

NetIQ Self Service Password Reset 4.7 Patch Update 2 Release Notes

January 2024

NetIQ Self Service Password Reset 4.7 Patch Update 2 includes several enhancements and software fixes.

The enhancement is 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 our products meet all your needs. You can post feedback in the [NetIQ Self Service Password Reset forum](#) on OpenText 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. 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 on the [NetIQ Self Service Password Reset Documentation \(https://www.netiq.com/documentation/self-service-password-reset-47/\)](https://www.netiq.com/documentation/self-service-password-reset-47/) page. To download this product, see the [Software Licenses and Downloads \(SLD\) \(https://sldlogin.microfocus.com/nidp/idff/sso?id=5&sid=0&option=credential&sid=0\)](https://sldlogin.microfocus.com/nidp/idff/sso?id=5&sid=0&option=credential&sid=0) website.

NOTE: NetIQ Self Service Password Reset 4.7 Patch 1 was shipped exclusively with IDM as a Managed Service (not as a standalone release).

- ♦ [“What’s New” on page 1](#)
- ♦ [“Resolved Issues” on page 2](#)
- ♦ [“Known Issue” on page 3](#)
- ♦ [“Planned End of Support” on page 4](#)
- ♦ [“Upgrade” on page 4](#)
- ♦ [“Contact Information” on page 5](#)
- ♦ [“Legal Notice” on page 5](#)

What’s New

Self Service Password Reset 4.7 Patch Update 2 provides the following:

- ♦ [“Enhancement” on page 2](#)
- ♦ [“Security Improvements” on page 2](#)

Enhancement

This release includes the following enhancement:

Enhanced Check Password API

In this release, the Check Password API is enhanced to enable proxy users or administrators to verify a specified password for the user against their current password and the password history related policies defined in the eDirectory.

If the specified password matches the current password or falls within the password history defined in the eDirectory, the proxy user checking the password through check password API will be notified that the specified password is not permissible.

To enable this functionality:

- ♦ If you are a proxy user, then you must have the **Allow the following to retrieve passwords** rights under the **eDirectory password policy > Password > Configuration Options** in the eDirectory.
- ♦ If you are an administrator, then you must have the **Allow admin to retrieve passwords** rights under the **eDirectory password policy > Password > Configuration Options** in the eDirectory.
- ♦ The **Read User Passwords** option must be enabled under **Settings > LDAP > LDAP Settings > NetIQ eDirectory > eDirectory Settings**.

Security Improvements

NetIQ Self Service Password Reset 4.7 Patch Update 2 includes the following security improvement:

- ♦ Red Hat Package Manager (RPM) packages version has been upgraded to enhance the security.
- ♦ The **Change Password** module, **People Search** module, and User enumeration are updated to address some security issues. We strongly recommend upgrading to the latest version of SSPR for enhanced security.

Resolved Issues

This release includes the following software fixes:

Component	Description
Administration Page	The failed login attempts through API are recorded only in the DEBUG logs and are not included in the Info logs within the SSPR logs.
Administration Page	The People Search module randomly fails to load, due to the extensive list of people.
Administration Page	In a clustered eDirectory environment, when the administrator disables the Enable Setup Responses option under Setup Security Questions, the User Debug tool fails to load the user information for the administrator. As a result, the administrator gets logged out and the following error is displayed in the logs: 5015 ERROR_INTERNAL

Component	Description
New User Registration	When a user initiates the New User Registration process, the Self Service Password Reset fails to send the token through email to the user's email address for confirmation. This happens because the SMTP server is adding the prefix to the user's email address, and the Self Service Password Reset is unable to disregard this prefix. Now, Self Service Password Reset disregards the prefix and considers only email addresses.
Administration Page	After the Online Upgrade of the Self Service Password Reset, the docker engine fails to start.
Helpdesk Page and Forgotten Password	When a Helpdesk user changes the user's password, or the user resets the password using the Forgotten Password option, the user does not receive a new password through SMS. Now, if the phone number in the SMS Destination Address LDAP Attribute is missing, then Self Service Password Reset checks the phone number in the Secondary SMS Destination Address LDAP Attribute and Tertiary SMS Destination Address LDAP Attribute to send the new password through SMS.
Administration Page	When an administrator tries to gracefully stop the SSPR docker container in the IDM environment using the <code>docker stop sspr-container</code> command, the container does not stop gracefully and exits with the below status: Exited (137)

Known Issue

Self Service Password Reset 4.7 Patch Update 2 includes the following known issue:

An Error While Upgrading the Self Service Password Reset Appliance to 4.7 Version

Issue: While upgrading the SSPR appliance to 4.7 version, the below error is displayed:

The Update process has reported a warning or error. Review the returned text below:

Workaround: This issue might occur due to the `xorg-x11` rpm package.

To check whether the `xorg-x11` rpm package is the cause of issue, run the below command in the terminal and try to upgrade from the user interface:

```
tail -f /var/log/zypper.log
```

If the above rpm package is causing the issue, then perform the below steps to resolve this issue:

- 1 Run the following command:

```
zypper -n remove xorg-x11-server-{version that is causing issue}
```

NOTE: While removing the xorg-x11 rpm package, the yast2-vabase-vainit package is being removed automatically.

- 2 Run the command to install the latest version of this rpm package:

```
zypper -n install xorg-x11-server-*
```

- 3 Add the removed package by using the below command:

```
zypper in yast2-vabase-vainit
```

- 4 Make sure to select the below solution always:

Solution 2: break yast2-vabase-vainit-15.1.2-33.1.noarch by ignoring some of its dependencies.

Planned End of Support

Hyper-V will be deprecated in the next release of Self Service Password Reset. For more information, see [Installation Procedure](#) in the [Self Service Password Reset 4.7 Installation Guide](#).

Upgrade

To upgrade Self Service Password Reset, see [Upgrading or Migrating Self Service Password Reset](#) in the [Self Service Password Reset 4.7 Installation Guide](#).

Self Service Password Reset Appliance Upgrade Considerations

You cannot directly upgrade the appliance from version 4.5 or earlier to version 4.7. You must first upgrade to version 4.6, which must occur via the appliance administration console (:9443). The suggested upgrade order from version 4.5 to version 4.6 is as follows:

- ◆ Upgrade SSPR 4.5 to its respective latest patch using Online Upgrade option in the appliance management console.
- ◆ Upgrade SSPR 4.5 latest patch to SSPR 4.6.0 using Product Upgrade option.
- ◆ Upgrade SSPR 4.6.0 to its respective latest patch using Online Upgrade option.
- ◆ Upgrade SSPR 4.6 latest patch to SSPR 4.7 using Product Upgrade option.
- ◆ Reboot the appliance based on the prompt.

Self Service Password Reset WAR File Upgrade Considerations

Before upgrading your Self Service Password Reset WAR file to 4.7, ensure that the environment complies with the new Java and Tomcat requirements. For more information, see [Deployment Requirements for Self Service Password Reset WAR File on Linux](#).

Contact Information

For specific product issues, contact Open Text Support at <https://www.microfocus.com/support-and-services/>.

Additional technical information or advice is available from several sources:

- ♦ General corporate and product information: [NetIQ Corporate Website \(https://www.microfocus.com/en-us/cyberres/identity-access-management\)](https://www.microfocus.com/en-us/cyberres/identity-access-management)
- ♦ The Open Text Community pages: <https://www.microfocus.com/communities/>

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.microfocus.com/about/legal/>.

© Copyright 2024 Open Text.

