ForgeRock

INTELLIGENT ACCESS SERIES

Introducing

ForgeRock Intelligent Access

Overview

Modern security demands that organizations defend against data breaches from any location and any type of user: their own workforce, partners, customers, and internet-connected things. To address these risks, Gartner's **Continuous Adaptive Risk & Trust Assessment (CARTA)**[1] security model recommends that organizations adopt an access management practice that enables continuous visibility and assessment of security decisions, established through multiple attributes, using the broadest and deepest insights to assess the risks of users interacting with their digital channels.

Forrester's **Zero Trust**[2] model suggests that there be no inherent trusted (versus untrusted) networks, users, devices, sessions, data, or services. Trust must be granted based on multiple contextual, behavioral, and risk-based signals. It is no longer sufficient to use one or two-factors for authentication, even if these are strong factors. Additional signals based on context, behavior, and risk (adaptive authentication) must also be considered.

As an Identity and Access Management (IAM) leader in your organization, it is critical that you consider how to incorporate these CARTA and Zero Trust principles while continuing to provide the secure and frictionless user experiences that your customers demand.

In this white paper, you will learn about the features and benefits of ForgeRock Intelligent Access, including user journeys, nodes, and the Trust Network. ForgeRock Intelligent Access is the world's only dynamic orchestration and intelligence engine that lets you design and manage seamless and secure user journeys for all your applications and services.

> Without writing a single line of code, you can use the Intelligent Access drag-and-drop interface to design, configure, measure, and adjust multiple user journeys.

Intelligent Access uses digital signals that provide continuous information about the user's device, context, behavior, choices, analytics, and risk. ForgeRock Software Development Kits (SDKs) provide even deeper insights into and data about the devices that access your systems, so you can define dynamic and granular access and authorization policies.

Using Intelligent Access, you will gain deep visibility into how people and devices interact with your applications and services. This will go a long way toward helping you increase security, improve the user experience, and deliver dynamic personalization.

Expanded Features

ForgeRock Intelligent Authentication is now known as Intelligent Access. The name has changed to reflect a feature set that extends beyond authentication to include additional functionality. We'll explore these in more detail in subsequent white papers. The extended features of Intelligent Access include:

- **ForgeRock Go:** ForgeRock's implementation of the FIDO2 WebAuthN standard enables users and devices to register and authenticate without usernames and passwords.

- **Intelligent Self-Service:** New capabilities make it easy to design journeys for users so they can manage their own preferences for registration, self-service password resets, account recovery, progressive profiling, and profile management.

- **Anti-Fraud:** If your goal is to reduce the total cost of fraud (TCOF), you can evaluate risk factors and detect fraudulent access using Intelligent Access trees, which integrate with third-party anti-fraud solutions offered in our ForgeRock Trust Network. You can combine these integrations with ForgeRock's transactional authorization capabilities to mitigate fraudulent transactions and reduce the total operational cost of ownership.

- **Secure Identity for Internet of Things (IoT):** This capability supports identity management and access journeys for internet-connected devices ("things"). It offers flexible onboarding for both smart and constrained things into Intelligent Access and full management of their identity lifecycle – provisioning, activating, de-activating, and discarding.

Design Powerful User Journeys

At the heart of ForgeRock Intelligent Access is its drag-and-drop visual interface that enables you to design modular, orchestrated, and personalized user journeys known as "trees." Beneath the surface of this drag-and-drop interface lies the most comprehensive and powerful IAM platform in the industry.

Trees

A user journey is the beginning, middle, and end of a user's interactions with your systems. It can start with a login or registration page and continue through various interactions with your identity store, website and applications. ForgeRock calls these journeys "trees" because a user journey can branch out into multiple paths and decision points.

> A tree created in Intelligent Access is the visual representation of a user journey.

Intelligent Access trees support user journeys for many different business use cases, including user registration, authentication and self-service. A Registration tree prompts a user to create an account, set their default credentials, register devices and set multiple preferences. An Authentication tree collects credentials, checks these credentials against an identity store, and sets pass/fail outcomes. A Self-Service tree enables users to request a password reset, manage their own profile information, and set their preferred devices. Intelligent Access supplies many pre-built trees that may be customized or used as-is.

