NetIQ Self Service Password Reset 4.6 Patch Update 2 Release Notes

February 2023

NetIQ Self Service Password Reset 4.6 Patch Update 2 includes a new features, enhancements, security vulnerability and a software fix.

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/) page. To download this product, see the NetIQ Downloads (https://dl.netiq.com/index.jsp) website.

- "What's New?" on page 1
- "Security Improvement" on page 3
- "Resolved Issues" on page 4
- "Installing or Upgrading Self Service Password Reset" on page 4
- "Verifying the Installation" on page 5
- "Contact Information" on page 5
- "Legal Notice" on page 5

What's New?

This release includes the following enhancements:

- "Bogus User Policy Supports Email Token Verification Method" on page 2
- "New API for Unlock Account" on page 2
- "Forgotten Password API provides an Option to Unlock the Account" on page 3
- "Added the Ability to Show/Hide the Entered Password" on page 3

Bogus User Policy Supports Email Token Verification Method

In this release, the **Enable Bogus User Policy** in the **Forgotten Password** module now supports the email token verification method.

New API for Unlock Account

In this release, Self Service Password Reset introduces a new API to unlock the user account.

When a user attempts to login with an incorrect password multiple times, the user account gets locked. The user can use the new Unlock API to unlock their account.

This API requires the user to provide certain information such as their username, email address, phone number, or any other configured LDAP search filter in the **Forgotten Password User Search Form** in the Identification stage to confirm their identity.

The API prompts for the verification method after the successful identity verification. Once the user validates the account using one of the configured verification methods, the account gets successfully unlocked, allowing the user to login with the existing password.

NOTE: To use this API, enable **Allow Intruder Unlock** option in the **Modules > Public > Forgotten Password > Profiles > default > Options**.

The following Unlock API configuration in the **Modules > Public > Forgotten Password > Profiles > default > Definition** is supported to the settings listed below:

- Verification Method
- Token Send Method
- Forgotten Password Recovery Mode
- Required LDAP Attributes (New Form Field)

Verification Method

Supports the following verification methods:

- LDAP Attributes
- Challenge/Response Answers
- SMS/Email Token Verification
- OTP (Mobile Device) Verification

Token Send Method

Supports the following methods for sending the token code or a new password to the user:

- Email-Send to the Email address
- SMS- Send via SMS
- User Choice- If both SMS and email address are available, user decides

Forgotten Password Recovery Mode

Supports only below recovery mode:

- Allow user to set password

Required LDAP Attributes (New Form Field)

The user can add the required LDAP attributes for unlock account authentication.

Forgotten Password API provides an Option to Unlock the Account

In this release, the Forgotten Password API provides an action choice to unlock their account by using Unlock API if it has been locked due to intruder activity.

When a user tries to reset their password using the Forgotten Password API and their account is locked, the API prompts the user with two action choices:

- Unlock: Unlock their account using the Unlock Account API
- New Password: Reset Password

If the user selects the **New Password** option, the user can proceed to reset their password using the forgotten password API. However, if users just want to unlock their account without resetting their password they can copy the state ID from the Forgotten Password API, launch the Unlock API, paste the copied State ID in the body, and run the Unlock API to unlock the user's account and allow them to log in again with the existing password.

NOTE: To unlock the account through Forgotten Password API, enable **Allow Intruder Unlock** and **Allow Forgotten Password when Locked** options in the **Modules > Public > Forgotten Password > Profiles > default > Options**.

Added the Ability to Show/Hide the Entered Password

This release adds the hide/show password eye icon to the **Current Password** field on the **Change Password** module.

Security Improvement

NetIQ Self Service Password Reset 4.6 Patch Update 2 includes the following security improvement:

- "Upgraded Docker Container Version" on page 3
- "SSPR Error Messages Display the More Details" on page 3

Upgraded Docker Container Version

In this release, Self Service Password Reset upgrades the docker container operating system version.

SSPR Error Messages Display the More Details

The **Show Detailed Error Messages** option under **Settings > Security > Application Security** is disabled by default.

NOTE:

In the older versions of SSPR, the Show Detailed Error Messages option is set to enable by default.

- If you are upgrading to Self Service Password Reset 4.6.0.2, the **Show Detailed Error Messages** option will not get disabled by default, the administrator must disable the **Show Detailed Error Messages** option manually in the **Settings > Security > Application Security**.
- If the user is installing the SSPR newly, the **Show Detailed Error Messages** option is disabled by default.

Resolved Issues

This release includes the following software fix:

Component	Description
Administration Page	When a user attempts to update the profile, a verification mail will be sent to the user's email address. When a user attempts to verify the email by clicking the verification link that is provided in the email, SSPR redirects the user to the **newuser** page and the following error message is displayed: `SSPR 5003 You are already authenticated.` **NOTE:** The SSPR session is specific to the browser that is being used. If the user copies the email verification link provided in the email manually, it is recommended to paste it into the same browser session in which the user initiated the SSPR process.

Installing or Upgrading Self Service Password Reset

To install Self Service Password Reset, see Installing Self Service Password Reset (https://www.netiq.com/documentation/self-service-password-reset-46/sspr-install/data/b14gnc8o.html) in the *Self Service Password Reset 4.6 Installation Guide*.

To Upgrade Self Service Password Reset, see Upgrading or Migrating Self Service Password Reset (https://www.netiq.com/documentation/self-service-password-reset-46/sspr-install/data/t41oc5qn0l18.html) in the *Self Service Password Reset 4.6 Installation Guide*.

To upgrade to Self Service Password Reset 4.6 Patch Update 2, you need to be on one of the following versions:

- Self Service Password Reset 4.6 Patch Update 1
- Self Service Password Reset 4.6

For more information to upgrade to Self Service Password Reset 4.6 Patch Update 2 from Self Service Password Reset 4.6.x, see Automatically Upgrading Self Service Password Reset (https://www.netiq.com/documentation/self-service-password-reset-46/sspr-install/data/t419d0vbdvv9.html#t43eiris18po).

Verifying the Installation

1. Log in to the Self Service Password Reset administration console as an administrator.
2. In the toolbar, click your name, and then click **Administration**.
3. Click the **About** tab and then verify that **SSPR Version** is the latest one.

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:

- Product documentation, Knowledge Base articles, and videos: https://www.microfocus.com/support-and-services/
- 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/ (https://www.microfocus.com/en-us/legal).

© Copyright 2023 Micro Focus or one of its affiliates.