OH|ID NEXT BRINGS POWER TO THE PEOPLE

Ohio's Identity Program takes it to the NEXT level with agency self-service tools and user account transparency

Category: Cybersecurity
State: Ohio

Contact: Katrina Flory, Interim State Chief Information Officer, Department of Administrative Services, State of Ohio; katrina.flory@das.ohio.gov

Project Initiation and End Dates: January 2020 – August 2020

Executive Summary

The Ohio Digital eXperience (ODX) was the first iteration of the State of Ohio's continuous efforts to be a leader in the areas of digital identity, security and privacy, and an intuitive user experience. That goal was built upon and rebranded as Ohio's Identity system (OH|ID). Beginning in January of 2020, as the world became aware of a global pandemic, efforts began on the third iteration of enhancements – OH|ID NEXT – which brought with it many new self-service tools and user account services. Notable among them:

- Audience Manager, a self-service tool for agencies to manage role-based access controls for their web-based applications.
- A secure Application Programming Interface (API) that allows agency applications to interact with Audience Manager and maintains a focus on automation, giving agencies the ability for Just-In-Time provisioning of both course-grained and fine-grained permissions within their applications.
- Within the citizen portal, users can opt to complete three levels of identity assurance, including "Basic" (account creation and email verification), "Intermediate" (verified via third-party identity proofing), and "Advanced" (linked to the valid, State-issued ID card on-file with the Bureau of Motor Vehicles, Ohio Department of Public Safety).
- A "Recent Activity" tab displays the geographic location of logins within the past 12 months and whether it was successful. Users can also report suspicious activity.
- A "Devices" tab shows the device used for each login attempt (desktop, mobile, etc.) and device activity for recent logins. The user can name or hide a listed device.

Of all the tools and account services in OH|ID NEXT, Audience Manager has proven to be the most revolutionary. Audience Manager provides agencies the ability to manage roles and access for their applications at the appropriate level within their organization. Anyone granted access to the application can create one of two different audience types for either course-grained or fine-grained access and manage ownership, membership, and (optionally) approvals for access to each of their federated applications. Those audiences can then be queried through a user token or API interface by an application to ensure that once a user is properly authenticated, they are also only getting the content for which they are authorized. Every action is logged back to a central repository, which provides full audit and compliance functionality that meets or exceeds National Institute of Standards and Technology, other federal, state, and accessibility regulations and standards.

OH|ID NEXT: FEATURES & ACCOMPLISHMENTS

- Automates user provisioning and de-provisioning in near real-time
- Expands automated user provisioning and consolidation via industry standard endpoint adapters
- Expanded Multifactor Authentication (MFA) availability
- Validates citizen identities using Experian Identity Proofing
- Securely manages 1.2 million active digital identities
- 345 audiences created via self-service in Audience Manager since Sept. 2020
- 19 agencies actively engaged with Audience Manager
- Completed on-time and within budget during the COVID-19 pandemic as employees transitioned to remote work

Citizens and the State workforce are also empowered to control the security surrounding their accounts. Any change to their account is communicated through their verified email address. Every login attempt and device is listed, and any suspicious activity can be immediately reported, without the user having to navigate to another screen. Agency applications for citizens or state employees can also choose to require Multifactor Authentication (MFA) to further protect against malicious activity from bad actors and protect the sensitive functions of integrated applications through the appropriate use of security controls.

Idea

The landscape of interaction with state governments has continued to move into the digital realm. The COVID-19 pandemic caused a massive shift to these digital interactions as offices closed and in-person transactions were abandoned in favor of remote interactions. Ohio was well positioned to react to this shift as the original

OH|ID project had already provided agencies with an efficient Single-Sign-On (SSO) self-service tool and onboarded several hundred applications. As a result, Ohio citizens and businesses had a unified experience without the need to keep track of separate credentials as they found themselves navigating between applications hosted by different agencies, perhaps for the first time. By utilizing the existing self-service SSO infrastructure, the InnovateOhio Platform (IOP) was able to meet increased demand, and the functions of OH|ID NEXT – specifically, the secure APIs and role-based access controls presented in Audience Manager – allowed both the State and its customers to easily navigate new digital challenges on a secure reliable platform.

