ForgeRock

INTELLIGENT ACCESS SERIES

Reduce Government Services Fraud

Incorporate Identity Proofing Into Citizen Registration and Authentication Journeys

Introduction

In today's ever-expanding digital identity landscape, stopping account-related exploits early in the process is paramount to eliminating identity theft, fraud, and loss of revenue. Identity and Access Management (IAM) plays an important role in helping government agencies combat fraud-related identity exploits associated with the way claimants register and authenticate to agency online portals.

ForgeRock offers an intelligent, flexible, and extensible orchestration platform to help government agencies incorporate identity-proofing into the registration and authentication process and minimize the likelihood of fraudulent claims.

In this white paper, you'll learn how ForgeRock enables modern identity for legacy applications; predicts, prevents, and remediates fraud; and incorporates leading identity-proofing from ForgeRock Trust Network partners, Onfido, and ID.me. The example journeys are a starting point to help you build identity-proofed citizen registration and access journeys.

Combating Fraud with Identity and Access Management (IAM)

Pandemic-related fraud skyrocketed in 2020 and 2021. Government agencies using antiquated, mainframe-based applications and legacy IAM systems for citizen sign-up and sign-in bore the brunt of the fraud. In the U.S., fraudsters – from transnational crime syndicates to prison inmates – have used stolen identity information purchased on the dark web to create false accounts and file claims on behalf of citizens and well-known individuals.[1] Globally, the situation is similar: In the U.K., normal verification checks were suspended to enable processing of new "Universal Credit" and other benefits, resulting in an estimated £8.5 billion of "overpaid" benefits in 2020 to 2021.[2] In France, more than €1.7 million of temporary unemployment insurance claims were nabbed by fraudsters.[3]

> In April 2020, the state of New Jersey issued a call for volunteers who knew how to program in COBOL to update the state's 40-year-old mainframe systems that power unemployment benefits. The state needed updates in order to handle the record level of unemployment claims due to the COVID-19 pandemic.[4]

Modern IAM can detect and prevent these types of fraudulent transactions, but to do so effectively, the solution requires more advanced capabilities. It must be scalable to support millions of external citizen transactions per second, providing continuous protection when citizens sign up for benefits, prove their identity, and log in. It should be able to detect compromised accounts and continuously evaluate constituents' risk posture for each additional transaction. To do so, it must be able to collect and interpret multiple signals about citizens – their devices, network, reputation, and known behaviors – and then make fine-grained access and authorization decisions for any high-stakes transaction. It should also be able to integrate with industry-leading solutions to detect fraudulent transactions through identity verification, ingestion, and processing external risk signals, compromised credentials, and the like.

Citizens should not have to pay the price for better security by having to endure a difficult user experience. IAM should be capable of working silently and in the background to verify a claimant's identity and reputation without requiring multiple disjointed and frustrating steps.

The ForgeRock Identity Platform: Modernizing and Securing Access to Legacy Government Systems

ForgeRock is the only full-suite IAM platform that can help government agencies modernize the web front-end for legacy government backend systems. The Modernize IAM accelerator kits support migrating and centralizing identities from multiple identity management systems onto the ForgeRock platform, so agencies can quickly and easily build on existing investments and streamline operations with zero disruption to end users.

Large, complex government organizations choose ForgeRock to help integrate, coexist with, and modernize legacy applications while using the same identity platform to support new applications and services.

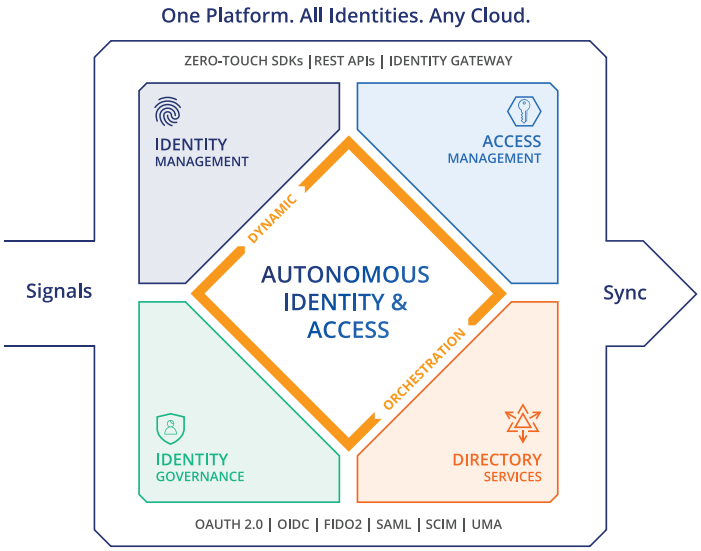

Figure 1: The ForgeRock Identity Platform

ForgeRock Intelligent Access

ForgeRock Intelligent Access, part of the ForgeRock Identity Platform, makes it easy to design secure and customized citizen user journeys without writing a single line of code.

