GENESYS

2026

Genesys Cloud FedRAMP

Secure Configuration Guide

Version 1.1 | Effective March 25, 2026

Table of Contents

1. Introduction 4
   1.1 Purpose 4
   1.2 Audience 4
   1.3 How to Use This Guide 4
   1.4 Related Documents 5
   1.5 Terminology 6
2. Administrative Account Management 6
   2.1 Account Types and Roles 6
   2.2 Initial Access and Provisioning 7
   2.3 Ongoing Operations 8
   2.4 Account Decommissioning 9
3. Authentication and Identity 10
   3.1 Single Sign-On (SSO) Configuration 10
   3.2 Multi-Factor Authentication (MFA) 11
   3.3 Password Policy (Defense-in-Depth) 11
4. Authorization and Access Control 13
   4.1 Role-Based Access Control (RBAC) 13
   4.2 Fine-Grained Access Control (Divisions) 15
   4.3 IP Address Filtering 16
   4.4 OAuth Client Security 16
   4.5 Invite Links and Allowed Email Domains 17
5. Data Protection 18
   5.1 Encryption Settings 18

6. Monitoring and Audit 19
6.1 Audit Logging 19
6.2 Session Management (Inactivity Timeout) 20
6.3 Security and Compliance Dashboard 21
7. Secure Defaults Reference 22
8. Programmatic Access and Automation 24
8.1 Platform API Overview 24
8.2 Export Capabilities 25
8.3 Known Limitations 25
9. Version History 25
Appendix A: Settings Quick-Reference Table 27
Appendix B: Requirement Traceability 29
Appendix C: Glossary 30

1. Introduction

1.1 Purpose

This Secure Configuration Guide (SCG) provides federal agency customers and FedRAMP participant customers with recommendations for securely configuring Genesys Cloud CX. It covers administrative account management, security-related settings, and their security implications to help customers maintain a strong security posture within their Genesys Cloud organization.

This guide is published in accordance with the FedRAMP Secure Configuration Guide Balance Improvement Release (SCG-CSO-RSC).

1.2 Audience

This guide is intended for two customer types with different compliance obligations:

- **Federal Agency Customers**: Federal agencies that consume Genesys Cloud under their own Authority to Operate (ATO). Federal agencies are subject to their internal NIST 800-53 audit requirements and should reference the Customer Implementation Summary (CIS) and Customer Responsibility Matrix (CRM) for their specific configuration obligations.
- **FedRAMP Participant Customers**: Non-federal organizations that consume Genesys Cloud under the FedRAMP Marketplace authorization. These customers are subject to the FedRAMP Addendum and Participant FedRAMP Requirements, which govern their configuration obligations.

Where guidance in this document applies to both customer types, it is stated without qualification. Where obligations differ, the applicable customer type is noted.

1.3 How to Use This Guide

This guide is organized by security domain (authentication, access control, data protection, etc.) rather than by FedRAMP requirement identifier. Each section describes:

1. What the setting or capability does
2. How to configure it (navigation path in the Genesys Cloud admin console)
3. The secure configuration
4. The security implications of misconfiguration

Administrators should review this guide during initial organization setup and periodically thereafter, particularly after Genesys Cloud platform updates that may introduce new security settings.

1.4 Related Documents

Document	Audience	Description
Customer Implementation Summary (CIS)	Federal agency customers	Details customer-responsible controls for NIST 800-53 compliance
Customer Responsibility Matrix (CRM)	Federal agency customers	Maps customer responsibilities to specific NIST 800-53 controls
Participant FedRAMP Requirements	FedRAMP participant customers	Governs configuration and operational obligations for non-federal customers
Genesys Cloud FedRAMP Compliance	All customers	Public FedRAMP compliance information
Hardening the Genesys Cloud Environment — Customer Guide (2026)	All customers	Comprehensive environment hardening reference. Includes ISO 27001/27002 and NIST 800-53 framework mappings.

The Genesys Cloud Hardening Guide covers additional security topics beyond the scope of this SCG that customers should review as part of a comprehensive security posture assessment:

- **Access Policies (ABAC):** Attribute-based access control extending RBAC with additional rules. See ABAC overview.
- **SCIM Identity Management:** Automated user provisioning and role assignment via your identity provider. See SCIM identity management.
- **Amazon EventBridge Integration:** SIEM integration for automated alerting beyond the 14-day audit viewer window. See EventBridge integration.
- **Data Actions Security:** Security enhancements for data actions integrations. See Security for data actions.
- **Outbound Calling Restrictions:** Limit outbound calling destinations to reduce toll fraud risk. See Number plan information.
- **Recording Encryption Key Rotation:** Manage encryption key rotation for recordings. See Encryption keys.