Among several major use cases, the Ohio Department of Health (ODH) and the Department of Administrative Services (DAS) were IOP designed, built, tested, provisioned, and deployed several applications in record time to react to the global pandemic. These applications dealt with contact tracing, registering vaccine providers, Personnel Protective Equipment (PPE), and a host of other pandemic activities. Privacy, security, and usability were paramount to the success of these projects as they dealt with Personally Identifiable Information (PII), Health Insurance Portability and Accountability Act (HIPAA) protected information, and other information that could be valuable to malicious actors.

The interagency cooperation led to a rapid continuous improvement cycle that drove regular accessibility and security updates. The result of months of effort and vendor partnership was a platform that improved Ohio's security posture through an API-first mentality, enhanced logging and traceability, and self-service security tools.

Ohio's Digital Identity Capabilities

The OH|ID Application Store provides employees and citizens with a customized dashboard of available and subscription-based applications with an intuitive user view. The view is customized based on role-based principles to ensure an end-user is only displayed what they are authorized to access.

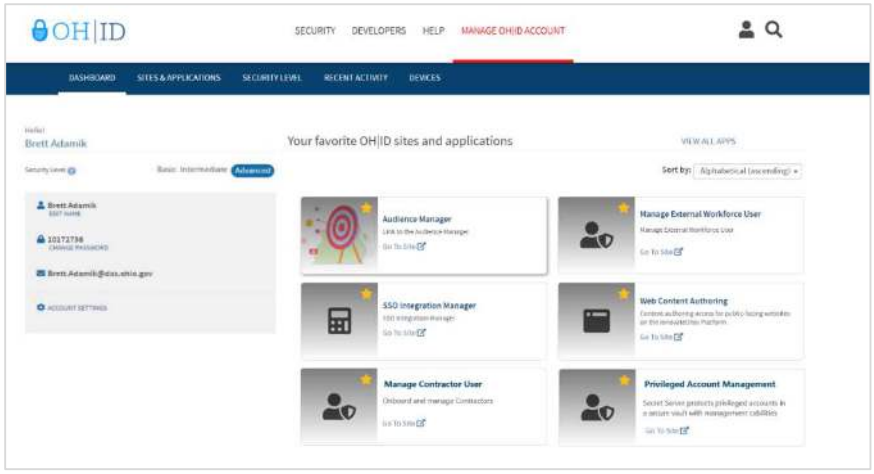

Figure 1: OH|ID NEXT User Dashboard

In addition, agencies can display applications that can be requested through a subscription process, like a mobile app store. Subscription-based apps can be restricted to be visible to certain account types (i.e. state workforce, citizen), and can either have an automatic approval workflow with immediate access, or they can be protected with an approval workflow that sends an automatic request to the defined approvers for that application. All the access controls can be delegated to the appropriate level so that the right people are making the best decisions, and all actions are fully auditable to ensure compliance and integrity.