You can combine citizen registration, authentication, and access capabilities with rich context and continuous runtime prediction, prevention, detection, and response. ForgeRock helps you validate and secure citizen claimants while providing continuous protection against fraudulent sign-ups or account hijacking. At the same time, Intelligent Access makes registration and authentication journeys frictionless for citizens, reducing frustration and making the claims process easier to navigate.

Using ForgeRock Intelligent Access, you can deliver rich login experiences, reduce the friction associated with login, enable contextual and adaptive multi-factor authentication, and support pre-integrated and tested identity proofing solutions that require no custom coding.

To learn more about Intelligent Access user journeys, read the white paper, An Introduction to ForgeRock Intelligent Access.

The ForgeRock Trust Network

ForgeRock has a large ecosystem of Trust Network partners and validated integrations to establish secure citizen identity and detect and prevent fraud while enabling citizen user journeys that are easy to use. The ForgeRock Trust Network includes tested and verified solutions for strong authentication, physical and behavioral biometrics, risk and fraud management, and identity-proofing and enrichment solutions.

To learn about how ForgeRock provides continuous protection against fraud using behavioral biometrics and artificial intelligence and machine learning for trust decisions, read the white paper, "Reduce the Total Cost of Fraud: Apply Intelligent Access to Your Anti-Fraud Initiatives."

Supporting Industry Best Practices

Government agencies handling benefits claims can use ForgeRock and its Trust Network solutions for identity proofing and strong authentication to help improve efficiencies and reduce the risk of fraudulent claims. ForgeRock adheres to industry best practices for identity proofing and authentication, such as those defined by the U.S. National Institutes of Standards and Technology (NIST). The National Institutes of Standards and Technology (NIST) Special Report 800-63-A provides requirements for how applicants can establish their identities and become enrolled as valid subscribers within an identity system. These requirements consist of identity assurance levels and authentication assurance levels.[5]

Identity Assurance Levels

The NIST guidelines specify three different identity assurance levels (IAL):

- IAL1 has no requirement to link the applicant to a specific real-life identity. This is known as "self-asserted identity," such as when an applicant registers online with a name and an email address.
- IAL2 requires a claimant to provide real-world proof of identity, such as through a government-issued identification (ID). This can be done either remotely via a software-based identity proofing solution or when presented physically to authorized personnel. As the applicant registers for an account, they must upload a valid government ID (state ID card, driver's license, or passport).
- IAL3 requires an applicant to be physically present, and their identifying attributes must be verified by an authorized and trained representative.

Two common identity-proofing solutions that ForgeRock government agencies customers are using come from third-party vendors, Onfido, or ID.me, and both conform to NIST IAL2.

The ID.me solution also has an option to establish a live video call between a citizen claimant presenting their identification and an authorized representative, closely approaching the requirements of NIST IAL3.

Authenticator Assurance Levels (AAL)

The NIST guidelines also specify what is known as authentication assurance levels (AAL).

- AAL1 protects low-risk content and requires the subscriber to control either a single-factor or a multi-factor authenticator bound to a citizen's account. It also mandates the use of secure communication protocols.
- AAL2 requires a high level of confidence that the citizen owns the authenticator tied to their account. Compliance with AAL2 requires a combination of both knowledge (password, PIN) and cryptographic software or hardware.
- AAL3 requires very high confidence that the subscriber controls the authenticators bound to their account, including proof of possession and control of a hardware-based authenticator as well as an impersonation-resistant authenticator. AAL3 requires two authentication factors and communication must be performed over approved cryptographic protocols.

