IDEAGEN GOVERNMENT CLOUD
FedRAMP Secure Configuration Guide

Document Version	v1.0
Publication Date	April 2026
SSP Version Referenced	v1.1 (January 6, 2026) – FedDoc-201
FedRAMP Package ID	FR2429166928
FedRAMP Impact Level	Moderate (FIPS 199: Moderate)
Digital Identity Level	IAL2 / AAL2 / FAL2
Authorization Path	Agency Authorization
Deployment Model	Public Cloud – AWS us-east-1 (US East)
Service Model	SaaS – Multi-tenant
Document Owner	Ideagen Product & Security Team
System Owner	John Molamphy, CTO – John.Molamphy@Ideagen.com
ISSO (Ideagen)	Josh Monk, VP Global Cyber Security – josh.monk@ideagen.com
Authentication Platform	Okta – FedRAMP Package F1512167750 (REQUIRED)
Security Contact	security@ideagen.com

CONTROLLED DOCUMENT NOTICE

This document contains security-relevant configuration guidance for Ideagen Government Cloud (IGC), a FedRAMP Moderate Authorized cloud service (Package ID: FR2429166928). Distribution is limited to agency Authorizing Officials, System Owners, ISSOs, and authorized administrators. Do not reproduce or distribute beyond authorized personnel without written consent from Ideagen.

Note: In accordance with FedRAMP SCG-CSO-PUB, a version of this guide is made publicly available through the FedRAMP Marketplace listing for Package FR2429166928. This controlled version contains full operational detail and is provided to authorized personnel only.

 © 2026 Ideagen. All rights reserved.

 © 2026 Ideagen. All rights reserved.

Document Revision History

Version	Date	Description
1.0	April 2026	Initial publication. Aligned to IGC SSP v1.1 (FedDoc-201, January 6, 2026). Addresses FedRAMP SCG-CSO-RSC, SCG-CSO-AUP requirements (Rev5 Balance Improvement Release, effective March 1, 2026). Includes Enhanced Capabilities statement (SCG-ENH-CMP through SCG-ENH-VRH). This guide is aligned to the IGC SSP v1.1 and will be reviewed annually or upon SSP revision, control baseline change, or updated FedRAMP configuration standards.

 © 2026 Ideagen. All rights reserved.

1. Introduction

1.1 Purpose

This Secure Configuration Guide (SCG) provides Federal agency customers with clear, actionable instructions for securely configuring Ideagen Government Cloud (IGC), the EHS Enterprise platform. It is published in accordance with FedRAMP Rev5 Balance Improvement Release requirement SCG-CSO-RSC (effective March 1, 2026) and is grounded in the IGC System Security Plan (SSP) v1.1 (FedRAMP Package ID: FR2429166928).

The guide explains the security implications of common settings, identifies required configurations for top-level administrative and privileged accounts, and empowers agency ISSOs, System Owners, and administrators to configure IGC in alignment with their FedRAMP compliance obligations.

1.2 How to Obtain and Use This Guide

> **FedRAMP Requirement – SCG-CSO-AUP**
> Providers MUST include instructions in the FedRAMP authorization package that explain how to obtain and use the Secure Configuration Guide. This section fulfils that requirement.

This guide is made available to authorized agency personnel through the following channels:

- FedRAMP Marketplace / Authorization Package: Referenced within the IGC FedRAMP authorization package (Package ID: FR2429166928) at https://www.fedramp.gov/marketplace/products/FR2429166928/. Agency ISSOs and System Owners are directed to this document as part of the authorization package.
- Ideagen Customer Support: The current version is available to agency customers through Ideagen's customer support channels under the FedRAMP / Compliance documentation category. Contact your Ideagen account representative for access.
- Direct Request: Agencies may request the latest version by contacting security@ideagen.com or their Ideagen Customer Success Manager.
- Public Version: In accordance with FedRAMP SCG-CSO-PUB, a version of this guide is made publicly available through the FedRAMP Marketplace listing for Package FR2429166928.

How to use this guide:

- Before Initial Provisioning: Review Sections 3, 4, and 5 in full before creating accounts or configuring SSO. This establishes the required security baseline.
- Initial Configuration Verification: Complete the checklist in Section 8 immediately after SSO configuration and initial account provisioning. Retain as evidence for SSP Appendix J (CRM).
- Annual FedRAMP Review: Re-verify all required items in the Section 8 checklist as part of each annual FedRAMP assessment cycle.
- Privileged Account Changes: Consult Section 3 (Application Administrator) or Section 4 (Product Administrator, Module Developer, Ideagen personnel access) before any changes to privileged accounts.
- ISSO Compliance Documentation: The Section 8 checklist serves as structured evidence for agency AC-2, IA-2, AU-2, and related control implementations. Document the verifying official and date for each line item.

1.3 Scope

 © 2026 Ideagen. All rights reserved.

This guide applies to all FedRAMP Moderate authorized deployments of Ideagen Government Cloud – EHS Enterprise (Package ID: FR2429166928). It covers:

- Top-level administrative account provisioning, configuration, and decommissioning
- Privileged account roles and security-relevant settings
- Identity and authentication configuration – including mandatory SSO integration with the agency Identity Provider (IdP)
- Audit logging and monitoring settings
- User and access management including deprovisioning
- Secure decommissioning procedures

Infrastructure-level controls – cloud hosting configuration, vulnerability scanning, EDR, and SIEM ingestion – are Ideagen-managed, documented in the SSP, and are not customer-configurable.

