NetIQ Self Service Password Reset 4.4 Release Notes

April 2019

NetIQ Self Service Password Reset 4.4 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 NetIQ 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 NetIQ 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.

- Section 1, “What’s New?,” on page 1
- Section 2, “System Requirements,” on page 4
- Section 3, “Installing or Upgrading NetIQ Self Service Password Reset,” on page 5
- Section 4, “Verifying the Installation or Upgrade,” on page 5
- Section 5, “Known Issues,” on page 5
- Section 6, “Contact Information,” on page 6
- Section 7, “Legal Notice,” on page 6

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:

- Section 1.1, “Security Improvements,” on page 1
- Section 1.2, “Enhancements and Software Fixes,” on page 2

1.1 Security Improvements

NetIQ Self Service Password Reset includes the following security improvements:

- Section 1.1.1, “Operating System Security Updates,” on page 2
- Section 1.1.2, “Updated Versions of Java and Apache Tomcat,” on page 2
- Section 1.1.3, “Allow Root-Certificate-Only Certificate Validation for Outbound TLS Connections,” on page 2

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. These updates include updates to the latest versions of Java and Apache Tomcat.

1.1.2 Updated Versions of Java and Apache Tomcat

With this release, the Java and Apache Tomcat have been updated for the appliance and the Windows MSI file.

Java: AdoptOpenJDK - Hotspot - 11.0.1+13

Apache Tomcat: 9.0.14

You must install Apache Tomcat and Java before you deploy the WAR file. For more information, see "Deployment Requirements for Self Service Password Reset WAR File on Linux" in the *Self Service Password Reset 4.4 Installation Guide*.

1.1.3 Allow Root-Certificate-Only Certificate Validation for Outbound TLS Connections

With this release, Self Service Password Reset allows only Root CA certificate validation for outbound TLS connections instead of requiring the entire certificate chain. For more information, see, "Configuring Security for Self Service Password Reset" in the *Self Service Password Reset 4.4 Administration Guide*. (Bug 1119582)

1.2 Enhancements and Software Fixes

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

- Section 1.2.1, "Password Expiration Notification with an LDAP Directory and a Remote Database," on page 2
- Section 1.2.2, "Support for Integration with Access Manager through OAuth2 to Provide Single Sign-on," on page 3
- Section 1.2.3, "Support for Invisible reCAPTCHA," on page 3
- Section 1.2.4, "Help Desk Module Enhancements," on page 3
- Section 1.2.5, "People Search Module Enhancements," on page 4
- Section 1.2.6, "Minimum Non-Alpha and Maximum Non-Alpha Setting Work Correctly," on page 4
- Section 1.2.7, "Added a 30 Day Warning Message about Administrator Password," on page 4
- Section 1.2.8, "Keystroke Validation Failing Using Internet Explorer During Challenge-Response Configuration," on page 4

1.2.1 Password Expiration Notification with an LDAP Directory and a Remote Database

With this release, Self Service Password Reset allows you to send notifications about passwords expiring with an LDAP directory or a remote database. You must use an LDAP directory or a remote database to store your users' information. For more information, see "Sending Notifications for Expiring Passwords" in the *Self Service Password Reset 4.4 Administration Guide*. (Bug 1119584, 1119586, 1119587)

1.2.2 Support for Integration with Access Manager through OAuth2 to Provide Single Sign-on

With this release, you can integrate Self Service Password Reset with Access Manager using OAuth2 to provide single sign-on for your customers. You create an OAuth2 application in Access Manager and perform additional configuration steps in the Configuration Editor to complete the integration. For more information, see "Configuring Single Sign-on with OAuth2 Tokens" in the *Self Service Password Reset 4.4 Administration Guide*. (`Bug 1093555`)

1.2.3 Support for Invisible reCAPTCHA

With this release, Self Service Password Reset supports Invisible reCAPTCHA. For more information, see "Configuring CAPTCHA" in the *Self Service Password Reset 4.4 Administration Guide*. (`Bug 1111101`)

1.2.4 Help Desk Module Enhancements

With this release, there are a number of Help Desk module enhancements.

- Section 1.2.4.1, "Help Desk Verification Process Masks Users' Values," on page 3
- Section 1.2.4.2, "Added an Advanced Search Option to the Help Desk Module," on page 3
- Section 1.2.4.3, "Help Desk Module Verification Process Allows Multiple Emails and SMS Numbers," on page 3
- Section 1.2.4.4, "Help Desk Module Only Displays the Enabled Options for the Users," on page 3
- Section 1.2.4.5, "Help Desk Module Displays the Selected Locale," on page 3

1.2.4.1 Help Desk Verification Process Masks Users' Values

With this release, during the Help Desk verification process, Self Service Password Reset masks the users' values of email, SMS number, and phone number. After the verification process completes, the help desk users can see these values. (`Bug 1104329`)

1.2.4.2 Added an Advanced Search Option to the Help Desk Module

With this release, Self Service Password Reset contains the ability to enable an advanced search option for the Help Desk module. By default, the advanced search is not enabled. You must configure the advanced search options to have it available for users. For more information, see "Configuring the Advanced Search for the Help Desk Module" in the *Self Service Password Reset 4.4 Administration Guide*.

