GA@WORK Security Education Session

Offered: April 9, 2025

NEXTGEN

Meeting Agenda

1. GA@WORK Security & Security Groups
2. GA@WORK for Agency Security Partners (ASPs)
3. GA@WORK for IdP Administrators & HR Partners
4. GA@WORK Multifactor Authentication
5. Questions

Please note:

This deck is from a session held in April 2025. It is shared as a resource.

Please remember to complete your GA@WORK training in preparation for go-live.

GA@WORK Security & Security Groups

NEXTGEN

GA@WORK Security

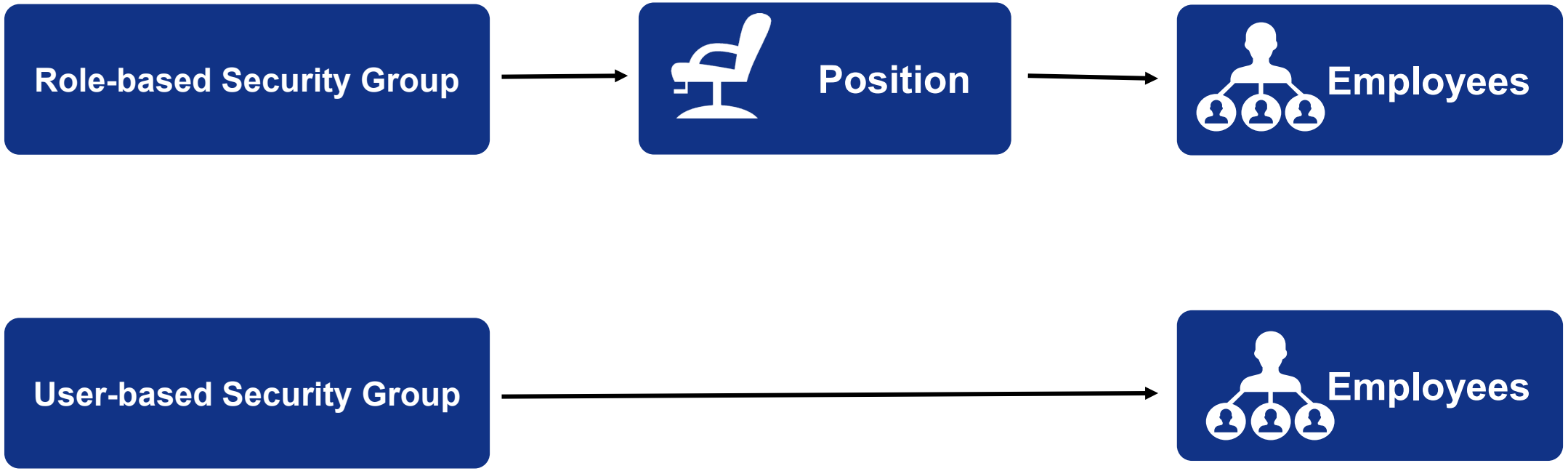
GA@WORK is the name we use to refer to Georgia's Workday system, a cloud-based enterprise resource planning (ERP) system that is replacing our 25-year-old TeamWorks/Peoplesoft system.

"**Security**" refers to the framework within GA@WORK that controls access to data, tasks, and functionality based on users and roles. GA@WORK Security ensures that employees, managers, HR personnel, financial personnel, and other users can only access the information and actions relevant to their job responsibilities.