1.4 Audience

- Authorizing Officials (AOs) – to understand the overall security posture achievable through correct configuration
- ISSOs – to verify and document configuration compliance against SSP controls and the Customer Responsibility Matrix (CRM)
- System Owners – to understand customer responsibilities in the IGC CRM
- Application Administrators (individuals holding the UACA role) – to implement and maintain secure configuration settings

1.5 Mandatory SSO Compliance Requirement

MANDATORY FedRAMP COMPLIANCE REQUIREMENT – Agency SSO Integration Required

For FedRAMP compliance, ALL agency users of Ideagen Government Cloud MUST authenticate via Single Sign-On (SSO). IGC uses Okta (FedRAMP Package ID: F1512167750), managed entirely by Ideagen, as its authentication platform. Agencies do not configure Okta directly. Instead, agencies connect their own Identity Provider (IdP) to the Ideagen Okta instance via SAML 2.0 or OIDC. Direct username/password authentication to IGC is NOT compliant with the IGC FedRAMP Moderate authorization.

The system's Digital Identity Level is IAL2/AAL2/FAL2, which requires multi-factor authentication via FIPS 140-validated cryptography. AAL2 MFA must be enforced by the agency IdP for all users accessing IGC.

Agencies that have not yet configured SSO must treat this as a Priority 1 remediation action and document the gap in their POA&M with a target completion date.

See Section 5 for complete SSO integration instructions.

1.6 Relationship to Other FedRAMP Documentation

This guide supplements but does not replace the following IGC FedRAMP documentation:

- SSP v1.1 (FedDoc-201, January 6, 2026) – the authoritative security blueprint for IGC (FedRAMP Package FR2429166928)
- SSP Appendix J – CIS and CRM Workbook – defines shared control responsibilities between Ideagen and agency customers
- SSP Appendix F – Rules of Behavior – governs acceptable use by agency personnel
- SSP Appendix I – Incident Response Plan

 © 2026 Ideagen. All rights reserved.

- SSP Appendix N – Continuous Monitoring Plan

> **NOTE**
> Where this guide conflicts with agency-specific policies, the more restrictive control applies. Document any deviations from recommended settings in the agency POA&M.

 © 2026 Ideagen. All rights reserved.

2. IGC EHS Enterprise – System Overview

2.1 Service Description

Ideagen Government Cloud (IGC) – EHS Enterprise is a FedRAMP Moderate Authorized, cloud-based Environment, Health, and Safety (EHS) management platform delivered as a multi-tenant SaaS offering. The platform provides EHS workflow management including incident reporting, corrective actions, audits, inspections, risk assessments, training management, and comprehensive audit trails. The highly configurable nature of the underlying no-code platform enables IGC customers to extend their implementation to any operational workflow through which data is ingested, routed, managed, and analyzed. It is available to federal, state, local, and tribal governments, as well as research institutions and federal contractors.

2.2 Authorization and Infrastructure

IGC holds FedRAMP Moderate Agency Authorization (Package ID: FR2429166928). The authorization boundary encompasses the application infrastructure hosted on Amazon Web Services (AWS) in the US East region, including compute, storage, and database services. All underlying infrastructure is hosted, managed, and secured by Ideagen – agency customers do not have access to or responsibility for configuring the infrastructure layer.

Authentication for all Huddle US users – both agency end-users and Ideagen internal personnel – is managed through Okta, the platform's designated authentication service. Agency customers interact with Okta solely through the SSO integration described in Section 5 of this guide.

Security operations at the infrastructure level – including vulnerability scanning, endpoint detection and response, security information and event management, and system health monitoring – are performed and managed by Ideagen's security team. These are not customer-configurable controls and are fully documented in the IGC SSP and FedRAMP authorization package

2.3 Account and Role Hierarchy

IGC implements fine-grained role-based access control, enabling agencies to apply the principle of least privilege with precision. Access is composed from discrete functional permissions – ensuring no user holds more access than their specific duties require. This guide uses the following account terminology, organised by privilege tier:

Account Type	Tier	Description	Security Guidance
Application Administrator (holds UACA role in IGC)	Privileged – Tier 1	Highest privilege within a customer organization's IGC instance. The Application Administrator holds the User Access Control Administrator (UACA) role – the only role able to grant or revoke all other roles, including additional Application Administrator accounts. Controls organization-wide settings: SSO	Named individuals only. Authenticated via agency IdP SSO with AAL2 MFA. Separate from day-to-day accounts. Minimum 2 accounts. Quarterly access review. See Section 3.

 © 2026 Ideagen. All rights reserved.

		configuration, user provisioning, role assignment, and audit access.	
Product Administrator	Privileged – Tier 2	Agency personnel with elevated access to one or more EHS program areas. Can manage module configurations, workflows, data, and reporting within assigned scope. Cannot provision users system-wide or access platform-level configuration.	Named individual accounts. Documented business justification. Semi-annual access review. See Section 4.1.
Module Developer (agency-assigned, advanced customers)	Privileged – Tier 2	Access to configure and extend IGC modules, workflows, and forms. Used by advanced agency customers who take on module customization in-house. Most agencies defer this work to Ideagen Application Engineers.	Treat as privileged-equivalent. Quarterly review. Scope to active development work; remove on project completion. See Section 4.2.
Product Debug	Non-Privileged	Diagnostic read access for troubleshooting. Does not include data modification or role assignment capability.	Assign only with documented need. Remove when troubleshooting activity concludes.
Product Participant	Non-Privileged	Standard end-users accessing EHS workflows and data. Access scoped to assigned modules and organizational units.	Least privilege applies. Remove promptly on role change or departure.

