

Release Notes

LexisNexis Risk Solutions – Dynamic Decision Platform / ThreatMetrix Nodes

Version 1.4.0
December 2025



TABLE OF CONTENTS

INTRODUCTION	2
QUALIFICATION STATEMENT.....	2
Ping AIC / ForgeRock Identity Cloud.....	2
PingAM / ForgeRock Access Management (On Premise)	2
KNOWN ISSUES	3
CHANGE LIST	3

INTRODUCTION

This document contains the release notes for the LexisNexis ThreatMetrix Nodes marketplace package available upon the PingOne Advanced Identity Cloud (Ping AIC) formerly known as ForgeRock Identity Cloud, as well as Ping Access Management (PingAM) formerly known as ForgeRock Access Management.

QUALIFICATION STATEMENT

Ping AIC / ForgeRock Identity Cloud

LexisNexis ThreatMetrix Nodes are tested on Ping AIC the latest release of software. The nodes are part of the Ping Identity release process and validated on a regular basis.

PingAM / ForgeRock Access Management (On Premise)

This section documents testing performed with LexisNexis ThreatMetrix Nodes. This table captures tested configurations. The intent is to demonstrate backwards compatibility. Newer versions of infrastructure compliant with Ping Identity published system requirements should be supported.

Component	AM 7.3	AM 7.4	AM 8.0
Java	OpenJDK11	OpenJDK11	OpenJDK17
Web Container	Tomcat 9	Tomcat 9	Tomcat 10

Note: The LexisNexis Dynamic Decision Platform ThreatMetrix Nodes version 1.4.0 are only compatible with PingAM / ForgeRock Access Management version 7.3 and later.

KNOWN ISSUES

This following is a complete list of currently known issues:

- There are no known issues at this time

CHANGE LIST

LexisNexis ThreatMetrix Nodes 1.4.0 – December 2025

- Added new configuration option the Unknown Session Action within the Query Node. The new value is “No Action” that will ignore the `unknown_session=yes` in the API Response and then use the `review_status` to make a decision. This allows for the policy to capture the unknown session, or other integrated products in the policy to generate a decision.
- Updated Apache Commons Text library version to address a potential security vulnerability.

LexisNexis ThreatMetrix Nodes 1.3.1 – September 2025

- Fixed a bug when using Shared State option to fetch optional attributes for the Query Node. This is specific to how PingAIC attribute collector nodes inject information into shared state, mainly how the attribute collector injects information into `objectAttributes`.

LexisNexis ThreatMetrix Nodes 1.3.0 – August 2025

- Fixed a bug in the ThreatMetrix Profiler Node to make the Page ID configuration optional. Previously the optional parameter was being required.
- Updated ThreatMetrix Query Node configuration with Base URL parameter replacing the Session Query URI and Attribute Query URI. The Base URL parameter configures the desired domain/region for sending the configured query API.
- Updated ThreatMetrix Query Node to include a parameter that defines where to locate additional query attributes. The parameter is a drop down list with two options, mainly User Directory or Shared State. Once configured, this defines the location for the list of additional query attributes to add to the API Request.
- Updated the ThreatMetrix Update Node to provide capability to send an “`update_review_status`” associated to a risk event, mainly to provide Final Review status of Pass or Fail. The existing “`update_event_tag`” with step-up / challenge retrospective truth data was maintained.
- Updated for most recent PingAM releases.

LexisNexis ThreatMetrix Nodes 1.2.0 – May 2023

- Compatibility with ForgeRock Identity Cloud and available in Marketplace
- Added configuration option to ThreatMetrix Query Node that maps ThreatMetrix attributes to ForgeRock Identity attributes. The interface allows for a rich set of attributes be provided to query APIs.
- Added configuration option in ThreatMetrix Query Node to allow for session-query API or attribute-query API. There are instances where device intelligence and fingerprinting are not required for LexisNexis ThreatMetrix policy products.
- Updated ThreatMetrix Update Node to provide Retrospective Truth Data to query events.
- Added administrative options to define actions/outcomes when ThreatMetrix Profiling fails and the ThreatMetrix Query node reports an “unknown session”. This permits the administrator to define a mapped outcome.
- Added the outcome “Error” to all ThreatMetrix nodes in compliance with ForgeRock integration patterns that were placed in effect with the ForgeRock v7.3.0 release, as well as compliance with the ForgeRock Identity Cloud.

LexisNexis ThreatMetrix Nodes 1.1.0 – October 2020

- Updated for OpenAM version 7 compatibility.

LexisNexis ThreatMetrix Nodes 1.0.0 – December 2019

- Initial Release.