As a citizen goes through an identity-proofing flow when signing up for an account, they can also register with a multi-factor authentication device such as their laptop or mobile phone with built-in biometrics, a hardware token such as a YubiKey, or a mobile phone authentication app. AAL3 is typically not required for citizen-level authentication and access.

Combining identity assurance at IAL2 or IAL3 at registration with authenticator assurance at AAL2 or AAL3 assures that the citizen claimant is valid. A fraudster is much less likely to gain access to citizen accounts using stolen usernames and passwords because they cannot present the required authenticator(s).

To learn more about the NIST Guidelines and how to achieve recommendations for identity assurance and authenticator assurance, read the white paper, ForgeRock and NIST Special Publication 800-63-3.

Identity-Proof Your Citizen Journeys

You can design identity proofing registration and authentication journeys, also known as "trees" in ForgeRock Intelligent Access using an identity-proofing solution to verify a claimant's identity as they sign up for services. You can integrate your agency's identity-proofing solution into ForgeRock using our free, pre-built, tested, and always updated partner integrations that are available in the ForgeRock Marketplace. There is no custom coding required in order to integrate them into your ForgeRock environment. Simply follow the instructions, and download and install them in ForgeRock Intelligent Access.

While each solution has its particular features and benefits, the authentication journeys in ForgeRock Intelligent Access are basically the same. The parameters for setting up registration and connecting the solution with ForgeRock are different, however, as they use different authentication and authorization protocols.

Onfido

Onfido uses AI-based technology to assess whether a user's government-issued identity, such as a driver's license or passport, is genuine or fraudulent. It compares the uploaded ID against the claimant's live facial biometrics such as a self-portrait ("selfie") image from the citizen's mobile phone, or a short video, to ensure the identity matches the person registering. Once a citizen has established their identity with Onfido, each time they authenticate, their identity will be confirmed via biometric authentication from their registered mobile device using fingerprint or facial recognition.

ID.me

ID.me is a federally certified identity-proofing service used by several government agencies to verify citizen identity for benefits claims. It verifies identity through biometrics, artificial intelligence, and real-time access to trillions of citizen records in authoritative data sources. Citizens can sign up for an ID.me account for individuals on the id.me website using an email address and password or through a social identity provider. ID.me integrates with ForgeRock via SAML 2.0. Once a citizen verifies their ID.me account through email verification, they can use the same email account to register for government services.

To verify their identity on the government services portal, applicants must upload a government-issued ID using a self-service web process, and take a self-portrait ("selfie") using their mobile device. They can also opt for a "Virtual In-Person Proofing" visit with a U.S.-based employee if the ID.me service cannot validate their identity – for example, if the citizen is newly naturalized, is a young adult, or has no credit history.

Configure ForgeRock Intelligent Access for Registration and Identity Proofing

1. After downloading and installing the Onfido or ID.me package from the ForgeRock Marketplace, open the ForgeRock Platform Intelligent Access User Interface.

2. Create a New Journey, name it according to which solution you're using (Onfido or ID.me), and choose the Users Identity Object.

