NetIQ Single Sign-on Release Notes

August 2024

Product Description

NetIQ Single Sign-on is a comprehensive access management solution that provides single sign-on and secure access to web-based applications, cloud applications, and federated business-to-business interactions. This service provides authorized users with adaptive, context-aware secure access to web, API, and cloud applications from anywhere and from any device.

Single Sign-on is an add-on solution for Advanced Authentication. It uses industry standards, such as SAML, OAuth, and OpenID Connect to deliver federated single sign-on and supports multi-factor authentication, access control, and API access.

If you are not the person that placed the purchase order but are an administrator, you must ensure that you have created an account for yourself on the Software Licenses and Downloads (https://sld.microfocus.com) portal. After you have an account, you must ask the person that placed the purchase order to delegate access to you for this unique URL and provide the password included in the email the first time you log in to the Micro Focus SaaS environment. After you configure the authentication service and Single Sign-on, you do not have to use that user account and password.

What's New

NetIQ Single Sign-on 24.3.0 includes several new features 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 Micro Focus community for Advanced Authentication (https://community.microfocus.com/cyberres/netiq-access-management/advancedauthentication/)on Open Text

Forums, our online community that also includes product information, blogs, and links to helpful resources. You can also share your ideas for improving the product in the Ideas Exchange (https://community.microfocus.com/cyberres/netiq-access-management/advancedauthentication/i/advauth).

Account Claiming Application

By default, Single Sign-on does not enable the Account Claiming application. The Account Claiming application allows you to provide a way for users to claiming existing accounts in the identity repository (SCIM database, Active Directory, and so forth). You configure the Account Claiming application through policies to have users provide additional information to validate the accounts. For more information, see "Configuring Account Claiming" in the *NetIQ Single Sign-on Administration Guide*.

Authorization Policies

Single Sign-on contains an authorization service that manages the rule-based authorization policies. You create the authorization policies when you create the applications or edit existing applications. You can also create authorization policies on stand-alone appmarks. For more information, see "Configuring Authorization Policies" in the *NetIQ Single Sign-on Administration Guide*.

Improved the Template Applications

Single Sign-on improved how fast the templates for the Application load by improving how the images in the templates load.

Known Issues

Micro Focus strives to ensure that our products provide quality solutions for your enterprise software needs. If you need assistance with any issue, visit CyberRes Support (https://support.cyberreshelp.com/hc), then select the appropriate product category.

The following issues are currently being researched for Single Sign-on.

Single Sign-on Does Not Support the Web Authentication Branding File

Single Sign-on inherits the custom branding configuration from Advanced Authentication, except for the option **Use Custom Branding File for Web Authentication** and the suboption **Web Authentication Branding File**. Currently, Single Sign-on does not support the **Web Authentication Branding File** that Advanced Authentication supports.

Obtaining Access to the Micro Focus SaaS Environment

If your organization has more than one service configured in the SaaS environment, contact the administrator of these services for an administrative account to be able to configure Single Sign-on and the URL.

If your company has no services configured, Micro Focus sends an email to the person that placed the purchase order for Single Sign-on. If you are the person that placed the purchase order, look for the email from Micro Focus with your unique URL.

If you are not the person that placed the purchase order but are an administrator, you must ensure that you have created an account for yourself on the Software Licenses and Downloads (https://sld.microfocus.com) portal. After you have an account, you must ask the person that placed the purchase order to delegate access to you for this unique URL and provide the password included in the email the first time you log in to the Micro Focus SaaS environment. After you configure the authentication service and Single Sign-on, you do not have to use that user account and password.

Contacting Micro Focus

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, please email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

For specific product issues, contact CyberRes Support (https://support.cyberreshelp.com/hc).

For general corporate and product information, see the Micro Focus Website (https://www.microfocus.com/en-us/home).

For interactive conversations with your peers and Micro Focus experts, become an active member of the Micro Focus Community https://www.microfocus.com/communities/. The Micro Focus online community provides product information, and 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 https:www.microfocus.com/about/legal (https://www.microfocus.com/about/legal)

Copyright 2023-2024 Open Text.

The only warranties for products and services of Open Text and its affiliates and licensors ("Open Text") are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.