IDEAGEN HUDDLE US

FedRAMP Secure Configuration Guide

Document Version	1.0
Publication Date	April 2026
SSP Version Referenced	v9.0 (January 22, 2025) — FedDoc-101
FedRAMP Package ID	F1408115175
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@huddle.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 Huddle US, a FedRAMP Moderate Authorized cloud service (Package ID: F1408115175). Distribution is limited to agency Authorizing Officials, System Owners, ISSOs, and authorised administrators. Do not reproduce or distribute beyond authorised personnel without written consent from Ideagen.

Document Revision History

Version	Date	Description
1.0	April 2026	Initial publication. Aligned to Huddle US SSP v9.0 (FedDoc-101, January 22, 2025), FedRAMP Moderate. Addresses RFC-0015 FRR-RSC-01 through FRR-RSC-10.

This guide is aligned to the Huddle US SSP v9.0 and will be reviewed annually or upon SSP revision, control baseline change, or updated FedRAMP configuration standards.

1. Introduction

1.1 Purpose

This Secure Configuration Guide (SCG) provides Federal agency customers with clear, actionable instructions for securely configuring Ideagen Huddle US. It is published in accordance with FedRAMP RFC-0015 (Recommended Secure Configuration Standard) and is grounded in the Huddle US System Security Plan (SSP) v9.0 (FedRAMP Package ID: F1408115175).

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 Huddle US in alignment with their FedRAMP compliance obligations.

1.2 Scope

This guide applies to all FedRAMP Moderate authorised deployments of Ideagen Huddle US (Package ID: F1408115175). It covers:

- Top-level administrative account (Company Administrator) provisioning and configuration
- Privileged account (Workspace Manager) roles and security-relevant settings
- Identity and authentication configuration — including mandatory SSO/Okta integration
- Workspace security controls: permissions, file sharing, and external collaboration
- Audit logging and monitoring settings
- Data protection controls
- User and access management including deprovisioning
- Secure decommissioning procedures

Infrastructure-level security controls — including network configuration, vulnerability management, endpoint protection, and security monitoring — are performed and managed by Ideagen. These are not customer-configurable and are fully documented in the Huddle US SSP and FedRAMP authorization package (Package ID: F1408115175).

1.3 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 Appendix J (CRM)
- System Owners — to understand customer responsibilities in the Huddle US CRM (SSP Appendix J, FedDoc-111)
- Company Administrators (Portal Admins) — to implement and maintain secure configuration settings

1.4 Mandatory SSO Compliance Requirement

MANDATORY FedRAMP COMPLIANCE REQUIREMENT — SSO Required

For FedRAMP compliance, ALL agency users of Ideagen Huddle US MUST authenticate via Single Sign-On (SSO) integrated with the agency Identity Provider (IdP). Direct username/password

authentication to Huddle US is NOT compliant with the Huddle US FedRAMP Moderate authorization. The system's Digital Identity Level is IAL2/AAL2/FAL2, which requires multi-factor authentication via FIPS 140-validated cryptography — this is achieved only through SSO integration with the agency IdP. 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.

1.5 Relationship to Other FedRAMP Documentation

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

- SSP v9.0 (FedDoc-101) — the authoritative security blueprint for Huddle US
- Appendix J — CIS and CRM Workbook (FedDoc-111) — defines shared control responsibilities between Ideagen and agency customers
- Appendix F — Rules of Behavior (FedDoc-007) — governs acceptable use by agency personnel
- Appendix I — Incident Response Plan (FedDoc-010)
- Appendix N — Continuous Monitoring Plan (FedDoc-015)

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.

2. Huddle US — System Overview

2.1 Service Description

Ideagen Huddle US is a FedRAMP Moderate Authorized, cloud-based secure collaboration and document management platform delivered as a multi-tenant SaaS offering. It is hosted on Amazon Web Services (AWS) in the us-east-1 (US East) region. The platform provides Workspace-based collaboration including document sharing, version control, approval workflows, task management, and comprehensive audit trails.