NOTE – Ideagen Personnel Roles (TAM / AE)

IGC Technical Account Manager (TAM) and Application Engineer (AE) are Ideagen-managed privileged roles used by Ideagen personnel during implementation and support engagements. They are not assigned by agencies. However, agencies should be aware these accounts may be active in their environment and should verify, document, and request removal when engagements conclude. See Section 4.3.

 © 2026 Ideagen. All rights reserved.

3. Application Administrator Account Configuration

This section fulfils SCG-CSO-RSC requirements 1 and 2 of the FedRAMP Rev5 Balance Improvement Release Secure Configuration Guide standard. It covers all security-relevant settings for the Application Administrator – the top-level administrative account in IGC.

DEFINITION – Application Administrator (UACA Role)

In this guide, Application Administrator refers to the individual who holds the User Access Control Administrator (UACA) role in Ideagen Government Cloud. This is the top-level administrative account within a customer organization's IGC instance. It is the only role with authority to grant or revoke all other roles in the system – including granting additional Application Administrator accounts. The Application Administrator controls all organization-wide settings: SSO configuration, user provisioning, role assignments, security policies, and audit access. All Application Administrator actions are captured in the IGC audit trail and forwarded to the SIEM.

IGC role name: User Access Control Administrator (UACA)

Access: Administration → Users → [select user] → Edit Roles

3.1 Accessing Application Administrator Settings

To manage Application Administrator accounts and organization-wide settings in IGC:

- Log in to Ideagen Government Cloud via your agency SSO-authenticated session
- Navigate to Administration in the main navigation
- Select Users to add or edit users or roles
- Organization-wide security settings are also accessible from the Administration menu

SECURITY NOTE

Application Administrator accounts must never be shared. Each individual with Application Administrator access requires their own named account authenticated via agency IdP SSO. Generic or shared admin accounts are prohibited under FedRAMP AC-2 and the IGC Rules of Behavior (SSP Appendix F, FedDoc-201).

3.2 Provisioning Application Administrator Accounts

The following steps must be followed when provisioning a new Application Administrator account:

- Submit a formal access request identifying the individual by name and documenting the business justification for Application Administrator access
- Obtain written approval from the agency System Owner (or designated account manager) prior to account creation
- Create a named individual account – do not use shared, generic, or role-based accounts
- Ensure the account is integrated with the agency IdP SSO and subject to AAL2 MFA enforcement before granting the UACA role
- Navigate to Administration → Users → [select user] → Edit Roles and assign the User Access Control Administrator role
- Record the account in the agency's privileged access register with the approval date and approver identity
- Verify the role assignment appears in the IGC audit trail

Constraints on Application Administrator accounts:

 © 2026 Ideagen. All rights reserved.

- A minimum of 2 Application Administrator accounts must be maintained at all times to ensure continuity of administrative access
- Application Administrator accounts must not be used for routine non-administrative work – maintain a separate standard user account for day-to-day EHS platform activities
- All Application Administrator accounts must be documented in the agency access register and reviewed quarterly by the ISSO
- The UACA role must never be assigned as a standing privilege to Ideagen support personnel – any Ideagen-side Application Administrator access must be time-limited, documented in the POA&M, and revoked immediately upon completion of the task requiring it

3.3 Application Administrator Settings – Security Implications

The following table describes all security-relevant settings accessible to the Application Administrator, their security implications, and relevant SSP control mappings.

Setting / Feature	Default State	Recommended Setting	Security Impact	Where to Configure
SSO / Agency IdP Integration	Disabled (default for new tenants)	REQUIRED: SSO must be enabled. Agency connects their Identity Provider (IdP) to the Ideagen-managed Okta instance via SAML 2.0 or OIDC. Contact Ideagen Support to complete federation setup. Non-negotiable for FedRAMP compliance at AAL2.	HIGH – AAL2 (multi-factor, FIPS 140-validated crypto) is only achieved through SSO integration with the agency IdP. Direct password auth is not FedRAMP compliant at Moderate. Maps to IA-2, IA-5, IA-8, SC-13.	Administration → Preferences → SSO Settings tab – provide agency IdP SAML metadata URL or OIDC configuration. Contact Ideagen Support to complete configuration and testing.
MFA Enforcement via Agency IdP	MFA is not enforced within IGC itself; enforcement must be configured in the agency IdP	REQUIRED: Agency must enforce AAL2 MFA in their own IdP for all users accessing IGC. PIV/CAC or FIDO2 must be enforced for Application Administrator and all other privileged accounts. Coordinate with Ideagen Support to verify end-to-end enforcement.	HIGH – Without AAL2 enforcement at the agency IdP, the system does not meet its FedRAMP Moderate digital identity level (IAL2/AAL2/FAL2). Maps to IA-2(1), IA-2(2).	Agency IdP admin console – configure AAL2 MFA policy for users accessing IGC. Confirm PIV/CAC or FIDO2 enforcement for Application Administrator accounts. Coordinate with agency ISSO to verify.

