Getting Started Guide

Configure ForgeRock with LexisNexis InstantID Question and Answer (IIDQA) Nodes

Guide for On Premise with Access Manager

Version 1.0

November 2023

LexisNexis®
RISK SOLUTIONS

Table of Contents

SCOPE

This document contains the detailed steps and supporting information required to install and configure the ForgeRock Access Management (AM) Single Sign-On (SSO) server with LexisNexis InstantID Question and Answer (IIDQA) Nodes. This guide is intended to install a simple configuration to support testing.

The following are architecture assumptions and limitations:

- ForgeRock Access Manager server has been previously installed
- Default configuration for ForgeRock SSO Server with a default configuration for OpenDJ as the Identity Store
- An existing ForgeRock Authentication Tree is configured that can be modified to integrate the IIDQA Nodes as an Inner Tree Evaluator Node

Document Organization

This document is divided into four sections as follows:

- **Scope.** Defines the purpose of this document.
- **LexisNexis IIDQA Nodes**. Provides on overview of the nodes available for ForgeRock authentication tree integration.
- **Nodes Installation.** Provides information to install the LexisNexis IIDQA nodes upon an on-premise ForgeRock Access Management (AM) server.
- **LexisNexis Dynamic Decision Platform Portal.** Provides detailed information regarding the configuration of LexisNexis Dynamic Decision Platform (DDP) to include configuration of a simple policy and how to access configuration parameters required for the ForgeRock authentication tree.
- **ForgeRock Authentication Tree Configuration.** Provides detailed steps to configure a ForgeRock authentication tree with LexisNexis IIDQA Nodes to perform Multi-Factor Authentication (MFA) in support of an existing ForgeRock journey tree.

LEXISNEXIS INSTANTID QUESTION AND ANSWERS NODES

The LexisNexis InstantID Question and Answer (IIDQA) Nodes are available in the Marketplace to be included within any new or existing ForgeRock authentication tree configurations. To include a LexisNexis IIDQA node in a journey, enter LexisNexis into the Filter nodes to get a listing of available capabilities. For IIDQA, the following nodes are available:

- LexisNexis InstantID Get Quiz
- LexisNexis InstantID Quiz Collector
- LexisNexis InstantID Quiz Decision

LexisNexis InstantID Get Quiz

This node calls the LexisNexis Dynamic Decision Platform (DDP) Authentication Hub for InstantID Question and Answer (IIDQA). The main purpose of this node is to call the DDP Authentication Hub to generate an IIDQA quiz. There is no interface displayed to the user by this node.

The LexisNexis IIDQA Get Quiz node is configured with an attribute mapping to gather parameters for the API Request to send to the DDP Authentication Hub for generating a knowledge based answer quiz. The attribute mapping defines the syntax to query parameters within ForgeRock that are then mapped to IIDQA attributes. Furthermore, the node provides the capability to gather the user attributes based on the configuration of the Attribute Source, mainly User Directory or Shared State. When the user directory is configured as the source for attributes, the node will assume that the username is contained in shared state from a previous node in the authentication tree/journey and use that username to query the user directory for user parameters and fulfill the attribute mapping. When the shared state is configured as the source for attributes, the node will inspect shared state for the user parameters to fulfill the attribute mapping.

The LexisNexis IIDQA Get Quiz Node has the following configuration parameters:

- **Org ID** - Org ID is the unique id associated your organization on the Dynamic Decision Platform (DDP).
- **API Key** - This is the unique API key generated via DDP Portal associated to the Org ID.
- **API URL** - This is the URL for the DDP Authentication Hub IIDQA API endpoint. The default URL is the Worldwide endpoint. This should be modified for specific regions such as EU, US or India.
- **Policy** - The DDP Portal policy to be used to integrate the DDP Authentication Hub with IIDQA
- **Attribute Source** - This determines where the IIDQA Get Quiz node will inspect and gather user parameters to be mapped into the attributes of the IIDQA API Request to get a quiz. This can be configured for User Directory or form Shared State. User Directory is typically configured in a orchestration where IIDQA is used for Multi-Factor Authentication (MFA) since the information for the user should be in the directory. The Shared State specification is typically configured in an orchestration where IIDQA is used for identity proofing for use cases such as new account origination since the user account does not exist. When Shared State is used there should be an interface in the tree/journey to collect the information which stores the data in shared state.

- **Attribute List** - Defines a mapping of user parameters to InstantID Q&A API attributes. The user parameters will be fetched based on the Attribute Source. The Key is the user parameter name from the source and the value is the attribute name to send to InstantID Q&A. For example, Attribute Source=Shared State, with attribute list key=`givenName` and value=`account_first_name` would signal the LexisNexis IIDQA Get Quiz node to fetch the user parameter `givenName` from shared state and then set the IIDQA attribute `account_first_name` to the value from shared state. The attributes to send to IIDQA should include `account_first_name`, `account_last_name`, `account_address_street1`, `account_address_city`, `account_address_state` and `account_address_zip` as this will have a good probably to match a record in the LexisNexis system resulting in a generated quiz.

The LexisNexis IIDQA Get Quiz Node has the following outcomes:

- **Success** - This outcome is triggered when the API Request results in a physical match to a person based on the Attribute List and a quiz is generated. The quiz is placed into Shared State for the IIDQA Quiz Collector Node, which will display the user interface for the quiz to collect the answers.
- **API Error** - This outcome is triggered when there is an issue with the API Request such as a network timeout or the service is unavailable.
- **Discovery Error** - This outcome is triggered when a physical match to a person cannot be made based on the attribute list provided in the IIDQA API Request. In this scenario, the journey/tree may display a secondary interface to collect additional user parameters such as DOB or SSN enabling a higher probability for an identity match.
- **Velocity Error** - This outcome is triggered based on the IIDQA policy configured within LexisNexis. Typically, we configure the system to only allow 3 quiz requests over a 30 minutes period to prevent guessing attacks.
- **Error** - This outcome is triggered when there is a fundamental integration error, or a new bug is discovered. First attempt to fix the integration error by looking at debug log files for the node to determine if the integration error is due to configuration. If the configuration looks accurate, then open a support case with LexisNexis.

