OutSystems 11 Platform

FedRAMP Secure Configuration Guide

Version: 1.0 **Date:** March 2026 **Classification:** Public **Applicable FedRAMP Baseline:** Moderate

---

Document Control

Version	Date	Author	Description
1.0	March 2026	Knox Systems	Initial Release

Table of Contents

---

1. Introduction

1.1 Purpose and Scope

This Secure Configuration Guide (SCG) provides federal agencies and FedRAMP Authorized organizations with comprehensive guidance for securely configuring OutSystems 11 FedRAMP platform, a high-productivity application platform (low-code/no-code) used for rapid application development and deployment.

This guide addresses:

- Administrative account management and lifecycle
- Identity and access management configuration
- Role-based access control implementation
- Security settings and hardening procedures
- Audit logging and monitoring requirements

Applicable FedRAMP Baseline: Moderate

1.2 How to Obtain This Guide

This Secure Configuration Guide is available at:
https://knoxsystems.com/secure-configuration-guides

For the latest version of this guide and related security documentation, visit the Knox Systems compliance resources portal. Organizations may also contact Knox Systems directly for assistance with FedRAMP implementation.

1.3 Related Documents and References

Document	Description
OutSystems 11 Documentation	https://success.outsystems.com/documentation/11/
OutSystems Trust Center	https://www.outsystems.com/trust
OutSystems Cloud Security Alliance Registry	https://cloudsecurityalliance.org/star/registry/outsystems/
NIST SP 800-53 Rev 5	Security and Privacy Controls
FedRAMP Security Controls Baseline	Moderate Impact Level

1.4 Document Conventions

This guide uses the following conventions:

- **MUST** - Mandatory requirement for FedRAMP compliance
- **SHOULD** - Strongly recommended security practice
- **MAY** - Optional configuration based on organizational requirements

1.5 OutSystems Architecture Overview

OutSystems 11 consists of the following key components:

Component	Description
LifeTime	Infrastructure management console for user management, deployments, and environment configuration
Service Center	Environment-level management console for application and security administration
Service Studio	Development environment for building applications
Users Application	End-user authentication and management for deployed applications

---

2. Top-Level Administrative Account Management

This section addresses FedRAMP requirement R1 for top-level administrative account management, including procedures to access, configure, operate, and decommission administrative accounts.

2.1 Users App Administrator Account

The Users application administrator ("admin") is the top-level account for managing end users in OutSystems applications.

2.1.1 Initial Configuration

To access and configure the Users App Administrator:

1. Log in to Service Center (`https://<environment_address>/ServiceCenter`)
2. Navigate to **Factory** > **Modules**
3. Search for **Users** and click the module name
4. Click the **Single Sign-On** tab
5. Click **Configure Administrator user**
6. Set the password meeting complexity requirements:
    - Minimum 12 characters
    - At least one number
    - At least one lowercase letter
    - At least one uppercase letter
7. Click **Apply**

Prerequisites:

- User MUST have **Change and Deploy Applications** permission level (or higher) for the Users app
- For environments managed by LifeTime, permission assignment occurs through LifeTime console

2.1.2 Security Implications

Action	**Security Impact**	**Risk Level**
Weak admin password	Unauthorized access to all end-user data and permissions	**HIGH**
Shared admin credentials	Loss of accountability, inability to audit individual actions	**HIGH**
Unchanged default password	Trivial compromise by attackers	**CRITICAL**
Admin account not configured	Users app inaccessible for management	**MEDIUM**

FedRAMP Requirement: Organizations MUST configure a unique, strong password for the Users app administrator before production deployment.

2.2 IT Administrator Role (Platform Level)

The IT Administrator role provides full control over the entire OutSystems infrastructure, including all environments and applications.

2.2.1 Access and Configure

To create an IT user with Administrator role:

1. Access LifeTime console (`https://<lifetime_env>/lifetime`)
2. Navigate to **USER MANAGEMENT** > **USERS**
3. Click **New User**
4. Complete required fields:
    - Username (unique identifier)
    - Email
    - Name
5. Set **Default Role** to **Administrator**
6. Set password meeting complexity requirements
7. Click **Create**

2.2.2 Built-in Administrator Role Capabilities

The Administrator role has the following **non-configurable** permissions:

Permission	**Scope**
Full Control	All environments
Change and Deploy Applications	All applications in all environments
Manage Environment Settings	Date formats, database connections, certificates
Manage Infrastructure	Front-end servers, zones, email/certificate settings
Manage IT Users and Roles	Create, modify, delete all users and roles
View Audit Logs	All infrastructure audit information

Security Implication: The Administrator role cannot be modified. Permissions are fixed and provide unrestricted platform access.