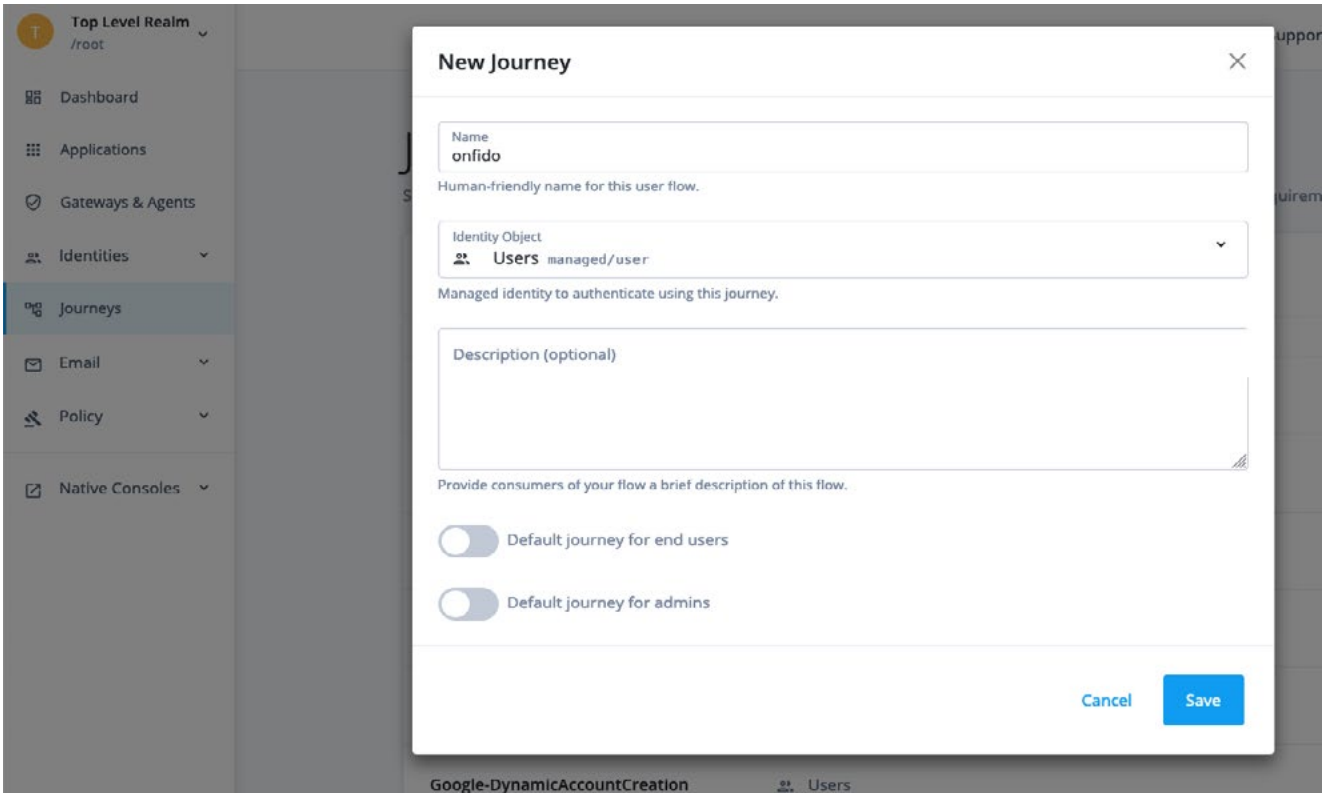

Figure 2: Create a New Journey for Users (Citizens)

3. From the left panel, search for each of the nodes for your particular solution as shown in the figure below, and drag them into the Intelligent Access configuration palette.

   In *Figure 3, Onfido Registration Journey*, the Identify Existing User node is pre-configured to identify a user who has already registered with the Onfido service.