LexisNexis InstantID Quiz Collector

This node displays the user interface for a quiz generated by the LexisNexis InstantID Get Quiz Node. The quiz questions are passed through shared state from the get quiz node to the quiz collector node. Once received, the interface will be displayed to the user for knowledge-based questions to be answered. Once submitted, the answers are placed into shared memory for the LexisNexis InstantID Decision Node.

The LexisNexis IIDQA Quiz Collector Node has the following configuration parameters:

- **N/A** - There are no configuration parameters for this node.

The LexisNexis IIDQA Quiz Collector Node has the following outcomes:

- **Next** - This outcome is triggered quiz answers are complete and the submit button is selected by the user.
- **Cancel** - This outcome is triggered when the user selects the cancel button to abort the quiz.

- **Error** - This outcome is triggered when there is a fundamental integration error, or a new bug is discovered. First attempt to fix the integration error by looking at debug log files for the node to determine if the integration error is due to configuration. If the configuration looks accurate, then open a support case with LexisNexis.

LexisNexis InstantID Quiz Decision

This node calls the LexisNexis Dynamic Decision Platform (DDP) Authentication Hub for InstantID Question and Answer (IIDQA). The main purpose of this node is to call the DDP Authentication Hub to validate answers for a quiz. There is no interface displayed to the user by this node. The quiz answers are passed through shared state from the quiz collector node to the quiz decision node. Once received, the DDP Authentication Hub IIDQA API Request is generated and API Response inspected for success or failure.

The LexisNexis IIDQA Quiz Decision Node has the following configuration parameters:

- **Org ID** - Org ID is the unique id associated your organization on the Dynamic Decision Platform (DDP).
- **API Key** - This is the unique API key generated via DDP Portal associated to the Org ID.
- **API URL** - This is the URL for the DDP Authentication Hub IIDQA API endpoint. The default URL is the Worldwide endpoint. This should be modified for specific regions such as EU, US or India.
- **Policy** - The DDP Portal policy to be used to integrate the DDP Authentication Hub with IIDQA. This policy configuration should be the same as the LexisNexis InstantID Get Quiz node configuration.

The LexisNexis IIDQA Quiz Decision Node has the following outcomes:

- **Pass** - This outcome is triggered when answers to a quiz are all passing according the DDP IIDQA policy
- **Fail** - This outcome is triggered when answers to a quiz are not passing according the DDP IIDQA policy
- **API Error** - This outcome is triggered when there is an issue with the API Request such as a network timeout or the service is unavailable.
- **Error** - This outcome is triggered when there is a fundamental integration error, or a new bug is discovered. First attempt to fix the integration error by looking at debug log files for the node to determine if the integration error is due to configuration. If the configuration looks accurate, then open a support case with LexisNexis.

NODES INSTALLATION

This section describes how to deploy the LexisNexis IIDQA Nodes to the ForgeRock Access Manager hosted on Apache Tomcat. The server will need to be stopped and restarted for the Nodes to be properly deployed. This instruction assumes a tomcat application web server.

1. Stop the Tomcat server
2. Remove any previously installed versions of LexisNexis IIDQA Nodes from the server:

   Directory: `<fgrkinstall>/tomcat/webapps/openam/WEB-INF/lib`
3. Copy the LexisNexis IIDQA Nodes media as follows:

   Filename: `lexisnexis-iidqa-1.0.0.jar`

   Directory: `<fgrkinstall>/tomcat/webapps/openam/WEB-INF/lib`
4. Restart Tomcat server from command line

DYNAMIC DECISION PLATFORM PORTAL CONFIGURATION

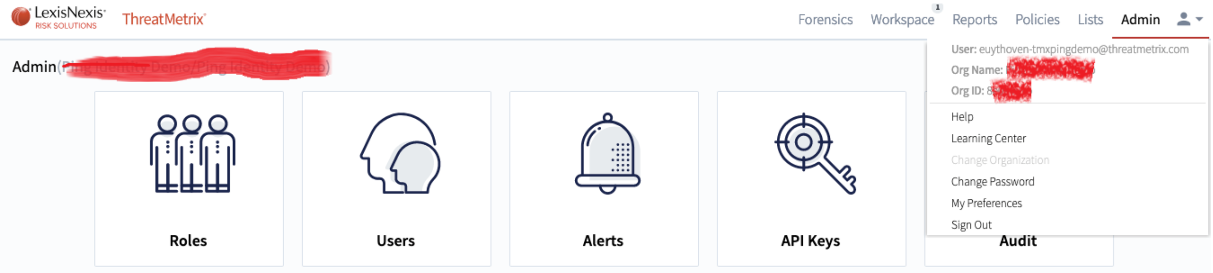
This section defines the high-level LexisNexis Dynamic Decision Platform (DDP) Portal configuration items that will be needed for the overall configuration. There are two main categories of configuration, mainly,

- Organization ID and API Key for the REST API interfaces. This information is needed by the LexisNexis IIDQA Nodes and will be entered as part of configuration.
- LexisNexis IIDQA Portal Policy. The configured policy within DDP provides the configuration for the Authentication Hub to access IIDQA services. For the purposes of the getting started guide and to have a simple test configuration for different outcomes, the "IIDQA" policy will be configured to directly integrate the Authentication Hub without any further policy rules.