- **Native MFA for Non-SSO Users:** Multi-factor authentication for users signing in with native credentials. See MFA overview.

1.5 Terminology

Term	Definition
Top-level administrative account	An account with the Admin role that has permissions to make any changes to a Genesys Cloud organization. This is the highest privilege level available to customers. In Genesys Cloud, this corresponds to the "Admin" default role.
Privileged account	An account with elevated permissions beyond a standard user, but below top-level admin. Examples include custom roles with administrative permissions scoped to specific divisions or functions.
Standard user account	An account with the "Employee" role or other non-administrative roles. The Employee role has the lowest level of permissions and is automatically assigned to all users.
Organization	A Genesys Cloud tenant representing a single customer deployment.
Division	A logical grouping within an organization used for fine-grained access control.

2. Administrative Account Management

This section covers the lifecycle of top-level administrative accounts: initial access, configuration, ongoing operations, and decommissioning.

2.1 Account Types and Roles

Genesys Cloud uses role-based access control (RBAC). Every user is assigned one or more roles that determine their permissions. For the purposes of this guide, accounts are categorized into three tiers:

Account Tier	Genesys Cloud Role(s)	Description
Top-level administrative	Admin	Full permissions to manage the organization. Assigned automatically to the organization creator.
Top-level administrative	Master Admin	All administrative permissions. Reserved for cross-organization administration and Genesys Customer Care engagements.
Privileged	Custom roles with administrative permissions; Supervisor roles with configuration access	Elevated permissions scoped to specific divisions or functions. Cannot modify organization-wide security settings.
Standard user	Employee (default), User, other non-admin roles	Employee role is automatically assigned to all users with the lowest permission level.

Privileged account separation (AC-5, AC-6(2)): Personnel who hold the Admin or Master Admin role must maintain a separate standard user account (e.g., Employee or User role) for day-to-day operations. Administrative accounts must only be used when performing actions that require elevated privileges. This limits the exposure window for the highest-privilege credentials and supports audit trail clarity by distinguishing routine activity from administrative actions.

Security implication: The Admin and Master Admin roles must be assigned to the minimum number of users necessary per AC-6. Anyone with either role can create, update, or delete anything within the organization, including other admin accounts and security settings. The Master Admin role must be reserved for cross-organization administration scenarios; use the Admin role for standard day-to-day administration.

Source: Roles and permissions overview, Authorize users and groups to work in your organization

2.2 Initial Access and Provisioning

When a new Genesys Cloud organization is provisioned for FedRAMP use, the initial top-level administrative account is created during the organization setup process. This account receives the Admin role automatically.

Required secure provisioning steps:

1. **Restrict invite links and allowed email domains.** Configure invite link settings and restrict allowed email domains to prevent unauthorized account creation. Rotate or invalidate open invitation links when no longer needed. See Section 4.5.
2. **Configure SSO immediately.** Before inviting additional users, configure single sign-on (SSO) integration with your organization's identity provider (IdP). This ensures all subsequent authentication flows through your IdP's security controls, including MFA enforcement. See Section 3.1.
3. **Disable Genesys Cloud native login.** After SSO is configured and verified, disable Genesys Cloud native login to enforce SSO-only authentication. Navigate to: Admin > Account Settings > Organization Settings > Authentication tab > set "Disable Genesys Cloud Login" to ON. See Section 3.1 for details.
4. **Enable MFA at the IdP level.** Genesys Cloud defers MFA enforcement to the customer's identity provider. MFA is REQUIRED for all users per NIST 800-53 IA-2(1) and IA-2(2). Ensure your IdP enforces multi-factor authentication for all users, especially those with the Admin role. See Section 3.2.
5. **Restrict the Admin role.** Assign the Admin role only to personnel who require organization-wide administrative access. Use custom roles with scoped permissions for other administrative functions.
6. **Configure IP address allowlisting.** Restrict access to your Genesys Cloud organization to known IP address ranges. See Section 4.3.
7. **Enable inactivity timeout.** Configure automatic session timeout to 10 minutes for administrative accounts per FedRAMP SC-10. See Section 6.2.
8. **Review OAuth client configurations.** Audit existing OAuth clients and ensure they follow least-privilege scoping. See Section 4.4.

Security implication: Failing to configure SSO and disable native login leaves the organization vulnerable to credential-based attacks that bypass your IdP's security controls (MFA, conditional access policies, session management).

2.3 Ongoing Operations

Top-level administrative accounts require ongoing management:

- **Role assignment reviews:** Periodically review which users hold the Admin role. Remove the Admin role from users who no longer require it.
- **Access reviews:** Conduct regular access reviews per your organization's NIST 800-53 AC-2 requirements (federal agencies) or Participant FedRAMP Requirements (FedRAMP participants). Use the products, roles, and permissions list to review current role assignments across the organization.

