

NetIQ Self Service Password Reset 4.7 Release Notes

July 2023

NetIQ Self Service Password Reset 4.7 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 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. 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.

- ♦ “What is New” on page 1
- ♦ “Resolved Issues” on page 3
- ♦ “Known Issue” on page 4
- ♦ “Planned End of Support” on page 5
- ♦ “Upgrade” on page 5
- ♦ “Contact Information” on page 5
- ♦ “Legal Notice” on page 6

What is New

Self Service Password Reset 4.7 provides the following:

- ♦ “New Feature” on page 1
- ♦ “Enhancement” on page 2
- ♦ “Security Improvements” on page 3

New Feature

This release includes the following feature:

New API For Password Policy

In this release, Self Service Password Reset introduces a new API to check the password policy configured for a user. When the users want to set or change their password, they can use the Password Policy API to display the password policies from thick clients or custom applications.

The Password Policy API ensures that passwords are strong and secure enough to protect the user accounts.

The Password Policy API also provides the ability to retrieve password policies for users belonging to multiple domains with the same username. To retrieve the password policy for users in a specific domain using the Password Policy API, you must include the domain name as a parameter in your API URL.

NOTE: To use this API:

- ♦ Enable the **Web Services** option in **Settings > Web Services > REST Services**.
 - ♦ Specify the LDAP filter to search for users with permission to authenticate using the REST web services. Navigate to **Settings > Web Services > REST Services > Web Services LDAP Authentication Permissions**.
 - ♦ Specify the LDAP filter to search for users with permission to authenticate using the REST web services and use the username as the parameter to specify in the third-party REST client. Navigate to **Settings > Web Services > REST Services > Web Services LDAP Third Party Permissions**.
-

The following are the types of configured password policies:

- ♦ Only Self Service Password Reset password policy
- ♦ LDAP password policy
- ♦ Merged Self Service Password Reset policy with LDAP password policy

For more information on how to configure the password policy, see [Configuring Password Policies](#) in [Self Service Password Reset 4.7 Administration Guide](#).

Enhancement

This release includes the following enhancements:

Support for Web Accessibility

This release improves the accessibility for the following pages:

- ♦ Login
- ♦ Home
- ♦ Change Password
- ♦ My Account

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 deployment.

Java: Eclipse Temurin-11.0.19+7

Apache Tomcat: 9.0.75

You must install the required versions of Java and Apache Tomcat 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 System Requirements](#) guide.

IMPORTANT: Upgrading to Apache Tomcat 9.0.75 requires a Java 11 environment. Ensure to first update your Java environment to version 11, then install Apache Tomcat 9.0.75.

Ability to Choose the OAuth HTTP Service Method Type

This release introduces the **OAuth Profile/UserInfo Service Method Type** configuration setting that allows an administrator to select the HTTP method. This HTTP method invokes the Identity server web service URL that returns user-related attribute data for the **Single Sign On (SSO)** and **Forgotten Password** modules.

For more information, see [Configuring OAuth Single Sign-On](#) in [Self Service Password Reset 4.7 Administration Guide](#).

Random Password API provides Multi-Domain Support

In this release, the Random Password API provides the ability to generate random passwords for users who belong to multiple domains with the same username. Users can now generate random passwords based on the password policies configured for each specific domain. This provides security and flexibility for organizations that manage users across different domains with different password requirements.

To generate a random password for a user in a specific domain using the Random Password API, you must include the domain name as a parameter in your API URL. This ensures that the generated password complies with the password policy set for that specific domain.

Added Localization Support for Norwegian Language

With this release, Self Service Password Reset now supports Norwegian language. For a complete list of all supported languages, see [Self Service Password Reset Key Features](#) in the [Self Service Password Reset 4.7 Installation Guide](#).

Security Improvements

Self Service Password Reset 4.7 supports the Active Directory configuration for LDAP server signing.

Resolved Issues

This release includes the following software fixes:

Component	Description
Administration Page	The Wordlist.ShareHistoryManager Localdb event log's age is frequently checked against the configured Maximum Age Localdb Events value. Even if the Wordlist.ShareHistoryManager Localdb event log's age is lesser than the configured value, the SSPR frequently displays the below log description: wordlist.ShareHistoryManager, wordDB reduction operation, status OPEN
Administration Page	When an administrator or Helpdesk administrator attempts to verify the identity of a selected user by using the Token Verification method, enters a token value in the Token field, and presses Enter, the Send Token button is selected instead of the Verify button.
Administration Page	When an administrator changes the SSPR configuration and attempts to save the changes, the SSPR session times out as it takes longer to save the changes. The following error message is displayed: RequestTimeoutError: Timeout exceeded This issue occurs due to the large SSPRConfiguration.xml file.
Single Sign-On	Self Service Password Reset sends an access token in both the header and body in the OAuth code resolve request. This issue occurs because Self Service Password Reset uses the POST method type to make the OAuth userinfo request to the identity provider that uses GET method type.
Forgotten Password	OAuth fails when invoking the Identity Server's OAuth Profile/UserInfo service URL. This is because Self Service Password Reset uses the POST method type to invoke the user data for the Forgotten Password module from an identity server that supports the GET method.

Known Issue

Self Service Password Reset 4.7 includes the following known issue:

Docker Creation Date Does Not Display Appropriately

Appliance Administration Console displays an inappropriate docker creation date.

An Issue with Change Password Module Accessibility

When the user enters the password in the **Current Password** field on the **Change Password** page and presses the Tab key, the **OK** button is clicked instead of Show/Hide eye icon on the page.

Pressing Enter Does Not Close the Error Message

Issue: When a user attempts to log in with invalid credentials, an error message is displayed. To close the message and try again, click OK. However, if the user presses Enter instead of click OK, it does not work.

Workaround: The user needs to press **Tab** followed by **Enter**.

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 Micro Focus 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 Micro Focus 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 2023 Micro Focus or one of its affiliates.