Common GA@WORK Security Group Types

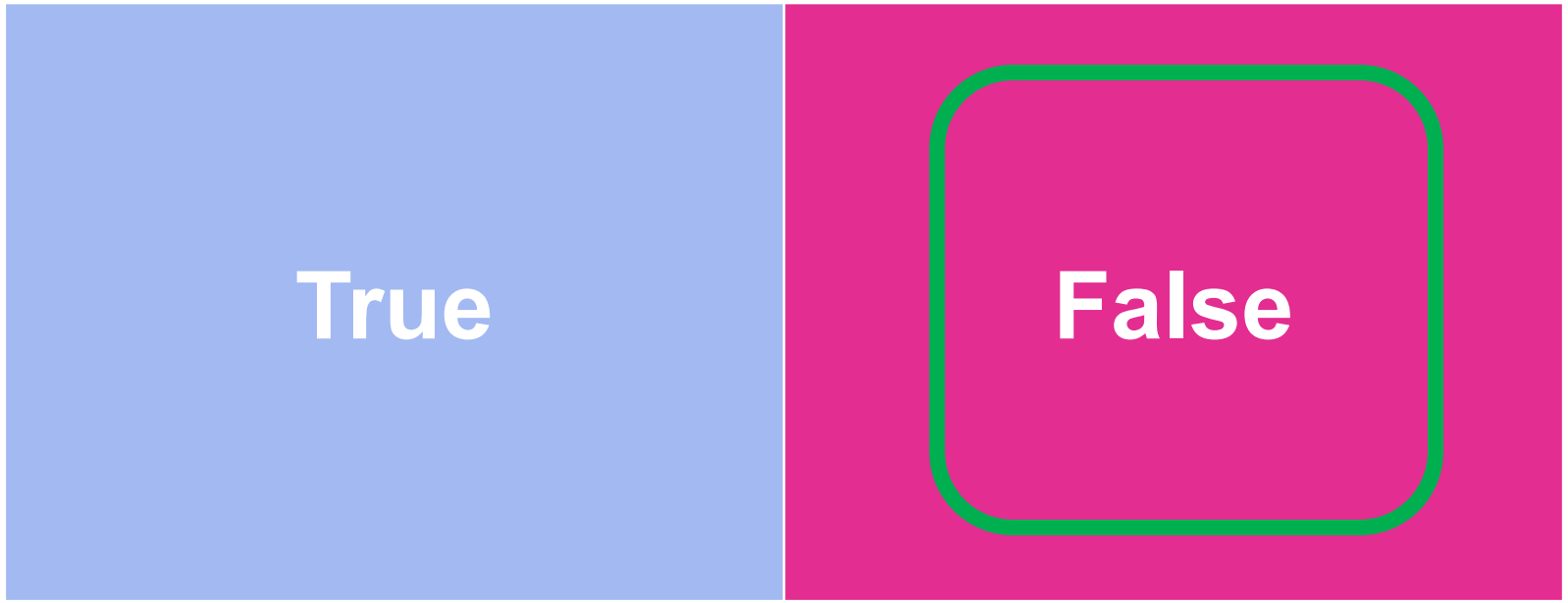
Role-based	User-based
Tied to assignable roles that are provisioned to a user's position. (Manager, Developer, etc.)	Assigned directly to users, not their position.
Primary type of security group for most assignable roles in GA@WORK.	Typically assigned when a specific user needs access beyond their day-to-day roles.
Example: Someone with the HR Partner role-based security group can review or approve a step in Hire Business Process.	Example: HR Administrator

Role-based and User-based Security Groups



Knowledge Check

True or False: Role Based and User Based Security Roles are the same thing.



False, Role Based and User Based Security Roles are not the same thing.

GA@WORK for Agency Security Partners (ASPs)

NEXTGEN

Session Objectives for ASPs

1. Definition of ASP
2. TeamWorks vs GA@WORK
3. Security Request Forms
4. Delegation of Authority
5. Quarterly/Annual SOD account reviews for ASPs
6. Summary

Agency Security Partner (ASP)

- An Agency Security Partner is the new term used in GA@WORK (this role was called Agency Security Officer in TeamWorks). These roles are named differently but perform the same functions.

- Each State of Georgia agency assigns a primary and secondary Agency Security Partner who is responsible for managing Security Request Forms to grant access to agency users.

- ASPs are responsible for partnering with the business owners to ensure appropriate access is approved and granted.

Before vs. After

TeamWorks		GA@WORK
Quarterly User Account reviews		Quarterly User Account reviews
SOD Annual reviews		SOD Annual reviews
Reset Password/Lock Account		Reset Password/Lock Account
Only native login was offered	vs.	Single Sign On (SSO) and Native Login with Multi Factor Authentication (MFA)
Only 1 type of Security Request Form		A total of 7 types Security Request Forms
Delegation of Authority not applicable for ASPs		Approval of delegation authorities
Security Request Form to delete access is required when worker is terminated		System automatically removes access when worker is terminated

Different Types of Security Request Forms

Security Request Forms	Description	Used By:
User-based HCM Security Request Form	Request access for users requiring user-based assignments within the HCM application for GA@WORK.	DOAS and SAO
User-based FIN/PRO Security Request Form	Request access for users requiring user-based assignments within the FIN/PRO application for GA@WORK.	DOAS and SAO
Auditor Security Request Form	Request access for users requiring user-based assignments within the HCM and FIN/PRO applications for GA@WORK.	OPB, DOAA, ERS, and General Assembly

