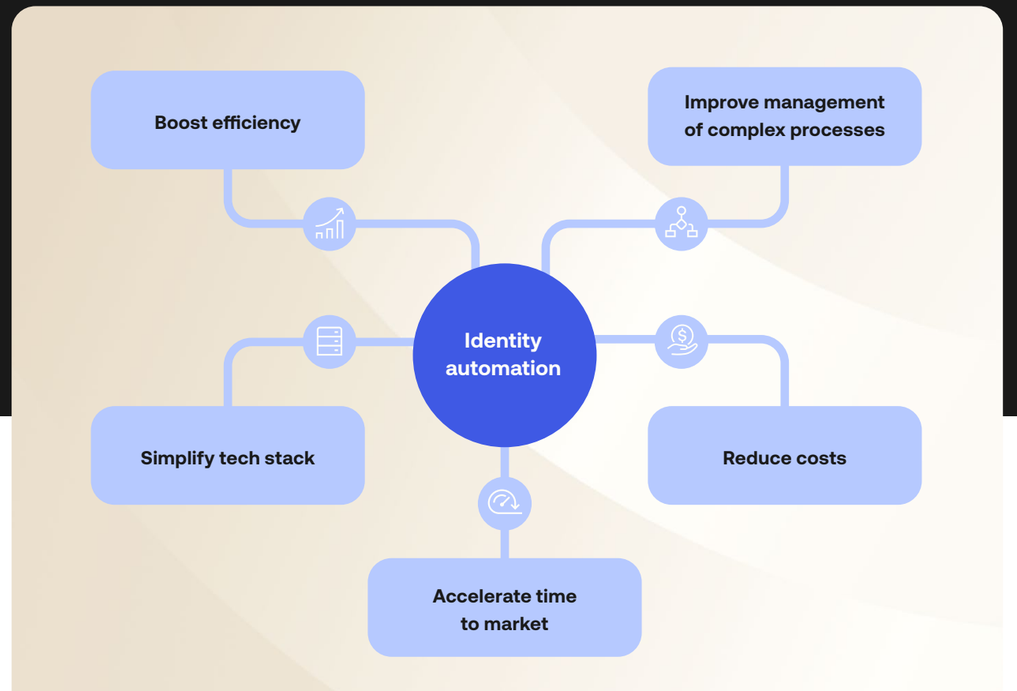
Strengthening core efficiencies: The case for leveraging Identity automation in U.S. government services



U.S. government organizations are racing against time to create better end-user experiences and leave behind outdated technology and development practices for modern solutions. To do this requires everyone in the personnel system — from IT leaders to customer researchers — and impacts a broad range of agency missions. While much of the pressure behind digital transformation in U.S. government services stems from legislative and industry pushes, it's also true that there are simply some aspects of modern work that have yet to reach U.S. government services. Catching up to core efficiency and productivity standards — including the adoption of tools that allow secure and easy access to essential resources — sets an agency apart.

IT leaders are particularly sensitive to this issue. The rapid digitization of public services over the past decade has produced complicated tech stacks whose benefits are outweighed by the inconvenience they build into essential functions. Tedious day-to-day tasks like requesting access to an application or system tank productivity levels, and can make it more difficult to retain and support employees.

In other words, these legacy tech stacks are in need of core automation functions to improve the performance of an agency and the morale of the employees who support them. Without automation, these agencies risk mission delays and failures that weaken their impact and undermine public trust.

Addressing this problem begins with Identity. Identity-powered security reduces silos across applications, systems, and organizations within agencies. What's more, modern Identity-centric automation tools offer teams low- to no-code options for building and managing complex functions, maintaining compliance standards, and improving experience management. The result is a more streamlined, more impactful set of processes that enhance the delivery of U.S. government services for benefit recipients and U.S. public sector employees alike.

This document includes information on:

- How automation tools can integrate with existing processes to boost efficiency and collaboration throughout and between U.S. government agencies and industry
- How the benefits of automation extend beyond IT departments
- Specific examples of automation-enabled use cases and how to get started

Unlocking Identity automation

Delivering secure and exceptional Identity experiences for end users is challenging because Identity is complex. With multiple users, apps, roles, and systems to manage, it's hard to balance productivity, security, and efficiency at the same time. Managing Identity is step one, but we believe automation will eliminate several of the next steps and is the answer to keeping up with the demands of business and modern approaches to working in today's landscape.