Nodes

Intelligent Access Nodes are small units of work that comprise a user journey. Each node has a single purpose: to define specific actions taken during a user journey. ForgeRock Intelligent Access has many pre-programmed nodes that detect digital signals, make decisions, and direct the user journey. You can combine nodes to collect signals that you configure in Intelligent Access to determine if a user's access levels should be modified during a session. These signals are stored in a session token that provides information about the user session to downstream applications.

Here's an example of how you would construct a user journey: One node collects a username, while another sends a push notification to a device. Another node pulled from the ForgeRock Trust Network calls out to a third-party fraud detection service to inform you about the authenticity and security of the user and their actions during the session.

You can connect these nodes together in a logical order in the Intelligent Access visual designer, like you would using flowcharting software. You can create sophisticated yet user-friendly experiences by linking nodes together, creating loops, and nesting nodes within the tree.

Types of Nodes

Intelligent Access has numerous built-in nodes that are included in the platform:

- **Basic Authentication Nodes** are used for basic user journey functions, like collecting usernames and passwords, along with Decision Nodes for authentication against identity stores such as LDAP, and Kerberos for desktop single sign-on (SSO).

- **Multi-factor Authentication Nodes** are for designing trees with multi-factor authentication capabilities, such as passwordless web authentication and push authentications.

- **Behavioral Nodes** adjust the behavior of authentication trees. The Increment Login Count Node works with the Login Count Decision node to trigger an action when a user's successful login count property reaches a specified number. For example, you can set the login count to "5" and direct the login count decision node to fail after five bad authentication attempts.

- **Risk Management Nodes** examine the perceived risk associated with the authentication and take action in response. There are nodes to increase or decrease the current authentication level, compare the current authentication level value against a configured value, or add CAPTCHA support to authentication trees. An Account Lockout Node locks or unlocks the authenticating user's account profile. Use this lockout node as the final result of a "fail" in the Login Count Decision Node.

- **Contextual Authentication Nodes** examine the context of an authentication and react in various ways – such as collecting and validating certificates and gathering, matching, and storing metadata about the device the user is authenticating with.

- **Device Nodes** are new in Intelligent Access and are contextually aware. They identify the devices a user logs in from, store device profiles for authentication without passwords, match a device to a known location, set geo-fencing around a device, and notify the system if the device has been compromised. The ForgeRock Intelligent Access web or mobile SDKs detect device hygiene (example: whether a device is using the latest OS or is jailbroken) and anomalies like impossible travel distance between where a login attempt occurs and the location of a trusted second factor device. For example, it will detect that an authentication attempt was made from a public coffee shop network in Las Vegas and that the user's registered mobile device is with the user in Singapore, making authorized access unlikely.

- **Federation Authentication Nodes** provide trees with federation capabilities, such as OAuth 2.0, OpenID Connect social authentication, SAML2, and account provisioning.

- **Identity Management Authentication Nodes** perform identity management tasks during a user journey, such as mapping anonymous users to a session, collecting user preferences for authentication, and setting preferences for social authentication.

- **Utility Authentication Nodes** include various utilities (tasks) that are triggered in a user journey, such as sending an address verification email to the user. You can also design Page Nodes that combine multiple tasks on a single page, such as requiring a user to enter their username and password and choose a multi-factor authentication (MFA) factor.

- **Nodes for IoT:** ForgeRock supports authentication and registration of IoT, including IoT devices, services, and an IoT Gateway.

There are many additional nodes available in the ForgeRock Trust Network and ForgeRock Marketplace that have been designed by partners and other contributors.

Building a Simple Tree

The basic building blocks of an authentication tree include the following:

- A **credential collection node** – e.g. for username and password, biometric, or hardware token. Use a Page Node to combine credential collection nodes together so that the user sees all elements on a single page.
- A **decision node** to check the authentication attempt for validity. For example, a Data Store Decision node can check a username and password against a directory. Another node can check browser type, whether a policy threshold is met, and other factors.
- An **outcome** defined as success/failure, true/false – or more arbitrary and dynamic outcomes.

Below is an example of an authentication tree with nodes to collect username and password. The Data Store Decision Node with True and False outcomes will allow the user access if they successfully authenticate against the data store, or it will return them back to the username and password page if authentication fails.