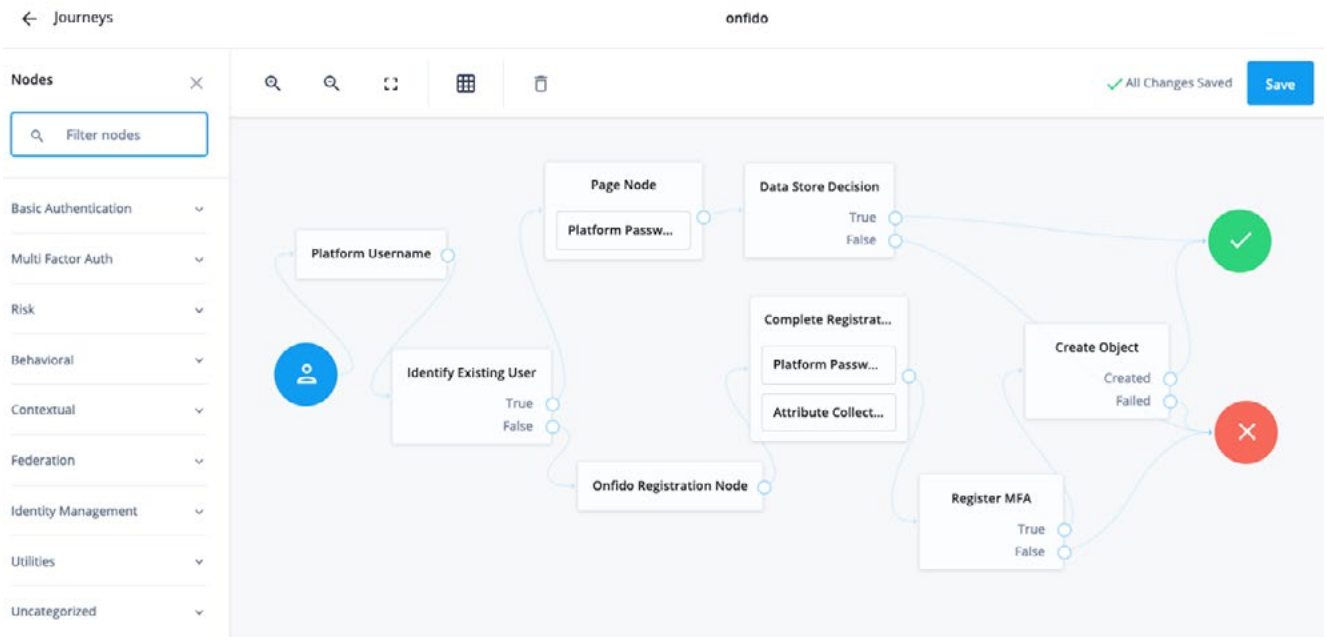

Figure 3: Onfido Registration Journey

In Figure 4, ID.me Registration Journey, the ID.me Registration node checks if the user has already registered an account on the ID.me website.

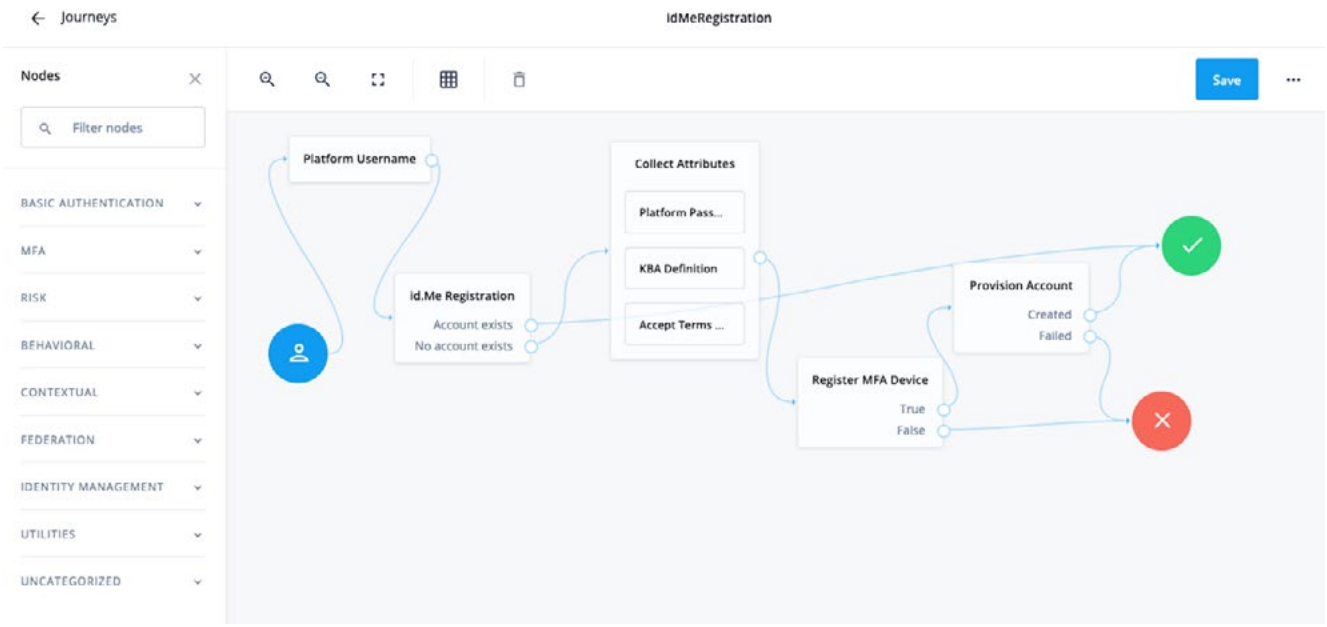

Figure 4: ID.me Registration Journey

4. Configure the connection between your identity-proofing service and ForgeRock:

   For Onfido, configure the registration node with an API token and secret, and enable Just in Time Provisioning.