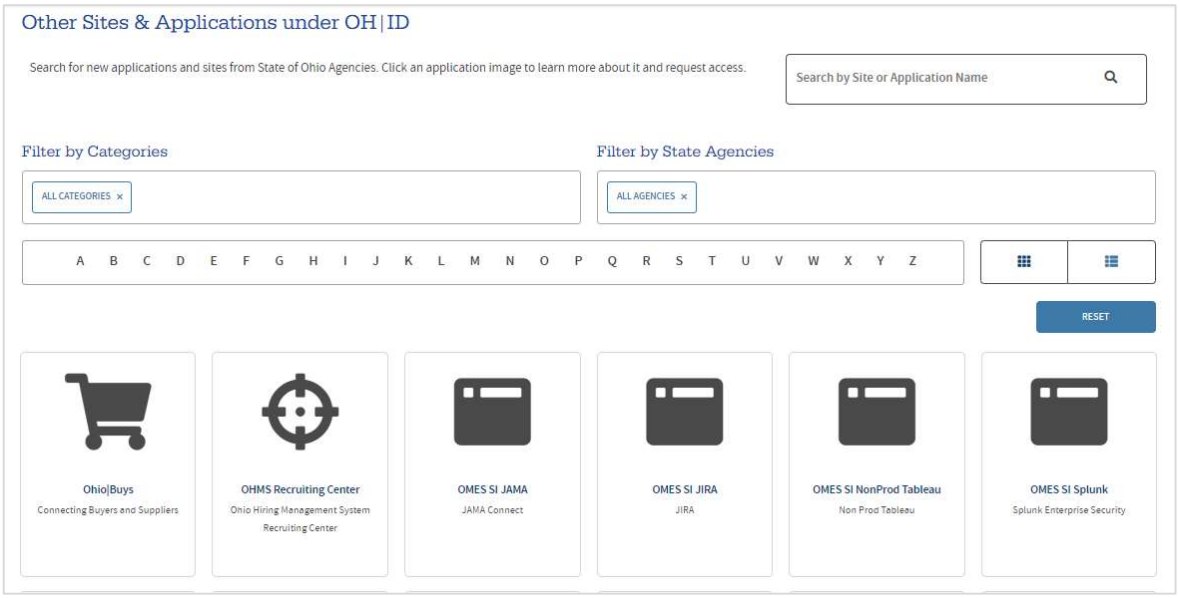

Figure 2: OH|ID NEXT Application Store

The tool that facilitates this automation, Audience Manager, gives authorized parties the ability to make user groups – called "Audiences" – through manual selection or automatically, through rule-based logic. These audiences are given "Owners," who can modify the audience, "Members," who are the audience, and, optionally, "Approvers," who serve as gatekeepers of access for sensitive applications or those that require a manual step before allowing access.