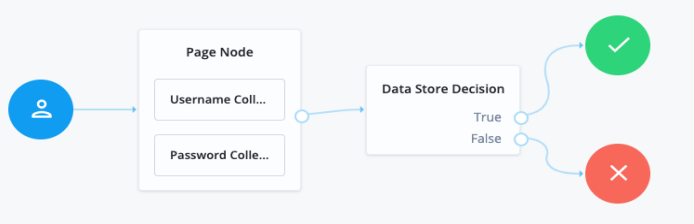

Figure 1: A Simple Authentication Tree

You can follow a similar process to design more complex authentication, registration, and self-service trees. You can find many example trees in the documentation, through the Trust Network and from Marketplace contributions from ForgeRock users.

Advantages of Using Intelligent Access to Build User Journeys

The Intelligent Access trees framework future-proofs your organization's authentication and access user journeys. Your teams can design consistent user interaction across modern and legacy applications and unify identity silos. You can gain more visibility into how users interact with your environment so you can deliver dynamic personalization and targeted risk reduction at every stage – from registration, authentication, user self-service, and managing privacy and consent options. Intelligent Access trees can meet virtually any business-related authentication and access requirement.

Below are just a few of the added benefits of Intelligent Access, along with some example trees for specific use cases. Note that any example trees are representations of how you could configure a user journey. Keep in mind you will likely need to make some adjustments to meet the specific requirements for your environment and use cases.

Save Time and Effort

Intelligent Access trees are a framework for building out user journeys using "clicks not code" for most use cases. Instead of designing user journeys on a per-application basis, you can design journeys once and enable them globally. Customers report that they are designing each user journey in a single session instead of spending weeks coding, testing, and re-coding the various integrations.

Reduce Customer Friction and Abandonment Rates

ForgeRock Intelligent Access reduces the friction that customers and workforce experience with account registration and authentication. Many times, users attempting to start a trial of a service encounter a lengthy registration page and ultimately abandon the site. With Intelligent Access, you can create simple and streamlined registration trees that give users access to

ForgeRock Intelligent Access takes into account the full context of how a user interacts with the system and monitors access continuously.

what they want, and gather information about the user experience.

Even before the initial authentication, Intelligent Access determines a number of user attributes, performs ongoing risk calculations, and alters the level of access or triggers the user to perform additional authentication steps for higher-risk transactions. By reducing friction and increasing security with Intelligent Access, you can:

- Know your audience and create exceptional user journeys at every stage of the user lifecycle.
- Provide customers with a less intrusive login journey, improving their relationship with the service.
- Leverage a single authentication and access model for all systems.
- Use built-in artificial intelligence (AI) to model the user session and remove more friction as confidence in the user session increases.

Require Step-Up Authentication When Necessary

Sometimes a bit of extra friction is a good thing – and it's something users have come to expect. Intelligent Access requires step-up authentication when necessary. For example, if a workforce user hasn't logged in recently, has deleted their cookie history, is logging in from an unusual location or network, or has lost their laptop or mobile device, they should expect to provide additional authentication before being granted access to corporate resources. Without any known trust signals, an authentication or access attempt could very well be from an attacker.

Intelligent Access is designed to set up trust signals for user accounts and provide users with choice and control over how they register and authenticate. During self-service registration, users may choose which MFA method to use. Enabling choice helps reduce any perceived friction because users become invested in their own security.

The tree in **Figure 2** gives the user five MFA options. Depending on the option selected, the subsequent nodes are activated until an authentication Success or Failure is generated.

