

Self Service Password Reset 4.1 Release Notes

January 2017



Self Service Password Reset 4.1 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 \(https://forums.novell.com/forumdisplay.php/1343-Self-Service-Password-Reset\)](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 \(https://www.netiq.com/documentation/self-service-password-reset/\)](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 5](#)
- ◆ [Section 3, "Installing or Upgrading Self Service Password Reset," on page 6](#)
- ◆ [Section 4, "Known Issues," on page 6](#)
- ◆ [Section 5, "Contact Information," on page 8](#)
- ◆ [Section 6, "Legal Notice," on page 8](#)

1 What's New?

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

- ◆ [Section 1.1, "New Delete My Account Module," on page 1](#)
- ◆ [Section 1.2, "New Integration with Advanced Authentication," on page 2](#)
- ◆ [Section 1.3, "Added OAuth as a Forgotten Password Identification Method," on page 2](#)
- ◆ [Section 1.4, "Updated the Look and Functionality of the People Search Module," on page 2](#)
- ◆ [Section 1.5, "Security Improvements," on page 2](#)
- ◆ [Section 1.6, "Enhancements and Software Fixes," on page 3](#)

1.1 New Delete My Account Module

Self Service Password Reset 4.1 contains a new **Delete My Account** module that appears on the user home page, after the user authenticates to Self Service Password Reset. This module allows users and help desk administrators to delete user accounts. For more information, see "[Configuring the Delete Account Module](#)" in the *Self Service Password Reset 4.1 Administration Guide*. (Bug 935829)

1.2 New Integration with Advanced Authentication

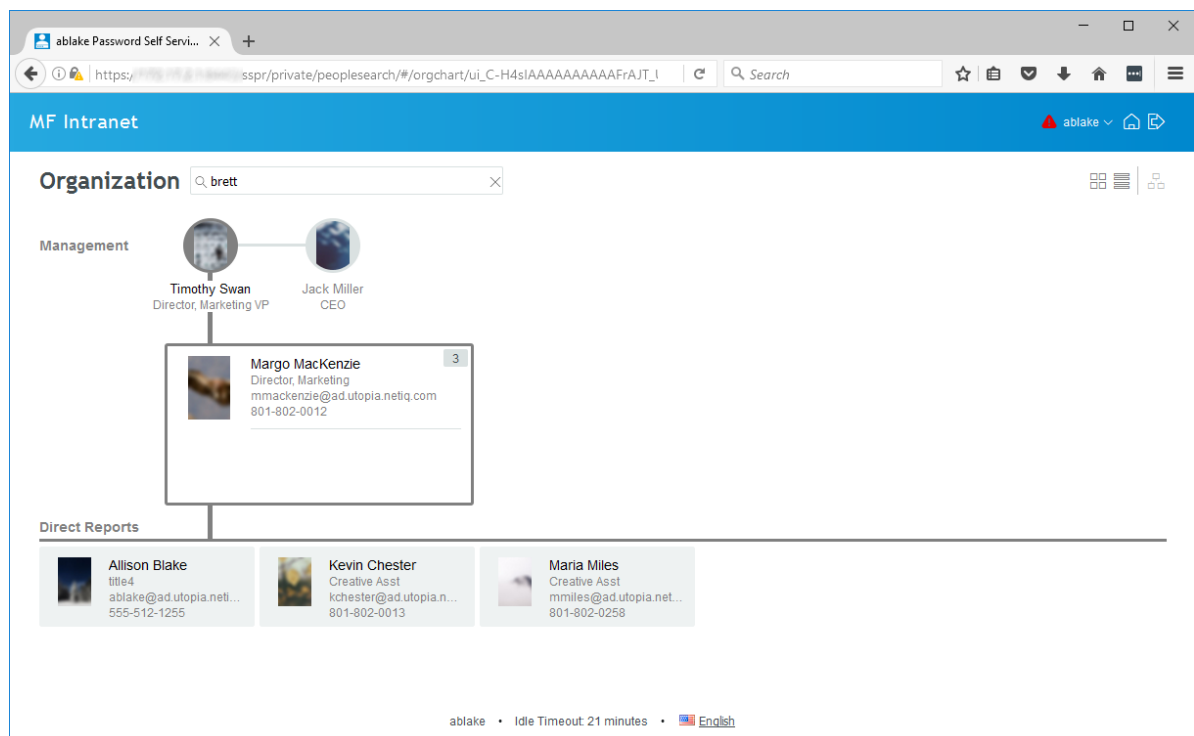
Self Service Password Reset 4.1 integrates with Advanced Authentication through an OAuth2 connection. This is a new integration method for this release. If you have integrated Self Service Password Reset with Advanced Authentication in the past, that configuration is still valid. The old options have been deprecated. For more information, see [“Integrating Self Service Password Reset with Advanced Authentication”](#) in the *Self Service Password Reset 4.1 Administration Guide*. (Bug 983595, 983598, 986288)