Per SSP Section 8.1, the key platform capabilities are: web-based Workspace areas for content access and collaboration; hierarchical file storage with document preview and metadata search; document workflows (approvals, comments, version history); permission models at folder and Workspace level; task creation and tracking; and a dashboard for team activity overview.

2.2 Authorization and Infrastructure

Huddle US holds FedRAMP Moderate Agency Authorization (Package ID: F1408115175, fully operational since April 17, 2015, SSP v9.0 dated January 22, 2025). 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 Huddle US SSP and FedRAMP authorization package (Package ID: F1408115175).

2.3 Account and Role Hierarchy

Huddle US uses a layered privilege model across three account types (per SSP Section 8.1 — Types of Users):

Account / Role	Description	Security Guidance
Company Administrator (Top-Level Admin Account)	Highest privilege within a customer organisation's Huddle US instance. Controls all organisation-wide settings: SSO configuration, user provisioning, Workspace creation, security policies, and audit access.	Named individuals only. Authenticated via agency IdP SSO with AAL2 MFA. Separate from day-to-day accounts. Minimum 2, maximum 5 accounts. All actions are audit-logged.

Account / Role	Description	Security Guidance
Workspace Manager (Privileged Account)	Elevated permissions within assigned Workspaces: inviting users, setting permissions, managing tasks/approvals, modifying Workspace settings. Cannot access Company Settings.	Grant only with documented business need. Review quarterly. All actions are audit-logged.
Standard / External User	Customer end-users accessing the platform via the web application. Access scoped to invited Workspaces. Permissions set by Workspace Manager.	Least privilege applies. Apply access expiry for external users. Remove promptly on role change or departure.

3. Top-Level Administrative Account Configuration

This section fulfils FRR-RSC-01 and FRR-RSC-02 of RFC-0015. It covers all security-relevant settings accessible only to the Company Administrator (top-level administrative account).

DEFINITION — Top-Level Administrative Account
In Huddle US, the Company Administrator is the top-level administrative account. It has complete control over the organisation's Huddle US instance including all users, Workspaces, SSO configuration, security settings, and billing. All Company Administrator actions are captured in the Huddle US audit trail. Access: Account menu (top-right) > Settings > Company Settings.

3.1 Accessing Company Administrator Settings

1. Log in to Ideagen Huddle US via your agency SSO/Okta authenticated session
2. Navigate to the account menu (top-right corner) and select Settings
3. Select Company Settings from the left-hand navigation panel
4. All organisation-wide security and configuration settings are available here

SECURITY NOTE
Company Administrator accounts must never be shared. Each individual with administrative access requires their own named account authenticated via agency IdP/Okta SSO. Generic or shared admin accounts are prohibited under FedRAMP AC-2 and the Huddle US Rules of Behavior (SSP Appendix F, FedDoc-007).

3.2 Company Administrator Settings — Security Implications

The following table describes all security-relevant settings operable exclusively by the Company Administrator, their security implications, and the relevant SSP control mappings.

Setting / Feature	Default State	Recommended Setting	Security Impact	Where to Configure
SSO Integration	Disabled (default for new tenants)	REQUIRED: Must be enabled and integrated with agency IdP. Non-negotiable for FedRAMP compliance at AAL2.	**HIGH — AAL2 (multi-factor, FIPS 140-validated crypto) is only achieved through SSO. Direct password auth is not FedRAMP compliant at Moderate. Maps to IA-2, IA-5, IA-8, SC-13.**	Settings > Company Settings > Security > Single Sign-On. Contact Ideagen for SAML 2.0 / OIDC configuration assistance.
MFA Enforcement	Not enforced within Huddle;	REQUIRED: Confirm AAL2 MFA is enforced in agency	**HIGH — Without AAL2**	Agency IdP admin console