Retrieve OrgID and API Key

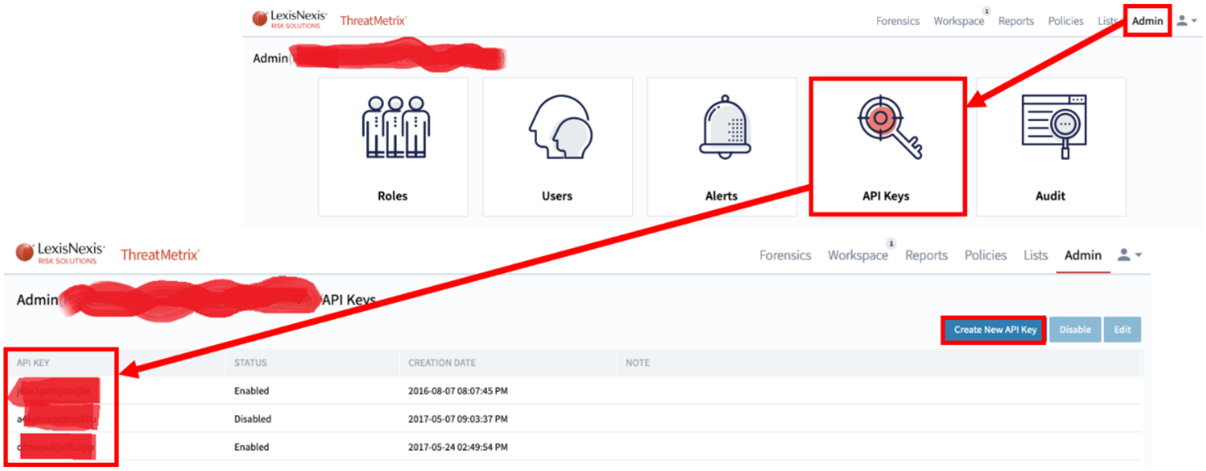
To retrieve the DDP Portal values for Organization ID and API Key, perform the following steps.

1. Access **DDP Portal** over the internet by logging into your administrative account with credentials provided by LexisNexis.
2. From the **DDP Portal** home page, select the user information dropdown that will display username, OrgName and OrgID. This will be the OrgID to enter into the configuration of the LexisNexis IIDQA Nodes.



User: euythoven-tmxpingdemo@threatmetrix.com
Org Name: [redacted]
Org ID: [redacted]

3. Within the **DDP Portal** home page, select **Admin** followed by selecting the **API Keys** tile. Retrieve the value for API Key. In the event no API Key is listed, select the **Create New API Key** button to generate a new key. This will be the API Key to enter into the configuration of the LexisNexis IIDQA Nodes. The API Key is to be protected. Do not email or keep this value in cleartext on any computer system.



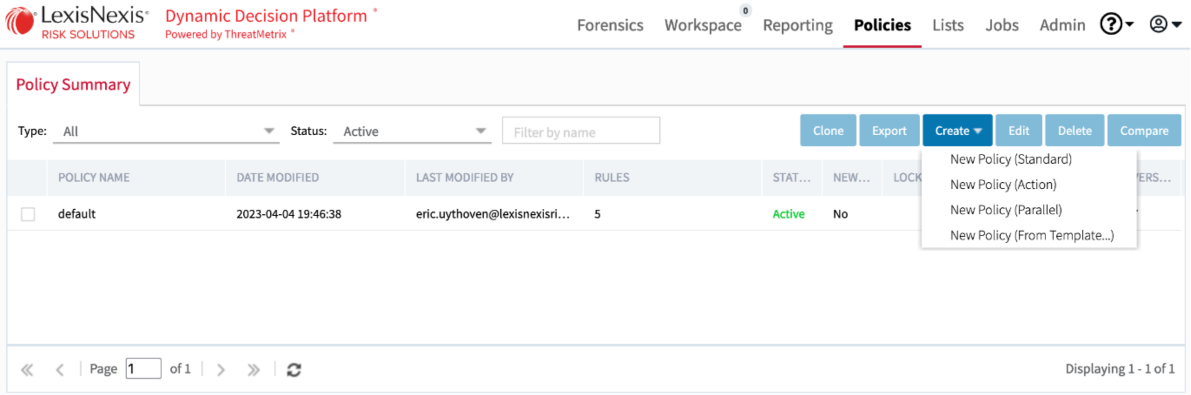
API KEY	STATUS	CREATION DATE	NOTE
[redacted]	Enabled	2016-08-07 08:07:45 PM	
[redacted]	Disabled	2017-05-07 09:03:37 PM	
[redacted]	Enabled	2017-05-24 02:49:54 PM	

Dynamic Decision Platform Portal Policy

For the purposes of the getting started guide and to have a simple test configuration for different outcomes, the “IIDQA” policy will be configured to directly integrate the Authentication Hub without any further policy rules. Perform the following steps.

1. Access **DDP Portal** over the internet by logging into your administrative account with credentials provided by LexisNexis.