1.3 Added OAuth as a Forgotten Password Identification Method

Self Service Password Reset 4.1 contains a new identification method of OAuth2. It uses this new method to integrate with Advanced Authentication, Identity Manager, and any other application that supports OAuth 2. For more information, see [“Configuring the OAuth2 Verification Method for the Forgotten Password Module”](#) in the *Self Service Password Reset 4.1 Administration Guide*. (Bug 983595)

1.4 Updated the Look and Functionality of the People Search Module

The People Search module in Self Service Password Reset contains new functionality and a new look. It now contains an organizational chart display or you can see the users in a table. If you use the table view, you can order the information by clicking on the column. Plus, users can now click on mobile phone numbers to make calls. (Bug 1003958, 1001233)



1.5 Security Improvements

Self Service Password Reset includes the following security improvements:

- ♦ [Section 1.5.1, “Removed Custom Embedded Stylesheet and Mobile Stylesheet,”](#) on page 3
- ♦ [Section 1.5.2, “Integrated CAPTCHA on the Same Page as the Data Form,”](#) on page 3

1.5.1 Removed Custom Embedded Stylesheet and Mobile Stylesheet

Self Service Password Reset 4.1 removes two options from the **Look & Feel** settings. The two options are:

- ◆ [Settings > User Interface > Look & Feel > Custom CSS Stylesheet Location](#)
- ◆ [Settings > User Interface > Look & Feel > Custom Mobile CSS Stylesheet Location](#)

NetIQ removed these options for security consideration. This option would allow you to reference an off-site script that could cause security issue with Self Service Password Reset.

Self Service Password Reset provides an embedded stylesheet and a mobile stylesheet for you to use, or to create a custom bundle. For more information, see [“Customizing the Branding of Self Service Password Reset”](#) in the *Self Service Password Reset 4.1 Administration Guide*. (Bug 1015611, 1004859)

1.5.2 Integrated CAPTCHA on the Same Page as the Data Form

In the past, Self Service Password Reset displayed the CAPTCHA form on a stand-alone page that was separate from the login page, the Forgotten Password forms, and other pages. Self Service Password Reset 4.1 now incorporates CAPTCHA with this pages and the separate page does not appear.

This change was made for security reasons as well as to simply the user experience. (Bug 1011910)

1.6 Enhancements and Software Fixes

Self Service Password Reset 4.1 includes the following software enhancements and fixes for this release:

- ◆ [Section 1.6.1, “Information for Upgrading the Appliance,” on page 4](#)
- ◆ [Section 1.6.2, “Enable CAPTCHA after a Certain Number of Failed Logins,” on page 4](#)
- ◆ [Section 1.6.3, “Health Screen in the Configuration Manager Displays Additional Information,” on page 4](#)
- ◆ [Section 1.6.4, “Configuration Manager Displays Certificate Information,” on page 4](#)
- ◆ [Section 1.6.5, “Changes to the Scope of the User Reports,” on page 4](#)
- ◆ [Section 1.6.6, “Customize the Forgotten Password Verification Method Labels and Descriptions,” on page 4](#)
- ◆ [Section 1.6.7, “Account Information Module Displays LDAP Attributes,” on page 4](#)
- ◆ [Section 1.6.8, “Public Pages Contain Appropriate Timeout Messages,” on page 5](#)
- ◆ [Section 1.6.9, “Mobile Enrollment Page Contains No Cancel Button,” on page 5](#)
- ◆ [Section 1.6.10, “Users See a Failure Message when Checking the Mobile Code,” on page 5](#)
- ◆ [Section 1.6.11, “Self Service Password Reset Sends No Emails to Users,” on page 5](#)
- ◆ [Section 1.6.12, “Blank Screen on the Appliance after Configuring the Network Information,” on page 5](#)