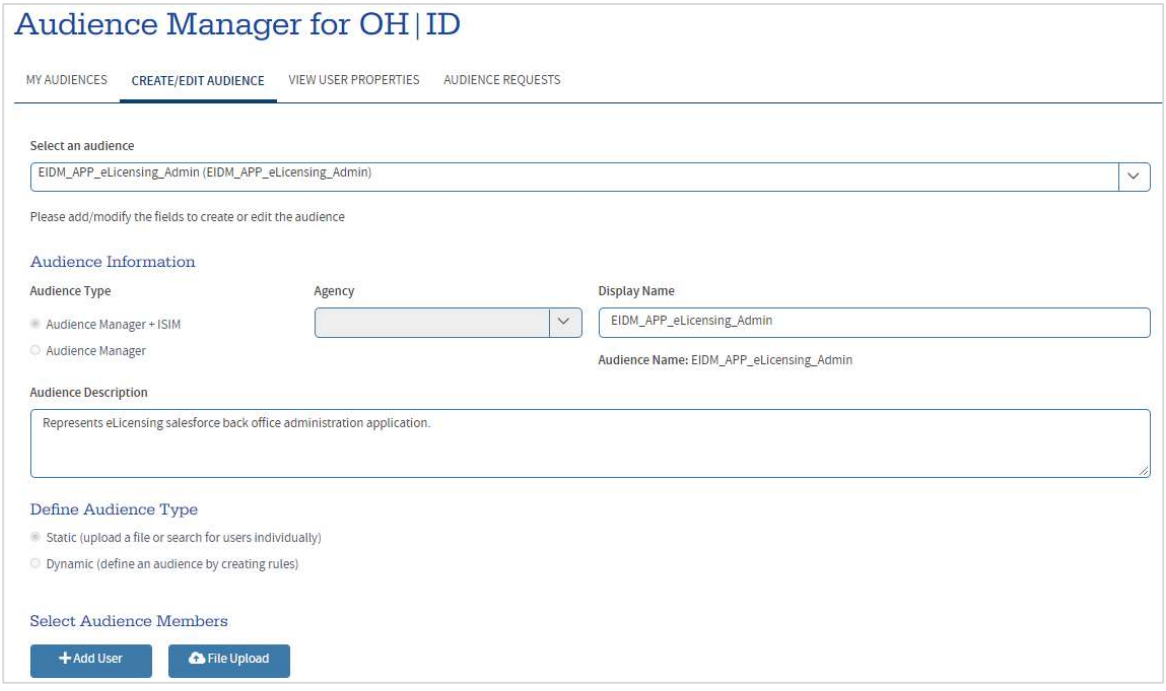

Figure 3: Audience Manager, Create/Edit Audience Screen

Audience Manager also offers an API to add, remove, and edit audiences and audience members and owners. Applications such as the DataOhio Portal leverage the API functionalities to ensure proper access controls and governance are in place and automated in sensible ways. This allows the DataOhio Portal administrators two methods to ensure access controls are applied quickly and efficiently, either through the Audience Manager

user interface, or programmatically through the API. Transactions with the API are secured through symmetric key encryption, and keys are rotated on a regular schedule or if there is suspicion of compromise. All API activities are auditable and fully compliant with industry standards.

OH|ID NEXT also offers its users three voluntary levels of identity assurance that can be leveraged by applications to help ensure the identity of the account owner has been verified, something useful for applications with sensitive data. Combined with Multifactor Authentication (MFA), these methods dramatically increase confidence that a user is who they say they are and ensure data is not shared with malicious actors.

The basic level of assurance is the default level and indicates the account owner has an email account that has been validated. The intermediate level of account security indicates that an account owner has been verified by a third-party identity service by answering a series of questions available to major credit agencies. The advanced level of security indicates the account owner has been through the intermediate step and was also able to link their information to data registered with the Bureau of Motor Vehicles, Ohio Department of Public Safety, on their State-issued ID card. To get a successful link in the intermediate and advanced steps, the account owner's information is passed to the relevant entity. If a name or birthday field is modified, then the account's assurance level is automatically downgraded to the basic level. These steps ensure attempts to compromise an account are likely to be unsuccessful.

Account Transparency

OH|ID NEXT also provides users insight into activity on their account that cannot be modified by a malicious actor. In this screen, the location of the Internet Service Provider (ISP) reported by the browser is shown with a geographic location plug-in so the account owner can see approximately where the activity originated.