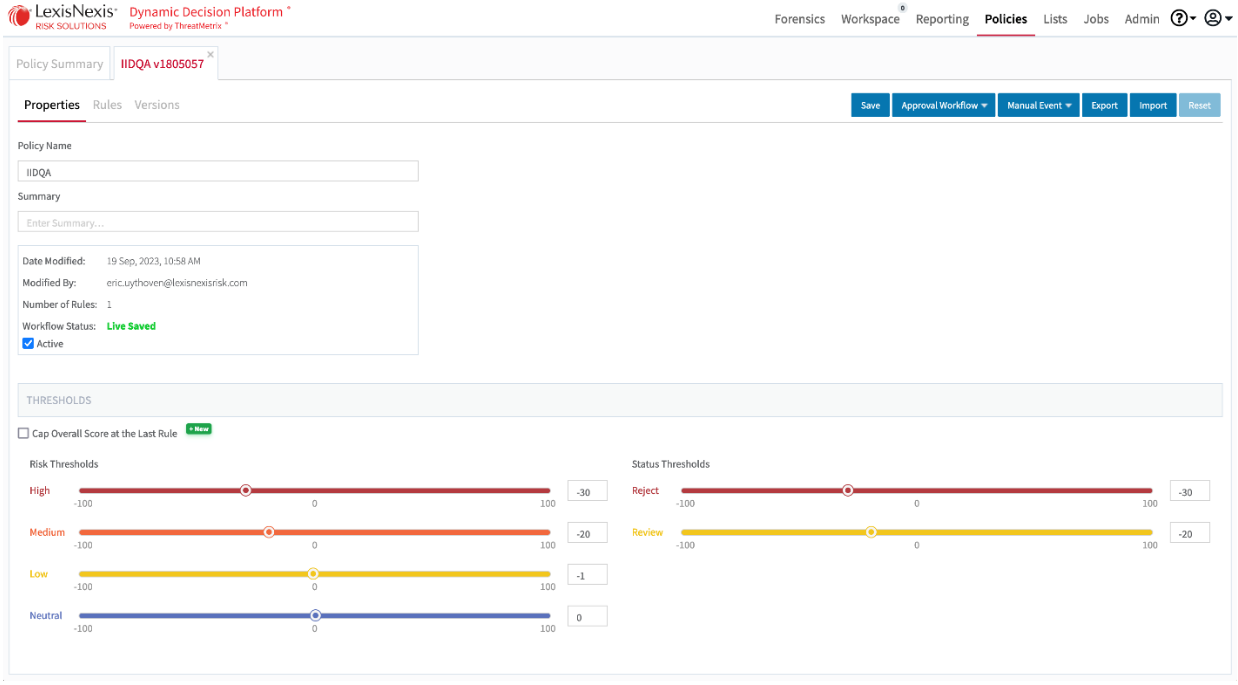
2. From the **DDP Portal** home page, select **Policies** from the menu bar. This will provide a listing of available policies. The first step is to select the **Create** dropdown menu followed by **New Policy (Standard)**.



Type: All | Status: Active | Filter by name

	POLICY NAME	DATE MODIFIED	LAST MODIFIED BY	RULES	STAT…	NEW…	LOCK	…ERS…
□	default	2023-04-04 19:46:38	eric.uythoven@lexisnexisri…	5	Active	No		

3. On the Policy Summary, the **Properties** interface tab will be displayed. Enter Policy Name = IIDQA, select the Active button, and update the Status Thresholds for Reject = -20 and Review = 20.



Policy Name: IIDQA

Summary: Enter Summary…

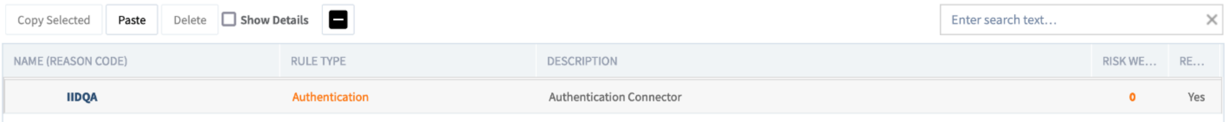
Date Modified: 19 Sep, 2023, 10:58 AM
Modified By: eric.uythoven@lexisnexisrisk.com
Number of Rules: 1
Workflow Status: Live Saved
☑ Active

□ Cap Overall Score at the Last Rule

Risk Thresholds
High: -30
Medium: -20
Low: -1
Neutral: 0

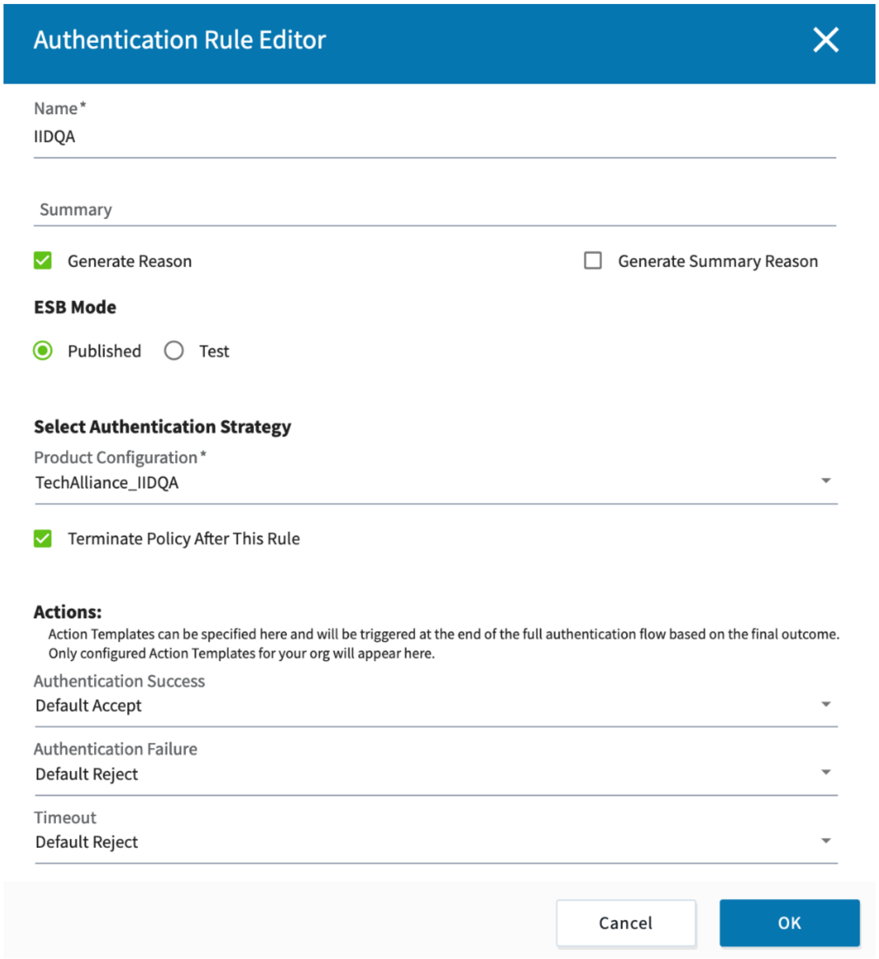
Status Thresholds
Reject: -30
Review: -20

4. To create the policy rules, select the **Rules** interface tab. The IIDQA policy will be a single **Authentication** rule to integrate the Authentication Hub as follows.