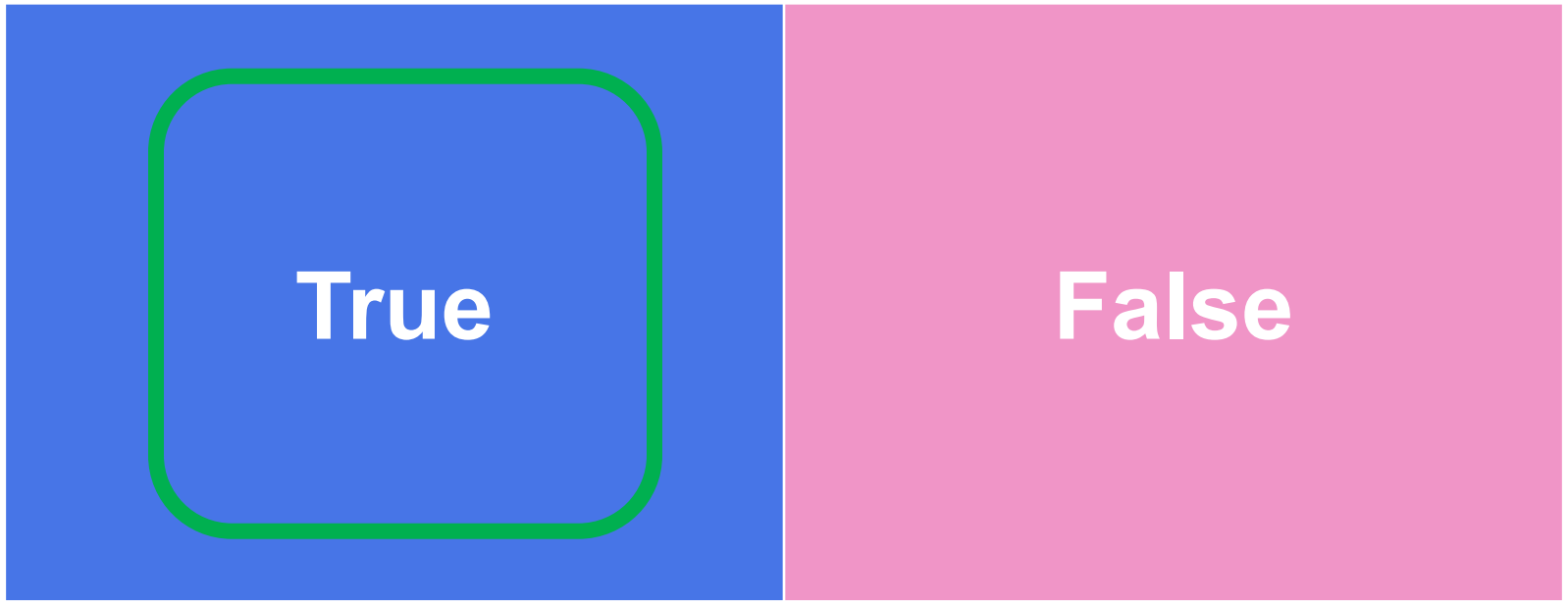
Continued…

*Note: GA@WORK does not prohibit one agency for submitting for another agency. Double check to be sure information is accurate for YOUR agency before submitting.

Security Request Forms	Description	Used By:
Hybrid Sign On Request Form	Used by HR Partners at Single Sign On (SSO) agencies when an employee needs to change their login from SSO to Native Login or vice versa.	DBHDD, DJJ, DNR, GDC, GVS, PAC, and DOL/OAG
Role-based HCM Security Request Form	Request access for positions requiring Role-based assignments within the FIN/PROC application for GA@WORK. Used by ASPs and Managers, at all agencies.	All Agencies
Role-based FIN/PRO Security Request Form	Request access for positions requiring Role-based assignments within the FIN/PROC application for GA@WORK. Used by ASPs and Managers, at all agencies.	All Agencies
Role-based PRO TGM Security Request Form	Request access for positions requiring Role-based assignments within the FIN/PROC application for GA@WORK. Used by ASPs and Managers, at all agencies.	All Agencies

Knowledge Check

True or False: It is important to double check to be sure the information is accurate for YOUR agency before you submit.



True: It is important to double check to be sure the information on the request you are submitting is accurate for YOUR agency before you submit.

Delegation of Authority

Delegation of Authority allows a manager to assign work tasks to peers or a higher level such that work continues in their absence.

Examples:

- Expense approvals
- Time off requests
- Performance reviews

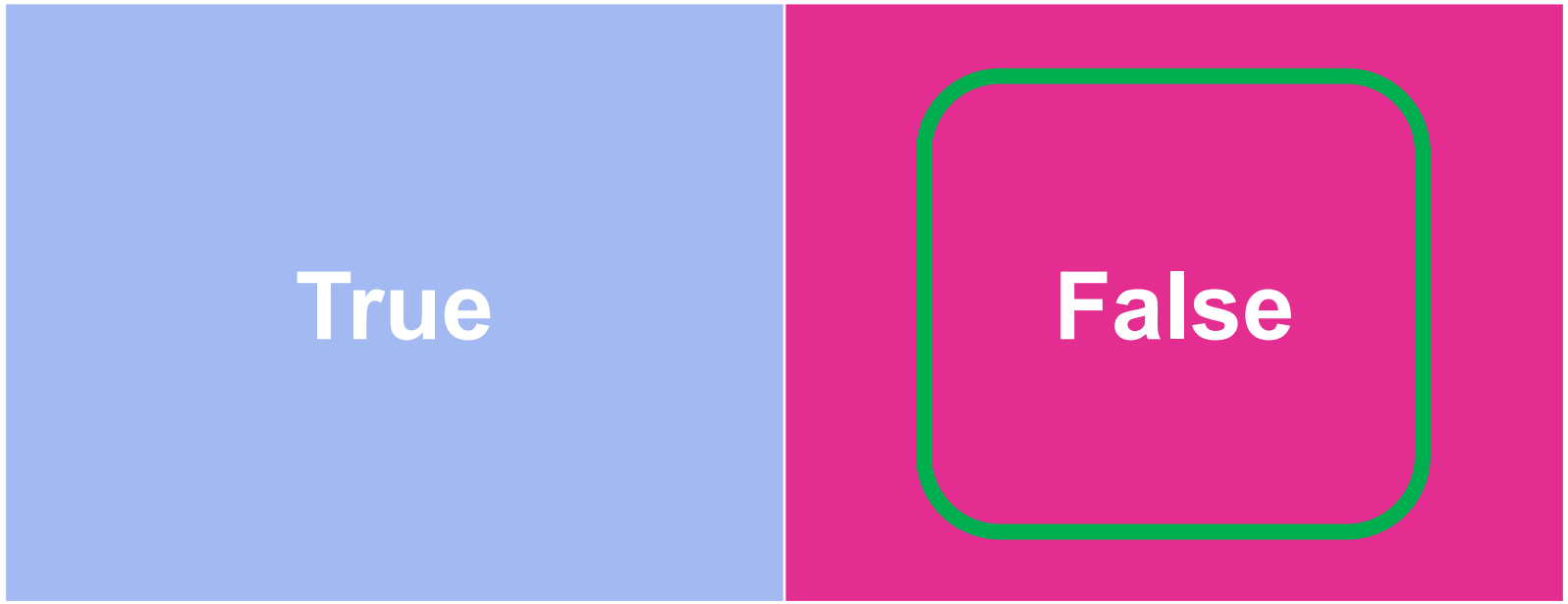
New Delegation of Authority Responsibilities for ASPs

Agency Security Partners are responsible to review and confirm the delegation of authorities submitted is appropriate by their agency personnel.

Agency Security Partners must run a quarterly delegation of authority report to review and request changes.

Knowledge Check

True or False: Any role is responsible to review and confirm the delegation of authorities submitted is appropriate by their agency personnel.



False! *It is the agency security partner who is responsible to review and confirm the delegation of authorities submitted is appropriate by their agency personnel.*

Quarterly Account Reviews for ASPs

Quarterly Account Users Review was required in TeamWorks and remains a requirement in GA@WORK. Below is a reminder of responsibilities:

- Receive and review the Quarterly Account User Review report.
- Submit and approve Security Request Form, in the ERP platform, for agency employees based on a review of the Quarterly Account User Review report.
- Complete the online attestation or request an extension by the deadline.

Note: Failure to complete attestations will result in a report of non-compliance to the State Accounting Officer.

Annual Segregation of Duties (SOD) Review

Annual SOD review was required in TeamWorks and remains a requirement in GA@WORK. Below is a reminder of responsibilities:

- Receive and review the SOD report.
- Submit and approve Security Request Form, in GA@WORK, for agency employees based on a review of the SOD report. For user access which conflicts with appropriate segregation of duties, mitigating controls must be in place. *Note: A Security Request Form must be submitted if a SOD conflict exists.*
- Complete the online attestation or request an extension by the deadline.

Note: Failure to complete attestations will result in a report of non-compliance to the State Accounting Officer.

Summary of ASP Responsibilities

Submit and approve the Security Request Form within GA@WORK

Authorize the delegation authorities

Perform Quarterly User Account reviews and Annual SOD reviews

GA@WORK for Identity Provider (IdP) Administrators & HR Partners

NEXTGEN

Session Objectives for Identity Provider (IdP) Administrators

1. Onboarding in GA@WORK
2. Onboarding Process Flow
3. Importance of Employee ID in GA@WORK
4. IdP Setup Process for New Hires/Terminations
5. Single Sign On (SSO)
6. Multifactor Authentication (MFA)
7. List of SSO Agencies by IdP Systems
8. IdP Administrators & HR Partners Responsibilities - Summary