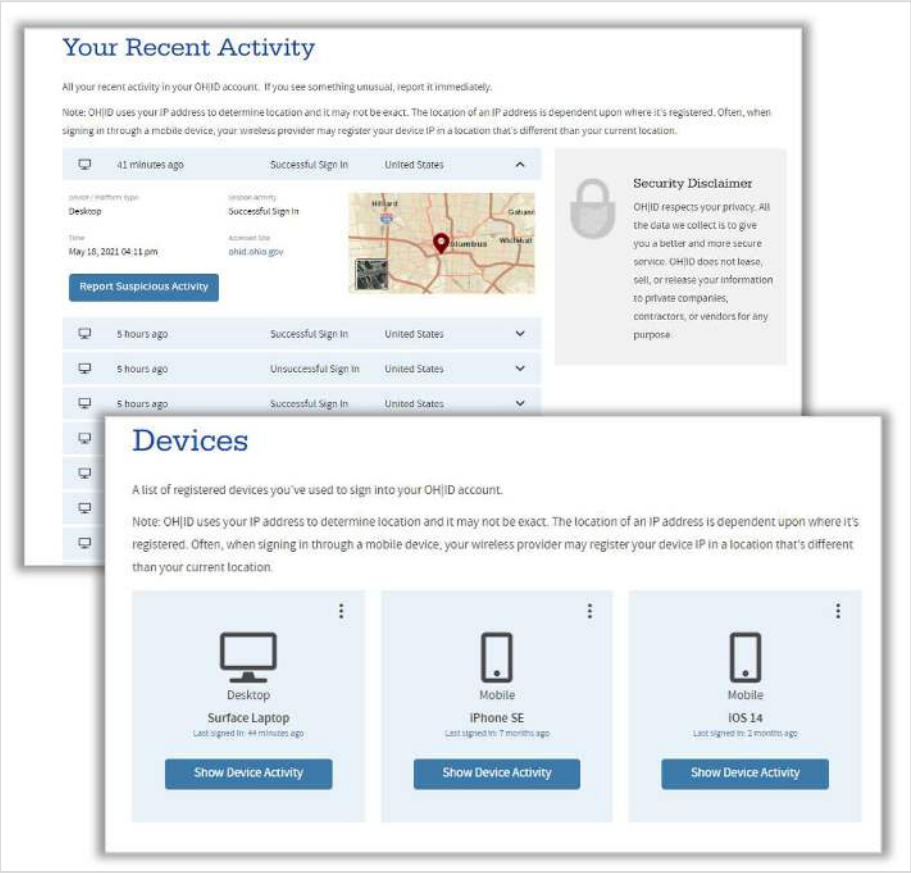

Figure 4: OH|ID NEXT Account & Device Activity

The screen displays both successful and failed login attempts, the type of device, date and timestamp, and which site the login activity originated from. If the account owner is concerned about any specific activity, they can submit a report with that information that can be analyzed by a security professional. By providing these self-service and transparent tools, those who utilize the InnovateOhio Platform can be confident that their account has not been compromised and have a clear way to engage with the State of Ohio in the event they notice concerning activity. In addition to recent activity, there is a view to highlight the devices used to access OH|ID. This view displays the type of device, operating system, and the last time the device was used. Users are also given the option to rename the device to a familiar name, hide the device, or launch a filtered view of activity specific to that device.

Implementation

Development efforts for OH|ID NEXT were well underway by March 2020, when the COVID-19 pandemic began shutting offices and limiting in-person interactions. The State of Ohio was able to leverage these efforts to quickly stand up a coronavirus dashboard that was a fusion of the identity platform, data analytics platform, and user experience. The State was able to launch a number of web-based services that helped the citizens and those who interact with the State in a secure and highly-available manner that was not possible at that speed and scale prior to the OH|ID efforts. In July 2020, during the heart of Ohio's stay-at-home order, the IOP team completed a full release of OH|ID NEXT functionality with a modern user interface, increased self-service functionality, and secure API-based features to enable a more secure and extensive online experience for Ohio citizens and businesses.

DataOhio Portal

On December 7, 2020, Lt. Governor Jon Husted and InnovateOhio, in partnership with DAS IOP, announced the launch of the DataOhio Portal, which offers a first-of-its kind service to Ohioans by delivering unprecedented transparency through an innovative, data-sharing platform. The DataOhio Portal is a public-facing portal that provides over 200 datasets and over 100 interactive visualizations to inform data-driven decision making for state agencies and their partners. It is a first-of-its-kind state technology, enabling data collaboration and sharing while also featuring enhanced security and privacy.

The DataOhio Portal hosts both public and private datasets. Especially through this pandemic, there has been a vital need to share secured datasets between state agencies and with designated members of the public, like private health organizations, local health departments, and university researchers. The portal has a great deal of authenticated content that is fed by the secure API architecture, retrieving disaggregated data from the IOP Data & Analytics Platform. The secure elements are protected through role-based access that is given out through the Audience Manager tool using manual provisioning, API-based provisioning, and automated approval workflow methods. Any data that is not publicly available is secured through the creation of user groups in Audience Manager. Owners of these groups, the data steward(s) for each respective dataset, can then provision appropriate access to properly screen and evaluate the access-requests submitted by public and private entities. Through API interactions with Audience Manager, IOP Data & Analytics Platform can ensure secured datasets are only displayed to people who are authorized to see them. The design of the system also guarantees privacy is maintained through disaggregation of data, as privacy is a core concern of the State.