1.6.1 Information for Upgrading the Appliance

The appliance was introduced with the Self Service Password Reset 4.0 release. NetIQ created the framework that will allow you to simply upgrade the appliance in future releases. However, there is a supported procedure of how to upgrade the appliance until the Product Upgrade options works in the appliance management console. For more information, see “[Upgrading the Self Service Password Reset Appliance](#)” in the *Self Service Password Reset 4.1 Installation Guide*. (Bug 957506)

1.6.2 Enable CAPTCHA after a Certain Number of Failed Logins

Self Service Password Reset 4.1 allows you to configure CAPTCHA to appear to users after x amount of failed login attempts. For more information, see “[Configuring CAPTCHA](#)” in the *Integrating Self Service Password Reset with Advanced Authentication*. (Bug 995688)

1.6.3 Health Screen in the Configuration Manager Displays Additional Information

Self Service Password Reset 4.1 now displays the health and configuration status of the appliance. It also displays a health check status if the minimum number of required character groups is higher than the total groups available. If you happen to configure Self Service Password Reset this way, no password are valid at any time. (Bugs 941499, and 992664). For more information, see “[Working with the Configuration Manager](#)” in the *Self Service Password Reset 4.1 Administration Guide*.

1.6.4 Configuration Manager Displays Certificate Information

Self Service Password Reset 4.1 now displays a summary of the imported certificates in the Configuration Manager. The Configuration Manager shows if your certificates are expired and must be updated. For more information, see “[Working with the Configuration Manager](#)” in the *Self Service Password Reset 4.1 Administration Guide*. (Bug 955291)

1.6.5 Changes to the Scope of the User Reports

Self Service Password Reset 4.1 contains an updated Data Viewer table. When you download the table as CSV, the report contains the columns you selected. For more information, see “[Configuring Reporting](#)” in the *Self Service Password Reset 4.1 Administration Guide* (Bug 984188)

1.6.6 Customize the Forgotten Password Verification Method Labels and Descriptions

Self Service Password Reset 4.1 allows you to customize the label and description of the Forgotten Password verification methods. You can change this options through the **Display Text** options in the Configuration Editor. For more information, see “[Customizing the Text of Self Service Password Reset](#)” in the *Self Service Password Reset 4.1 Administration Guide*. (Bug 977839)

1.6.7 Account Information Module Displays LDAP Attributes

Self Service Password Reset 4.1 allows the Account Information module to display LDAP attributes to the users on the My Account tile. You must configure the Account Information module to display the attributes to the users. For more information, see “[Configuring the Account Information Module](#)” in the *Self Service Password Reset 4.1 Administration Guide*. (Bug 977708)

1.6.8 Public Pages Contain Appropriate Timeout Messages

Self Service Password Reset allows you to configure timeouts for public modules and pages. In the past, if a user was on one of these pages and the timeout occurred, they would see a message stating `You have been signed out, but they were never signed in to Self Service Password Reset.` The message now states `Inactive Timeout Your session has timed out due to inactivity.` (Bug 987241)

1.6.9 Mobile Enrollment Page Contains No Cancel Button

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

1.6.10 Users See a Failure Message when Checking the Mobile Code

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) Self Service Password Reset 4.0.0.1 resolved this issue. The fix is now included in Self Service Password Reset 4.1.

1.6.11 Self Service Password Reset Sends No Emails to Users

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) Self Service Password Reset 4.1 resolves this issue.

1.6.12 Blank Screen on the Appliance after Configuring the Network Information

After you have configured the network information for the appliance, the console screen is completely blank. (Bug 987433) Self Service Password Reset 4.0.0.1 resolved this issue. The fix is now included in Self Service Password Reset 4.1.

2 System Requirements

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

- ♦ Red Hat Enterprise Linux Server 7.3 or later (64-bit)
- ♦ SUSE Linux Enterprise Server 12 SP 2 or later (64-bit)
- ♦ SUSE Linux Enterprise Server 11 SP 4 (64-bit)
- ♦ Windows Server 2012 R2 (64-bit)

Self Service Password Reset is also available as an appliance since the 4.0 release. The appliance runs on the following virtual systems:

- ♦ Hyper-V 4.0 and 3.0
- ♦ VMware 5.5 or later

Self Service Password Reset also supports the Edge browser in this release.