- **Audit log monitoring:** Monitor the Audit Viewer for administrative actions. See Section 6.1.
- **SSO provider maintenance:** Ensure SSO integrations remain current. Genesys Cloud supports up to 30 SSO integrations with the same or different identity providers.

2.4 Account Decommissioning

When a top-level administrative account holder departs or no longer requires administrative access, the following actions must be completed within the specified timeframes per NIST 800-53 AC-2:

Immediate actions (within 4 hours of trigger event):

1. **Disable the user account** at your identity provider to immediately prevent authentication to Genesys Cloud.
2. **Remove the Admin or Master Admin role** from the user's account. Navigate to: Admin > People & Permissions > select the user > remove the role.
3. **Revoke any OAuth clients** created by the departing administrator to prevent continued API access.

Follow-up actions (within 7 days):

4. **Reassign ownership** of any resources, configurations, or integrations owned by the departing admin to another authorized administrator.
5. **Review audit logs** for administrative actions taken by the departing user in the last 90 days to ensure no unauthorized changes were made.
6. **Verify no unauthorized accounts were created** by the departing administrator.
7. **Disable or delete the user account** in Genesys Cloud per your organization's offboarding procedures. If the account is managed via SCIM provisioning from your IdP, deprovisioning at the IdP level will propagate to Genesys Cloud.

Security review (within 30 days):

8. **Conduct a post-decommissioning audit** to verify no residual access remains and the audit trail is complete.
9. **Document the decommissioning** in your access management records.

Security implication: Failing to promptly remove administrative access from departing personnel creates a window for unauthorized access. Because the Admin and Master Admin roles grant unrestricted access to the entire organization, timely decommissioning is critical. Disabling the account at the IdP first (step 1) is the fastest way to cut off access when SSO-only mode is enabled.

Decommissioning procedure notes:

- When removing the Admin role from a user, the platform displays a licensing change notification because the Admin role expands user licensing. Acknowledge the notification to proceed.
- When disabling or deleting a user account, the platform prompts for a reason for the state change. Enter a descriptive reason (e.g., "Personnel departure — admin decommissioning per AC-2") and click Save.
- Use "Set Inactive" for the initial decommissioning (step 7) to preserve audit history. After the 30-day security review period (step 8), delete the account if appropriate for your organization's records retention requirements.

3. Authentication and Identity

3.1 Single Sign-On (SSO) Configuration

Genesys Cloud supports SAML 2.0-based single sign-on with any compliant identity provider. Organizations can configure up to 30 SSO integrations.

Navigation: Admin > Integrations > Single Sign-on

Secure configuration:

Setting	Required Value	Security Implication
SSO Provider	Configure at least one SAML 2.0 IdP	Centralizes authentication through your organization’s identity controls
Disable Genesys Cloud Login	ON	Prevents bypass of IdP security controls (MFA, conditional access). When ON, all password requirement options are disabled since Genesys Cloud authentication is not used.
Single Logout URI	Configure per IdP documentation	Ensures synchronized logout between Genesys Cloud and the IdP, preventing orphaned sessions

To enable SSO-only authentication:

1. Navigate to Admin > Account Settings > Organization Settings
2. Select the Authentication tab

3. Set “Disable Genesys Cloud Login” to ON
4. Click Save and accept the acknowledgment

Important considerations:

- When Genesys Cloud login is disabled, existing password settings are preserved in case native authentication needs to be re-enabled
- Administrators cannot delete all SSO providers while “Disable Genesys Cloud Login” is ON
- Each user is prompted to choose which SSO provider to use when logging in (if multiple are configured)

Security implication: Native Genesys Cloud login credentials are not subject to your IdP’s MFA, conditional access, or session policies. Disabling native login ensures all authentication flows through your IdP’s security controls.

Source: Configure Genesys Cloud to authenticate with SSO only

3.2 Multi-Factor Authentication (MFA)

Genesys Cloud defers MFA enforcement to the customer’s identity provider. There is no native MFA toggle within Genesys Cloud itself.

Secure configuration:

- MFA is REQUIRED for all accounts (privileged and non-privileged) per NIST 800-53 IA-2(1) and IA-2(2). Configure enforcement at your identity provider.
- Require phishing-resistant MFA methods (e.g., FIDO2/WebAuthn, hardware tokens) for top-level administrative accounts
- Configure conditional access policies at your IdP to require MFA for all Genesys Cloud access

Security implication: Without MFA enforced at the IdP level, compromised credentials provide direct access to Genesys Cloud. This is especially critical for accounts with the Admin role, where a single compromised credential could grant unrestricted access to the entire organization.