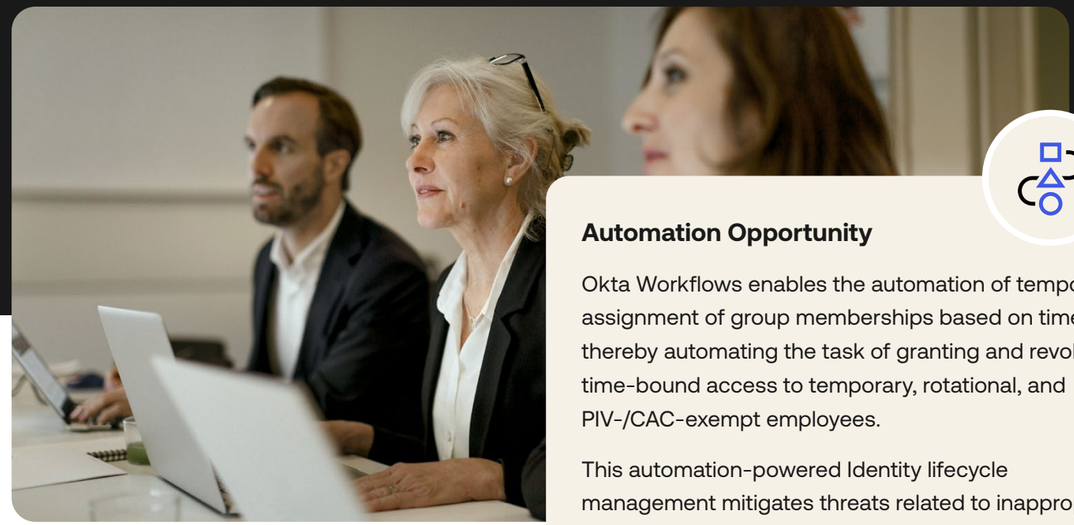
Okta Workflows[1] is a low- to no-code Identity automation and orchestration platform that enables your teams to build Identity-based, automation-enhanced experiences without coding experience. Using simple "if-this-then-that" logic, Workflows makes it easy to embed automation into any Identity-related process, such as customizing users' on- or off-boarding, streamlining audits and reporting, and strengthening your security posture.

[1] Okta Workflows is Authorized for our Okta for Government High (FedRAMP High) environment. This means a FedRAMP authorized Workflows is available to all Okta for Government High and eligible Okta for Government Moderate customers. To use this new feature, customers must be on the Okta Identity Engine (OIE). Learn more about how to turn on early access features here.

okta

Use Case 1

Granting time-bound access for talent mobility



Challenge

More than four million Americans work for the Federal U.S. government.[2]

To reimagine and build a modern workforce for our public servants, agencies must invest in work models that don't fit into the traditional paradigm of full-time work: PIV- or CAC-exempt, temporary, and rotational employees.

From unpredictable deployments to critical pathways into public service through internships and the contractors who provide support for a preset term or a particular project, these temporary and/or on-call workforces require access to core systems. But manually managing access across a diverse set of assignments is time-consuming and creates opportunities for security lapses, including a short-term employee retaining access beyond the timeline of their assignment.

Automation Opportunity

Okta Workflows enables the automation of temporary assignment of group memberships based on time, thereby automating the task of granting and revoking time-bound access to temporary, rotational, and PIV-/CAC-exempt employees.

This automation-powered Identity lifecycle management mitigates threats related to inappropriate or overlong access. It's a win-win: better security with less manual work for administrators.

