Self Service Password Reset 4.0 Release Notes

August 2016

Self Service Password Reset 4.0 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-40/) page. To download this product, see the NetIQ Downloads (https://dl.netiq.com/index.jsp) website.

1 What's New?

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

1.1 Operating System Support

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

- Red Hat Enterprise Linux Server 6.2 or later (64-bit)
- SUSE Linux Enterprise Server 12 SP 1 (64-bit)
- Windows Server 2012 R2 (64-bit)

Self Service Password Reset is also available as an appliance for 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 more information, see "Installing Self Service Password Reset" in the *Self Service Password Reset 4.0 Administration Guide*.

1.2 Security Improvements

Self Service Password Reset includes the following security improvements:

- Section 1.2.1, "Enhanced Security for SSH on the Self Service Password Reset Appliance," on page 2
- Section 1.2.2, "Added Support for Additional Hashing Methods," on page 2

1.2.1 Enhanced Security for SSH on the Self Service Password Reset Appliance

The appliance for Self Service Password Reset contains enhance security for SSH to the appliance. You must have the latest SSH clients to access the appliance through SSH.

1.2.2 Added Support for Additional Hashing Methods

Self Service Password Reset uses hashing to store user credentials securely. The 4.0 release now includes support for PBKDF2WithHmacSHA256 and PBKDF2WithHmacSHA512. For more information, see "Understanding Challenge-Response Storage Methods" in the *Self Service Password Reset 4.0 Administration Guide*.

1.3 Enhancements and Software Fixes

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

- Section 1.3.1, "An Appliance for Self Service Password Reset," on page 2
- Section 1.3.2, "High Availability and Load Balancing," on page 3
- Section 1.3.3, "Simplified the Configuration of Self Service Password Reset with Updates to the Configuration Guide," on page 3
- Section 1.3.4, "LDAP Permissions Tool," on page 3
- Section 1.3.5, "Enhanced Management of Profiles," on page 3
- Section 1.3.6, "Added Support for Multi-Valued Attributes to Some Modules," on page 3
- Section 1.3.7, "Enhanced User Update Process," on page 4

1.3.1 An Appliance for Self Service Password Reset

Self Service Password Reset 4.0 contains an appliance you can deploy in your virtual environment.There is a version of the appliance for VMware and Microsoft Hyper-V. For more information, see "Deploying the Self Service Password Reset Appliance" in the *Self Service Password Reset 4.0 Administration Guide*.

1.3.2 High Availability and Load Balancing

Self Service Password Reset now supports high availability and load balancing. For more information, see "High Availability and Load Balancing" in the *Self Service Password Reset 4.0 Administration Guide*.

1.3.3 Simplified the Configuration of Self Service Password Reset with Updates to the Configuration Guide

The Configuration Guide contains updates to simplify configuring your environment for Self Service Password Reset.

- ◆ **Automated Creation of Certificates:** In previous versions, you would have to manually create certificates to the establish secure connections between Self Service Password Reset and the LDAP directory. The Configuration Guide does this for you now.

- ◆ **Schema Extended for LDAP Directories:** To have Self Service Password Reset work with LDAP directories to store the challenge-response information, you must extend the schema for the LDAP directory. The Configuration Guide extends the schema for you if you are using eDirectory. If you are using Active Directory or Oracle Directory Server, you must manually extend the schema.

- ◆ **Schema Extended for External Database:** The Configuration Guide now extends the schema for the external database instead of requiring you to extend the schema.

These are just some of the changes made to the Configuration Guide. We recommend that you use the Configuration Guide instead of manually configuring your environment for Self Service Password Reset. For more information, see "Using the Configuration Guide" in the *Self Service Password Reset 4.0 Administration Guide*.

1.3.4 LDAP Permissions Tool

If you use an LDAP directory to store the challenge-response information, you must assign specific rights in the LDAP directory for Self Service Password Reset to work. Every time you enable a new module, you must ensure that the LDAP directory has the correct rights to work with Self Service Password Reset.

