

Advanced Authentication as a Service (SaaS) Release Notes 2022

In addition to the existing on-premises and cloud-based deployments, Advanced Authentication is now available in the Software as a Service (SaaS) model. Micro Focus hosts and maintains the Advanced Authentication Servers with their databases. You can use it to secure access to your corporate resources, such as various portals, workstations, and VPN servers.

For more information about Advanced Authentication and its features, see [Introduction to Advanced Authentication](#).

The following are the key differences between SaaS and non-SaaS models:

Feature	Advanced Authentication	Advanced Authentication as a Service
Setup	Installation is required	Installation is not required
Billing	License-based	Subscription-based
Hardware	Must meet the recommended system requirements	Does not require extensive hardware

For the list of other documents related to Advanced Authentication, see the [Advanced Authentication NetIQ Documentation](#) page. For more information about the product and support, see the [Advanced Authentication Product \(https://www.microfocus.com/en-us/cyberres/identity-access-management/advanced-authentication\)](https://www.microfocus.com/en-us/cyberres/identity-access-management/advanced-authentication) website.

If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of the specific page in the HTML version of the documentation posted at the [Advanced Authentication NetIQ Documentation](#) page.

The release number is in the YYYY.M.RELEASE NUMBER format.

2022.3.1 Update

Advanced Authentication as a Service 2022.3.1 includes the following updates:

- ◆ [“Enhancements” on page 2](#)
- ◆ [“Software Fixes” on page 3](#)

Enhancements

Enhancement	Description
An Option to Validate the OTP Methods Manually	<p>This release introduces the following options in the respective OTP methods:</p> <ul style="list-style-type: none">♦ Verify email address: This option is introduced in the Email OTP method and helps to send the verification code to a specified email address. This option allows the users to validate the email address during the manual enrollment. For more information, see Email OTP in the <i>Advanced Authentication - Administration</i> guide.♦ Verify phone number: This option is introduced in the SMS OTP and Voice OTP methods to send the verification code to a specified phone number. This option lets users verify whether the phone number is valid before the manual enrollment. For more information, see SMS OTP and Voice OTP in the <i>Advanced Authentication - Administration</i> guide.
Timeout Options	<p>This release introduces the following options in the Login Options policy:</p> <ul style="list-style-type: none">♦ Logon timeout (seconds): This option allows you to set the maximum duration of the logon session. The user must specify the login credentials within this duration to prevent the session termination.♦ Logon inactivity timeout (seconds): This option allows you to set the maximum inactivity timeout of the logon session, and a user can remain idle within this duration. For more information, see Login Options in the <i>Advanced Authentication - Administration</i> guide.
Renamed FIDO 2.0	<p>In this release, the FIDO 2.0 method is renamed to FIDO2.</p>
Ability to Retrieve the Risk Score	<p>After integrating a product with Advanced Authentication, the administrators can use the following API call to retrieve the Risk Score of an authenticated user after successful authentication:</p> <pre>api/v1/logon/{logon_process_id}/do_logon</pre>
Support for HANIS Face Method	<p>Advanced Authentication provides the Home Affairs National Identification System (HANIS) method that facilitates citizens of South Africa to authenticate using their face that has been enrolled in the National Identification System. During authentication, the Advanced Authentication server forwards the user details to the third-party service provider that is integrated with National Identification System where the validation takes place. The user gets authenticated to the required resource or endpoint based on the validation result.</p> <p>For more information, see HANIS Face in the <i>Advanced Authentication - Administration</i> guide.</p>

Software Fixes

Component	Issue Description
Administration Portal	After the full synchronization of the Cloud Bridge External repository, the following error message is displayed: <code>'NoneType' object has no attribute 'append'</code>
Administration Portal	When eDirectory is configured as the external repository in Advanced Authentication, and the user entries include multiple CN values, then synchronization fails and displays an error message.
Administration Portal	When an administrator tries to change the Cache expiration time in the Cache Options policy, the updated expiration time is not saved, and changes are not applied.
Administration Portal	When the Cloud Bridge Agent is down and the administrator tries to verify the configuration using the Test Configuration button, an invalid message Gateway Timeout is displayed without stating the cause.
Administration Portal	When the full synchronization on the Web server is in progress and if the fast synchronization is initiated on the Master server simultaneously, the full synchronization fails and results in an error.
Enrollment Portal	When a user tries to test the FIDO2 method in the Enrollment portal, the test fails, and the following message is displayed: <code>expected 'status' to be 'string', got: error.</code>

Contact Information

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 detailed contact information, see the [Support Contact Information website](#).

For general corporate and product information, see the [NetIQ Corporate website](#).

For interactive conversations with your peers and NetIQ experts, become an active member of our [community](#). The NetIQ online community provides product information, useful links to helpful resources, blogs, and social media channels.

Legal Notice

© Copyright 2022 Micro Focus or one of its affiliates.

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

For additional information, such as certification-related notices and trademarks, see <https://www.microfocus.com/en-us/legal> (<https://www.microfocus.com/en-us/legal>).

