Self Service Password Reset 4.0.0 Patch Update 1

September 2016

MICRO FOCUS®

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.netiq.com/forumdisplay.php?119-Self-Service-Password-Reset) on NetIQ Communities, our online community that also includes product information, blogs, and links to helpful resources.

1 What's New?

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

1.1 Operating System Security Updates

If you are running the Self Service Password Reset Appliance, this patch update contains operating system, security updates, and the latest version of Tomcat (Bug 999744).

1.2 Enhancements and Software Fixes

Self Service Password Reset includes software fixes that resolve several previous issues.

1.2.1 Identity Manager 4.5 Supports Self Service Password Reset 4.0.0 Patch Update 1

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`. (Bugs 979153, 999064)

Fix: Apply patch update 1 or later and Self Service Password Reset now integrates with Identity Manager 4.5 without an errors.

1.2.2 Added Support for an Xodus Locale Database Implementation

Added support for an Xodus local database implementation to perform extensive testing before enabling for all deployments of Self Service Password Reset. (Bug 998940)

1.2.3 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)

Fix: Apply patch update 1 and the mobile enrollment page displays the **Cancel** and **Back** buttons.

1.2.4 Added Support for an Xodus Locale Database Implementation

Added support for an Xodus local database implementation to perform extensive testing before enabling for all deployments of Self Service Password Reset. (Bug 998940)

1.2.5 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)

Fix: Apply patch update 1 and the users do not see the failure message when checking the mobile code.

1.2.6 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)

Fix: Apply patch update 1 and Self Service Password Reset allows underscores in the domain part of the email address from the **Default From Address** in the Email Settings.

1.2.7 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)

Fix: Apply patch update 1 and a reboot of the appliance is no longer required.

1.2.8 Change Password Fails with Error Rule Requirements not Met

Issue: If users use **Change Password** to change their passwords, the password changes fails with the error `Rule Requirement not Met`. However, if users use **Forgotten Password**, the passwords change without any errors.

Fix: Apply patch update 1 and the error no longer occurs in **Change Password**.

1.2.9 Configuration Editor in Internet Explorer 11 Returns an Error 5027

Issue: Logging in to the Configuration Editor as a user with administrative rights, using Internet Explorer 11, causes an error 5072 to occur.

Fix: Apply patch update 1 and the error no longer occurs.

1.2.10 LDAP Permissions not Showing the Correct Rights

Issue: The LDAP Permissions tool does not show the correct rights for **People Search**. (Bug 993157)

Fix: Apply patch update 1 and the LDAP Permissions tools shows the correct rights for **People Search** to work properly.

1.2.11 OTP and PIN Fields Are Missing on RADIUS Logins with Advanced Authentication

Issue: If you have integrated Self Service Password with Advanced Authentication, the RADIUS logins are missing the OTP and PIN fields. (Bug 993589)

Fix: Apply patch update 1 and the RADIUS login page now displays the OTP and PIN fields.

1.2.12 Logging in to Self Service Password Reset with Active Directory and Multiple Profiles Returns Error 5016

Issue: If you user store is Active Directory and the users have multiple profiles, when the users log in to Self Service Password Reset, it returns an error of 5016.

Fix: Apply patch update 1 and the error 5016 no longer occurs if users have multiple profiles.

1.2.13 Missing Audit Event LocalDB Max Size Setting

Issue: Self Service Password Reset was missing the audit event **LocalDB Max Size** setting. As a result, the locale database could fill and cause disk space issues on the server. (Bug 993733)

Fix: Apply patch update 1 to have the **LocalDB Max Size** setting appear in the Configuration Editor.

1.2.14 Syslog or Sentinel Output is Corrupt if the Length is Longer than 1024 Characters

Issue: The Syslog or Sentinel output for audit logs in corrupt is the length of the audit message is longer than 1024 characters. (Bug 997124)

Fix: Apply patch update 1 to no longer have the output from Syslog and Sentinel corrupted.

1.2.15 Setup Response Page Does Not Enable the Save Answer Button

Issue: If you have configure Self Service Password Reset integrated with Access Manager, the Setup Response page does not enable the Save Answer Button. (Bug 997153)

Fix: Apply patch update 1 to solve this issues.

1.2.16 Users Not Forced to Answer Challenge Response Questions

Issue: If you are using the trial version of Self Service Password Reset, it would not force users to answer the challenge response questions. (Bug 997781)

Fix: Use the full version of Self Service Password Reset 4.0. This issue will be resolved in trial versions during a future release.

1.2.17 Audit Events in the Local Database not Constrained by Limits

Issue: Self Service Password Reset is not expunging audit events from the local database based on the maximum count and maximum age limit settings. This can cause out of disk space errors to occur. (Bug 999523)

Fix: Apply patch update 1 to solve this issue.

1.2.18 Removed an Unnecessary Health Warning

Issue: The Configuration Manager displays a unnecessary health warning stating `Requires HTTPS setting should be set to true for proper security`. There is not Requires HTTPS setting. (Bug 999072)

Fix: Apply patch update 1 and the Configuration Manager no longer displays this warning.

2 System Requirements

This Patch Update 1 requires Self Service Password Reset 4.0.

For detailed information on hardware requirements and supported operating systems and browsers, see "Installation Requirements" in the *Self Service Password Reset 4.0 Administration Guide*.

3 Installing Patch Update 1

To upgrade Self Service Password Reset to the latest patch, see "Adding a Patch Update" in the *Self Service Password Reset 4.0 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.

   `https://localhost:port/sspr`

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

3 Click the **About** tab, then verify the **SSPR Version** is v4.0.0.1 b502 r38946.

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/.