 © 2026 Ideagen. All rights reserved.

Application Administrator Role Assignment	Manual via Administration → Users → Edit Roles	REQUIRED: Named individual accounts only. All Application Administrator accounts documented in agency access register with formal approval. Minimum 2 accounts.	HIGH – Uncontrolled provisioning creates privilege escalation risk; the UACA role can self-assign any other role. Maps to AC-2, AC-6.	Administration → Users → [select user] → Edit Roles → User Access Control Administrator. Provision via formal agency access request process.
Password Policy (non-SSO fallback / break-glass)	Platform default	REQUIRED: Min 14 chars, complexity (upper/lower/number/special), 60-day rotation, last-24 history, 5-attempt lockout / 15-min reset. Apply to any emergency or service accounts outside SSO scope.	HIGH – Protects residual non-SSO accounts. All agency users should be on SSO; apply this policy to any exceptions. Maps to IA-5.	Administration → Preferences → Password Policy
Session Timeout	Platform-managed default	RECOMMENDED: 30 minutes inactivity maximum. Align agency IdP session policy to match.	MEDIUM – Extended sessions on unattended devices risk unauthorized access. Maps to AC-11, AC-12.	Contact Ideagen to adjust the IGC session timeout. Configure a matching inactivity timeout in the agency IdP for the IGC application.
User Account Deprovisioning	Manual; agency IdP deprovisioning auto-revokes IGC access for SSO accounts	REQUIRED: Revoke within 24 hours of offboarding. For SSO deployments: configure and test agency IdP user lifecycle management so that deprovisioning in the IdP automatically revokes IGC access.	HIGH – Orphaned accounts are persistent access vectors. Maps to AC-2(j), PS-4.	Agency IdP admin console – configure user deprovisioning to propagate to IGC. Test the full deprovisioning flow before go-live. For non-SSO accounts: Administration → Users → [select user] → Edit Roles (remove all roles) or deactivate account.
External API / Integration Permissions	Controlled via role assignment	REQUIRED: Restrict API access and external integrations to documented, approved connections only. Only Application Administrators can assign roles that enable API access. Review quarterly.	HIGH – Uncontrolled external integrations may expose Federal data. Maps to AC-17, AC-20, CA-3.	Administration → Users → Edit Roles. API-capable roles (e.g., SQL & Dataset Administrator) must be assigned only with documented business justification.

 © 2026 Ideagen. All rights reserved.

3.4 Operating Application Administrator Accounts – Day-to-Day Guidance

Application Administrators must follow these operational practices at all times:

- Log in only via the agency IdP SSO-authenticated session – never via direct password authentication for FedRAMP-scope work
- Use the Application Administrator account only for administrative tasks – switch to a standard user account for routine EHS platform use
- Never share credentials or allow another individual to operate under your Application Administrator account
- Exercise particular caution when assigning roles – the UACA role can self-escalate to any other role in the system; review all assignments carefully before saving
- Immediately report any suspected compromise of Application Administrator credentials to the agency ISSO and to security@ideagen.com
- Review the IGC audit log for Application Administrator actions at least monthly (see Section 6)
- Complete all required annual security awareness training before administrative privileges are renewed

3.5 Decommissioning Application Administrator Accounts

When an Application Administrator account must be decommissioned (departure, role change, or privilege reduction):

- For SSO accounts: deprovision the user in the agency IdP – verify IGC access is revoked within 24 hours
- For any non-SSO emergency/break-glass accounts: navigate to Administration → Users → [select user] → Edit Roles and remove all roles, then deactivate the account within 24 hours of the deprovisioning trigger
- Verify at least one other active Application Administrator account remains before removing the departing account (minimum 2 must be maintained)
- Reassign or close any outstanding administrative tasks associated with the account
- Update the agency privileged access register to reflect the deprovisioning, including date and approver
- Retain all audit records associated with the account per the retention policy (Section 6) – satisfies AU-11
- Document the deprovisioning action in the agency access review log – satisfies AC-2(j)

> **SECURITY NOTE – Immediate Revocation**
>
> Application Administrator account deprovisioning must occur within 24 hours of any offboarding trigger – including voluntary departure, termination, or role change. Do not wait for a scheduled access review cycle.
>
> For SSO-integrated deployments, test the end-to-end deprovisioning flow (agency IdP removal → IGC access revocation) as part of initial SSO configuration and re-verify annually.

 © 2026 Ideagen. All rights reserved.

4. Privileged Account Configuration

This section fulfils SCG-CSO-RSC requirement 3 of the FedRAMP Rev5 Balance Improvement Release Secure Configuration Guide standard. It covers agency-managed privileged accounts below Application Administrator level, including Product Administrator and Module Developer roles. It also provides agency awareness guidance on Ideagen personnel access (TAM and AE roles) that may be active in a customer environment.

4.1 Product Administrator

DEFINITION – Product Administrator

The Product Administrator role grants elevated access to one or more EHS program areas in IGC. A Product Administrator can manage module configurations, workflows, data, and reporting within their assigned scope. Unlike the Application Administrator (UACA role), a Product Administrator cannot provision users system-wide, assign privileged roles, or access platform-level configuration settings.

Product Administrators are agency personnel – typically EHS program managers or team leads with a documented operational need for elevated program access. All Product Administrator actions are captured in the IGC audit trail.