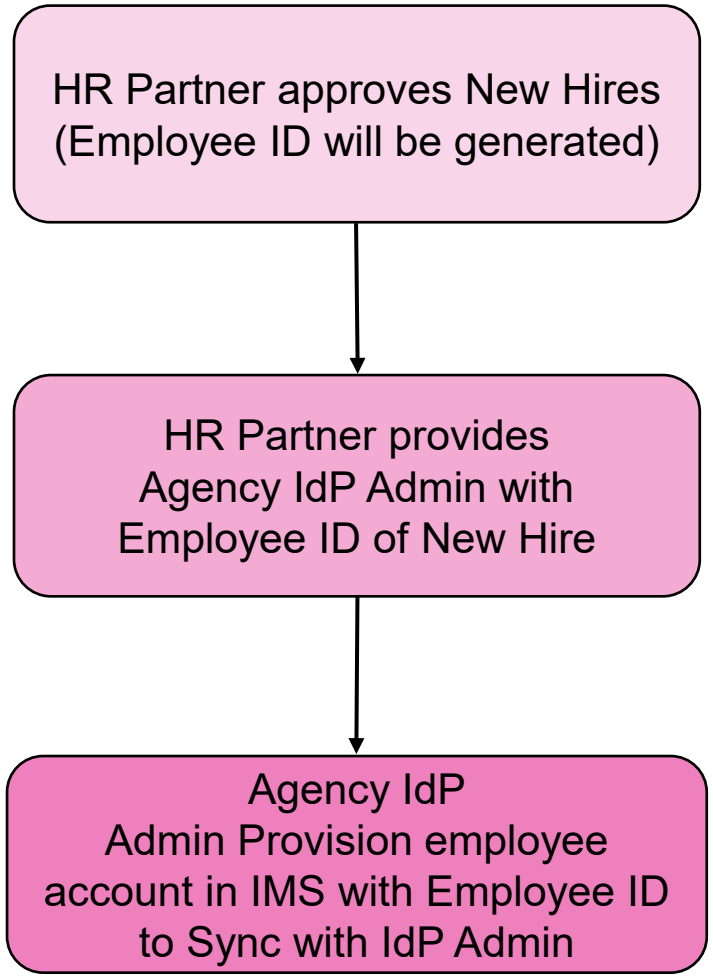
Onboarding in GA@WORK: IdP for SSO Agencies

- Onboarding helps you enroll new workers (employees and contingent workers) into your agency *("Onboarding" is a word used in GA@WORK for Hiring Process)*
- Each SSO agency must follow a GA@WORK defined Onboarding Business Process

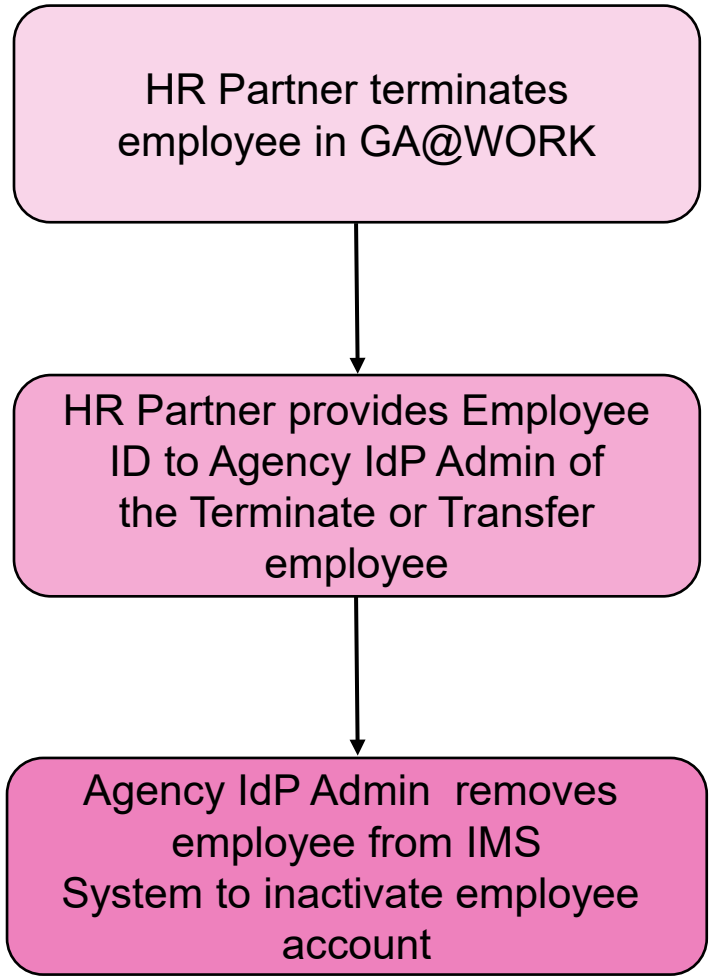
IMPORTANT NOTE FOR ALL SSO AGENCIES:

- Ensure new workers are entered into GA@WORK and into your agency's IdP
- New step must be included in Onboarding process to send your Employee ID and details to IdP Admin