Benefits by role

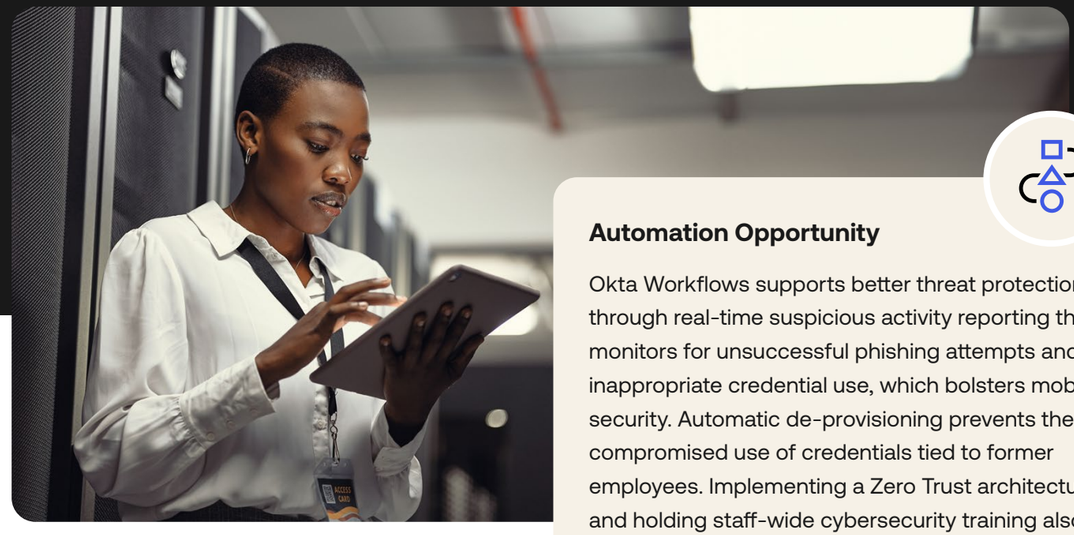
IT Leaders
Strengthen security in scenarios where PIV/CAC issuance locations are far away, someone forgets or loses their PIV/CAC, and for those who need to use an alternative MFA, ensuring the policies are accepted for a set or limited period of time (e.g., 24 hours).

Human Resources / Talent Management
Designate apps with a timed provisioning and de-provisioning of access when filling talent gaps through rotational assignments, exchanges, fellowships, or "tours of duty".

[2] Strengthening and Empowering the Federal Workforce, PMA

Use Case 2

Enhancing real-time alerts of suspicious activity



Challenge

The U.S. public sector attracts a remarkable amount of malicious activity: More than half of all phishing attacks target U.S. government agencies.[3]

As U.S. government services increasingly move toward digital means of service delivery, citizens' private data and sensitive national security information lands in the crosshairs of bad actors. The shift to remote and hybrid work has also triggered an increased reliance on unmanaged mobile devices amongst the federal workforce, which further exacerbates the problem.

Cyberattacks are extraordinarily disruptive. Ordinary citizens are left without access to urgent, high-impact services and benefits like court and public utility electronic systems. To minimize the likelihood of these breaches, service providers need timely warnings that their systems are under attack.

Automation Opportunity

Okta Workflows supports better threat protection through real-time suspicious activity reporting that monitors for unsuccessful phishing attempts and inappropriate credential use, which bolsters mobile security. Automatic de-provisioning prevents the compromised use of credentials tied to former employees. Implementing a Zero Trust architecture and holding staff-wide cybersecurity training also go a long way in supporting cyber hygiene efforts.

Benefits by role

IT Specialists (InfoSec/SysAnalysis)
Receive automated alerts in the event of suspicious activity for heightened threat readiness and strengthened risk mitigation. Can also create an audit and report that informs who has failed to complete required training, prompting Mission Owners to revoke access to high-impact apps until completed.

Public Affairs Specialist
Craft real-time communications responses that inform employees and stakeholders of suspected cyber incidents and provide context-specific guidance.

[3] Rise in Mobile Phishing Credential Theft Targeting U.S. Public Sector, Lookout

okta

Use Case 3

Reducing churn to public benefits and services through data-sharing initiatives

Challenge

Agencies are committed to rebuilding customer experience (CX) — and trust — in the 21st century.

The success of service delivery is closely tied to regularly capturing customer feedback and incorporating customer voices in the agency decisions that ultimately reduce churn to public benefits and services.

However, manually soliciting this feedback, like checking for survey completion, makes the process of deploying, qualifying, and presenting it cumbersome, inefficient, or delayed.

Feedback frameworks driven by customer research have also transformed the public's ability to get federally funded benefits and resources they are eligible for when communication channels extend beyond just mail.

Automation Opportunity

Okta Workflows automates notifications and communications with common apps like Microsoft Teams and Slack which notify teams of project developments and milestones, helping streamline reporting data publicly and boosting agencies' ability to act strategically.

Okta Workflows can also aggregate data across multiple agencies and levels of U.S. government to drive critical multi-channel notification pilot programs like Notify.gov.