Although Product Administrator is classified as a non-privileged account in the current IGC Access Control Procedures (FedProc-001), this guide treats it as privileged-equivalent because it grants elevated access to federal EHS program data and workflows. The following controls apply:

NOTE – Privilege Classification

Product Administrator accounts are treated as privileged in this guide consistent with the principle of least privilege (AC-6) and the sensitivity of EHS program data. The IGC Access Control Procedures (FedProc-001) will be updated in its next revision to formally classify Product Administrator as a privileged account. In the interim, apply the controls described in this section.

Security requirements for Product Administrator accounts:

- Named individual accounts only – no shared or generic Product Administrator accounts
- Authenticated via agency IdP SSO with AAL2 MFA enforced
- Document each Product Administrator account in the agency access register with business justification and written approval
- Product Administrator access must not be combined with Application Administrator (UACA) access on the same account
- Semi-annual access review by the agency ISSO or designated account manager; remove access promptly on role change or departure

4.2 Module Developer Role

The Module Developer role grants access to configure and extend IGC modules, workflows, and forms. It is available to advanced agency customers who take on module customization in-house. This role is also included in the Ideagen Application Engineer (AE) role bundle used during implementation and maintenance engagements.

NOTE – Most Agency Customers

Most agencies defer module development and customization to Ideagen Application Engineers to ensure smooth implementation. The Module Developer role is appropriate for agency staff only where there is a documented operational need and sufficient technical capability. If your agency plans to take

 © 2026 Ideagen. All rights reserved.

on this work internally, coordinate with your Ideagen Technical Account Manager for a proper handoff and training.

If the Module Developer role is assigned to agency personnel:

- Treat as privileged-equivalent – apply the same access controls as Product Administrator
- Named individual account; document in the agency access register with business justification
- Quarterly access review – Module Developer access should be scoped to active development work and removed when the project concludes
- Do not assign to the same account used for standard Product Participant access

4.3 Ideagen Personnel Access – Agency Awareness

Scope Note – Ideagen-Managed Privileged Roles (TAM / AE)

IGC Technical Account Manager (TAM) and Application Engineer (AE) are Ideagen-managed privileged roles. They are assigned by Ideagen to Ideagen personnel during customer implementation and support engagements. Agencies do not configure or assign these roles. However, because TAM and AE accounts appear in agency customer environments and constitute third-party privileged access to a federal system, agencies must be aware of them, include them in access reviews, and request their removal when engagements conclude.

TAM and AE are classified as privileged accounts in the IGC Access Control Procedures (FedProc-001).

Ideagen personnel role bundles for reference:

Ideagen Personnel Role	Standard Role Bundle	Purpose / Scope
IGC Technical Account Manager (TAM) (Ideagen-managed)	Module Developer Module Viewer Data Import Administrator Notifications Administrator Team Administrator User Administrator Personal Role Administrator Procedures & Forms Viewer	Platform configuration management and technical support activities conducted by Ideagen personnel on behalf of a customer. Scope limited to assigned customer environments. Does not include SQL/dataset access or Application Administrator (UACA) privileges.
IGC Application Engineer (AE) (Ideagen-managed)	Module Developer Procedures & Forms Author Data Import Administrator SQL & Dataset Administrator Module Viewer Data & Analysis Administrator Interface Developer Module Importer	Module build, workflow configuration, and data engineering activities. Used for implementation projects and ongoing platform development. Includes SQL/dataset access for report and ETL development.

What agencies should do regarding TAM/AE access:

- Request a list of any active TAM or AE accounts in your IGC environment at any time – contact your Ideagen Customer Success Manager or security@ideagen.com
- Verify that any active TAM/AE access is time-limited and associated with an active, documented engagement or support activity
- Include Ideagen personnel access in quarterly privileged account access reviews – document as 'Ideagen-managed, verified [date]' in the agency access register

 © 2026 Ideagen. All rights reserved.

- Request removal of TAM/AE access when the associated engagement concludes – do not allow access to persist indefinitely after implementation or support work ends
- Disclose active Ideagen personnel access in the agency SSP CRM (Appendix J) – coordinate with Ideagen for the current access list

IMPORTANT – Time-Limiting Third-Party Privileged Access

Any active TAM or AE account in your IGC environment constitutes third-party privileged access to a federal system. Per AC-2 and PS-7, such access must be time-limited, documented, and reviewed. Do not allow TAM/AE access to persist indefinitely after an implementation or support engagement concludes.

If you are uncertain whether any Ideagen personnel currently have active privileged access to your IGC environment, contact security@ideagen.com immediately.

4.4 Privileged Account Access Review

The following review cadence applies to all privileged accounts in IGC. Document all review outcomes in the agency access review log – satisfies AC-2(j).

Account Type	Review Frequency	Review Actions
Application Administrator (UACA role)	Quarterly	Confirm continued business need. Verify account is named individual, separate from day-to-day account. Minimum 2 accounts maintained. Remove if no longer required.
Product Administrator	Semi-annual	Confirm continued business need. Verify scope of access is appropriate to current duties. Reduce or remove if responsibilities have changed.
Module Developer (agency-assigned)	Quarterly	Confirm active development work justifies continued access. Remove upon project completion. Do not allow to persist as a standing access.
Ideagen Personnel (TAM / AE)	Quarterly (agency-verified, Ideagen-managed)	Verify with Ideagen that access is still associated with an active, documented engagement. Request removal if engagement has concluded. Document as 'Ideagen-managed, verified [date]' in agency access register.