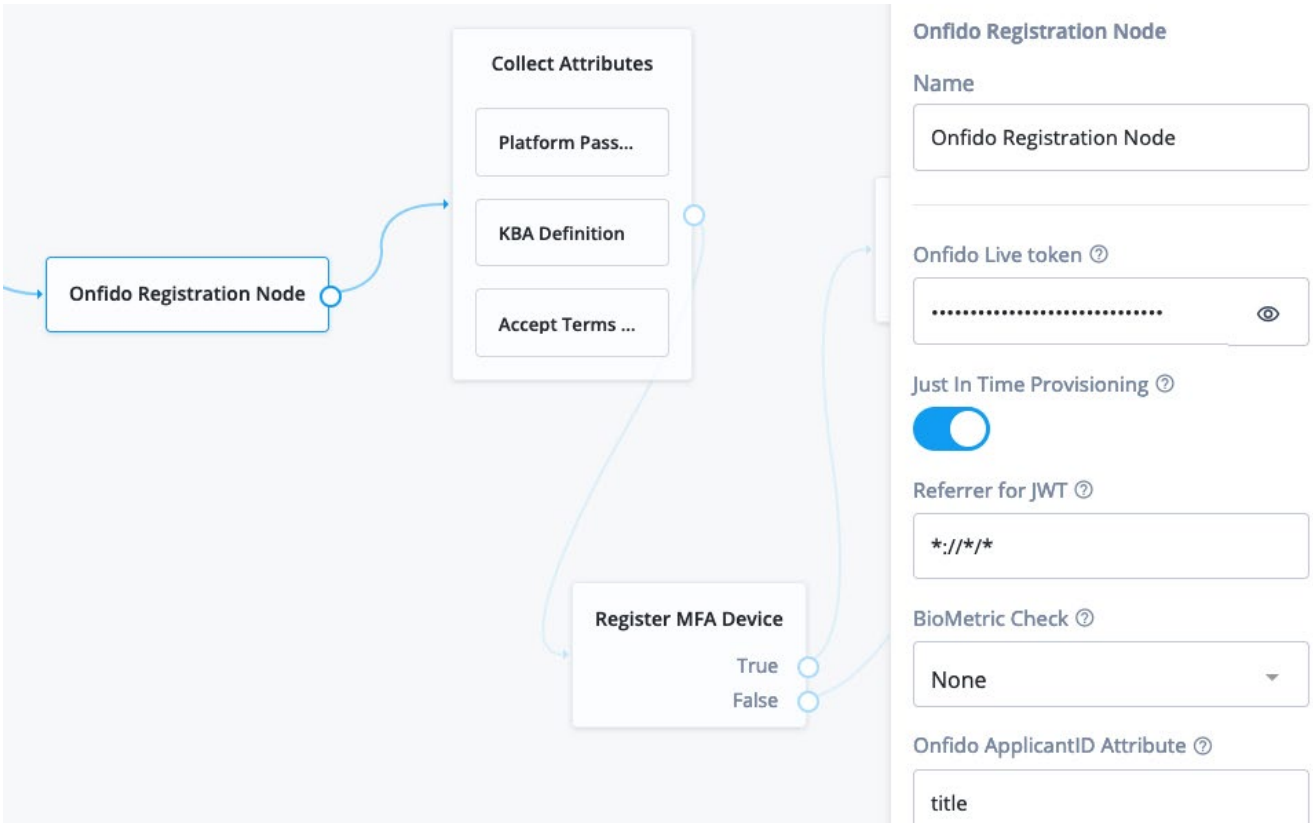

Figure 5: Configuring the Onfido Registration Tree Attributes

For ID.me, which uses the SAML 2.0 protocol, follow the instructions on the ID.me page in the ForgeRock Marketplace to configure the attributes and also install a SAML2 Auth Tree Node.

Figure 6: ID.me Registration Tree Details presents how to configure the SAML2 Authentication attributes to work with the ID.me registration node.