Setting / Feature	Default State	Recommended Setting	Security Impact	Where to Configure
	enforced at agency IdP level	IdP for Huddle US users. Verify PIV/CAC enforcement for privileged accounts. This is an IdP-level control — not configurable within Huddle US.	**enforcement, the system does not meet its FedRAMP Moderate digital identity level (IAL2/AAL2/FAL2). Maps to IA-2(1), IA-2(2).**	— apply MFA sign-on policy for the Huddle US SSO application. Verify with agency ISSO.
Company Administrator Provisioning	Manual account creation	REQUIRED: Named individual accounts only; 2–5 admins. All admin accounts documented in agency access register with formal approval.	**HIGH — Uncontrolled admin provisioning creates privilege escalation risk. Maps to AC-2, AC-6.**	Settings > Company Settings > Users & Permissions. Provision via formal agency access request process.
Workspace Creation Permissions	All users can create Workspaces	RECOMMENDED: Restrict to Company Administrators only. Prevents unmanaged data repositories with inconsistent security controls.	**MEDIUM — Unrestricted Workspace creation produces data stores outside ISSO visibility. Maps to CM-7 (least functionality).**	Settings > Company Settings > Workspace Settings > Workspace Creation
External User Invitation Policy	Any user can invite external guests	REQUIRED: Restrict external invitations to Company Administrators and Workspace Managers only.	**HIGH — Unrestricted external invitation exposes Federal data to unvetted parties. Maps to AC-17, AC-20.**	Settings > Company Settings > Security > External Sharing
Public File Sharing Links	Disabled by default	REQUIRED: Confirm disabled. Do not enable under any circumstances in a FedRAMP deployment. Verify at each annual review.	**HIGH — Public links bypass all authentication. Federal data must never be accessible via unauthenticated URLs. Maps to AC-3, AC-4. Attempted enablement should generate a security alert.**	Settings > Company Settings > Security > File Sharing. Document verification in ISSO configuration record.
Password Policy (non-	Platform default	REQUIRED: Min 14 chars, complexity (upper/lower/number/special),	**HIGH — Protects residual non-SSO accounts. All**	Settings > Company Settings >

Setting / Feature	Default State	Recommended Setting	Security Impact	Where to Configure
SSO fallback accounts)		60-day rotation, last-24 history, 5-attempt lockout / 15-min reset. Apply to any emergency or service accounts outside SSO scope.	**agency users should be on SSO; apply this policy to any exceptions. Maps to IA-5.**	Security > Password Settings
Session Timeout	Platform-managed default	RECOMMENDED: 30 minutes inactivity maximum. Align Okta session policy to match.	**MEDIUM — Extended sessions on unattended devices risk unauthorised access. Maps to AC-11, AC-12.**	Settings > Company Settings > Security > Session Settings. Also configure matching timeout in Okta.
Audit Log Retention	Platform default	REQUIRED: Minimum 30 months total retention. Ideagen retains audit records for 30 months as part of the platform's FedRAMP continuous monitoring obligations.	**HIGH — Supports AU-11 (Audit Record Retention). Retention is managed by Ideagen at the platform level.**	Settings > Company Settings > Audit & Compliance > Log Retention. Contact Ideagen support to confirm retention configuration for your tenancy.
User Account Deprovisioning	Manual; SSO deprovisioning auto-revokes Huddle access	REQUIRED: Revoke within 24 hours of offboarding. For SSO deployments: confirm Okta/IdP deprovisioning automatically revokes Huddle access. Test this flow.	**HIGH — Orphaned accounts are persistent access vectors. Maps to AC-2(j), PS-4.**	Settings > Company Settings > Users & Permissions. For SSO: confirm Okta SCIM or JIT deprovisioning is configured and tested.
IP Allow-Listing	Not enabled by default	RECOMMENDED: Restrict access to agency network CIDR ranges and approved VPN blocks to reduce the external attack surface.	**MEDIUM — Reduces attack surface by limiting access to known network origins. Maps to SC-7.**	Settings > Company Settings > Security > Network Access

Setting / Feature	Default State	Recommended Setting	Security Impact	Where to Configure
Security Alert Notifications	Default email to admin	RECOMMENDED: Direct notifications to agency ISSO and SOC/security team email. Supports AU-6 and IR-6 obligations.	**MEDIUM — Security events not reaching the right personnel delay incident response. Maps to AU-6, IR-6.**	Settings > Company Settings > Notifications & Alerts

4. Privileged Account Configuration

This section fulfils FRR-RSC-03 of RFC-0015. It covers settings operable by Workspace Manager accounts (privileged accounts) and their security implications.