 © 2026 Ideagen. All rights reserved.

5. Identity and Authentication Configuration

5.1 SSO Architecture – Ideagen-Managed vs Agency-Managed

Scope Clarification – What Ideagen Manages vs What Agencies Configure

Ideagen-managed (not customer-configurable): Okta (FedRAMP Package F1512167750) is Ideagen's authentication platform. Ideagen owns and operates the Okta instance, sets IGC application-level authentication policies within Okta, and maintains the FIPS 140-validated cryptographic assertions. Agencies do not have access to the Ideagen Okta admin console.

Agency-managed: Agencies configure their own Identity Provider (IdP) – such as Azure AD, ADFS, or another FedRAMP-authorized identity service – and connect it to the Ideagen Okta instance via SAML 2.0 or OIDC. The agency IdP controls MFA policy, PIV/CAC enforcement, user lifecycle management, and session policies for their users.

IGC-configurable: The agency IGC administrator configures the SSO connection in Administration → Preferences → SSO Settings by providing the agency IdP SAML metadata URL or OIDC configuration. Ideagen Support completes the federation setup on the Okta side.

Authentication for IGC at FedRAMP Moderate is delivered through Ideagen's Okta instance (FedRAMP Package ID: F1512167750). All users – both agency end-users and Ideagen personnel – authenticate through Okta. This architecture achieves AAL2: FIPS 140-validated multi-factor cryptography with signed and encrypted assertions at FAL2.

The SSO integration (agency IdP → Ideagen Okta → IGC) delivers:

- AAL2/MFA enforcement via the agency IdP – satisfies IA-2(1) and IA-2(2)
- FIPS 140-validated cryptography in authentication assertions at FAL2 – satisfies SC-13
- Account lifecycle management tied to the agency's authoritative identity source – satisfies AC-2
- Automatic access revocation upon agency IdP deprovisioning – satisfies AC-2(j), PS-4
- Remote identity proofing at IAL2 with trusted referee where applicable – satisfies IA-12

To initiate SSO configuration: navigate to Administration → Preferences → SSO Settings tab, enter the agency IdP SAML metadata URL or upload the OIDC configuration, then contact Ideagen Support (support.ideagen.com) to complete federation on the Okta side and test the end-to-end authentication flow. Contact Ideagen Support to initiate this process. SSO must be configured and verified before any agency user accounts are provisioned in IGC.

5.2 Agency IdP Configuration Checklist

The following items must be configured and verified within the agency's own Identity Provider before IGC SSO go-live. These are agency responsibilities — they are not configurable by Ideagen. Coordinate with Ideagen Support to test the end-to-end authentication and deprovisioning flows.

- AAL2 MFA policy: enforced in the agency IdP for all users accessing IGC
- PIV/CAC or FIDO2: enforced via agency IdP for all UACA and privileged accounts (Section 5.3)
- SMS OTP: not permitted as an authentication method for IGC users in the agency IdP
- Session timeout: agency IdP session aligned to 30-minute inactivity maximum for IGC
- User deprovisioning: agency IdP lifecycle management configured and tested – IGC access revoked within 24 hours of IdP deprovisioning
- Agency IdP authentication audit logs: captured and forwarded to agency SIEM for AU-6 compliance

 © 2026 Ideagen. All rights reserved.

5.3 Federal PIV/CAC Requirement

FEDERAL REQUIREMENT – PIV/CAC Enforcement

OMB M-22-09 requires federal agencies to use phishing-resistant MFA for all access to agency systems. PIV/CAC or FIDO2 hardware keys must be enforced for all privileged accounts (UACA, TAM, AE). Agencies must configure their IdP to enforce PIV/CAC or FIDO2 authentication for IGC users. Ideagen Support can assist in verifying that PIV-authenticated assertions are correctly passed through to IGC.

SMS OTP is not a permitted authentication factor for IGC. Ensure it is disabled in the agency IdP policy for users accessing IGC.

5.4 Emergency / Break-Glass Account Policy

For any break-glass or emergency accounts outside SSO scope (e.g., during initial tenant setup before SSO is configured), apply and document the following:

- Minimum 14-character password with complexity (upper/lower/number/special character)
- 60-day maximum password age; prohibit last-24 password reuse
- 5-failed-attempt lockout with 15-minute reset
- Document all such accounts in the agency POA&M as exceptions until SSO is fully operational
- Review quarterly; disable immediately once SSO is confirmed working
- Log and review all use of emergency accounts after each incident

 © 2026 Ideagen. All rights reserved.

6. Audit Logging and Monitoring

6.1 Audit Trail Architecture

IGC maintains a tamper-evident audit trail of all user and administrative activity. Audit logging is a platform-level control and cannot be disabled by customers. AWS CloudTrail provides additional infrastructure-level audit logging for all AWS API activity within the authorization boundary.

Customer-relevant events captured in the IGC audit trail include:

- Authentication events – login (success/failure), logout, session creation/termination, MFA challenges
- Administrative actions – account creation/deletion/modification, role assignment/removal, SSO configuration changes
- Data actions – record creation, modification, deletion, export, approval/rejection
- Module management – configuration changes, workflow modifications, permission changes
- Any integration or API access events

Audit records include: UTC timestamp, user identity (authenticated via SSO), action type, target object, source IP address, and outcome (success/failure). These align to AU-2 (Audit Events) and AU-3 (Content of Audit Records) control implementations in SSP v1.1.