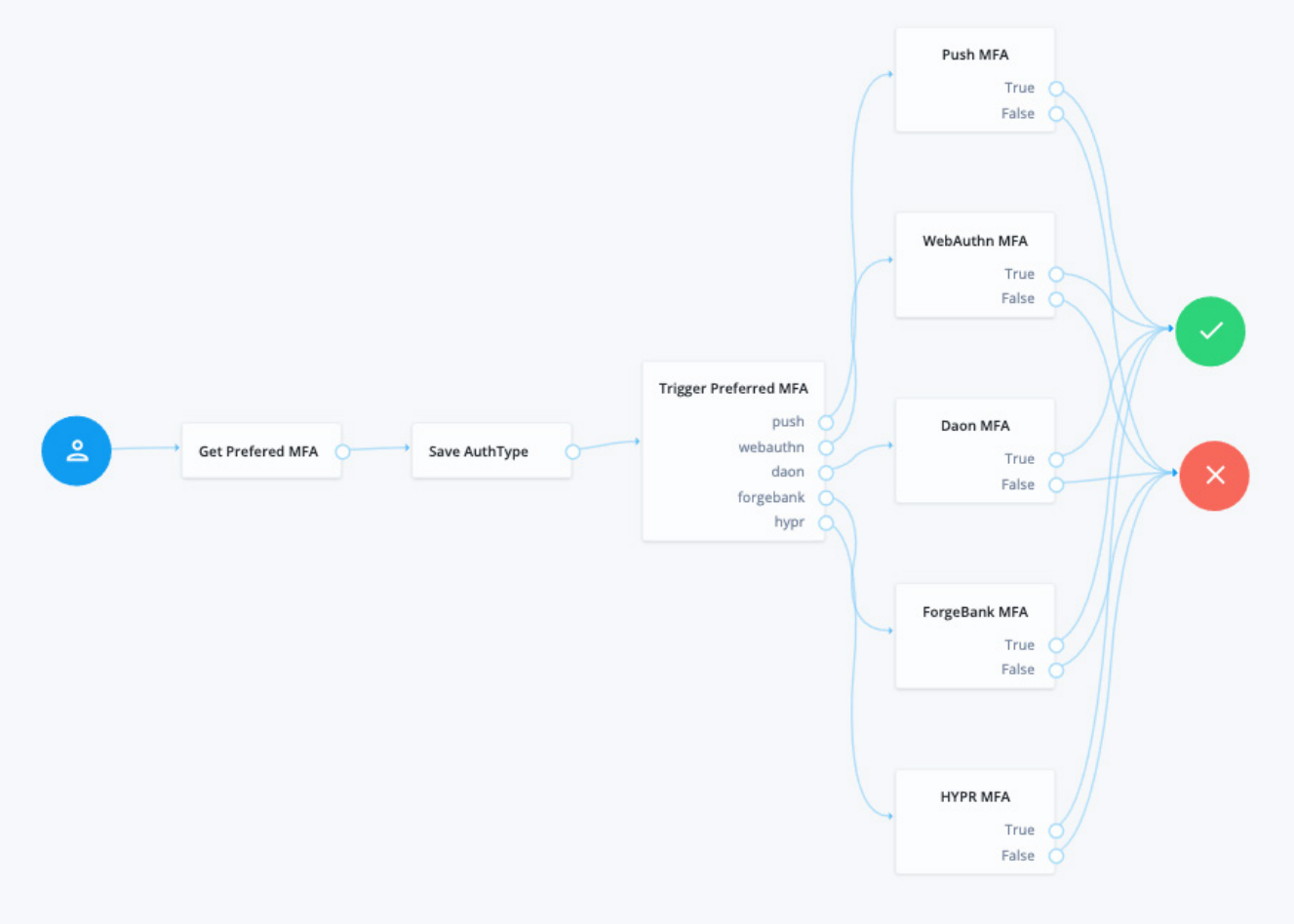

Figure 2: A Step-Up Authentication Tree

Analyze User Login Attributes

Intelligent Access includes user login analytics tools that you can use to design multiple authentication journeys and test the effectiveness of each. By analyzing how users authenticate, you can build user journeys that increase user adoption rates and improve the customer experience, and automatically redirect suspicious users for further monitoring.

In **Figure 3**, an IP Address Decision Node captures users' IP addresses when they log in. You can configure ranges of IP addresses to block and prevent authentication by users arriving from these source IP addresses.

The third node on the right captures the authentication based on users' geographic region. Then, a node counts the number of logins from each geographic region, then, whether the login is from a mobile device. The Browser Collector Node checks the browser types and sets decision nodes to mark browsers as trusted or untrusted.

All of this information is stored in a session token that downstream applications can use to decide whether or not to accept traffic based on any of these criteria. These signals improve security and can also optimize user experiences (example: users logging in from Spain using a mobile device are redirected to mobile-optimized Spanish language pages).