NAME (REASON CODE)	RULE TYPE	DESCRIPTION	RISK WE…	RE…
IIDQA	Authentication	Authentication Connector	0	Yes

5. The **Authentication Rule Editor** can follow the template shown here. Within this interface, the **Product Configuration** is the Authentication Hub configuration that is established via LexisNexis ThreatMetrix Professional Services. The services configure the LexisNexis IIDQA service as an interface associated to the customer account.



Name*
IIDQA

Summary

☑ Generate Reason   □ Generate Summary Reason

ESB Mode

● Published ○ Test

Select Authentication Strategy

Product Configuration*
TechAlliance_IIDQA

☑ Terminate Policy After This Rule

Actions:
Action Templates can be specified here and will be triggered at the end of the full authentication flow based on the final outcome. Only configured Action Templates for your org will appear here.

Authentication Success
Default Accept

Authentication Failure
Default Reject

Timeout
Default Reject

6. Save the policy.

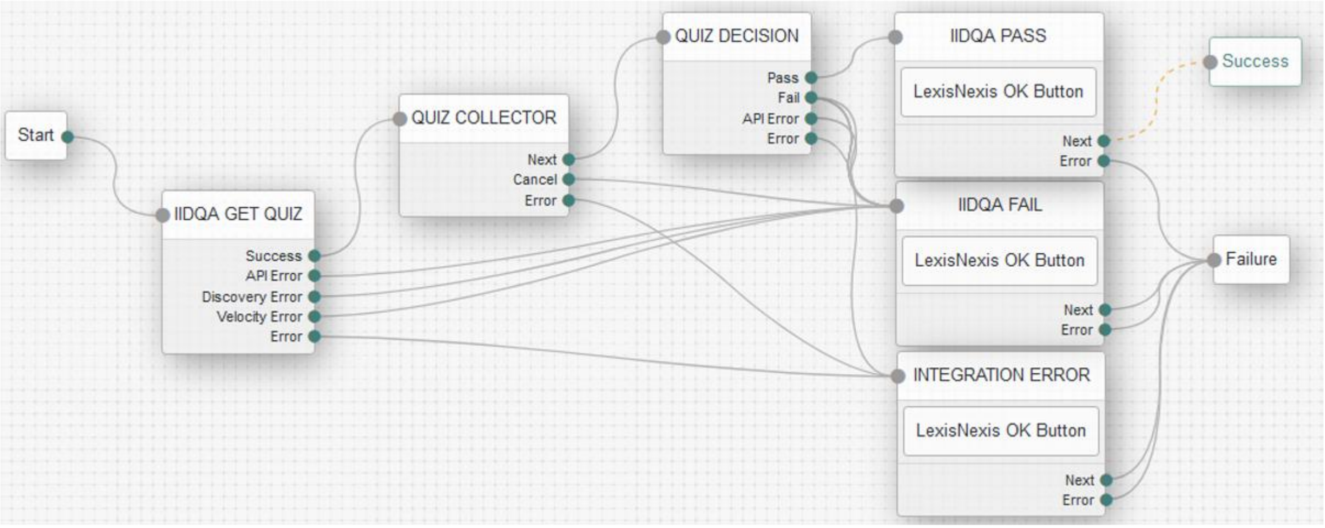
7. Consult with LexisNexis ThreatMetrix services for a more comprehensive policy configuration.

FORGEROCK-LEXISNEXIS AUTHENTICATION TREE

Authentication Tree: LNRS-StepUp-IIDQA

This section provides the steps to configure a ForgeRock Authentication Tree with LexisNexis IIDQA nodes from the marketplace. The workflow in this section is focused on the general flow of IIDQA nodes, which can be called as a ForgeRock Inner Tree from higher level journey/tree.

The workflow starts with the LexisNexis IIDQA Get Quiz node. This node has been designed to support use cases for MFA of an existing managed user, as well as first time Identity Proofing for a new account origination The key is how the LexisNexis IIDQA Get Quiz node gathers parameters from the ForgeRock environment, mainly from a user credential store to support MFA workflows, or from a user interface and shared state to support new account origination workflows.



The flow is as follows:

- LexisNexis IIDQA Get Quiz Node. The configuration determines whether to pull user parameters from: (i) a user credential store, or (ii) from ForgeRock shared state in the journey/tree.
- LexisNexis IIDQA Quiz Collector Node. This node will display the quiz generated via the LexisNexis IIDQA Get Quiz Node. The user is expected to select the correct answers and click the submit button.
- LexisNexis IIDQA Quiz Decision Node to determine if the quiz answers collected from the user are valid and pass the test.
- Page Nodes with messages and a single OK button that will display the results and/or error conditions.

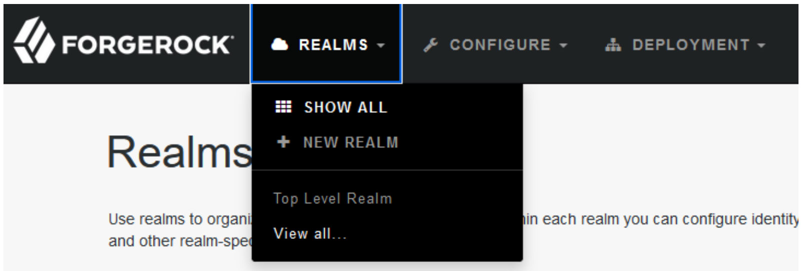
To configure the Authentication Tree, perform the following to configure the server:

1. From a workstation, launch a browser and enter the following URL:

   `https://<SSO-SVR-NAME>:<SSO-SVR-HTTPS-PORT>/openam`

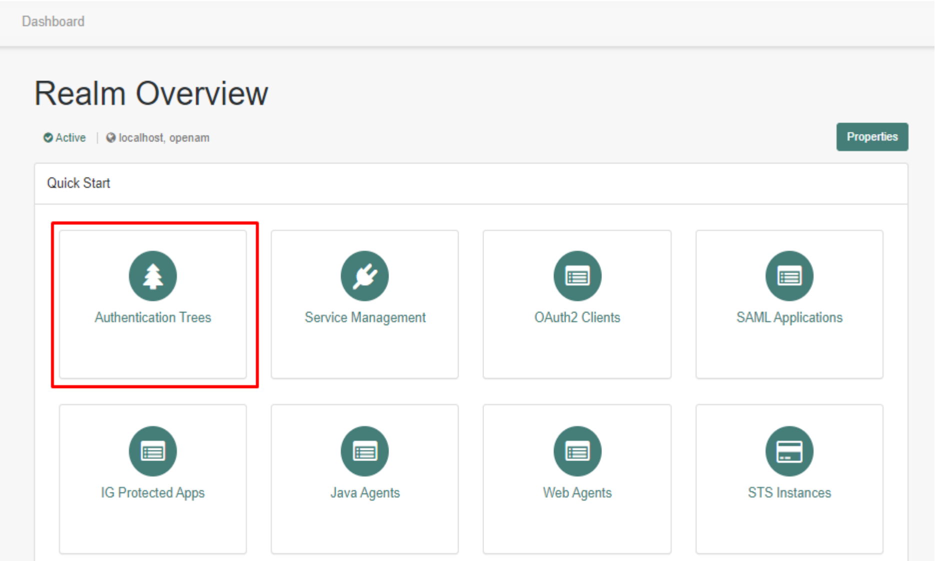
   Example: `https://sso.threatmetrix.com:8443/openam`

2. Login with amadmin and credentials
3. Upon login, select the **Realms** dropdown menu and click **Top Level Realm**.

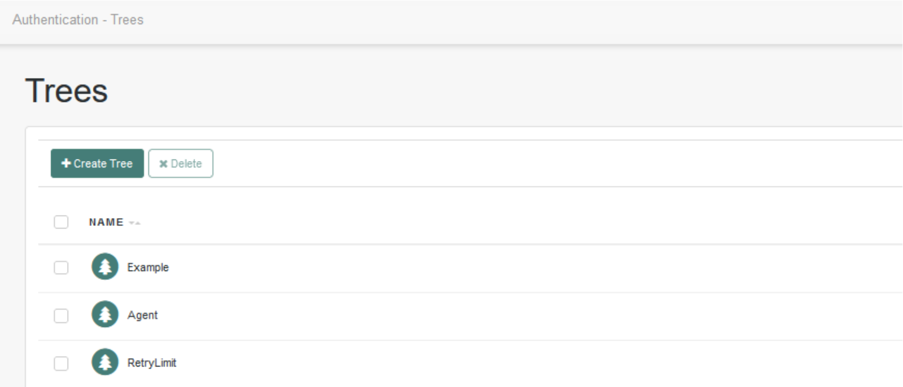


Use realms to organi in each realm you can configure identity and other realm-spec

4. On the **Realm Overview** display, click the **Authentication Trees** tile.

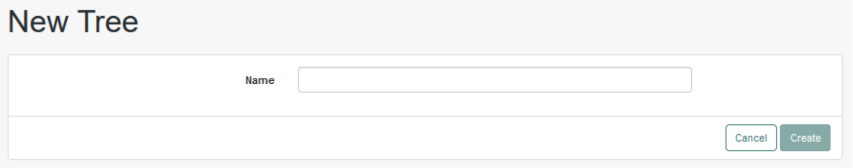


5. On the **Authentication Trees** display, click the **Create Tree** tile.



	NAME
□	Example
□	Agent
□	RetryLimit

6. On the **New Tree** display, enter “LNRS-IIDQA” followed by the **Create** button.



7. The result is the **Authentication Trees > LNRS-IIDQA** display. This is the interface to build up the authentication policy as a tree depiction showing the nodes in the policy. At this point, the tree will be built by drag-n-drop of Components on the left side of the screen. Each node in the policy will then be configured.

8. Build the IIDQA GET QUIZ Screen, do the following:

   - On the **Components Filter** on the left side of the interface, enter **lexisnexis**. When the **LexisNexis InstantID Get Quiz** is displayed as a component, drag and drop it into the authentication tree.

   - Select the **LexisNexis InstantID Get Quiz** Node component to display the configuration properties on the right side of the interface. Enter the following property values.

Org ID	<ENTER ORG ID FROM DDP PORTAL>
API Key	<ENTER API KEY FROM DDP PORTAL>
API URL	https://h-api.online-metrix.net/authentication/v1/iidqa/
Policy	<ENTER THE POLICY NAME AS CONFIGURED IN DDP PORTAL>
Attribute Source	Select either "User Directory" or "Shared State"

Attribute List	Defines the user parameter mapping from the Attribute Source to IIDQA attributes. For example
	Key=givenName, Value=account_first_name
	Key=sn, Value=account_last_name
	Key=postalCode, Value=account_address_zip

Note: In the DDP Portal when the policy is established, the reason code that is configured is dynamic, thus the rationale for the configuration parameter. In the example screen snapshots in section entitled "Dynamic Decision Platform Portal Policy", the name of the policy is "IIDQA" and the reason code is "IIDQA".

Note: The toggle for Attribute Source allows flexibility in the journey/tree. This determines where the IIDQA GET QUIZ node will inspect and gather user parameters to be mapped into the attributes of the IIDQA API Request to get a quiz. This can be configured for User Directory or from Shared State. User Directory is typically configured in an orchestration where IIDQA is used for Multi-Factor Authentication (MFA) since the information for the user should be in the directory. The Shared State specification is typically configured in an orchestration where IIDQA is used for identity proofing for use cases such as new account origination since the user account does not exist.

Note: The Attribute List defines a mapping of user parameters to InstantID Q&A API attributes. The user parameters will be fetched based on the Attribute Source. The Key is the user parameter name from the source and the value is the attribute name to send to InstantID Q&A.

