS; if no SMS number is available, send via email)
- **Email First** (Try to send token via email; if no email address is available, send via SMS)

If either setting is in use, Self Service Password Reset will display a warning on the health screen indicating the deprecation. (Bug 1053735)

1.4 Enhancements and Software Fixes

Self Service Password Reset includes the following software enhancements and fixes for this release:

1.4.1 User Debug Tool

With this release, Self Service Password Reset now contains a User Debug tool that shows you detailed information about any user account. The information that the tool displays allows you to troubleshoot when users cannot log in or do not have access to a specific Self Service Password Reset module, among many other items. For more information, see “Obtaining the User Debug Information” in the *Self Service Password Reset 4.2 Administration Guide*.

1.4.2 Feature Usage Statistics

With this release, Self Service Password Reset now contains a feature that enables NetIQ to gather statistics about the usage of features. This allows NetIQ to focus more development resources on the most used features. You can enable and disable this feature through the Configuration Guide and the Configuration Editor. For more information, see “Configuring the Telemetry Options ”in the *Self Service Password Reset 4.2 Administration Guide*. (Bugs 1034510 and 1034507)

1.4.3 Added Localization Support for More Languages

With this release, Self Service Password Reset now supports Canadian English, Canadian French, and Hebrew. For a complete list of all supported languages, see “Self Service Password Reset Key Features” in the *Self Service Password Reset 4.2 Installation Guide* (Bug 902751).

1.4.4 New Upgrade Option for Appliances

With this release, the appliance contains a new upgrade option that simplifies the upgrade process if your current appliance is version 4.1.*x*.*x*. For more information, see “Upgrading Self Service Password Reset 4.1.0.5 to 4.2” in the *Self Service Password Reset 4.2 Installation Guide*.

1.4.5 New Page to Monitor Nodes in the Configuration Manager

With this release, there is a new Nodes page in the Configuration Manager that lets you monitor the status of the nodes in the L4 switch if you have configured it for load balancing and high availability. For more information, see "High Availability and Load Balancing" in the *Self Service Password Reset 4.2 Installation Guide*. (Bug 1049729)

1.4.6 Added a Specific Redirect URL for Users after Registration

With this release, Self Service Password Reset now allows you to use a specific redirect URL for your users after they complete the new user registration process. By default, Self Service Password Reset uses the **After Registration Redirect URL** setting to redirect users after they complete the registration process. Now you can send your users to a specific URL. For more information, see "Creating Accounts for Social Users in Self Service Password Reset Using the New User Registration Module" in the *Self Service Password Reset 4.2 Administration Guide*. (Bug 1038360)

1.4.7 Custom Links on the Update Profile Page

With this release, Self Service Password Reset allows you to add custom links to the Update Profile page if you have enabled and configured the Update Profile module. For more information, see "Adding the Device Management Link to the Update Profile Page" in the *Self Service Password Reset 4.2 Administration Guide*. (Bugs 1034782, 1031433, and 1043893)

1.4.8 New User Registration Module Can Create a Randomly Generated Password for Users

With this release, Self Service Password Reset does not require new users to create a password; it is able to create a randomly generated password for users. For more information, see "Configuring the New User Registration Module" in the *Self Service Password Reset 4.2 Administration Guide*. (Bug 1038546)

1.4.9 Delete Account Module Can Delete Accounts from Integrated Products

With this release, the Delete Account module deletes the user account information from Self Service Password Reset as well as any integrated products. The Delete Account module can delete both user accounts if the integrated product contains a REST call to delete the accounts from the integrated product. This module does require configuration to work. For more information, see "Configuring the Delete Account Module to Delete Accounts from Integrated Products" in the *Self Service Password Reset 4.2 Administration Guide*. (Bug 1035049)

1.4.10 Performance Enhancements

With this release, Self Service Password Reset contains a number of different performance enhancements:

- Increase in performance when searching multiple LDAP profiles. (Bug 938137)
- Increase in performance of the remote database when the Self Service Password Reset is under load. (Bug 1043470)
- Increase in performance of the administration or proxy connections to Self Service Password Reset. (Bug 1043483)
- Decrease in latency for email tokens when users reset their passwords. (Bug 1042573)

The enhancements affect all platform deployments of Self Service Password Reset.

1.4.11 People Search Module Enhancements

With this release, the People Search module in Self Service Password Reset contains the following enhancements:

- Self Service Password Reset 4.2 now sorts the People Search results and the Organizational Chart alphabetically by first line. In previous versions, they were sorted according to the order returned by the LDAP directory. (Bug 1048418)
- The Organizational Chart now contains an option for an assistant in the hierarchical organizational chart. In addition, you can specify an assistant attribute name in the People Search settings. (Bug 1048417)

1.4.12 Error 5035 When a Help Desk Administrator Changes a User's Password

With this release, a help desk administrator no longer receives a 5035 error after changing a password for a user. (Bug 1042771)

1.4.13 Graceful Handling of Non-Canonical DN Values in the Configuration

With this release, Self Service Password Reset matches the exact syntax for the LDAP DNs. This allows Self Service Password Reset to handle non-canonical DN values. (Bug 990394)

1.4.14 Added Log Rotation of Apache Tomcat Files of Deployments on Windows Servers

With this release, the logs on the Windows deployment automatically rotate at 10 MB. The behavior of prior deployments was the default behavior of logging by Apache Tomcat. (Bug 1045742)

1.4.15 Improved Usability of Saving the Configuration File

With this release, Self Service Password Reset contains a new message when you save the configuration file. You must click **Store**, and then click **Save changes** in the toolbar for the changes to take effect. (Bug 1023254)

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
- VMware 5.5 or later

For detailed information on system requirements, supported operating systems, and browsers, see "Deployment Requirements of Self Service Password Reset" in the *Self Service Password Reset 4.2 Administration Guide*.

3 Installing or Upgrading Self Service Password Reset

To install Self Service Password Reset, see “Installing Self Service Password Reset” in the *Self Service Password Reset 4.2 Installation Guide*.

To upgrade your current deployment of Self Service Password Reset to this version, see “Upgrading Self Service Password Reset” in the *Self Service Password Reset 4.2 Installation Guide*.

4 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).

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

6 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/.