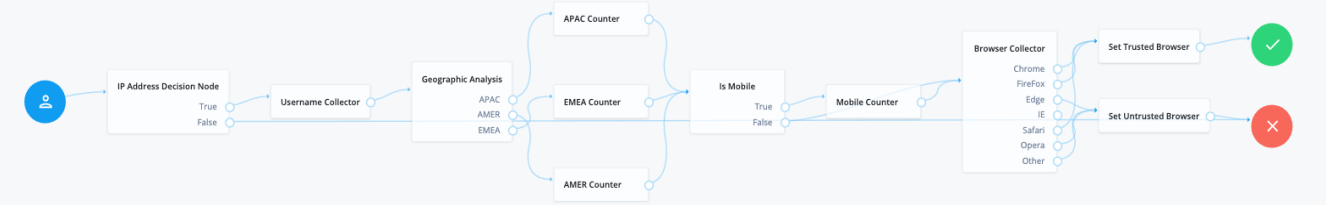

Figure 3: User Login Analysis

Improve Service Level Agreements

Intelligent Access facilitates compliance with service level agreements (SLAs) for third-party services by measuring the time it takes for the login journey and the time it takes for the service to respond.

The Intelligent Access Timer Start and Timer Stop nodes may be dropped into an authentication tree to measure how long it takes for users to authenticate.

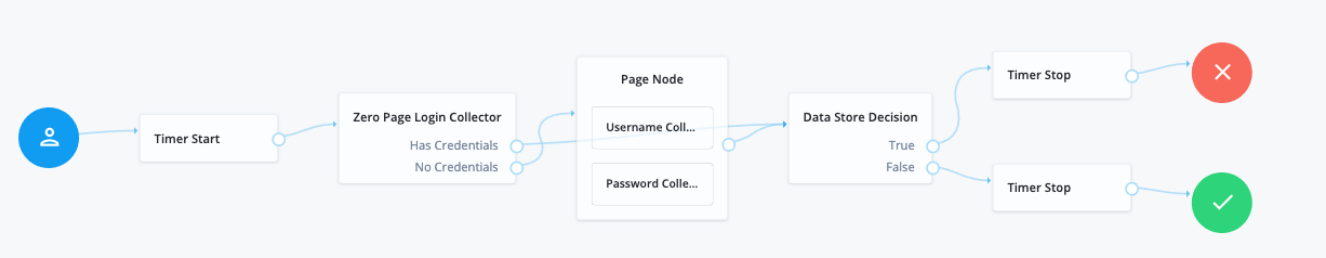

Figure 4: Timer Nodes Measure How Long It Takes for a User to Authenticate

You can nest a sub-tree with nodes to extract information, such as where users are logging in from, the number of registration abandonments versus successful authentications, and how much time each authentication journey takes. You can set up two different flows as an A/B test and push a small percentage of traffic to each flow to analyze it for usability with different audiences and regions, latency, and more. You can also expose the data via Metric Keys.

Intelligent Access gives you the power to design the best, most robust user journeys and continually improve them over time.

Figure 5: Metric Keys Display Timer Data

Facilitate Transactional Authorization

Transactional authorization improves security by requiring a user to perform additional authentications every time they want to access a resource that's protected by an authorization policy.

You can easily tailor the authentication flow to incorporate multiple signals and enforce step-up authentication based on a policy trigger. Unlike privilege elevation, transactional authorizations grant users access to a protected resource only once. Each additional authorization requires another authentication.

Authorization policies can be triggered contextually based on what users or customers have defined. For example, a bank customer may set up a $100 threshold for automated online bill payments. Any bill below that amount is paid automatically, and any bill above $100 triggers a push notification to the customer's mobile device to allow or deny the transaction.

In a workforce scenario, an organization could require a user to respond to a push notification on their mobile device before allowing them to access applications with sensitive data.

The figure below shows a transaction policy for authenticated users. The policy invokes an MFA response based on the user-defined transfer policy. The script shown in the Environments field invokes a transaction authorization tree that prompts for an MFA challenge. The policy relies on the user-defined threshold, so it will only trigger the Transaction Authorization tree (**Figure 7**) if the user's threshold is exceeded. This type of transaction policy is aligned with the CARTA principle of continuous authentication and fine-grained authorization decisions.