InstantID Q&A must have a physical data record match in order to generate a quiz. The minimum parameters to send are first/last name and zip code. Based on the workflow, additional parameters may be needed such as address, data of birth or social security number. When designing the workflow, be sure to take into account the information needed and whether or not the Discovery Error outcome can be used to fetch additional information.

9. Build the IIDQA QUIZ COLLECTOR, do the following:

    - The LexisNexis InstantID Quiz Collector Node may optionally be placed into a Page Node container for additional heading and messaging, or as a standalone node. This decision is up to the administrator. For the purposes of simplicity, this instruction will document the standalone configuration.

    - On the **Components Filter** on the left side of the interface, enter **lexisnexis**. When the **LexisNexis InstantID Quiz Collector** is displayed as a component, drag and drop it into the authentication tree.

    - Select the **LexisNexis InstantID Quiz Collector** Node component to display the configuration properties on the right side of the interface. This node does not have any configuration parameters.

10. Build the IIDQA QUIZ DECISION, do the following:

    - On the **Components Filter** on the left side of the interface, enter **lexisnexis**. When the **LexisNexis InstantID Quiz Decision** is displayed as a component, drag and drop it into the authentication tree.

    - Select the **LexisNexis InstantID Quiz Decision** Node component to display the configuration properties on the right side of the interface. Enter the following property values.

Org ID	<ENTER ORG ID FROM DDP PORTAL>
API Key	<ENTER API KEY FROM DDP PORTAL>
API URL	https://h-api.online-metrix.net/authentication/v1/iidqa/
Policy	<ENTER THE POLICY NAME AS CONFIGURED IN DDP PORTAL>

Note: The Policy configured in the LexisNexis InstantID Quiz Decision node shall be the same as the LexisNexis InstantID Get Quiz. This is because DDP maintains state between isuuance of the quiz and the submittal of quiz answers.

11. Build Message Nodes for IIDQA Pass, IIDQA Fail, and Integration Error to support testing. This can be accomplished with Message Nodes or Page Nodes with an OK Button Node. The nodes are meant to display outcomes to the user.

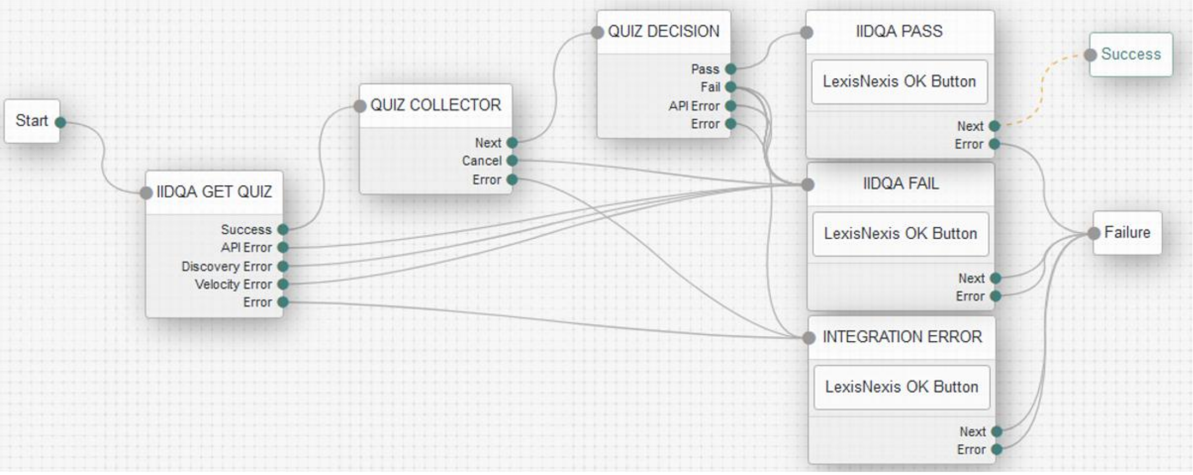
12. Link together the nodes of the authentication tree

    - To connect the nodes of the authentication tree, click on the output dot of one node and then drag it to the input dot of another node. The following connections should be made.

Start	IIDQA GET QUIZ
IIDQA GET QUIZ (Success)	QUIZ COLLECTOR
IIDQA GET QUIZ (API Error)	IIDQA FAIL
IIDQA GET QUIZ (Discovery Error)	IIDQA FAIL
IIDQA GET QUIZ (Velocity Error)	IIDQA FAIL
IIDQA GET QUIZ (Error)	INTEGRATION ERROR
QUIZ COLLECTOR (Next)	QUIZ DECISION
QUIZ COLLECTOR (Cancel)	IIDQA FAIL
QUIZ COLLECTOR (Error)	INTEGRATION ERROR
QUIZ DECISION (Pass)	IIDQA PASS
QUIZ DECISION (Fail)	IIDQA FAIL
QUIZ DECISION (API Error)	IIDQA FAIL
QUIZ DECISION (Error)	INTEGRATION ERROR
IIDQA PASS (Next)	Success
IIDQA PASS (Error)	Failure

IIDQA FAIL (Next)	Failure
IIDQA FAIL (Error)	Failure
INTEGRATION ERROR (Next)	Failure
INTEGRATION ERROR (Error)	Failure

- At this point you should have the following

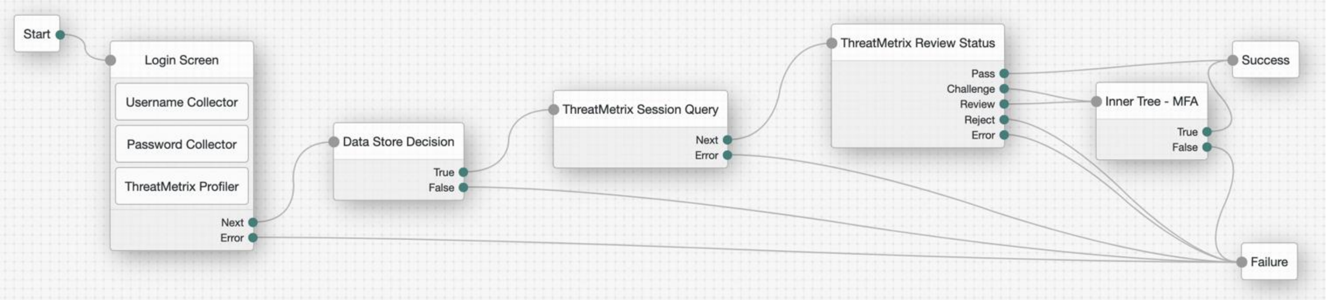


Authentication Tree: IIDQA as Second Factor

InstantID Question and Answer (IIDQA) technology can be used as a second factor (e.g. Multi-Factor Authentication [MFA]) for many workflows and journeys. One common scenario is a User Login when a second factor for a high-risk transaction is needed. In this case, the user is known due to the first factor authentication, as well as it is assumed that user has enough information within the user credential store to perform an IIDQA transaction.

