

NetIQ Self Service Password Reset 4.3 Release Notes

April 2018



NetIQ Self Service Password Reset 4.3 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 \(https://forums.novell.com/forumdisplay.php/1343-Self-Service-Password-Reset\)](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 \(https://www.netiq.com/documentation/self-service-password-reset/\)](https://www.netiq.com/documentation/self-service-password-reset/) page. To download this product, see the [NetIQ Downloads \(https://dl.netiq.com/index.jsp\)](https://dl.netiq.com/index.jsp) website.

- ♦ [Section 1, "What's New?," on page 1](#)
- ♦ [Section 2, "System Requirements," on page 7](#)
- ♦ [Section 3, "Installing or Upgrading NetIQ Self Service Password Reset," on page 8](#)
- ♦ [Section 4, "Known Issues," on page 8](#)
- ♦ [Section 5, "Contact Information," on page 9](#)
- ♦ [Section 6, "Legal Notice," on page 10](#)

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 3](#)

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 for Windows," on page 2](#)
- ♦ [Section 1.1.3, "Self Service Password Reset Only Supports TLS 1.2 After an Upgrade," on page 2](#)
- ♦ [Section 1.1.4, "Added Macro Support for Hashing Values," on page 2](#)

- ♦ [Section 1.1.5, “Updated the Self Service Password Reset Web Services Implementation,” on page 2](#)
- ♦ [Section 1.1.6, “Removed Ganglia from the Appliance Due to Security Concerns,” 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 for Windows

For the Windows versions of Self Service Password Reset, Java and Apache Tomcat have been updated. Due to a bug in Java we cannot use the latest version of 8u172. (Bug 1078891)

Java: JRE-8u162

Apache Tomcat: 8.5.30

1.1.3 Self Service Password Reset Only Supports TLS 1.2 After an Upgrade

By default, Self Service Password Reset only enables TLS 1.2 after the upgrade. Ensure that your browsers support TLS 1.2 or the users will not be able to log in after the upgrade. The most recent versions of the supported browsers support TLS 1.2. If you want to change this setting to a different protocol, you can access the setting in the Configuration Editor under **Settings > HTTPS Servers > TLS Protocols**.

1.1.4 Added Macro Support for Hashing Values

With this release, Self Service Password Reset 4.3 macros now support hashes for:

- ♦ md5
- ♦ sha1
- ♦ sha256
- ♦ sha512

(Bug 1055982)

1.1.5 Updated the Self Service Password Reset Web Services Implementation

This release of Self Service Password Reset contains an updated web services implementation. The changes have increased the security of the product. (Bug 1055592, 1054323)

1.1.6 Removed Ganglia from the Appliance Due to Security Concerns

With this release, the Self Service Password Reset appliance no longer contains Ganglia because of security issues in Ganglia. (Bug 1087366)

