Risk Service 2.0 Release Notes

September 2020

NetIQ Risk Service protects against high-risk authentication and application access requests. It evaluates the level of risk during each access attempt by using contextual information without influencing the end-user experience. This prevents fraudulent access to secured web resources.

For more information about this release and for the latest release notes, see the Documentation page. If you have suggestions for documentation improvements, click **Comment on this topic** at the top or bottom of the specific page in the HTML version of the documentation posted at the Documentation page.

- "What's New" on page 1
- "Known Issues" on page 2
- "Contacting Micro Focus" on page 2
- "Legal Notice" on page 2

What's New

Risk Service 2.0 includes the following new features and updates:

- "Support for the External Parameters Rule" on page 1
- "Support for Behavioral Analytics Using Micro Focus Interset" on page 2
- "Support for Risk Scores" on page 2

Support for the External Parameters Rule

The **External Parameters Rule** enables you to fetch inputs from external providers to evaluate the risk associated with an access attempt.

For example, if a user is already authenticated with an external authentication provider, Risk Service receives authentication details from that provider, such as the method used for the authentication. Risk Service can use this information for evaluating the risk.

For more information, see "Configuring Risk Rules" in the *Risk Service 2.0 Administration Guide*.

Support for Behavioral Analytics Using Micro Focus Interset

To enable detection of an unknown threat or anomalies, Risk Service integrates with Interset and leverages its User and Entity Behavioral Analytics (UEBA) capability.

Using the organization's data, Interset establishes the normal behavior for the organizational entities and then, using advanced analytics and machine learning, identifies the anomalous behaviors that constitute potential risks such as compromised accounts, insider threats, or other unknown cyber threats.

For more information, see Enabling Behavioral Analytics Using Interset for Access Manager and Enabling Behavioral Analytics Using Interset for Advanced Authentication.

Support for Risk Scores

Risk Service 2.0 introduces risk scores for rules as an advanced setting. The risk score indicates the priority and criticality of the rule.

For example, if you have configured a set of rules in a risk policy. You want one of these rules to be the most important rule. To achieve this, assign that rule a higher risk score compared to other rules. If the rule evaluation is successful, the risk score is set to zero.

If a rule evaluation is not successful, the risk score is set as the value of the rule. If you have configured multiple rules, the total risk score is the sum of risk scores of all the failed rules.

For more information about how to configure the risk score, see "Configuring Advanced Settings for a Risk Policy" in the *Risk Service 2.0 Administration Guide*.

Known Issues

Risk Service 2.0 has no 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 Micro Focus Support (https://www.microfocus.com/support-and-services/), then select the appropriate product category.

Contacting Micro Focus

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 page

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 2020 Micro Focus or one of its affiliates.