3.3 Password Policy (Defense-in-Depth)

SSO-only mode with native Genesys Cloud login disabled is required for FedRAMP (see Section 3.1). When SSO-only is enabled, your identity provider enforces all password policies and the native Genesys Cloud password settings are inactive.

The native password settings documented below should be hardened as a defense-in-depth measure. They apply only during initial organization setup before SSO is configured, or if native login is temporarily re-enabled for emergency access. Configure these settings to FedRAMP requirements so that if native login is ever active, accounts are still protected.

Navigation: Admin > Account Settings > Organization Settings > Authentication tab

Configurable settings:

Setting	Default Value	Required Value (native login)	Security Implication
Minimum Length	8 characters	15 characters	FedRAMP requirement per IA-5(1). Longer passwords resist brute-force attacks. Maximum is 400 characters.
Minimum Letters	0	1+	Ensures password complexity
Minimum Lowercase Letters	1	1+	Ensures character variety
Minimum Uppercase Letters	1	1+	Ensures character variety
Minimum Numerals	1	1+	Ensures character variety
Minimum Special Characters	1	1+	Ensures character variety. Allowable: !“#$%&’()*+,-./:;<=>?@[]^_`{
Password Expiration	Disabled (unchecked)	60 days	FedRAMP requirement per IA-5(1). Forces periodic credential rotation.
Minimum Age	Disabled (unchecked)	1 day	FedRAMP requirement per IA-5(1). Prevents rapid password cycling to reuse old passwords.

Your identity provider is the primary enforcement point. Configure the following at your IdP to meet FedRAMP requirements:

- Password minimum length: 15 characters per IA-5(1)
- Password expiration: 60 days maximum per IA-5(1)
- Password history: 24 generations per IA-5(1)
- Password minimum age: 1 day per IA-5(1)
- Account lockout: 3 failed attempts with administrator unlock per AC-7

Source: Set Genesys Cloud password requirements

4. Authorization and Access Control

4.1 Role-Based Access Control (RBAC)

Genesys Cloud controls access through roles and permissions. Each role contains one or more permissions that allow users to perform specific tasks.

Navigation: Admin > People & Permissions > Roles & Permissions

Key default roles:

Role	Privilege Level	Description
Master Admin	Top-level administrative	All permissions necessary to administer the organization. Primarily used for cross-organization (authorized organization) administration and Genesys Customer Care support engagements.
Admin	Top-level administrative	Full permissions to make any changes to the organization. Assigned automatically to the organization creator. Standard top-level role for day-to-day administration.
People Admin	Privileged (administrative)	User management permissions. Only exists in organizations created after June 2022.
Telephony Admin	Privileged (administrative)	Infrastructure configuration: Edge devices, phones, numbers, and call routing.

Role	Privilege Level	Description
Content Management Admin	Privileged (administrative)	Content workspace management and administration.
Authorized User Admin	Privileged (administrative)	Cross-organization access management and trust relationship administration.
Quality Evaluator	Privileged (functional)	Recording access, evaluation forms, audit trails, and encryption key creation.
Supervisor	Privileged (functional)	Contact center supervision: dashboards, reporting, and agent-level settings.
User	Standard user	Contact center operations access.
Employee	Standard user (base)	Lowest permission level. Automatically assigned to all users. Cannot be removed. Includes: read organization, edit own profile, edit own location.

Secure configuration:

- Assign the Admin role to the minimum number of users necessary
- Create custom roles for administrative functions that do not require full Admin access
- Use the principle of least privilege: assign only the permissions each user needs for their job function
- Periodically review role assignments and remove unnecessary elevated roles
- When restoring a default role to its original state, be aware that any custom permission additions are removed and any deleted permissions are restored
- Review the role backfill setting to control whether new feature permissions are automatically added to existing roles. Navigate to: Admin > People & Permissions > Roles & Permissions. Automatic backfill can grant unintended permissions when new platform features are released. Consider setting this to manual assignment for administrative roles so new permissions are reviewed before being granted.

Custom roles: Administrators can create custom roles to match specific job functions. For example, a "Content Manager" role with only the Content Management Admin permission. Custom roles can be assigned, unassigned, or disabled at any time.

Security implication: Over-provisioning of the Admin role is the most common access control risk. The Admin role grants unrestricted access to the entire organization, including the ability to modify security settings, delete users, and access all data. Use custom roles to scope administrative access to specific functions.

Source: Roles and permissions overview, Automatically backfill roles with new permissions

4.2 Fine-Grained Access Control (Divisions)

Genesys Cloud supports fine-grained access control through divisions, which allow administrators to segment resources and grant selective permissions.