6.2 Agency Access to Audit Records

IGC provides UACA accounts with an in-application audit trail view accessible via Administration → Admin Audit Trail. This view surfaces user and administrative activity recorded by the platform and supports agency AU-6 (Audit Review, Analysis, and Reporting) obligations at the application level.

> **NOTE – SIEM Access**
>
> The underlying SIEM infrastructure is Ideagen-managed and is not directly accessible by agency customers. Agencies requiring SIEM-level audit data – for example, to satisfy AU-6 reporting obligations or incident investigation – should submit a request to Ideagen. Ideagen will provide relevant log extracts in response to documented agency requests.

6.3 Log Retention

- IGC audit logs are retained by Ideagen for a minimum of 30 months, satisfying AU-11

6.4 Priority Events for Agency Monitoring

- Multiple failed authentication attempts from a single account or IP – potential credential attack
- Successful authentication from an IP outside agency network ranges
- Changes to Application Administrator (UACA) accounts or SSO configuration
- Assignment or removal of privileged roles (Application Administrator/UACA, Product Administrator, Module Developer, TAM/AE)
- Bulk data exports – particularly from modules containing CUI
- UACA logins outside normal business hours
- Any use of emergency/break-glass accounts
- SQL & Dataset Administrator role assignment or any direct database query activity

 © 2026 Ideagen. All rights reserved.

7. Secure Decommissioning

7.1 Offboarding Individual Users

See Section 3.5 for Application Administrator account decommissioning. For standard and privileged users:

- For SSO accounts: deprovision in agency Okta/IdP – verify IGC access is revoked within 24 hours
- For non-SSO accounts: navigate to Administration → Users → [select user] → Edit Roles, remove all roles, and deactivate the account within 24 hours
- Reassign any outstanding tasks, approvals, or assigned records
- Retain all audit records associated with the user per retention policy (Section 6.3) – satisfies AU-11
- Document deprovisioning action in agency access review log – satisfies AC-2(j)

7.2 Full Tenant Decommissioning

- Notify Ideagen (security@ideagen.com and account representative) at least 30 days in advance
- Export all data, records, and audit logs before account suspension
- Upon suspension: Ideagen provides 90 days of restricted access for data retrieval
- After 90-day suspension window: content permanently deleted per SSP v1.1 data deletion policy
- Obtain written data deletion confirmation from Ideagen – required for MP-6 (Media Sanitization) documentation
- Revoke IGC application from agency Okta tenant and remove SSO configuration

 © 2026 Ideagen. All rights reserved.

8. Recommended Secure Configuration Checklist

This checklist covers the minimum customer-configurable items for ISSO verification at initial configuration and each annual review. It fulfils SCG-CSO-RSC and supports SCG-ENH-CMP (comparison to baseline). Retain as part of agency SSP Appendix J (CRM) evidence.

> **NOTE – Scope**
> This checklist covers agency-configurable and agency-verifiable items only. Ideagen-managed infrastructure is documented in the SSP and is not included here.

Configuration Item	Status	Verified By / Date
SSO integration: agency IdP connected to Ideagen Okta (F1512167750) via SAML 2.0 or OIDC – configured and tested with Ideagen Support	REQUIRED	
AAL2 MFA enforced in agency IdP for all IGC users	REQUIRED	
SMS OTP not permitted in agency IdP for IGC users	REQUIRED	
PIV/CAC or FIDO2 enforced via agency IdP for Application Administrator and all privileged accounts	REQUIRED	
Agency IdP user deprovisioning tested end-to-end: IGC access revoked within 24 hours of IdP deprovisioning	REQUIRED	
Application Administrator accounts (UACA role): named individuals only – minimum 2 accounts maintained	REQUIRED	
Application Administrator accounts: separate from day-to-day user accounts	REQUIRED	
Application Administrator accounts: documented in agency privileged access register	REQUIRED	
Product Administrator accounts: named individuals only, documented with business justification in agency access register	REQUIRED	
Module Developer role (agency-assigned): assigned only for active development work, documented, removed on project completion	REQUIRED if applicable	
SQL & Dataset Administrator: assigned only with documented business justification	REQUIRED	
Ideagen personnel privileged access (TAM/AE): time-limited, verified by ISSO, documented in agency access register	REQUIRED	
Ideagen personnel access: removal requested upon conclusion of engagement – no standing access permitted	REQUIRED	

 © 2026 Ideagen. All rights reserved.

Break-glass / non-SSO accounts: password policy applied (14+ chars, 60-day rotation, lockout) and documented in POA&M	REQUIRED if applicable	
Session timeout: 30 minutes inactivity maximum (IGC + agency IdP aligned)	REQUIRED	
Quarterly privileged account access review: Application Administrator, Module Developer, Ideagen personnel – completed and documented	REQUIRED	
Semi-annual access review: Product Administrator accounts – completed and documented	REQUIRED	

 © 2026 Ideagen. All rights reserved.

9. Enhanced Capabilities Statement

The FedRAMP Rev5 Balance Improvement Release includes recommendations (SCG-ENH-*) for enhanced configuration management capabilities. These recommendations apply to all cloud service offerings in the FedRAMP Marketplace. This section documents IGC's current capability status against each recommendation.