DEFINITION — Privileged Account (Workspace Manager)
Workspace Managers have elevated permissions within assigned Workspaces: inviting users, setting file/folder permissions, managing tasks/approvals, and modifying Workspace settings. They cannot access Company Settings (organisation-wide configuration). All Workspace Manager actions are audit-logged.

4.1 Workspace Manager Settings — Security Implications

Setting / Feature	Default State	Recommended Setting	Security Impact	Where to Configure
Workspace Membership Management	Workspace Manager can invite any registered user	RECOMMENDED: Limit to users with documented need-to-know. Review quarterly. Remove users whose role no longer requires access.	**MEDIUM — Overly broad membership violates AC-6 (least privilege). Federal information accessible only to those with documented need-to-know.**	Within Workspace > Members tab
File / Folder Permission Levels	View, Edit, or Upload — set per user or team	REQUIRED: Grant minimum necessary permission. Default new members to View-only; escalate to Edit only where documented. Avoid Edit for all members by default.	**HIGH — Overly permissive access allows unauthorised modification of controlled documents. Maps to AC-3, AC-6.**	Within Workspace > Folder Properties > Permissions
External User Access Duration	No default expiry date	REQUIRED: Explicit access expiry date for ALL external/guest users at invitation. Maximum 90 days without formal ISSO-approved renewal review.	**HIGH — Permanent external access violates AC-2 account lifecycle. Maps to AC-2(j).**	Within Workspace > Invite External User > Access Expiry
Approval Workflow Configuration	Optional; not enforced by default	RECOMMENDED: Enable mandatory approval	**MEDIUM — Documents without approval workflows**	Within Workspace > Document

Setting / Feature	Default State	Recommended Setting	Security Impact	Where to Configure
		workflows for controlled or regulated documents to enforce review and sign-off.	**lack required review controls. Maps to CM-9, SA-10.**	Settings > Approval Workflows
File Version Control	Enabled by default	REQUIRED: Do not disable. Retain all versions. This is a core audit trail capability aligned to the SSP.	**HIGH — Disabling version control removes recovery capability and breaks audit continuity. Maps to AU-9, CP-9.**	Within Workspace > Settings > Version Control. Do not change this default.
Workspace Visibility	Private (invite-only) by default	REQUIRED: Maintain private visibility. Do not enable open or organisation-wide access.	**HIGH — Open Workspaces expose all content to any authenticated user, bypassing intended access controls. Maps to AC-3, AC-4.**	Within Workspace > Settings > Workspace Visibility. Do not change this default.
File Download Restrictions for External Users	Permitted by default	RECOMMENDED: Restrict download for external users on Workspaces containing CUI. Configure View-only members without download for sensitive content.	**MEDIUM — Unrestricted external download creates data exfiltration risk. Maps to AC-4, MP-5.**	Within Workspace > Folder Properties > Download Settings
Comment and Annotation Visibility	All Workspace members can view comments	RECOMMENDED: Review for sensitive deliberative threads. Ensure comment access aligns with document permissions for controlled content.	**LOW — Comments may contain sensitive deliberative content not intended for all participants. Maps to AC-3.**	Within Workspace > Document Comments Settings

5. Identity and Authentication Configuration

5.1 How Authentication Works in Huddle US

Huddle US uses a federated authentication model. Understanding the split between what Ideagen manages and what the agency configures is essential before setup.