Navigation: Admin > People & Permissions > Access Control

Key concepts:

- Divisions are logical groupings that categorize resources (queues, campaigns, flows, users, etc.)
- Users can be granted permissions scoped to specific divisions, limiting their access to only the resources in those divisions
- A user can have different roles in different divisions

Secure configuration:

- Use divisions to segment resources by business unit, department, or sensitivity level
- Assign privileged roles (e.g., Supervisor, custom admin roles) only within the divisions where the user needs access
- Avoid granting roles across all divisions unless the user requires organization-wide access
- Review division assignments periodically as organizational structure changes

Security implication: Without divisions, all users with a given role have access to all resources of that type across the entire organization. Divisions enable the principle of least privilege at a granular level, reducing the blast radius of a compromised privileged account.

Source: Access control overview

4.3 IP Address Filtering

Genesys Cloud allows administrators to restrict access to the organization to users connecting from specified IP addresses.

Navigation: Admin > Account Settings > Organization Settings > Settings tab > Allowed IP Addresses

Secure configuration: Configure CIDR blocks for your organization's known IP ranges. If left empty, all IP addresses can access the organization.

Configuration details:

- Enter CIDR blocks (e.g., 192.168.100.0/22), one per line, up to 150 entries
- Only IPv4 addresses are supported
- The system verifies that the configuring administrator's IP is included in the allowlist
- The allowlist also applies to applications interfacing with Genesys Cloud via API
- Data Actions integration IPs are automatically allowed
- WebRTC Media Helper and Genesys Tempo are allowed by default

Security implication: Without IP address filtering, any user with valid credentials can access the organization from any network. IP filtering provides a network-layer access control that complements authentication controls, reducing the risk of unauthorized access from compromised credentials used outside your organization's network.

Source: Allow IP addresses

4.4 OAuth Client Security

Genesys Cloud uses OAuth 2.0 for API authentication. Administrators can create OAuth clients that grant programmatic access to the platform. OAuth clients are high-sensitivity credentials that must be managed with the same rigor as administrative accounts.

Navigation: Admin > Integrations > OAuth

Secure configuration:

Setting	Required / Recommended Value	Security Implication
OAuth scopes	Minimum scopes required for the integration's function (REQUIRED per AC-6)	Over-scoped OAuth clients can access data and perform actions beyond what the integration needs

Setting	Required / Recommended Value	Security Implication
Client credential storage	Treat as high-sensitivity secrets; store in a secrets manager (REQUIRED per IA-5)	Exposed OAuth credentials provide direct API access that bypasses interactive login controls
Client credential rotation	Rotate periodically per your organization's credential management policy (REQUIRED per IA-5)	Long-lived credentials increase the window of exposure if compromised

Required practices:

- Apply the principle of least privilege when assigning OAuth scopes to each client. Only grant the scopes the integration requires.
- Inventory all OAuth clients periodically. Remove or disable clients that are no longer in use.
- Do not embed OAuth client secrets in source code, configuration files, or other locations accessible to unauthorized personnel.
- When an administrator who created OAuth clients departs, revoke and recreate those clients under a current administrator's ownership (see Section 2.4, step 3).
- Monitor OAuth client usage through the Audit Viewer for unexpected access patterns.

Security implication: An over-scoped or compromised OAuth client can perform any action its scopes allow, without requiring interactive authentication or MFA. Unlike user sessions, OAuth client credentials do not expire via inactivity timeout. Least-privilege scoping and periodic rotation are the primary mitigations.

Source: About OAuth scopes for applications, View, edit, or delete OAuth clients

4.5 Invite Links and Allowed Email Domains

Genesys Cloud allows administrators to control how new users are invited to join the organization through invite links and email domain restrictions.

Navigation: Admin > Account Settings > Organization Settings > Invite Links

Secure configuration:

- Restrict allowed email domains to your organization's verified domains only. This prevents users with unauthorized email addresses from joining the organization.

- Treat open invitation links as sensitive. Rotate or invalidate invite links when they are no longer needed.
- Do not distribute invite links through unsecured channels.

Security implication: Unrestricted invite links and email domains can allow unauthorized users to create accounts in your organization. While these accounts would only receive the default Employee role, unauthorized account creation increases the attack surface and complicates access reviews.

Source: Configure invite links

5. Data Protection

5.1 Encryption Settings

Genesys Cloud encrypts data at rest and in transit by default. Customers have additional options for managing encryption keys.

Provider-managed encryption: Genesys Cloud encrypts all data at rest using AES-256 encryption with keys managed by the Genesys Cloud platform. This is the default configuration and requires no customer action.

Customer-managed encryption keys (Local Key Management): Customers who require control over their encryption keys can configure Local Key Management, which allows the customer to manage encryption keys through their own AWS KMS instance.