Onboarding Process Flow

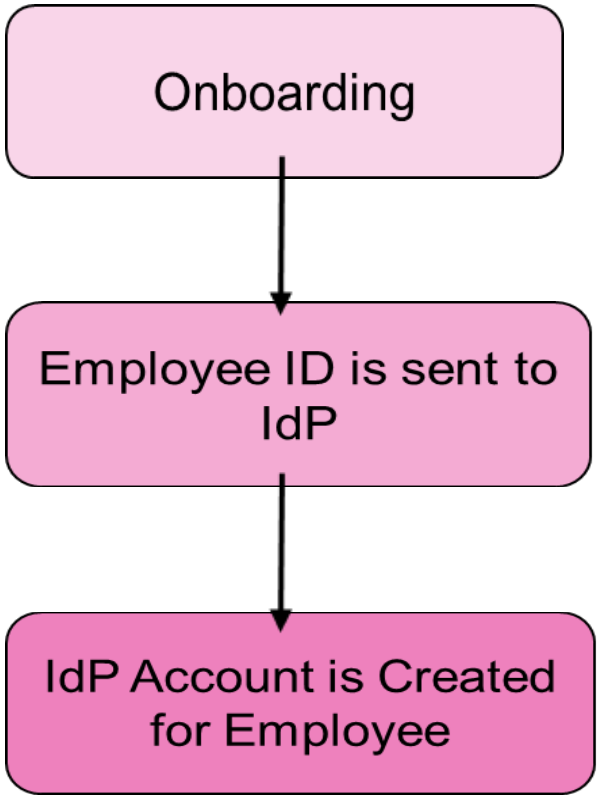


Transfer/Termination Process Flow



Importance of Employee ID in GA@WORK / IdP

- Employee ID is a must in GA@WORK.
- IdP is setup with "Employee ID" as a Unique Identifier in the name space (Employee ID must have 8-digit numbers (Ex – 00123456))



IdP Setup Process for New Hires

Prerequisites:

- Employee record is created in GA@WORK with a unique Employee ID.
- Employee information (Employee ID, Name, Email, Department) should be sent to IdP Admin to synchronize employee data.

Setup Process:

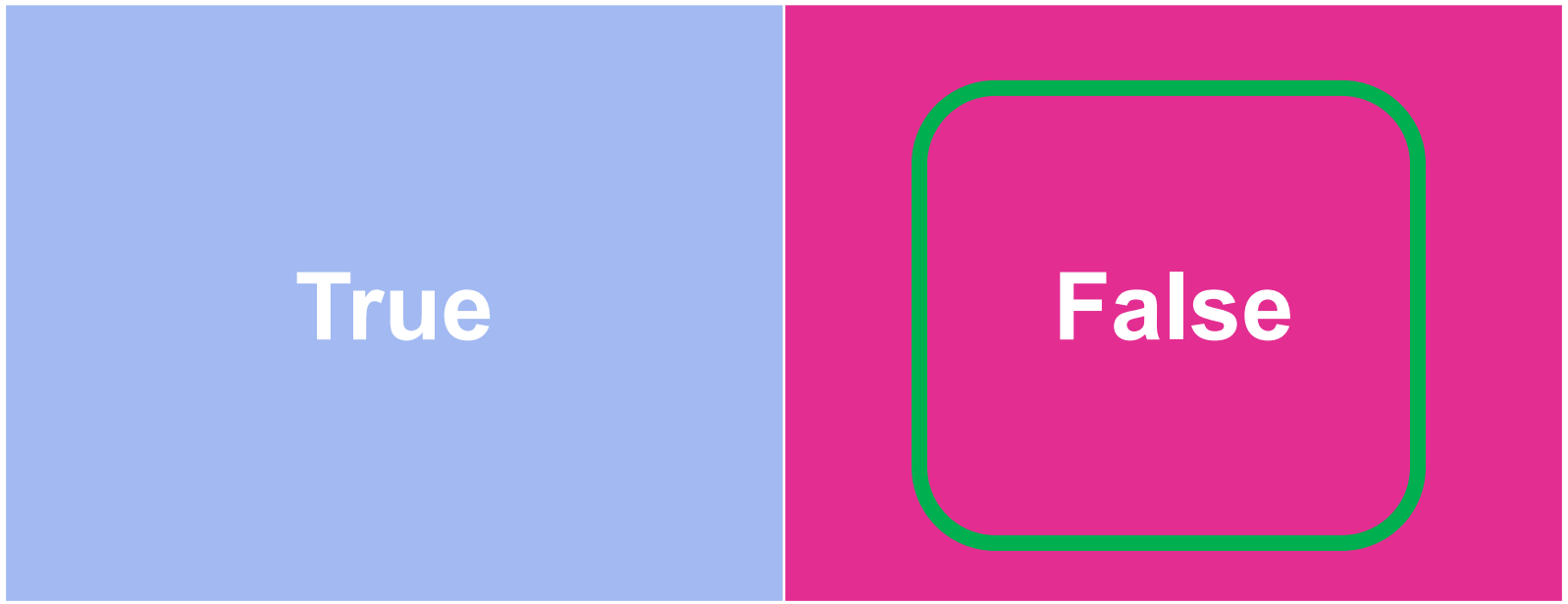
- IdP account for the employee is created using Employee ID as a unique identifier.
- SSO is configured in the Identity Provider (e.g., Azure AD, ADFS, Okta) using Employee ID for authentication.
- GA@WORK validates SSO token to grant access.
- Once this process is done, Employee can access GA@WORK with SSO directly.

