Release Notes

LexisNexis Risk Solutions – One-Time Passcode (OTP) Nodes

Version 1.1.1

September 2025

LexisNexis®
RISK SOLUTIONS

TABLE OF CONTENTS

INTRODUCTION

This document contains the release notes for the LexisNexis One-Time Passcode (OTP) 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 One-Time Passcode (OTP) 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 One-Time Passcode (OTP) Nodes.

Java Environment

- OpenJDK 11, OpenJDK 17

Web Application Container Environment

- Apache Tomcat 9

Versions Tested

- PingAM / ForgeRock 7.3, PingAM / ForgeRock 7.4

> **Note:** The LexisNexis One-Time Passcode (OTP) Nodes are only compatible with PingAM / ForgeRock Access Management version 7.3 and later. If support for a previous release versions are needed, please contact LexisNexis Risk Solutions.

KNOWN ISSUES

This following is a complete list of currently known issues:

- There are no known issues at this time

CHANGE LIST

LexisNexis One-Time Passcode Nodes 1.1.1 – September 2025

- Fixed a bug when using Shared State option to fetch optional attributes for the Send OTP 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 One-Time Passcode Nodes 1.1.0 – August 2025

- Added a new LexisNexis OTP Selector node that displays an interface for the end user to select which type of OTP is desired to be sent. The list includes Email Address, SMS Text and Voice. The node will place the value into shared state variable `otp_type_select`. By default, this is the shared state variable that the LexisNexis OTP Send node accepts to determine which type of OTP to send to the end user.
- Updated LexisNexis OTP Send node to only send OTP codes, such that the selector capability was placed into the LexisNexis OTP Selector. In order to define the type of OTP to send, the shared state variable `otp_type_select` is read at runtime. The valid of values is: EMAIL, SMS and VOICE.
- Updated LexisNexis OTP Send node to include a parameter that defines where to locate user attributes such as mobile number and email address. The parameter is a drop-down list with two options, mainly User Directory or Shared State. Once configured, this defines the location for the attributes to utilize as part of API Request processing.
- Fixed LexisNexis OTP Send node to detect if the SMS Body Message is greater than 160 characters.
- Fixed LexisNexis OTP Decision node to detect if the OTP code entered is greater than 10 characters, which is the maximum allowed by the LexisNexis service. A friendly user error will be generated for this condition versus an integration error.
- Updated for most recent PingAM releases.

LexisNexis One-Time Passcode Nodes 1.0.0 – November 2023

- Initial Release