Navigation: Admin > Conversation Intelligence > Recording and Policies > Encryption Keys > Encryption Key Configuration

Secure configuration:

- Evaluate whether your organization's data protection requirements necessitate customer-managed keys
- If using Local Key Management, ensure your AWS KMS key policies follow the principle of least privilege
- Monitor key usage and rotation per your organization's key management policy

Security implication: Provider-managed encryption meets FedRAMP requirements for data at rest encryption. Customer-managed keys provide additional control and the ability to revoke Genesys Cloud's access to your data by disabling the key, but introduce operational complexity (key rotation, availability, disaster recovery).

Source: Local key management

6. Monitoring and Audit

6.1 Audit Logging

Genesys Cloud maintains audit logs of administrative and system events. Customers can view these logs through the Audit Viewer.

Navigation: Admin > Audit Viewer (full-page viewer) or via the footer of any Admin page (mini viewer)

Capabilities:

- View audit events for the current day by default
- Search events by date range (up to 14 days of real-time events)
- Filter by service (e.g., queue, flow, user management)
- Search by entity ID or by user
- View detailed event information including the user, timestamp, and specifics of each change

Tracked event categories include:

- User and role management changes
- Organization settings modifications
- Integration configuration changes
- Recording and evaluation actions
- Workforce management changes

Secure configuration:

- Designate personnel responsible for regular audit log review per AU-6
- Establish a review cadence aligned with your organization's continuous monitoring requirements per AU-6
- Investigate unexpected administrative actions, particularly changes to roles, SSO configuration, or organization settings
- For long-term retention beyond 14 days, use the Genesys Cloud Platform API audit endpoints to export audit data to your organization's SIEM or log management system

Security implication: Audit logs provide the evidentiary basis for detecting unauthorized administrative actions, investigating security incidents, and demonstrating compliance during assessments. Without regular review, unauthorized changes to security settings may go undetected.

Source: View audit events

6.2 Session Management (Inactivity Timeout)

Genesys Cloud can automatically log out users after a specified period of inactivity.

Navigation: Admin > Account Settings > Organization Settings > Settings tab > Security & Compliance

Configurable settings:

Setting	Default	Required Value	Security Implication
Enable Inactivity Timeout	OFF	ON (REQUIRED)	Terminates idle sessions, reducing the risk of unauthorized access from unattended workstations
Timeout Minutes	N/A (disabled)	10 minutes for administrative accounts per FedRAMP AC-11, AC-12, and SC-10 (REQUIRED).	Shorter timeouts reduce exposure window but may impact user experience
Default APIs to Exclude from Inactivity Timeout	Several default APIs	Keep defaults enabled (recommended by Genesys)	Excluding certain APIs prevents background application activity from resetting the idle timer

Behavior when enabled:

- User presence changes to Offline and they are returned to the login prompt
- After re-login, users return to the same page they were on before timeout
- Agents who are On Queue have their routing status changed to Off Queue
- The timeout applies to all organization members across desktop app, web app, embedded client, and custom clients

- Works for organizations using SSO

Security implication: Without inactivity timeout, sessions remain active indefinitely. An unattended workstation with an active admin session represents a significant security risk, as anyone with physical access to the workstation gains the admin's full permissions.

Source: Set an automatic inactivity timeout

6.3 Security and Compliance Dashboard

Genesys Cloud provides a security and compliance settings view that shows the current state of key security settings for the organization.

Navigation: Admin > Account Settings > Organization Settings > Settings tab > Security & Compliance

This dashboard provides visibility into:

- Inactivity timeout status and configuration
- Sensitive data redaction settings (payment cards and personal information)
- Chat controls (file uploads, message retention, edit window)
- HIPAA and PCI DSS compliance toggles
- Voicemail and fax notification PII controls
- Genesys Cloud embedding restrictions and allowed domains
- Allowed IP addresses - OAuth scope enforcement (Enforce Scopes)
- Role Backfill setting (automatic vs. manual permission assignment)
- Division-Aware Role Management
- Attribute Based Access Control (ABAC)

Secure configuration:

- Review the Security & Compliance dashboard periodically to verify settings remain in their secure state
- Use this dashboard as a quick health check during access reviews and continuous monitoring activities

7. Secure Defaults Reference

This section documents the default security settings for a newly provisioned Genesys Cloud FedRAMP organization and identifies which defaults are secure and which require customer action.

