

NetIQ Self Service Password Reset 4.5 Release Notes

February 2020

NetIQ Self Service Password Reset 4.5 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.

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

What’s New?

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

- ♦ “Security Improvements” on page 2
- ♦ “Enhancements” on page 2
- ♦ “Software Fixes” on page 4

Security Improvements

This release includes the following security improvements:

- ♦ [“Base Operating System Update in Appliance” on page 2](#)
- ♦ [“Updated Angular JS Libraries” on page 2](#)
- ♦ [“Updated Versions of Java and Apache Tomcat” on page 2](#)

Base Operating System Update in Appliance

With this release, the SSPR appliance base operating system has been updated to SUSE Linux Enterprise Server 12 Service Pack 4.

Updated Angular JS Libraries

With this release, the Angular JS libraries have been updated to address some security issues.

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 - 11.0.5_10

Apache Tomcat: 9.0.30

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 4.5 Installation Guide*.

Enhancements

This release includes the following software enhancements:

- ♦ [“Provision to Calculate Password Strength Using the Entropy Calculator” on page 2](#)
- ♦ [“Support to Display the Distinguished Name in the Manager Attribute of Help Desk Profile” on page 3](#)
- ♦ [“Ability to Send SMS Notifications to Users for Change Password and Update Profile” on page 3](#)
- ♦ [“Ability to Log the User ID for the Password Reset Event Done Through OTP” on page 3](#)
- ♦ [“Provision to Customize the CEF Messages” on page 3](#)
- ♦ [“Enhanced Password Recovery Event Log” on page 3](#)
- ♦ [“Provision to Enable Breach Database Check” on page 3](#)

Provision to Calculate Password Strength Using the Entropy Calculator

Self-Service Password Reset evaluates the strength or entropy of a password based on its length and the number of characters it contains. You can use Nist - Entropy calculator as the Strength meter algorithm to determine strength of password on the Change Password screen.

When a user changes the password, the entropy calculator evaluates the strength of specified password. The evaluated strength is used to automatically apply specific password policy defined in eDirectory and determine the expiration date of the password mapped to a specific user account.

NOTE: Currently, localization is not supported for the Entropy Calculator interface.

For more information, see [Calculating Password Strength Using the Entropy Calculator](#) in the *Self Service Password Reset 4.5 Administration Guide*.

Support to Display the Distinguished Name in the Manager Attribute of Help Desk Profile

With this release, Self Service Password Reset allows you to display the Distinguished Name (DN) of a Manager in the Help Desk > Profile tab. To achieve this, manager attribute must be set to **userDN** in **Configuration Editor > Modules > Authenticated > Help Desk > Profiles > default > Details**.

To display more than one manager who has been mapped to a specific user, enable **MutiValue** for the manager attribute.

Ability to Send SMS Notifications to Users for Change Password and Update Profile

Self Service Password Reset introduces Change Password SMS Text and Update Profile SMS Text to customize SMS notification text sent to users when users update their profile or change password. SMS is delivered to users using the configured SMS Gateway. For more information, see [Configuring the SMS Messages](#) in the *Self Service Password Reset 4.5 Administration Guide*.

Ability to Log the User ID for the Password Reset Event Done Through OTP

With this release, Self Service Password Reset saves the user ID in the log for the password reset event with OTP. The password reset with OTP event log is displayed in the following format:

INFO, forgottenpw.ForgottenPasswordServlet, {506} checking entered OTP for <user dn>

Provision to Customize the CEF Messages

With this release, Self Service Password Reset allows you to customize the default CEF messages with additional parameters for any event. For more information, see [CEF Audits and Customization](#) in the *Self Service Password Reset 4.5 Administration Guide*.

NOTE: To customize the fields in the CEF message, we recommend you to contact the SSPR Support team for assistance.

Enhanced Password Recovery Event Log

With this release, the log captures the method used in the Password Recovery process. A new parameter Methods used ["<method used for password recovery>"] is included in the Password Recovery event log.

For example, if a user uses Email OTP method for recovering password then log captures as follows:

Methods used ["Email OTP"]

Provision to Enable Breach Database Check

Self Service Password Reset introduces **Enable Breach Database Check** to generate unique and secure passwords that are passed through the breach check to ensure that it is not a compromised password.

Software Fixes

This release includes the following software fixes:

- ♦ [“No Intruder E-mail Notification Is Sent for Failed Login Attempts” on page 4](#)
- ♦ [“An Invalid Request Displays the Server-Specific Details in the Error Message” on page 4](#)
- ♦ [“A User Login Fails After Configuring reCaptcha Version 3” on page 4](#)

No Intruder E-mail Notification Is Sent for Failed Login Attempts

This release resolves the issue when a user provides an incorrect login password more than the **Maximum login attempts**, the user account gets temporarily blocked. However, the intruder email notification is not sent to the user. *(Bug 1161444)*

An Invalid Request Displays the Server-Specific Details in the Error Message

This release resolves the issue where sending an invalid request returns the server specific details in the error message. Now, the server specific details are suppressed in the error message. *(Bug 1148162)*

A User Login Fails After Configuring reCaptcha Version 3

This release resolves the issue when users try to log in to SSPR after configuring the reCaptcha version 3, an error message ERROR for site owner: Invalid key type is displayed. This message appears before user specifies the credentials. *(Bug 1160696)*

Now, while configuration reCaptcha administrator must set the **reCAPTCHA Mode** to **reCaptcha version 3 - Invisible** in **Configuration Editor > Settings > Captcha**.

System Requirements

This release 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, 12 SP4, and 12 SP5 (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 4.5 Installation Guide*.

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 4.5 Installation Guide*.

Self Service Password Reset 4.4 or later contains a schema change for password notifications of expired emails. 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](#) in the “[Self Service Password Reset 4.5 Administration 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 4.5 Installation Guide*.

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 Click the **About** tab, then verify that the **SSPR version** is v4.5.0.0 b51 r7db460d8.

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).

- ♦ “[Issue with Password Entropy](#)” on page 6
- ♦ “[Delay in Random Pass-Phrase Generation](#)” on page 6
- ♦ “[Configuration Summary Is Not Displayed After the Appliance Installation](#)” on page 6

Issue with Password Entropy

The Password Entropy feature does not work as expected under the following configurations:

- ♦ If the **Password Policy Source** is set to **Local** in **Configuration Editor > Settings > Password Settings**.
- ♦ When the Random pass phrase generation window does not generate pass phrases based on the configured policy on the **Change Password** screen.

NOTE: You can use the Password Entropy functionality with any strength meter algorithms. However, it is tested and recommended to use it with the Nist - Entropy calculator. With other algorithms, it might not provide the required results.

Delay in Random Pass-Phrase Generation

If you experience a delay in random passphrase generation, disable the **Check Breach Database for Auto Generated Randoms** option in **Configuration Editor > Modules > Authenticated > Change Password**.

Configuration Summary Is Not Displayed After the Appliance Installation

After installing the SSPR 4.5 appliance, the configuration message summary with the AMC URLs is not displayed in the VM console.

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.

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 <http://www.microfocus.com/about/legal/>.

Copyright © 2020 NetIQ Corporation. All Rights Reserved.