For detailed information on system requirements, supported operating systems, and browsers, see “[Installing Self Service Password Reset](#)” in the *Self Service Password Reset 4.1 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 4.1 Installation 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 4.1 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, “Public Access People Search Page Icons are Distorted,” on page 6](#)
- ◆ [Section 4.2, “Enable Showing Masked Fields Setting Does Not Accept Chinese Characters,” on page 6](#)
- ◆ [Section 4.3, “Cancel Button on the Setup Security Questions Page Does Not Work,” on page 6](#)
- ◆ [Section 4.4, “Clicking Cancel While Updating the Profile Returns Error 5043,” on page 7](#)
- ◆ [Section 4.5, “Using LDAP as the Toke Storage Method While Sending New User Email Verifications Returns Error 5203,” on page 7](#)
- ◆ [Section 4.6, “Incorrect Site URL Value Can Cause Form Updates to Fail and Repeat,” on page 7](#)
- ◆ [Section 4.7, “Self Service Password Reset is Not Executing HTML Tags for Error Codes and Display Strings,” on page 7](#)
- ◆ [Section 4.8, “Redirection to the Forward URL Does Not Occur when Integrated with the Identity Applications,” on page 7](#)
- ◆ [Section 4.9, “Forgotten Password Module Error after Upgrading from Self Service Password Reset 3.2 or Prior Versions,” on page 8](#)

4.1 Public Access People Search Page Icons are Distorted

Issue: If you enable the People Search module and allow public access, the icons on the public People Search page are distorted. (Bug 1018946)

Workaround: There is no workaround at this time.

4.2 Enable Showing Masked Fields Setting Does Not Accept Chinese Characters

Issue: If you have are using the Chinese locale (ch-tw) and you have enabled the **Enable Showing Masked Fields** setting, the fields only accept answers in English, not Chinese. (Bug 987653)

Workaround: There is no workaround at this time.

4.3 Cancel Button on the Setup Security Questions Page Does Not Work

Issue: The **Cancel** button on the Setup Security Questions page does not work. Users should be filling out the answers to proceed. (Bug 1018430)

Workaround: There is no workaround at this time.

4.4 Clicking Cancel While Updating the Profile Returns Error 5043

Issue: When user is updating their profile and they are on the form to enter the code, if they click cancel instead of entering the code it returns a 5043 error. (Bug 1019639)

Workaround: There is no work around at this time.

4.5 Using LDAP as the Token Storage Method While Sending New User Email Verifications Returns Error 5203

Issue: If you have enabled Self Service Password Reset to send a verification email to new users through the New User Registration module and changed the Token Storage Method to be LDAP, when a new user fills in the details for the new user information and click Continue, Self Service Password Reset returns error 5203. (Bug 1012170)

Workaround: Do not use LDAP as the storage method for the Token Storage Method option.

4.6 Incorrect Site URL Value Can Cause Form Updates to Fail and Repeat

Issue: If the setting **Site URL** contains an incorrect value, it can cause form updates to fail and repeat. The setting is located in the Configuration Editor, under **Settings > Application > Application > Site URL**. (Bug 1020196)

Workaround: A workaround for this issue is to change both settings for session management from **Encrypted Cookie** (default value) to **Local**. The settings are found in the Configuration Editor here: **Settings > Application > Application > Session Management**. The settings to change are **Login Session Mode** and **Module Session Mode**.

4.7 Self Service Password Reset is Not Executing HTML Tags for Error Codes and Display Strings

Issue: After changing error strings or display string in Self Service Password Reset to contain HTML tags or variables, it displays the variables and the HTML tags instead of the output of the HTML tags and variables. (Bug 10199924)

Workaround: There is no workaround at this time.

4.8 Redirection to the Forward URL Does Not Occur when Integrated with the Identity Applications

Issue: When you integrated Self Service Password Reset with the Identity Applications from Identity Manager and a user cancels out of the Change My Password process, Self Service Password Reset redirects the user to `http://ipaddress/sspr/private` instead of to the Identity Manager landing page at `http://ipaddress/landing`. (Bug 1019310)

Workaround: There is no workaround at this time.

4.9 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.**

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 © 2017 NetIQ Corporation. All Rights Reserved.