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, “Changed the Minimum Memory Required for the Appliance to be 3 GB,” on page 3](#)
- ♦ [Section 1.2.2, “Users Can Upload Photos through Update Profile,” on page 4](#)
- ♦ [Section 1.2.3, “Help Desk Users Can Modify Multiple Attributes at the Same Time,” on page 4](#)
- ♦ [Section 1.2.4, “Added the Ability to Send a Notifications to Users about Passwords Expiring,” on page 4](#)
- ♦ [Section 1.2.5, “REST Enhancements,” on page 4](#)
- ♦ [Section 1.2.6, “Contains Enhancements for Validation Tokens,” on page 4](#)
- ♦ [Section 1.2.7, “User Reports Display Validation Methods,” on page 4](#)
- ♦ [Section 1.2.8, “Added Support for Multiple SMTP Servers,” on page 4](#)
- ♦ [Section 1.2.9, “Default Word List Contains the Challenge-Response Answers,” on page 5](#)
- ♦ [Section 1.2.10, “Added Support for the Common Event Format in Auditing,” on page 5](#)
- ♦ [Section 1.2.11, “Added Support for a Fail-Over Syslog Server,” on page 5](#)
- ♦ [Section 1.2.12, “Added a Password Strength Estimation Option,” on page 5](#)
- ♦ [Section 1.2.13, “Changed the Behavior of the Change Password Fields,” on page 5](#)
- ♦ [Section 1.2.14, “Deprecated Token Send Methods of SMSFIRST, EMAILFIRST, and BOTH,” on page 5](#)
- ♦ [Section 1.2.15, “Deprecated JavaScript Option from New User Form Fields,” on page 5](#)
- ♦ [Section 1.2.16, “Advanced Authentication Endpoint Session Timeouts with OAuth2 Configured in the Forgotten Password Module,” on page 5](#)
- ♦ [Section 1.2.17, “Added Trusted Certificates for the SMS Gateway,” on page 6](#)
- ♦ [Section 1.2.18, “Ability to Add Additional Entries to the Hosts File for the Appliance,” on page 6](#)
- ♦ [Section 1.2.19, “New Generic Forgotten Password Policy,” on page 6](#)
- ♦ [Section 1.2.20, “Enhanced HTML Editor for Email Templates,” on page 6](#)
- ♦ [Section 1.2.21, “Added Enhancements for Screen Reader Software,” on page 6](#)
- ♦ [Section 1.2.22, “OTP Module Contains Profile Settings,” on page 6](#)
- ♦ [Section 1.2.23, “Password Policy Maximum Length Increased,” on page 6](#)
- ♦ [Section 1.2.24, “Added a Configurable URL for the Home Page,” on page 6](#)
- ♦ [Section 1.2.25, “Support Option in the Appliance Accepts 12 Digit Service Request Numbers,” on page 7](#)
- ♦ [Section 1.2.26, “Detailed Error Messaging Enabled During Configuration,” on page 7](#)
- ♦ [Section 1.2.27, “Updated Error Message in the Forgotten Password Module,” on page 7](#)
- ♦ [Section 1.2.28, “Fixed Help Desk Timeout Issue,” on page 7](#)
- ♦ [Section 1.2.29, “Allow Forgotten Password Unlock Sequence When within Minimum Lifetime Password Window,” on page 7](#)

1.2.1 Changed the Minimum Memory Required for the Appliance to be 3 GB

With this release, the minimum memory requirement has changed from 2 GB to 3 GB. (Bug 1090431)

1.2.2 Users Can Upload Photos through Update Profile

With this release, Self Service Password Reset allows the users to upload their own photos through the **Update Profile** option. The organizational chart and People Search display the photo of the users. You must enable this feature. It is not enabled by default. For more information, see [Configuring the Update Profile Module](#) in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 1052820)

1.2.3 Help Desk Users Can Modify Multiple Attributes at the Same Time

With the release, the help desk users can modify multiple attributes on the users at the same time. You must enable this feature. It is not enabled by default. For more information, see “[Configuring the Help Desk Module](#)” in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 943679)

1.2.4 Added the Ability to Send a Notifications to Users about Passwords Expiring

With this release, Self Service Password Reset has the ability to send passwords to users warning them that their passwords are about to expire. For more information, see “[Sending Email Warnings about Passwords that Are to Expire](#)” in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 1045437)

1.2.5 REST Enhancements

With this release, Self Service Password Reset contains enhancements for its REST calls and the REST documentation. (Bug 1065548, 1083776, 1086120, 1067246, 1084159, 1077797, 906031, 914133)

1.2.6 Contains Enhancements for Validation Tokens

With this release, Self Service Password Reset contains enhancement for tokens customers user for validation. For example:

- ♦ Support for multiple email addresses and SMS addresses
- ♦ Built-in value masking
- ♦ Extensible interface for programmatic control of masking
- ♦ Re-sending of tokens as a standard feature
- ♦ Improve user interface for enrollment and selection of token destination values

This improves the experience for the customers using token validations. (Bug 1031159, 1054167)

1.2.7 User Reports Display Validation Methods

With this release, the report for the users in Self Service Password Reset displays the validation methods that the users have registered. You can view the users reports through the Administration module. For more information, see “[Configuring Data Analysis](#)” in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 1057214)

1.2.8 Added Support for Multiple SMTP Servers

With this release, Self Service Password Reset supports multiple SMTP servers. You can add additional servers if the SMTP server you use is not available for any reason. For more information, see “[Configuring Email Settings](#)” in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 991977)

1.2.9 Default Word List Contains the Challenge-Response Answers

With this release, Self Service Password Reset can add the users' change-response answers to the default word list. There is a new toggle button on the **Random Questions** that allows the option to include the answers in the word list or not to include the answers in the word list.