Layer	Managed By	Description
Authentication platform	Ideagen	Ideagen operates and maintains the authentication infrastructure that underpins Huddle US. This is an Ideagen-managed control and is not accessible or configurable by agency customers. Details are documented in the Huddle US SSP and FedRAMP authorization package.
SSO integration (agency IdP to Huddle US)	Agency	The agency configures the connection between its Identity Provider (IdP) and Huddle US using SAML 2.0 or OpenID Connect (OIDC). This is the primary configuration action the agency must complete.
MFA policy enforcement	Agency	MFA requirements are enforced by the agency's IdP or SSO policy — not within Huddle US itself. The agency is responsible for ensuring AAL2 MFA is applied to all Huddle US users through its identity governance.
Account lifecycle (provisioning / deprovisioning)	Agency	The agency's IdP governs when accounts are created and revoked. Deprovisioning a user in the agency IdP automatically revokes their Huddle US access when SSO is correctly configured.

5.2 SSO Integration — Required Configuration

SSO integration is mandatory for FedRAMP compliance. Direct username/password authentication to Huddle US is not compliant with the Huddle US FedRAMP Moderate authorization. The system's Digital Identity Level is IAL2/AAL2/FAL2, which requires multi-factor authentication via FIPS 140-validated cryptography — this is only achieved through SSO integration with the agency IdP.

Configuring SSO delivers the following security outcomes for the agency:

- Centralised AAL2/MFA enforcement through the agency's existing identity governance — satisfies IA-2(1) and IA-2(2)
- FIPS 140-validated cryptography in signed and encrypted authentication assertions (FAL2) — satisfies SC-13
- Automatic account lifecycle management tied to the agency's authoritative identity source — satisfies AC-2
- Immediate access revocation on IdP deprovisioning — satisfies AC-2(j), PS-4

To configure SSO, navigate to Settings > Company Settings > Security > Single Sign-On and provide your agency IdP SAML metadata URL or OIDC configuration. Contact Ideagen Support for

configuration assistance specific to your IdP. SSO must be fully configured and tested before agency user accounts are provisioned.

FEDERAL REQUIREMENT — PIV/CAC and Phishing-Resistant MFA
OMB M-22-09 requires phishing-resistant MFA for all access to federal agency systems. PIV/CAC or FIDO2 hardware keys must be enforced for privileged accounts accessing Huddle US. This is configured in the agency IdP and applied through the SSO integration — it is not a setting within Huddle US. SMS OTP must not be used as an MFA factor for Huddle US access.

5.3 Agency IdP Configuration Checklist

The following must be verified by the agency's identity or SSO administrator as part of Huddle US setup:

- SSO integration configured using SAML 2.0 or OIDC, connected to the agency IdP
- AAL2 MFA enforced for all users accessing Huddle US through the agency IdP policy
- SMS OTP disabled as an MFA factor for Huddle US
- PIV/CAC or FIDO2 enforced for Company Administrator and Workspace Manager accounts
- SCIM or JIT provisioning configured to synchronise user lifecycle from agency IdP to Huddle US
- Session timeout aligned to 30-minute inactivity maximum (configured in the agency IdP session policy)
- Deprovisioning flow tested end-to-end: confirm that removing a user in the IdP revokes Huddle US access

5.4 Emergency / Break-Glass Account Policy

For any accounts that must exist outside SSO scope (e.g., during initial tenant setup before SSO is configured), the following password policy applies and must be documented:

- Minimum 14-character password with complexity (uppercase, lowercase, number, and special character)
- Maximum 60-day password age; prohibit reuse of last 24 passwords
- Account lockout after 5 failed attempts with 15-minute reset
- Document all such accounts in the agency POA&M as exceptions with a target SSO completion date
- Review quarterly; disable immediately once SSO is confirmed operational
- Log and review all use of emergency accounts after each activation

6. Audit Logging and Monitoring

6.1 Audit Trail Capabilities

Huddle US maintains a tamper-evident audit trail of all user and administrative activity within the platform. Audit logging is a platform-level control managed by Ideagen and cannot be disabled by customers. All security and activity events are captured automatically and retained for a minimum of 30 months in accordance with FedRAMP AU-11 requirements.