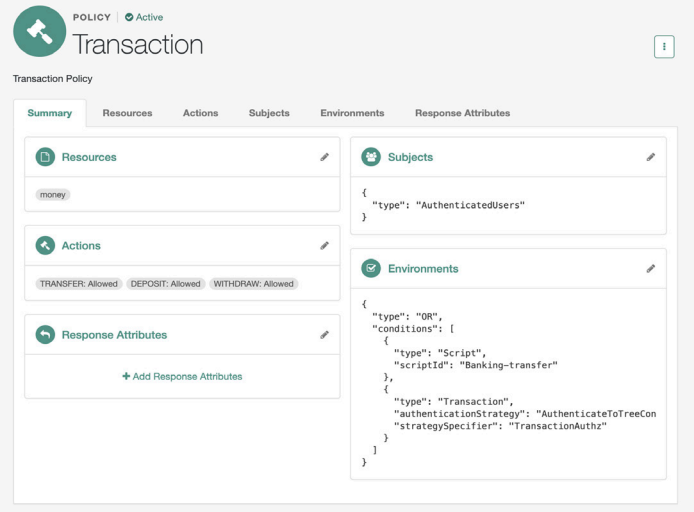

Figure 6: Transaction Policy for a Banking Transfer

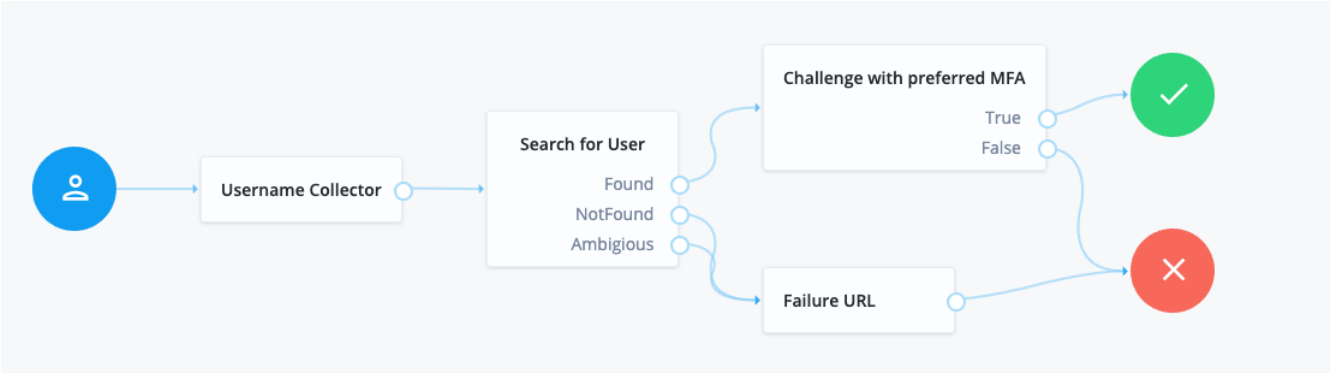

Figure 7: Transactional Authorization Challenge With Preferred MFA Method

Extend and Customize User Journeys

Extensibility is a key feature of the ForgeRock Identity Platform. While you can design most user journeys using built-in nodes and the drag-and-drop user interface (UI), you'll inevitably encounter situations that require you to customize journeys to meet your specific access needs.

ForgeRock Intelligent Access supports custom business logic with Scripted Nodes. Scripted Nodes invoke lightweight scripts that make calls out to REST-based services. In many cases, this is sufficient for integrating basic authentications. For example, an insurance company may need to validate a user's insurance policy number before authorizing a transaction. You can write a Scripted Decision Node using JavaScript or Groovy that validates the insurance policy number stored in the user's session before authenticating the user. You can also integrate these Scripted Nodes into your homegrown applications using the ForgeRock web or mobile (iOS or Android) SDKs.

Figure 8 shows an example of how a financial services institution would write a script to capture native device data when a user registers for their service. **Figure 9** shows how that Scripted Node (second from the left) fits into a registration tree.