Setting	Default Value	Secure?	Customer Action Required
Genesys Cloud Native Login	Enabled (ON)	No	Disable after configuring SSO (Section 3.1)
SSO Configuration	Not configured	No	Configure SSO with your IdP (Section 3.1)
MFA	Not enforced (deferred to IdP)	No	Enable MFA at your IdP (Section 3.2)
Inactivity Timeout	Disabled (OFF)	No	Enable and set to 10 minutes per SC-10 (Section 6.2)
IP Address Filtering	Not configured (all IPs allowed)	No	Configure IP allowlist (Section 4.3)
Password Minimum Length	8 characters	Partial	Increase to 15 characters if native login is used (Section 3.3)
Password Minimum Letters	0	No	Increase to 1+ if native login is used (Section 3.3)
Password Complexity	1 each: lowercase, uppercase, numeral, special	Yes	No action required if native login is used
Password Expiration	Disabled (unchecked)	No	Set to 60 days if native login is used (Section 3.3)
Password Minimum Age	Disabled (unchecked)	No	Set to 1 day if native login is used (Section 3.3)

Setting	Default Value	Secure?	Customer Action Required
Account Lockout	6 attempts, 5-minute lockout	Yes	No action required
Password History	10 previous passwords	Yes	No action required
Admin Role Assignment	Assigned to organization creator	Yes	Review and restrict to minimum necessary users (Section 2.1)
Employee Role	Assigned to all users automatically	Yes	No action required — this is the least-privilege default
Encryption at Rest	AES-256, provider-managed	Yes	Evaluate customer-managed keys if required (Section 5.1)
Enforce Scopes (OAuth)	ON	Yes	No action required — enforces OAuth scope approval
Role Backfill	OFF	Yes	Review setting; OFF means new permissions require manual assignment (Section 4.1)
Sensitive Data Redaction (Payment Cards)	OFF	Partial	Enable if handling payment card data
Sensitive Data Redaction (Personal Info)	OFF	Partial	Enable if handling PII in interactions
Restrict Genesys Cloud Embedding	OFF	No	Enable and configure allowed domains to prevent clickjacking
Allow PII in Email Notifications	ON	No	Disable to prevent PII exposure in email notifications

Setting	Default Value	Secure?	Customer Action Required
Division-Aware Role Management	OFF	Partial	Enable if using divisions for FGAC (Section 4.2)
Attribute Based Access Control	OFF	Partial	Enable if using ABAC policies

8. Programmatic Access and Automation

8.1 Platform API Overview

Genesys Cloud provides a Platform API that customers can use to programmatically manage certain security settings. The API uses OAuth 2.0 for authentication and supports granular permission scoping through OAuth scopes. API access is subject to the same RBAC permissions as the admin console.

For complete API documentation, regional base URLs, SDKs, and developer tools, refer to the Genesys Developer Center.

API-accessible security operations include:

- User and role management (create, read, update, delete users and role assignments)
- Division management for fine-grained access control (full CRUD operations)
- Audit log queries for programmatic export
- OAuth client management
- Inactivity timeout configuration (PUT /api/v2/tokens/timeout - set timeout between 300-28800 seconds, enable/disable)

UI-only security settings (not API-accessible):

- Organization-level settings (e.g., Disable Genesys Cloud Login, SSO configuration)
- Password policy settings

Security implication: Organization-level security settings cannot be managed through infrastructure-as-code or automated compliance checks. Customers should include manual verification of UI-only settings in their continuous monitoring procedures.

8.2 Export Capabilities

Customers can export security-related data via the Platform API in JSON format:

- Audit logs (via Audit API endpoints)
- User and role assignments (via Users API + Authorization API)
- Division assignments (via Authorization API)

Organization-level security settings are not exportable via API and must be reviewed manually in the admin console.

8.3 Known Limitations

The following capabilities are not currently available in Genesys Cloud:

Capability	Current Status	SCG Requirement
Compare current settings to secure defaults	Not available	SCG-ENH-CMP
Export all security settings in machine-readable format	Partial (audit logs and FGAC only)	SCG-ENH-EXP
API access for all security settings	Partial (org-level settings are UI-only)	SCG-ENH-API
Machine-readable SCG (OSCAL / JSON)	Not yet available	SCG-ENH-MRG

These items are documented here for transparency. As capabilities become available, this guide will be updated accordingly.

9. Version History

Version	Date	Changes
1.0	2026-03-01	Initial release. Covers all SCG requirements (SCG-CSO-RSC, SCG-CSO-AUP, SCG-CSO-PUB, SCG-CSO-SDF, SCG-ENH-CMP, SCG-ENH-EXP, SCG-ENH-API, SCG-ENH-MRG, SCG-ENH-VRH).

Version	Date	Changes
1.1	2026-03-25	Formatting aligned with Genesys Corporate Word Template (2026)

This guide will be updated when:

- Genesys Cloud introduces new customer-configurable security settings
- Secure configuration defaults change
- FedRAMP SCG requirements are updated
- Platform API capabilities for security settings are expanded

Appendix A: Settings Quick-Reference Table

This table provides a consolidated view of all customer-configurable security settings covered in this guide.