Customer-relevant events captured in the Huddle US audit trail:

- Authentication events — login (success/failure), logout, session creation and termination
- Administrative actions — account creation, deletion, and modification; permission changes; SSO configuration changes
- Document actions — upload, download, view, edit, version creation, deletion, approval, and rejection
- Workspace management — creation, deletion, membership changes, and permission modifications
- External user invitation and access events
- Any file sharing configuration changes

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

6.2 Accessing Audit Logs

Company Administrators access audit logs via: Settings > Company Settings > Audit & Compliance > Activity Log. Logs are filterable by date range, user, action type, and Workspace and can be reviewed directly within the portal.

6.3 Log Retention

- Huddle US 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 (requires IP allow-listing, Section 3.2)
- Changes to Company Administrator accounts or SSO/Okta configuration
- Addition of external users to Workspaces containing CUI
- Bulk file downloads from sensitive Workspaces
- Company Administrator logins outside normal business hours
- Any attempt to enable public file sharing links

7. Data Protection and Encryption

7.1 Cryptographic Modules

Per SSP Section 10, Huddle US employs FIPS 140-validated cryptographic modules configured in approved mode for all required encryption functions. Full details are in SSP Appendix Q (Cryptographic Modules Table, FedDoc-118). The encryption implementation is validated by the 3PAO during the annual security assessment. Only FIPS-approved algorithms are used.

7.2 Data in Transit

All data transmitted between users and Huddle US is encrypted using TLS 1.2 or higher. TLS 1.0 and 1.1 are disabled. HTTP traffic is automatically redirected to HTTPS. No agency configuration is required for transport encryption — this is enforced at the platform level by Ideagen.

7.3 Data at Rest

All customer content stored in Huddle US is encrypted at rest using AES-256. Encryption is enforced at the storage layer by Ideagen and is not configurable by agency customers. No agency configuration is required for at-rest encryption.

7.4 Data Residency

Huddle US operates exclusively in the AWS US East region. All Federal data remains within United States territory. Data replication for disaster recovery purposes uses US-only cloud regions. No agency configuration is required for data residency — confirm specific residency requirements with your Ideagen account representative if needed.

7.5 Data Exfiltration Controls

The following customer-configurable settings must be verified by the ISSO:

- Public link sharing: confirm disabled (Section 3.2) — default state, must not be changed
- External user download restrictions: configure per Workspace for CUI content (Section 4.1)
- IP allow-listing: configure agency network ranges to limit exfiltration vectors (Section 3.2)

CRITICAL — Public Sharing Links Prohibited
Public file sharing links must remain disabled for all FedRAMP deployments. This is the platform default. Any enablement constitutes a material configuration deviation requiring immediate POA&M entry and emergency remediation. The ISSO must verify this setting at initial configuration and at each annual review.

8. User and Access Management

8.1 Account Provisioning

- Each user must have a unique, individually named account — shared accounts are prohibited
- For SSO-integrated deployments, provision accounts via JIT provisioning or SCIM through the agency IdP — this is the preferred FedRAMP-compliant approach
- Where manual provisioning is used: a formal access request, approved by the System Owner or delegated account manager, must be completed and documented prior to account creation
- New accounts receive only the permissions required for the immediate function (AC-6 least privilege)

8.2 Access Review and Deprovisioning Schedule

Aligned to SSP AC-2(j):

- Company Administrator accounts: reviewed quarterly by ISSO; results documented in access review record
- Workspace Manager accounts: reviewed quarterly by System Owner or delegated manager
- Standard user accounts: reviewed semi-annually or on role/project change
- External / guest accounts: reviewed monthly; removed immediately on project/contract completion

For SSO/Okta-integrated deployments, deprovisioning the user in the agency IdP automatically revokes Huddle US access. Verify and document that this deprovisioning flow works correctly as part of initial SSO configuration testing. For any residual non-SSO accounts, the Company Administrator must manually deactivate within 24 hours of the deprovisioning trigger.