IdP Process for Terminations

- Termination
  - As soon as employee is Terminated or Contract has ended, your agency will need to determine a process to send update to your agency IdP Admin for removing employee access.

Knowledge Check

True or False: Onboarding does not require coordination between IdP admins and HR Partners for SSO agencies?



False! *A step must be included in Onboarding process to send the Employee ID details to IdP Admin*

Ways to Login to GA@WORK

SSO allows users to access GA@WORK using their agency credentials without needing a separate username and password. It integrates with an agency's IdP to provide seamless authentication and enhanced security.

Native Login with MFA allows users to access GA@WORK using their username and password to directly login to GA@WORK.

Key Components of SSO

Component	Description
Identity Provider (IdP)	Manages user authentication and issues security token. (e.g., Okta, Azure AD, Duo)
Service Provider (SP)	Workday is the service provider, which relies on the IdP to authenticate users and grant access to the GA@WORK application
Active Directory	Centralized user directory which stores and manages user credentials.
SSO Flow	User requests access → Redirected to IdP → Authenticated(via AD) → Security token(SAML) sent to Workday → Access granted

Summary of IdP Administrators & HR Partners Responsibilities

Onboarding in GA@WORK/IdP

IdP Admin

- Process for New Hires
- Process for Existing Employees (One time update is needed due to Project Implementation)
- Process for Termination

Configure Agency IdP system for SAML message to GA@WORK

Communicate configuration details with NextGen Security Team to configure in GA@WORK Tenant

Educate employees on usage of GA@WORK app setup in IdP

GA@WORK Multifactor Authentication

NEXTGEN

Native Login with Multifactor Authentication (MFA)

- Native Login into GA@WORK uses MFA for most users.
- Multifactor Authentication is a method of confirming the identity of a user by requiring more than 1 type of identity verification.

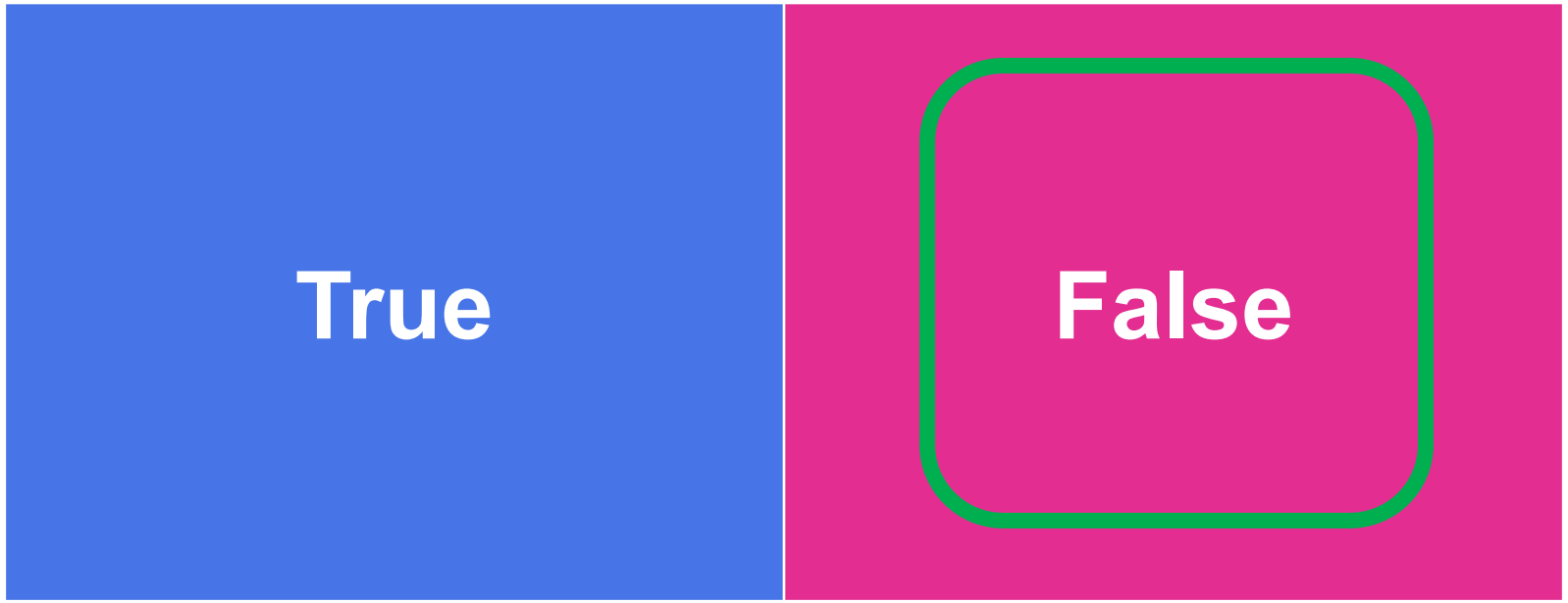
Multifactor Authentication (MFA) Options