Setting	Navigation Path	Required (R) / Recommended (r)	Default	Section
SSO Configuration	Admin > Integrations > Single Sign-on	(R) Configure at least one SAML 2.0 IdP	Not configured	3.1
Disable Genesys Cloud Login	Admin > Organization Settings > Authentication	(R) ON	OFF	3.1
Password Minimum Length	Admin > Organization Settings > Authentication	(R) 15 characters (if native login used)	8 characters	3.3
Password Expiration	Admin > Organization Settings > Authentication	(R) 60 days	Disabled	3.3
Inactivity Timeout	Admin > Organization Settings > Settings > Security & Compliance	(R) ON	OFF	6.2
Timeout Minutes	Admin > Organization Settings > Settings > Security & Compliance	(R) 10 minutes for admin accounts per SC-10	N/A (disabled)	6.2
IP Address Allowlist	Admin > Organization Settings > Settings > Allowed IP Addresses	(R) Configure org IP ranges	Empty (all allowed)	4.3
Admin Role Assignment	Admin > People & Permissions > Roles	(R) Minimum necessary users	Org creator only	2.1
Division Configuration	Admin > People & Permissions > Access Control	(r) Segment by business unit/sensitivity	Single default division	4.2

Setting	Navigation Path	Required (R) / Recommended (r)	Default	Section
Local Key Management	Admin > Conversation Intelligence > Recording and Policies > Encryption Keys	(r) Per data protection requirements	Provider-managed	5.1
OAuth Client Scopes	Admin > Integrations > OAuth	(R) Minimum scopes required per client	N/A (per client)	4.4
OAuth Client Credential Rotation	Admin > Integrations > OAuth	(R) Rotate periodically	No expiration	4.4
Invite Link Email Domains	Admin > Organization Settings > Invite Links	(R) Restrict to verified org domains	Unrestricted	4.5
Role Backfill	Admin > People & Permissions > Roles & Permissions	(r) Manual for admin roles	Automatic	4.1

Appendix B: Requirement Traceability

This appendix maps sections of this guide to the FedRAMP Secure Configuration Guide (SCG) requirement identifiers for assessor reference. Obligation levels follow RFC 2119 conventions: MUST indicates a mandatory requirement; SHOULD indicates a recommended practice.

Requirement ID	Requirement Title	Obligation	Guide Section(s)
SCG-CSO-RSC (RSC.1)	Top-level admin account lifecycle	MUST	2.1, 2.2, 2.3, 2.4
SCG-CSO-RSC (RSC.2)	Security settings for top-level admin accounts	MUST	3.1, 3.2, 3.3, 4.1, 4.3, 4.4, 4.5, 5.1, 6.1, 6.2, 6.3
SCG-CSO-RSC (RSC.3)	Security settings for privileged accounts	SHOULD	4.1, 4.2, 4.4
SCG-CSO-AUP	Use instructions	MUST	Separate document: Authorization Package Instructions
SCG-CSO-PUB	Public guidance	SHOULD	This guide (published publicly per RI-03)
SCG-CSO-SDF	Secure defaults	SHOULD	7
SCG-ENH-CMP	Comparison capability	SHOULD	8.3 (documented as not available)
SCG-ENH-EXP	Export capability	SHOULD	8.2, 8.3
SCG-ENH-API	API capability	SHOULD	8.1, 8.3
SCG-ENH-MRG	Machine-readable guidance	SHOULD	8.3 (planned: OSCAL + JSON)
SCG-ENH-VRH	Versioning and release history	SHOULD	9

Appendix C: Glossary

Term	Definition
Admin role	The Genesys Cloud default role with full permissions to make any changes to the organization
CIDR	Classless Inter-Domain Routing — a method for specifying IP address ranges
CIS	Customer Implementation Summary — documents customer-responsible controls for federal agency customers
CRM	Customer Responsibility Matrix — maps customer responsibilities to NIST 800-53 controls for federal agency customers
Division	A logical grouping in Genesys Cloud used for fine-grained access control
Employee role	The Genesys Cloud default role with the lowest permission level, automatically assigned to all users
FGAC	Fine-Grained Access Control — Genesys Cloud's division-based access control mechanism
IdP	Identity Provider — the external authentication service (e.g., Okta, Azure AD, Ping) used for SSO
MFA	Multi-Factor Authentication
OAuth	Open Authorization — a protocol for delegated API access using client credentials and scoped permissions
OSCAL	Open Security Controls Assessment Language — a NIST standard for machine-readable security documentation
RBAC	Role-Based Access Control
SAML	Security Assertion Markup Language — the protocol used for SSO integration

Term	Definition
SCG	Secure Configuration Guide — this document
SCIM	System for Cross-domain Identity Management — a protocol for automated user provisioning
SSO	Single Sign-On