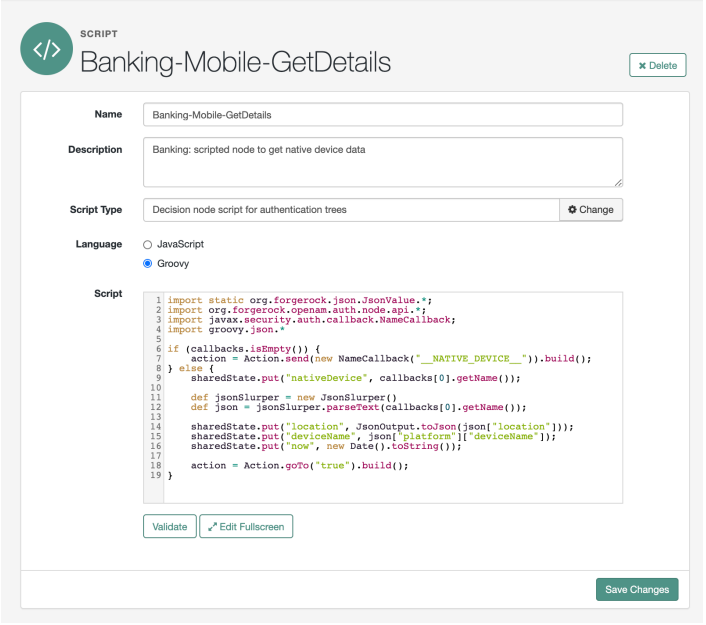

Figure 8: Script for Capturing Mobile Device Details

For deeper integrations with non-standard or unsupported third-party services, you can also write your own Custom Nodes to perform identity validation, authentication, risk assessment, or assurance.

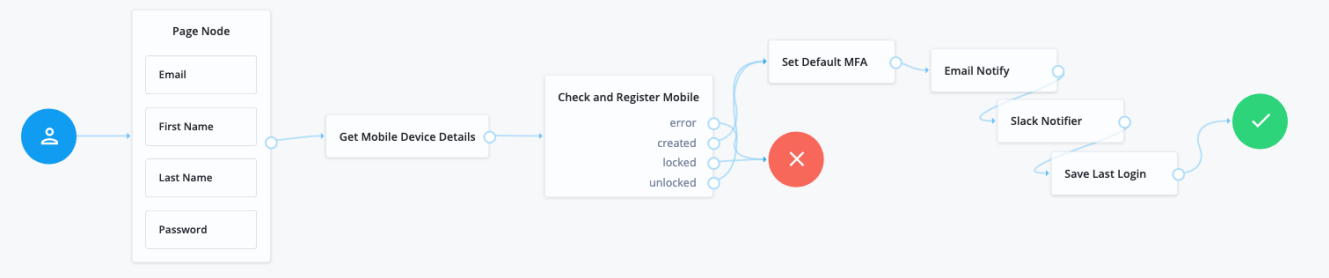

Figure 9: Example Banking Tree with Scripted Node

The ForgeRock Trust Network

Intelligent Access is easy to use, extensible, and customizable. In addition to the nodes, you can access a vast array of solutions through ForgeRock's ecosystem of third-party technology partners. There are over 80 pre-integrated nodes in the ForgeRock Trust Network that have been tested and validated by ForgeRock, including nodes for strong authentication, fraud and risk management, behavioral biometrics, and identity proofing.

In addition to the nodes available with the ForgeRock platform and from the ForgeRock Trust Network, there is a wide range of community-contributed nodes available in the ForgeRock Marketplace. The ForgeRock Marketplace is a central store for nodes that are not shipped in the product or part of the Trust Network.

Conclusion

ForgeRock Intelligent Access is a powerful orchestration platform that makes it possible for you to design flexible user journeys that support complex, fine-grained decisioning and incorporate multiple signals and analytics at every point of the user journey.

The result is a stronger security landscape that mitigates identity-related data breaches and fraud, while offering personalized and friction-free access to your users.

[1] https://www.gartner.com/en/webinars/3891406/the-7-imperatives-of-continuous-adaptive-risk-and-trust-assessme

[2] https://go.forrester.com/blogs/category/zero-trust-security-framework-ztx/