GA@WORK supports the following MFA options:

- Authenticator App accessed by smartphone
  - Any app that supports TOTP (Time-Based One-Time Passcode)
  - One-time passcodes sent via SMS
  - One-time passcodes sent via E-mail

Knowledge Check

True or False: SSO configuration for GA@WORK is entirely an agency responsibility?



False! *SAO will work closely with Agencies throughout configuration, testing, and maintaining SAML certificate expiry.*

As of April 2025

List of SSO Agencies by IdP Systems

IdP System	Agencies
SafeNet	Georgia Dept. of Banking and Finance
DUO	Georgia Student Finance Commission
Google	Department of Community Supervision Georgia Public Safety Training Center State Board of Pardons and Paroles
MS Azure	Audits and Accounts Community Affairs Criminal Justice Coordinating Council Department of Early Care & Learning General Assembly Georgia Department of Law / Office of the Attorney General Georgia Department of Transportation Georgia Dept. of Education Georgia Employees Retirement System Georgia Public Service Commission Georgia Vocational Rehabilitation Agency Judicial Council Administrative Office of the Courts Office of Planning and Budget Office of Inspector General Prosecuting Attorneys' Council of the State of Georgia

As of April 2025

List of SSO Agencies by IdP Systems (continued)

IdP System	Agencies
MS Azure (cont)	Georgia Public Broadcasting Viewpoint Health/CSB-Gwinnett, Rockdale, Newton
Okta	Aviation Authority Department of Administrative Services Department of Behavioral Health and Developmental Disabilities DHS - Family and Children Services, Division of Department of Driver Services Department of Human Services Department of Juvenile Justice Department of Natural Resources Department of Revenue Georgia Bureau of Investigation Georgia Correctional Industries Georgia Office of the State Treasurer Georgia Technology Authority Office of State Administrative Hearings Professional Standards Commission State Ethics Commission / Government Transparency & Campaign Finance Commission State Accounting Office Public Health, Department of Corrections, Department of

As of April 2026

Hybrid Agencies (SSO and Native)

GETS* **Agencies using Hybrid** *Allows Agencies to use both methods (i.e., SSO and Native Login) as needed*	
Department of Behavioral Health and Developmental Disabilities	
Department of Corrections	Department of Natural Resources
Department of Juvenile Justice	Department of Driver Services
Department of Human Services	Office of The Governor
Department of Revenue	

Non-GETS* **Agencies using Hybrid** *Allows Agencies to use both methods (i.e., SSO and Native Login) as needed*	
Administrative Office of the Courts	Department of Education
Superior Courts of Georgia	Office of Planning and Budget
Vocational Rehabilitation of Georgia	

As of April 2025

SSO/IdP Agency Administrators & SAO Security Administrators Responsibilities

IdP Administrators	SAO Security Administrators
• Configure Agency IdP system during Login: ➢ Issuer/Entity ID ➢ x509/Base64 SAML certificate ➢ Name ID/Namespace with Employee ID ➢ IdP Login URL ➢ Workday Tenant URL	• Configure GA@WORK Tenant/Environment with Issuer/Entity.
• Share below details with SAO Security Administrators to configure in GA@WORK Tenant: ➢ Issuer/Entity ID ➢ x509/Base64 SAML certificate ➢ IdP Login URL	• Update GA@WORK with ID, x509/Base64 Certificate and IdP Login URL which is shared by each Agency's IdP Administrators.
• Share the renewed x509/Base64 certificate, annually with SAO Security Administrator.	• Update the x509/Base64 certificate, annually, which is renewed by each state agency.

Who to Contact for Support

When to Contact Agency IdP Admin
Initial Setup/Installation process for SSO.
Product related/configuration questions.

When to Contact SAO Security Team
Questions related to requirement for establishing an SSO connection at GA@WORK. NextGen_SecMap@sao.ga.gov
Questions related to Troubleshooting SSO connection/Request Troubleshooting SSO Connection. NextGen_SecMap@sao.ga.gov

Questions, Requests, Concerns:

NextGen_SecMap@sao.ga.gov


NEXTGEN
Thank You