You must enable this option per locale that you use in your environment. For more information, see “[Configuring a Profile for a Challenge-Response Policy](#)” in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 994665)

1.2.10 Added Support for the Common Event Format in Auditing

With this release, Self Service Password Reset supports the common event format (.cef) files for auditing. This change means that Self Service Password Reset now supports ArchSight as a connected auditing system. (Bug 1045676)

1.2.11 Added Support for a Fail-Over Syslog Server

This release of Self Service Password Reset added support for a fail-over syslog server. In the past, Self Service Password Reset only allowed one syslog server to be configured. Now, you can configure multiple syslog servers to provide fail-over support for the audit events. For more information, see “[Auditing for Self Service Password Reset](#)” in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 1065744)

1.2.12 Added a Password Strength Estimation Option

This release of Self Service Password Reset allows you to not only turn on the strength-o-meter but includes a password strength estimator. To access the new option:

- 1 Log in to Self Service Password Reset at <https://dns-name/sspr> as an administrator.
- 2 In the toolbar click **Configuration Editor**.
- 3 Click **Modules > Authenticated > Change Password**.
- 4 Find the option **Use zxcvbn for Strength Meter Algorithm**, then enable this new option.

(Bug 975706)

1.2.13 Changed the Behavior of the Change Password Fields

With this release, the Change Password fields behavior changed. In the past, if a user typed too fast and hit enter the password change would be canceled. Now, when a user enters the new password, Self Service Password Reset performs a keystroke validation. Plus, the Change Password button is never disabled. (Bug 1052346)

1.2.14 Deprecated Token Send Methods of SMSFIRST, EMAILFIRST, and BOTH

This release deprecates the token send methods of **SMSFIRST**, **EMAILFIRST**, and **BOTH**. These options added complexity to the product that was not needed. (Bug 1052844)

1.2.15 Deprecated JavaScript Option from New User Form Fields

This release deprecates the JavaScript option from the New User form fields. (Bug 1058147)

1.2.16 Advanced Authentication Endpoint Session Timeouts with OAuth2 Configured in the Forgotten Password Module

The release of Advanced Authentication 6.0 contains the fix for the issue where the Advanced Authentication endpoint session timeouts when you have OAuth2 configured in the Forgotten Password module. (Bug 1049204)

1.2.17 Added Trusted Certificates for the SMS Gateway

With this release, there is a new setting for SMS Gateway that allows you to import the trusted certificates that Self Service Password Reset has to the SMS Gateway. For more information, see [“Configuring SMS Notification Settings”](#) in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 1062557)

1.2.18 Ability to Add Additional Entries to the Hosts File for the Appliance

With this release, you can add additional entries to the hosts file for the appliance. You must manually edit the `/etc/opt/novell/base/hosts.appliance` file. For more information, see [“Adding Additional Hosts to the Hosts File”](#) in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 1013863)

1.2.19 New Generic Forgotten Password Policy

With this release, there is new a generic Forgotten Password policy that prevents guessing of a user name in the Forgotten Password module. If an invalid user name is entered, the challenge is still presented to the user but the answers are always wrong. (Bug 980071)

1.2.20 Enhanced HTML Editor for Email Templates

With this release, the Configuration Editor contains a new HTML editor for the email templates. (Bug 1045223)

1.2.21 Added Enhancements for Screen Reader Software

With this release, Self Service Password Reset contains enhancements to make screen reader software work. (Bug 1057414)

1.2.22 OTP Module Contains Profile Settings

With this release, the OTP module contains profile setting like the other Self Service Password Reset modules. This means you can enforce a set of users to use OTP while others users are not required. (Bug 1075456)

1.2.23 Password Policy Maximum Length Increased

With this release, the password policy maximum has increased. The old limit of 100 characters is no longer enforced. This allows for long passwords. (Bug 1081287)

1.2.24 Added a Configurable URL for the Home Page

With this release, you can configure the URL for the Home page to be what you want. The new setting of Home URL is located in the Configuration Editor under **Settings > Application**. For more information, see [“Configuring Application Settings”](#) in the *Self Service Password Reset 4.3 Administration Guide*. (Bug 898313)

1.2.25 Support Option in the Appliance Accepts 12 Digit Service Request Numbers

With this release, the **Support** option in the Self Service Password Reset appliance accepts service request numbers that are 12 digits. (Bug 1072969)