> **NOTE**
> All items in this section are FedRAMP SHOULD recommendations, not MUST requirements. The statements below reflect IGC's current capabilities and planned enhancements as of the publication date of this guide.

9.1 Comparison Capability (SCG-ENH-CMP)

FedRAMP Guidance: Providers SHOULD offer the capability to compare all current settings for top-level administrative accounts and privileged accounts to the recommended secure defaults.

IGC Status: IGC does not currently offer an automated in-platform configuration comparison tool. The Section 8 checklist in this document is provided as a structured manual comparison baseline. Agencies should use this checklist to assess current settings against the recommended configuration at initial setup and during each annual review cycle.

Planned Enhancement: Ideagen is evaluating automated configuration drift detection as a future platform enhancement. Any such capability will be documented in subsequent versions of this guide.

9.2 Export Capability (SCG-ENH-EXP)

FedRAMP Guidance: Providers SHOULD offer the capability to export all security settings in a machine-readable format.

IGC Status: The IGC audit trail (Administration → Admin Audit Trail) provides exportable records of all role assignment and configuration change events. This supports point-in-time documentation of the security configuration state. UACA holders may export audit trail data from this view.

A dedicated security configuration export in a structured machine-readable format is under evaluation for a future release. Agencies requiring a full security settings export may contact security@ideagen.com.

9.3 API Capability (SCG-ENH-API)

FedRAMP Guidance: Providers SHOULD offer the capability to view and adjust security settings via an API or similar capability.

IGC Status: Role and access management is currently performed through the application interface (Administration → Users → Edit Roles). IGC does not currently expose a dedicated security configuration management API.

Ideagen is evaluating API-based configuration management capabilities for future releases. Updates will be reflected in subsequent versions of this guide and communicated to agency customers via the FedRAMP security inbox.

9.4 Machine-Readable Guidance (SCG-ENH-MRG)

FedRAMP Guidance: Providers SHOULD provide the Secure Configuration Guide in a machine-readable format that can be used by customers or third-party tools to compare against current settings.

 © 2026 Ideagen. All rights reserved.

IGC Status: This guide is currently published in document form (.docx), referenced in the FedRAMP authorization package and available via the Ideagen support portal. A machine-readable version of the secure configuration baseline (e.g., OSCAL-compatible format) is under evaluation.

Ideagen will notify agency customers via the FedRAMP security inbox upon availability of a machine-readable version.

9.5 Versioning and Release History (SCG-ENH-VRH)

FedRAMP Guidance: Providers SHOULD provide versioning and a release history for recommended secure default settings for top-level administrative accounts and privileged accounts as they are adjusted over time.

IGC Status: This guide is version-controlled as reflected in the Document Revision History on the cover page. Version history tracks material changes to security settings recommendations aligned to IGC SSP revision cycles. Ideagen publishes updated versions of this guide concurrent with any changes to the recommended security baseline, with a summary of changes in the revision history table.

Agencies subscribed to the FedRAMP marketplace listing for Package FR2429166928 will be notified of guide updates via the FedRAMP security inbox process.

 © 2026 Ideagen. All rights reserved.

10. Support and Contact Information

10.1 Ideagen Contacts

Contact Type	Contact Details
System Owner	John Molamphy, CTO – John.Molamphy@Ideagen.com | +44 115 857 6824 ext 21531
ISSO (Ideagen)	Josh Monk, VP Global Cyber Security – josh.monk@ideagen.com | +44 115 857 6824 ext 20063
Security Incidents & Vulnerability Reports	security@ideagen.com P1 Critical/System Outage: 1-hour response target P2 High: 2-hour | P3 Normal: 8-hour | P4 Low: 12-hour
FedRAMP / Configuration Support	Contact Ideagen Customer Support – select the FedRAMP / Compliance category. For SSO configuration, SIEM integration, or access to the FedRAMP authorization package, contact your Ideagen account representative.
FedRAMP Package Access	Package FR2429166928 – available via FedRAMP Marketplace at https://www.fedramp.gov/marketplace/products/FR2429166928/ Contact your Ideagen account representative for PMO repository access.

10.2 Key References

- IGC System Security Plan (SSP) v1.1 – FedDoc-201 (January 6, 2026) – FedRAMP Marketplace, Package FR2429166928
- SSP Appendix J – CIS and CRM Workbook (FedDoc-211) – defines customer control responsibilities
- SSP Appendix F – Rules of Behavior (FedDoc-007)
- SSP Appendix I – Incident Response Plan (FedDoc-010)
- SSP Appendix N – Continuous Monitoring Plan (FedDoc-015)
- SSP Appendix Q – Cryptographic Modules Table (FedDoc-218)
- Ideagen Federal Access Control Procedures (FedProc-001) – IGC Application Role Definitions
- FedRAMP Rev5 Balance Improvement Release – Secure Configuration Guide (SCG-CSO-RSC) – fedramp.gov
- NIST SP 800-53 Rev5 – Security and Privacy Controls
- NIST SP 800-63B – Digital Identity Guidelines: Authentication and Lifecycle Management
- OMB M-22-09 – Moving the U.S. Government Toward Zero Trust Cybersecurity Principles

DOCUMENT CONTROL

This document is subject to annual review aligned to the IGC SSP revision cycle. For the most current version, contact your Ideagen Customer Success Manager or security@ideagen.com.

 © 2026 Ideagen. All rights reserved.