Benefits by role

Customer Researchers / Outreach Teams
Automatically notify teams when program participants complete a survey, increasing the speed with which that feedback can be incorporated into better service.

CX Strategists / Digital Strategy Leaders
Support customized notification campaigns that inform agency staff and participants who opt-in to receive critical information such as application deadlines, interview reminders, fraud reduction, and other critical service updates.

Use Case 4

Supporting hybrid, secure Identity proofing

Challenge

For agencies in the middle of their digital transformation journey, service delivery must be *digital first* but not *digital only*. This especially rings true for Identity verification options that should be inclusive of people's ability to access technology.

Identity-proofing and age-verification measures that require a higher level of Identity assurance — everything from applying for benefits, I-9 verifications, and online gambling regulation — must include non-digital authentication pathways for citizens and eligible non-citizens that either:

- Need a higher level of Identity assurance
- Need a fallback option when digital proofing fails

This hybrid approach to Identity verification improves the timeliness of connecting the right people to the right benefits: the cornerstone of public services. The Department of Labor (DOL) has already begun a pilot program for unemployment insurance (UI) in partnership with the U.S. Postal Service.

But to execute this approach effectively and expand it beyond UI, agencies need to provision identities and correlate intelligence across a number of different proofing technologies.

Automation Opportunity

Okta supports hybrid Identity proofing by uniting diverse back-end proofing technologies in a central, cloud-based directory. This enables agencies to give the public more options for online and/or in-person Identity verification.

With Okta Workflows, agencies can take things a step further by supporting in-person registration/enrollment with integrations that generate a barcode that end users can print out and present at their local post office; and a postal application can inform agencies like the DOL when verification has occurred.

Benefits by role

Digital Transformation Leads
Overcome the digital divide that limits some populations to request and receive key benefits and services with a vendor-neutral solution that supports in-person Identity verification and online verification.

Fraud Detection Analysts
Cross-reference suspected incidents of fraud with a reliable, centralized directory that accounts for assurances of both digital and in-person Identity verification options.

okta

Glossary of resources

Use case 1: Granting time-bound access for talent mobility

- Template: Assign group memberships temporarily based on time
- Template: Create contractor expiry notifications

Use case 2: Enhancing real-time alerts of suspicious activity

- Template: Detect suspicious MFA push notifications
- Template: Subscribe to Microsoft alerts to notify admins of potential security issues
- Template: Suspicious activity event alerts in PagerDuty
- Template: Suspicious activity reported in Slack

Use case 3: Reducing churn to public benefits and services through data-sharing initiatives

- Video Tutorial: Learn how to build a notification flow
- Video Tutorial: Notify user assigned to application
- Connectors: Microsoft Teams Connector, Slack Connector

Use case 4: Supporting hybrid, secure Identity proofing

- Template: New user registration
- Template: Validate email domains during registration
- Template: MFA fatigue detection

Get up to speed on Workflows

- Free, self-paced training: Workflows: Foundations for Flowgrammers
- Workflows Community Team: How-to guides and tutorials, videos, and tips
- Office Hours: Come with questions on your flow
- Pre-built Templates: Pre-built Workflows templates

For U.S. government agencies, efficiency is more than a cost issue. It's a core metric of the mutual trust and civic pride they share with the American public. Prioritizing efficient service delivery is a core strategy for rebuilding that trust. And as agencies work to strengthen their interactions with the public, they understand the importance of developing their tech stack with and for their users to ensure it solves actual problems. An effective solution will also automate and scale impact for both citizens, other eligible persons, and U.S. government employees.

Identity automation is a decisively important part of this strategy. By streamlining inefficient processes and creating new opportunities for enhanced service, Identity automation delivers noticeably improved outcomes to U.S. government employees and benefit recipients alike. Your agency will be able to simplify complex functions, heighten security, reduce developer costs, and accelerate the speed with which you can enact CX improvements.

The value of Identity-powered functionality is not reserved to Identity-centric roles within U.S. government agencies. As the examples in this resource demonstrate, the value of Identity automation extends to human resources, public affairs, and customer research teams, among others.

To learn more about Okta Workflows and the impact it can make on your service delivery, check out additional information at okta.com/platform/workflows/#industries or contact our sales team at okta.com/contact-sales.

okta