1.2.26 Detailed Error Messaging Enabled During Configuration

With this release, Self Service Password Reset enables detailed error messaging while you run the Configuration Guide. The detailed error messages are left on by default and should be disabled in a production environment. It causes performance issues if you leave the detailed error messaging running. (Bug 1052873)

1.2.27 Updated Error Message in the Forgotten Password Module

With this release, the Forgotten Password module contains an updated error message when users select an authentication method that is not available to them. The message provides details to help the users resolve the issue. (Bug 1068784)

1.2.28 Fixed Help Desk Timeout Issue

With this release, the Help Desk module is honoring the idle timeout setting. (Bug 1085745)

1.2.29 Allow Forgotten Password Unlock Sequence When within Minimum Lifetime Password Window

With this release, Self Service Password Reset allows users that use the Forgotten Password module and have the LDAP intruder password locked and are within the minimum password lifetime of the effective password policy to use the Forgotten Password module to unlock their passwords. The users cannot use the Forgotten Password module to reset their passwords in this use case. No other actions in the Forgotten Password module are allowed.

The new Configuration Editor setting that controls this functionality is located under **Modules > Public > Forgotten Password > Profiles > profile > Options > Minimum Password Lifetime Options**. (Bug 1045859)

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 5.5 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 or later (64-bit)
 - ♦ 12 SP3
 - ♦ 11 SP4
- ♦ Amazon Web Service EC2 SUSE Linux Enterprise Server 12 SP 3
 - ♦ 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 4.3 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 4.3 Installation Guide*.

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

- ♦ [Section 4.1, “The Windows MSI Installs a Different Version Number than the Appliance and WAR File,” on page 8](#)
- ♦ [Section 4.2, “Pressing Enter on Any Input Field Using Internet Explorer 11 Causes the First Button To Be Clicked,” on page 9](#)
- ♦ [Section 4.3, “Unique Attribute Scoping Does Not Work in Update Profile,” on page 9](#)
- ♦ [Section 4.4, “LDAP Entry ID Definition Does Not Work with Multiple Added Values,” on page 9](#)
- ♦ [Section 4.5, “Some Settings Missing Using Internet Explorer 11,” on page 9](#)
- ♦ [Section 4.6, “REST /sspr/public/rest/challenges DELETE Method Fails when Target is the REST User,” on page 9](#)

4.1 The Windows MSI Installs a Different Version Number than the Appliance and WAR File

Due to an issue, the Windows MSI file installs a different version number of Self Service Password Reset than the Appliance and the WAR file.

To view the installed version:

- 1 Log in to the Self Service Password Reset administration console as an administrator.
- 2 In the toolbar, click your name, then click **Administration**.

3 To display the version, click the **About** tab.

- ♦ **Appliance and WAR file version:** 4.3.0.0 b336 r 39490
- ♦ **Windows MSI version:** 4.3.0.0 b337 r39491

4.2 Pressing Enter on Any Input Field Using Internet Explorer 11 Causes the First Button To Be Clicked

Issue: If the users are using Internet Explorer 11 and they have enter information into a input field, when they press Enter, the first button on the pages is clicked. (Bug 1087672)

Solution: Use any browser but Internet Explorer 11. The issue does not occur in Edge, Chrome, or Firefox.

4.3 Unique Attribute Scoping Does Not Work in Update Profile

With this release, the Unique Attribute does not work in the Update Profile module. There is no work around at this time. The bug will be fixed in a future release. (Bug 1089446)

4.4 LDAP Entry ID Definition Does Not Work with Multiple Added Values

With this release, when you add multiple rows in the LDAP Entry ID Definition for New User Registration, SSPR only uses the top row in the LDAP ID Definition. There is no workaround at this time. The bug will be fixed in a future release. (Bug 1089739)

4.5 Some Settings Missing Using Internet Explorer 11

Issue: With this release, when accessing the Configuration Editor or Configuration Manager sometimes not all of the settings appear. Labels and panels in the UI are missing. (Bug 1089590)

Workaround: Refresh the page and the settings appear.

4.6 REST /sspr/public/rest/challenges DELETE Method Fails when Target is the REST User

Issue: With this release, the /sspr/public/rest/challenges DELETE Method fails with an error of 5013 ERROR_MISSING_PARAMETER. (Bug 1087344)

Workaround: You must specify a username as a parameter for this REST method to work.

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) (<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.

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/>.

Copyright © 2018 NetIQ Corporation. All Rights Reserved.