The authentication tree in the section **Authentication Tree: LNRS-IIDQA** provides an example of the workflow, which is an orchestrated workflow where the LexisNexis InstantID Get Quiz node has a dependency upon the attribute “username” being in shared state. The IIDQA GET QUIZ node will be configured to get the users parameters from the user directory.

To accomplish this overall workflow and orchestration, the ForgeRock Inner Tree Evaluator node is used at the point where MFA is required.



For the purposes of brevity, the entire login workflow authentication tree will not be documented here, rather a simple documentation of the inner tree evaluator to integrate the LNRS-IIDQA tree from the previous section.

1. From a workstation, launch a browser and navigate to the Access Manager Admin Console.
2. Login with amadmin and credentials
3. Upon login, select the **Realms** dropdown menu and click **Top Level Realm**.
4. On the **Realm Overview** display, click the **Authentication Trees** tile.
5. On the **Authentication Trees** display, select the existing authentication tree to modify.
6. To leverage the IIDQA authentication tree, add an Inner Tree Evaluator node.
   - On the **Components Filter** on the left side of the interface, enter **inner**. When the **Inner Tree Evaluator** node is displayed as a component, drag and drop an instance into the authentication tree. This node will be used to invoke the LNRS IIDQA authentication tree. Enter the following property values.

Node name	Inner Tree - MFA
Tree Name	LNRS-IIDQA

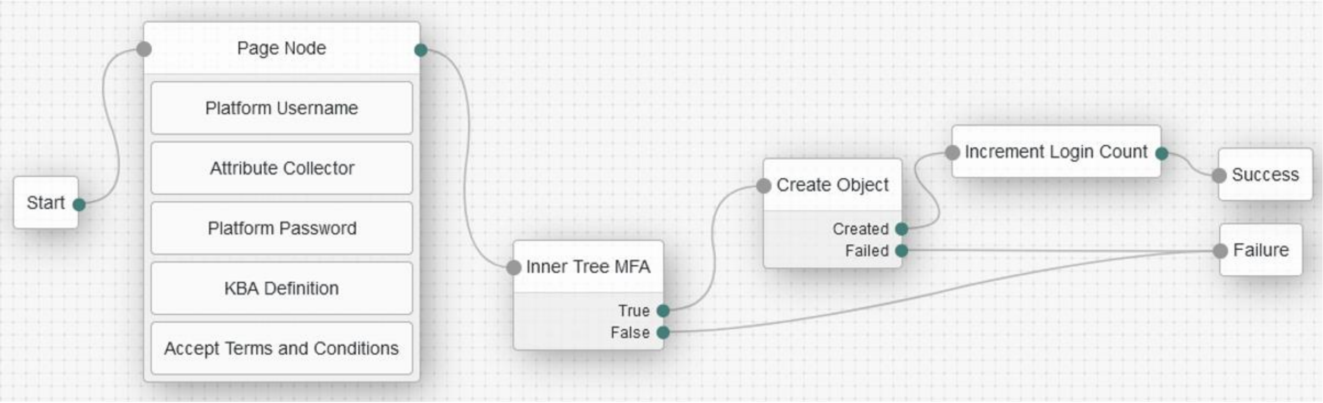
   - Connect the nodes of the authentication tree and save the authentication tree.

Authentication Tree: IIDQA within New Account Origination

InstantID Question and Answer (IIDQA) technology can be used for Identity Proofing within a New Account Origination (NAO) workflow. This is done to validate the digital account is tied to a physical user, where the physical user information is validated, cutting down on synthetic accounts.

The authentication tree in the section **Authentication Tree: LNRS-IIDQA** provides an example of the workflow, which is an orchestrated workflow where the LexisNexis InstantID Get Quiz node has a dependency upon user parameters being available in shared state. The IIDQA GET QUIZ node will be configured to get the users parameters from shared memory.

NAO workflows will have an interface for gathering information from the user at runtime that will include attributes used for the IIDQA Quiz. To accomplish this overall workflow and orchestration, the ForgeRock Inner Tree Evaluator node is used at the point where IIDQA is required.



For the purposes of brevity, the entire NAO workflow will not be documented here, rather a simple modification to the out-of-the-box Platform Registration workflow will be performed to insert a inner tree evaluator for the LNRS-IIDQA tree.

1. From a workstation, launch a browser and navigate to the Access Manager Admin Console.
2. Login with amadmin and credentials
3. Upon login, select the **Realms** dropdown menu and click **Top Level Realm**.
4. On the **Realm Overview** display, click the **Authentication Trees** tile.
5. On the **Authentication Trees** display, select the existing authentication tree to modify.
6. To leverage the IIDQA authentication tree, add an Inner Tree Evaluator node before the user account object is created.
   - On the **Components Filter** on the left side of the interface, enter **inner**. When the **Inner Tree Evaluator** node is displayed as a component, drag and drop an instance into the authentication tree. This node will be used to invoke the LNRS IIDQA authentication tree. Enter the following property values.

Node name	Inner Tree - MFA
Tree Name	LNRS-IIDQA

   - Connect the nodes of the authentication tree and save the authentication tree.