8.3 Privileged Access Controls

- Company Administrator accounts must not be used for routine non-administrative work — maintain separate standard user accounts for day-to-day activities
- Maintain minimum 2, maximum 5 Company Administrator accounts
- Review all privileged account activity monthly via the audit log (Section 6.2)
- Enforce AAL2 MFA for all privileged accounts through Okta regardless of standard user MFA policy

9. External Collaboration Security Controls

9.1 Governing Policy

External collaboration is a primary use case for Huddle US. Per SSP Section 8.1 (Types of Users), External Users are customer end-users and Huddle employee end-users who access the platform from outside the system boundary via public-facing web services. Their permissions are managed within the Huddle application.

The following controls align to SSP controls AC-17 (Remote Access) and AC-20 (Use of External Information Systems):

- External user invitation rights: restricted to Company Administrators and Workspace Managers (Settings > Company Settings > Security > External Sharing)
- All external users: individually named — no group or generic external accounts
- External user permissions: minimum necessary — view-only where edit is not required
- Access expiry dates: mandatory for ALL external users at invitation — maximum 90 days without ISSO-approved renewal
- Workspace scope: external users must not have access beyond the scope of their specific engagement
- Documentation: categories of external users (contractors, auditors, oversight bodies) must be documented in the agency SSP with applied controls, per AC-20

9.2 External User Access Review

- Active external users reviewed monthly by responsible Workspace Manager
- Remove users immediately on engagement completion — do not rely solely on expiry date
- Company Administrator generates quarterly external user report for ISSO review — Settings > Company Settings > Audit & Compliance > User Reports

10. External Services and System Interconnections

The following external services without FedRAMP authorization are used by Ideagen in the operation of Huddle US (documented in the Huddle US SSP, Section 7). These are Ideagen-managed integrations — agency customers do not interact with or configure these services. They are listed here so that agency ISSOs are aware of them when reviewing the system boundary:

Service	Type	Data Handled	Mitigation	Agency Note
Atlassian Opsgenie	Non-FedRAMP SaaS	Notification data only — sanitised of Federal data/metadata before transmission	All notification data is sanitised of Federal content prior to transmission. ISO 27001 certified.	Ideagen-managed. No agency configuration required.
Atlassian Jira	Non-FedRAMP SaaS (FedRAMP Moderate In Process)	IT infrastructure maintenance data (Low impact)	Mitigated by ISO 27001, ISO 27018, SOC2, PCI DSS compliance. FedRAMP authorization in process.	Ideagen-managed. No agency configuration required.
Microsoft Office 365 EU	Non-FedRAMP SaaS (EU hosted)	Customer communication — potential Federal metadata only	Mitigated by Microsoft compliance programs. Use is limited to communications, not Federal content storage.	Ideagen-managed. Agency may wish to note under AC-20 in the agency SSP.
Windows Update Services	Update service (Inbound only)	OS update packages — no Federal data	Standard patching service. No Federal data involved.	Ideagen-managed. No agency action required.

11. Secure Decommissioning

11.1 Offboarding Individual Users

5. For SSO accounts: deprovision in the agency IdP — verify Huddle US access is revoked within 24 hours
6. For non-SSO accounts: manually disable in Settings > Company Settings > Users & Permissions within 24 hours
7. Notify Workspace Managers to reassign outstanding tasks or approvals
8. Retain all audit records associated with the user for the duration of the log retention period — satisfies AU-11
9. Document the deprovisioning action in the agency access review log — satisfies AC-2(j)

11.2 Decommissioning a Workspace

10. Export all content and audit records before deletion (Workspace > Settings > Export)
11. Remove all external users before decommissioning
12. Archive or delete the Workspace via Company Administrator settings
13. Retain exported audit records per agency records schedule and AU-11 requirements