5. Review attribute mappings (see the documentation from the ID.me page in the ForgeRock Marketplace) and Save.

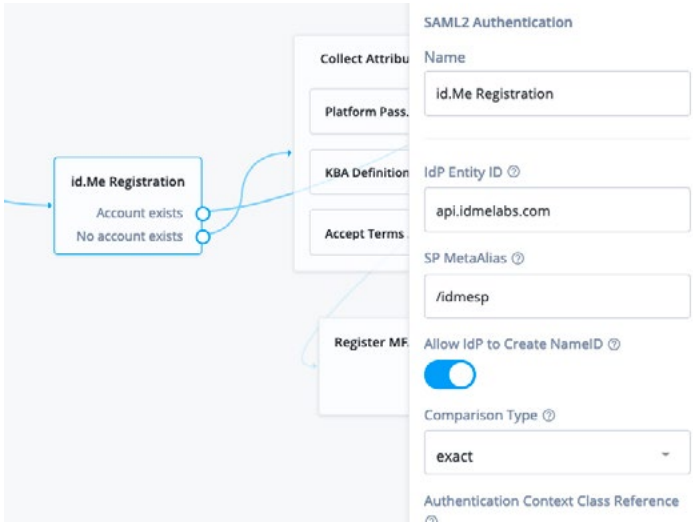

Figure 6: ID.me Registration Tree Details

Configure an Authentication Journey

Once a citizen is registered for a new account using either Onfido or ID.me, they must also have a way to authenticate themselves into your online government services portal using a trusted strong authentication factor.

As you can see in Figures 7 and 8 below, the authentication tree for either Onfido or ID.me looks the same. However, you must select the correct authentication nodes for the solution you are using. Search for them by name in the Nodes search window on the left, and wire them together as follows:

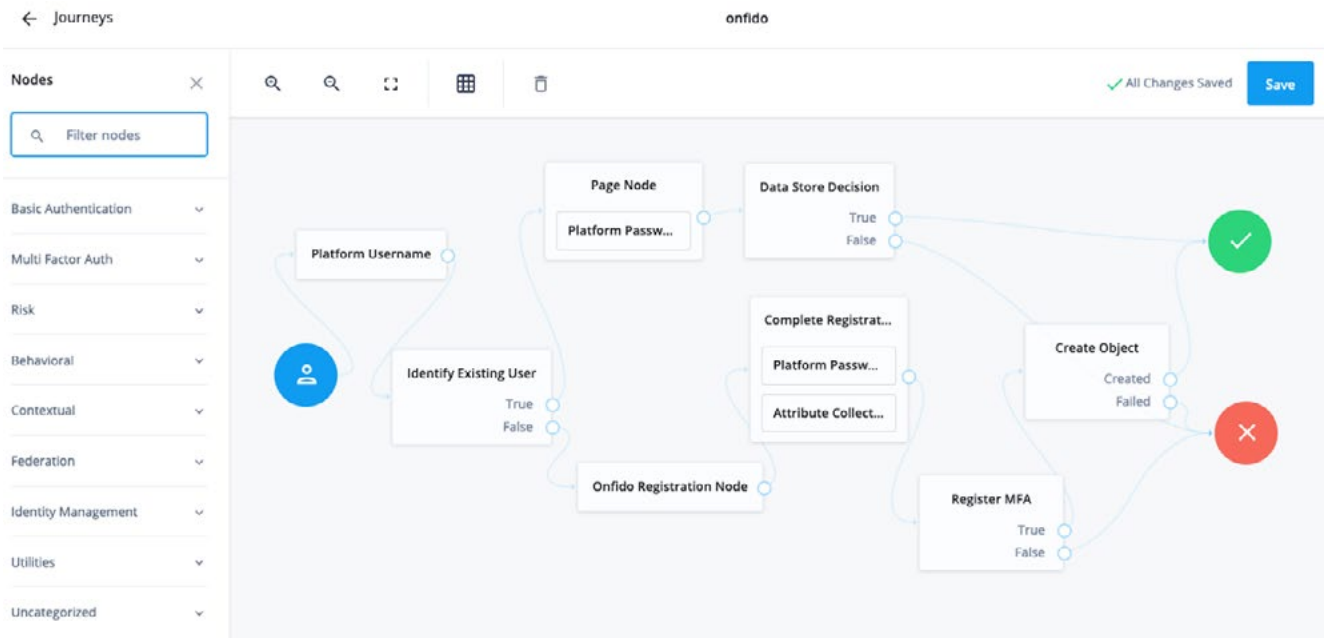

Figure 7: Onfido Authentication Tree

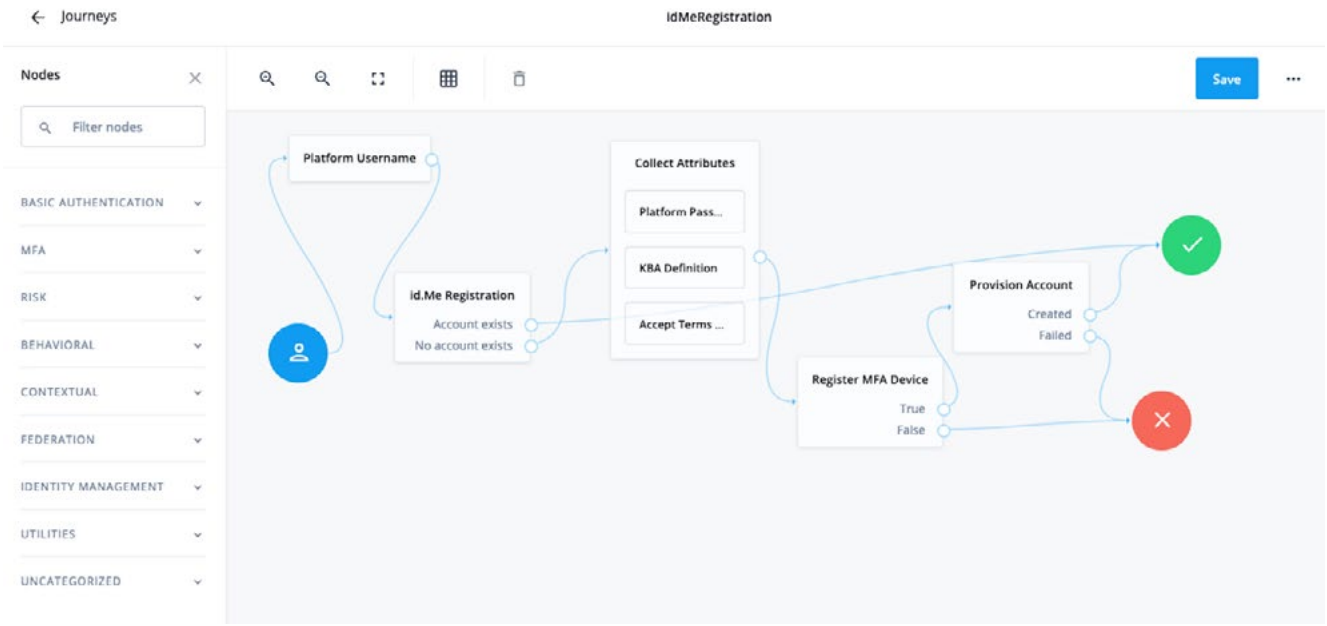

Figure 8: ID.me Authentication Tree

If the citizen has already registered their account with the Onfido or ID.me service, they can complete the authentication using their registered multi-factor authentication device.

If they haven't yet registered with the identity proofing service, they can complete their authentication using the platform password. However, when they need to perform a transaction that requires a higher level of assurance (IAL2 or higher), you can require them to register through the identity proofing service.

Conclusion

You can reduce the impact and frequency of fraudulent government benefits claims by using modern IAM as a front-end to your legacy, on-premises systems. With modern IAM from ForgeRock, you can incorporate modern identity-proofing directly into the registration and authentication flows at an assurance level that can stop fraud based on fake account sign-ups and stolen credentials.

Combine ForgeRock's modern IAM with industry-leading identity-proofing solutions to provide secure access without impacting the citizen experience. ForgeRock is an effective part of your agency's security initiatives, providing continuous assurance of citizen identity throughout their interactions with your systems.

[1] AP News, "Fraud overwhelms pandemic-related unemployment programs," https://apnews.com/article/pandemics-health-coronavirus-pandemic-asia-pacific-ohio-b651def05a8a049637c4a1047f788631

[2] https://www.theguardian.com/society/2021/may/13/record-levels-benefit-fraud-universal-credit-first-year-pandemic-in-britain

[3] https://www.euronews.com/2020/07/10/coronavirus-france-investigating-massive-fraud-of-temporary-unemployment-scheme

[4] https://www.cnbc.com/2020/04/06/new-jersey-seeks-cobol-programmers-to-fix-unemployment-system.html

[5] National Institutes of Standards and Technology NIST Special Publication 800-63 Revision 3, "Digital Identity Guidelines," https://pages.nist.gov/800-63-3/sp800-63-3.html