1.2.4.3 Help Desk Module Verification Process Allows Multiple Emails and SMS Numbers

With this release, you can select the primary email address or SMS number for the Help Desk verification process as well as two additional emails or SMS numbers. (`Bug 1110810`)

1.2.4.4 Help Desk Module Only Displays the Enabled Options for the Users

With this release, the Help Desk module only displays the enabled options for the user. In prior releases, the Help Desk module displayed all options whether they were enabled or not. (`Bug 1103616`)

1.2.4.5 Help Desk Module Displays the Selected Locale

With this release, the Help Desk module displays the locale you select in the settings. (`Bug 1113099`)

1.2.5 People Search Module Enhancements

With this release, Self Service Password Reset contains a number of enhancements for the People Search module. The People Search module enhancements are not enabled by default. You must enable these features in the Configuration Editor for the People Search module to enable these enhancements. The new enhancements are:

- Added the ability to print the organization chart view. (`Bug 1100465`)
- Added a link to email all members of a team. (`Bug 1100457`)
- Added the ability to export the organization chart. (`Bug 1056670`)
- Added an Advanced option for searching. The users have the ability to configure the user search by selecting attributes. (`Bug 1052614`)
- Fixed the tool tips. (`Bug 111403`)

For more information, see "Configuring the People Search Module" in the *Self Service Password Reset 4.4 Administration Guide*.

1.2.6 Minimum Non-Alpha and Maximum Non-Alpha Setting Work Correctly

In prior versions, the **Minimum Non-Alpha** and **Maximum Non-Alpha** password policy setting for eDirectory did not work correctly. This release resolves this issue and these setting work correctly. (`Bug 1093467`)

1.2.7 Added a 30 Day Warning Message about Administrator Password

With this release, in the Configuration Manager, the Health displays a warning starting 30 days before the administrator's password is going to expire. (`Bug 1105699`)

1.2.8 Keystroke Validation Failing Using Internet Explorer During Challenge-Response Configuration

This patch resolves the issue where the keystroke validation fails when users perform the initial configuration for the challenge-response information using Internet Explorer. (`Bug 1128752`)

2 System Requirements

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

- **Appliance:** You can deploy the Self Service Password Reset appliance in the following virtual systems:
  - Hyper-V version 4.0
  - VMware ESX 6.5 or later
- **Windows .msi File:** You can deploy the Self Service Password Reset `.msi` file on the following platforms:
  - Windows Server 2016
  - Windows Server 2012
  - Amazon Web Services EC2 Windows 2016
  - Microsoft Azure Marketplace Windows 2016
- **WAR File:** You can deploy the Self Service Password Reset WAR file on the following platforms:
  - Red Hat Enterprise Linux Server 7.4 or later (64-bit)

- SUSE Linux Enterprise Server
  - 12 SP3 or later (64-bit)
  - 11 SP4 or later (64-bit)
- Amazon Web Services EC2 SUSE Linux Enterprise Server 12 SP3
  - Red Hat Enterprise Linux 7.4
  - SUSE Linux Enterprise Server 12 SP3
- Microsoft Azure Marketplace
  - Red Hat Enterprise Linux 7.4
  - SUSE Enterprise Server 12 SP3

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 4.4 Administration Guide*.

3 Installing or Upgrading NetIQ Self Service Password Reset

To install Self Service Password Reset, see "Installing Self Service Password Reset" in the *Self Service Password Reset 4.4 Installation Guide*.

Self Service Password Reset 4.4 or later contains a schema change for email notifications of expired passwords. You must extend the schema again to use the new attribute or you can use an existing LDAP attribute instead. For more information, see *Configuring Self Service Password Reset for Password Expiration Notifications with an LDAP Directory* in the "Self Service Password Reset 4.4 Administration Guide". (`Bug 1119587`)

To upgrade your current deployment of Self Service Password Reset to this version, see "Upgrading or Migrating Self Service Password Reset" in the *Self Service Password Reset 4.4 Installation Guide*.

4 Verifying the Installation or Upgrade

Complete the following steps to verify that the installation or update was successful.

1. Log in to the Self Service Password Reset administration console as an administrator.

   `https://dns-name:port/sspr`

2. In the toolbar, click your name, then click **Administration**.
3. Click the **About** tab, then verify that the **SSPR version** is v4.4.0.0 b306 r39665.

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).

- Section 5.1, "Not Able to Connect to the LDAP Directory," on page 6
- Section 5.2, "Issues with Right-to-Left Text," on page 6

5.1 Not Able to Connect to the LDAP Directory

Issue: Java 9 enables the LDAPS (LDAP over TLS) endpoint identification. If the subject name of the LDAP server certificate does not match the DNS name of the LDAP server, no LDAP connections can be made to the LDAP server. (`Bug 1118684`)

Solution: You must update the subject name of the LDAP server certificate to match the DNS name of the LDAP server. We recommend this option to avoid any security issues.

Workaround: If you are not immediately able to update the name of the LDAP server certificate, see the following technical support document for other workarounds 7023419 (https://support.microfocus.com/kb/doc.php?id=7023419).

5.2 Issues with Right-to-Left Text

Issue: With this release, there are issues with the right-to-left text in the Help Desk and People Search modules.

Solution: The right-to-left issues will be addressed in a future patch.

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 © 2019 NetIQ Corporation. All Rights Reserved.