Self Service Password Reset 4.0 now contains an LDAP Permissions tool that reads the Self Service Password Reset configuration file and lists all of the required rights you must change in the LDAP directory for Self Service Password Reset to work. For more information, see "Viewing LDAP Permissions Recommendations" in the *Self Service Password Reset 4.0 Administration Guide*.

Also, you can view a video demonstrating the LDAP Permissions Tool.

1.3.5 Enhanced Management of Profiles

Self Service Password Reset 4.0 now allows you to rename and copy profiles in the Configuration Editor. You can also create multiple update profiles, which allows you to define a unique set of update profile configuration options for each LDAP group or for each LDAP filter.

1.3.6 Added Support for Multi-Valued Attributes to Some Modules

The Help Desk module and the People Search module now supports multiple attributes. This expands the search capabilities of both modules.

1.3.7 Enhanced User Update Process

In previous versions, users could not update their own email addresses or telephone numbers through the Forgotten Password module. Self Service Password Reset 4.0 now allows users to set up their own email addresses and telephone numbers as follows:

1. The user chooses to update the email address and phone number through the Update module.

2. The user enters the new email address and phone number.

3. Self Service Password Reset validates the new email address and phone number using tokens you have configured.

4. Self Service Password Reset updates the LDAP attributes that contain the email address and phone number.

2 System Requirements

Self Service Password Reset 4.0 has an appliance you can install in a virtual environment. This release supports VMware and Hyper-V.

For detailed information on system requirements, supported operating systems, and browsers, see "Installing Self Service Password Reset" in the *Self Service Password Reset 4.0 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 4.0 Administration 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 4.0 Administration 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 Mobile Enrollment Page Contains No Cancel Button

Issue: There is no **Cancel** or **Back** button on the mobile enrollment page when users enroll their devices in the same session. (Bug 990048)

Workaround: Users must close the browser and log in again. They do not lose any information. Self Service Password Reset enrolls their devices without any problems. Users must log in again to perform any additional actions.

4.2 Users See a Failure Message when Checking the Mobile Code

Issue: When users enroll their mobile devices and they check the mobile code in the same session, they receive a failure message on their mobile devices. (Bug 990053)

Workaround: The enrollment did not fail even though users see the failure message. For the users not to see the failure message, they must perform the enrollment in the following order:

1. The users log in to Self Service Password Reset and enroll their mobile devices.
2. The users must log out of Self Service Password Reset.
3. The users log in to Self Service Password Reset.
4. The users access the mobile authentication section, then select **Check code**.

4.3 Self Service Password Reset Sends No Emails to Users

Issue: You have configured Self Service Password Reset to send emails to users and no emails are being sent. The issue is that the **Default From Address** field contains an email address with underscores in the domain name. For example, test_user@sspr_testing.com. (Bug 989629)

Workaround: Currently, the Configuration Editor allows you enter an email address with underscores in the domain name. However, underscores in the domain name are not supported by the SMTP server. To fix this issue, remove the underscore from the domain name.

4.4 Blank Screen on the Appliance after Configuring the Network Information

Issue: After you have configured the network information for the appliance, the console screen is completely blank. (Bug 987433)

Workaround: Reboot the appliance. You can do that through your virtual appliance tools. After you reboot the appliance, the screen shows how to access Self Service Password Reset to configure it for your environment.

4.5 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**.

4.6 Login Errors when Integrated with Identity Manager 4.5

Issue: When you integrate Self Service Password Reset 4.0 with Identity Manager 4.5, users are unable to authenticate. The error in the `catalina.out` file is `Client-supplied redirect URI is not registered`. (Bug 999064)

Solution: Install Patch Update 1 or later for Self Service Password Reset 4.0. The patch update contains the fix for this issue. For more information about how to install a patch update, see "Adding a Patch Update" in the *Self Service Password Reset 4.0 Administration Guide*. Ensure that you have installed the latest service pack for Identity Manager 4.5 as well.

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/.