Impact

The InnovateOhio Platform has continued to expand upon the OH|ID NEXT foundation by leveraging Amazon Web Services (AWS) such as CloudFront and Shield Advanced to enhance platform availability and security, by continuing to provide citizens and workforce users with "best of breed" cybersecurity.

Through its focus on consuming cloud-based services, the State of Ohio has demonstrated its ability to successfully handle massive spikes in web requests – more than 18x our typical volume – during Governor

DeWine's daily press conferences, as well as other significant events that have generated unpredictable patterns.

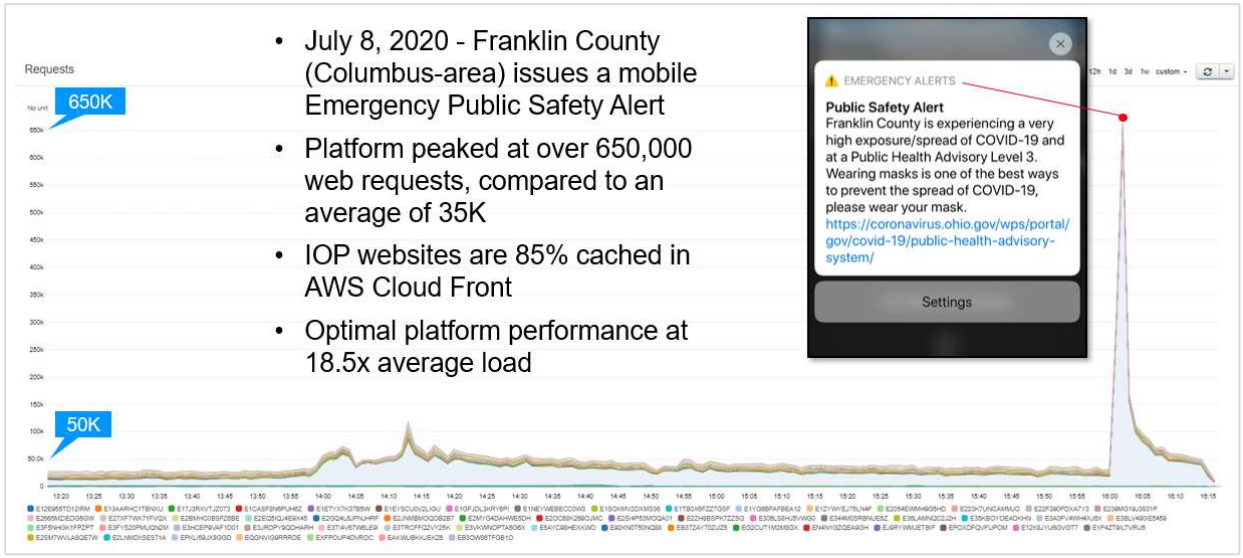

Figure 5: Platform elasticity in action

The global pandemic shifted many of our daily activities online, which made cybersecurity of paramount importance. The flexibility and secure framework offered by OH|ID and the net-new offerings of the OH|ID NEXT project positioned the State of Ohio as a leader in the tidal shift to life online by:

- Managing 1.2 million active digital identities and counting
- Supporting 659 applications in IOP's production environments (May 2021)
- Secure, API-first framework for fine-grained, precise role-based access management
- Verified email address for all new accounts and optional Experian identity-proofing for identity assurance and citizen account recovery.

The ability to scale infrastructure appropriately, respond to cyber threats proactively and reactively, as well as the security-minded toolkit available have positioned Ohio as a leader in state government digital presence. The foundations of Ohio's Identity Program and the features of OH|ID NEXT have positioned the state to continue a journey toward zero-trust and multiple layers of defense, a "defense in depth" security posture. Cybersecurity has never been more important to effective government, and the State of Ohio will continue to lead the way.