11.3 Full Tenant Decommissioning

14. Notify Ideagen (security@ideagen.com and account representative) at least 30 days in advance
15. Export all data, documents, and audit records before account suspension
16. Upon suspension: Ideagen provides restricted admin access for 90 days for data retrieval
17. After 90 days suspension: Workspaces deleted; content permanently deleted within further 90 days
18. Obtain written data deletion confirmation from Ideagen — required for MP-6 (Media Sanitisation) documentation
19. Remove the Huddle US SSO integration from the agency IdP

12. Recommended Secure Configuration Checklist

This checklist consolidates the customer-configurable settings for ISSO verification at initial deployment and each annual review. It fulfils RFC-0015 FRR-RSC-04 (secure defaults) and supports FRR-RSC-05 (comparison to baseline). Retain as part of agency CRM evidence.

Configuration Item	Recommended Default	Verified By / Date
SSO configured and integrated with agency IdP (SAML 2.0 or OIDC)	REQUIRED	_____
AAL2 MFA enforced for all Huddle US users via agency IdP policy	REQUIRED	_____
SMS OTP disabled as an MFA factor for Huddle US access	REQUIRED	_____
PIV/CAC or FIDO2 enforced for Company Administrators and Workspace Managers	REQUIRED	_____
IdP deprovisioning tested: revoking agency IdP account removes Huddle US access	REQUIRED	_____
Session timeout: 30 minutes inactivity maximum (aligned in both Huddle and IdP session policy)	REQUIRED	_____
Company Administrator accounts: named individuals only (2–5 accounts)	REQUIRED	_____
Company Administrator accounts: separate from day-to-day user accounts	REQUIRED	_____
Company Administrator accounts: documented in agency access register with formal approval	REQUIRED	_____
Workspace creation: restricted to Company Administrators only	RECOMMENDED	_____
External user invitation: restricted to Workspace Managers and Admins only	REQUIRED	_____
Public file sharing links: confirmed disabled — do not change default	REQUIRED	_____
Password policy for non-SSO emergency accounts: 14+ chars, 60-day rotation, 24-password history, 5-attempt lockout	REQUIRED if applicable	_____
Emergency / break-glass accounts: documented in POA&M with target remediation date, reviewed quarterly	REQUIRED if applicable	_____
Security alert notifications: directed to agency ISSO and security contact	RECOMMENDED	_____
IP allow-listing: agency network ranges and approved VPN blocks configured	RECOMMENDED	_____

Configuration Item	Recommended Default	Verified By / Date
All external users: explicit access expiry date set at invitation (max 90 days)	REQUIRED	_____
External user quarterly report: reviewed by ISSO and documented	REQUIRED	_____
Workspace visibility: private (invite-only) confirmed on all Workspaces	REQUIRED	_____
File version control: enabled and not disabled on any Workspace	REQUIRED	_____
External user download restrictions: configured on Workspaces containing CUI	RECOMMENDED	_____
Audit logs: regularly reviewed by ISSO via the Activity Log	REQUIRED	_____

13. Support and Contact Information

13.1 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@huddle.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	support.ideagen.com — select FedRAMP / Compliance category. For SSO configuration assistance, configuration questions, or access to the FedRAMP authorization package.
Customer Success Manager	Contact your named Ideagen CSM (details in onboarding documentation)
FedRAMP Package Access	Package F1408115175 — available via FedRAMP Marketplace. Contact your Ideagen account representative for PMO repository access.
Procurement / Sales Support	salessupport@ideagen.com

13.2 Key References

- Huddle US SSP v9.0 — FedDoc-101 (January 22, 2025) — FedRAMP Marketplace, Package F1408115175
- SSP Appendix J — CIS and CRM Workbook (FedDoc-111) — 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-118)
- FedRAMP RFC-0015 Recommended Secure Configuration Standard — 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 Huddle US SSP revision cycle. For the most current version, contact your Ideagen Customer Success Manager or security@ideagen.com.