2.2.3 Centralized User Management

LifeTime is the **master of data** for IT user credentials

- Changes to IT users in LifeTime propagate to all environments
- Service Center user management is **disabled** for environments
- User synchronization occurs automatically

2.3 Account Lifecycle Management

2.3.1 Create Account

Step	Procedure	Security Consideration
1	Access LifeTime USER MANAGEMENT	Requires existing admin privileges
2	Click New User	N/A
3	Assign Default Role	Follow least privilege principle
4	Set initial password	MUST meet complexity requirements
5	Communicate credentials securely	Use secure channel, require password change

2.3.2 Modify Account

Action	Procedure	Security Consideration
Change password	User profile or admin reset	Invalidates existing sessions
Change role	Edit user, select new Default Role	Role changes are immediate
Add team membership	Edit user, assign to team	Team role overrides default role
Add application permissions	Grant Role in Applications	Application role overrides team and default roles

2.3.3 Deactivate Account

To deactivate an IT user:

1. Access LifeTime USER MANAGEMENT
2. Select the user to deactivate
3. Click **Deactivate User** (or remove from all teams and set to No Access role)
4. Confirm deactivation

Security Implications:

- Deactivated users CANNOT log in to any OutSystems tools
- User audit history is preserved
- Associated sessions are invalidated

2.3.4 Delete Account

To permanently delete an IT user:

1. Access LifeTime USER MANAGEMENT

2. Select the deactivated user
3. Click **Delete User**
4. Confirm deletion

Security Implications:

- User record is permanently removed
- Audit logs referencing the user remain intact
- Action is **irreversible**

FedRAMP Requirement: Organizations SHOULD deactivate rather than delete accounts to maintain audit trail integrity.

2.4 Emergency Access (Break-Glass) Procedures

If external IdP authentication is misconfigured and preventing login:

1. Navigate directly to the Users app login page:

```
None
https://<your_server_name>/Users/Login.aspx
```

2. Log in with an administrator account (must have UserManager role)
3. This bypasses the configured authentication method
4. Fix the incorrect IdP settings

Security Implications:

- Break-glass access bypasses SSO/MFA controls
- All break-glass access MUST be logged and reviewed
- Organizations SHOULD establish procedures for emergency access notification

---

3. Identity and Access Management

This section covers Single Sign-On (SSO), Multi-Factor Authentication (MFA), and external Identity Provider (IdP) integration.

3.1 Authentication Methods Overview

OutSystems supports multiple authentication mechanisms:

Method	**Use Case**	**Security Level**
Internal Authentication	Default, username/password	Basic
SAML 2.0	Enterprise SSO integration	High
OpenID Connect (OIDC)	Modern SSO for IT users	High
Microsoft Entra ID	Microsoft ecosystem integration	High
Okta	Okta-based organizations	High
LDAP/Active Directory	On-premises directory integration	Medium-High

FedRAMP Requirement: Organizations MUST implement SSO with MFA for all privileged users.

3.2 SAML 2.0 Configuration for End Users

SAML 2.0 enables SSO for end users of OutSystems applications.

3.2.1 Prerequisites

- Platform Server Release Jul.2019 CP2 (11.0.542.0) or later
- Identity Provider metadata and configuration details

3.2.2 Configuration Steps

1. Access the Users application
2. Click **Configure Authentication** in the sidebar
3. Select **SAML 2.0** from the Authentication dropdown
4. Configure IdP settings:
    - IdP Entity ID
    - IdP SSO URL
    - IdP Certificate
5. Enable security options:
    - **Accept Only Signed Login Responses** (enabled by default) - **MUST** remain enabled
    - Configure matching setting in your IdP
6. Configure attribute mapping for user claims

3.2.3 Security Settings

Setting	**Recommended Value**	**Security Implication**
Accept Only Signed Login Responses	**Enabled**	Prevents SAML response forgery
Assertion Signing	**Required**	IdP MUST sign assertions
HTTPS Only	**Enabled**	Protects credentials in transit

Security Implications:

- Disabling signed response validation allows SAML response tampering
- Multi-tenancy is NOT supported with SAML 2.0
- Only Service Provider-initiated flows are supported

3.3 OpenID Connect for IT Users

OIDC provides secure authentication for IT users (developers, administrators, operators).

3.3.1 Prerequisites

- Platform Server 11.18.1 or later
- LifeTime 11.16.1 or later
- Service Studio 11.53.13 or later

- All environments MUST meet version requirements

3.3.2 Affected Tools

When OIDC is enabled, the following tools use external IdP login:

- Service Center
- LifeTime
- Service Studio
- Integration Studio
- Factory Configuration

3.3.3 Configuration Steps

1. Access LifeTime console
2. Navigate to authentication settings
3. Configure OIDC provider:
    - Discovery URL
    - Client ID
    - Client Secret
4. Map IdP claims to OutSystems attributes
5. Test authentication flow
6. Enable for all environments

3.3.4 Security Implications

Configuration	**Security Impact**
OIDC Enabled	Passwords cannot be set/changed for IT users (except local admins)
Weak Client Secret	Token compromise, unauthorized access
Missing PKCE	Reduced protection against code interception
No MFA at IdP	Single-factor authentication only

FedRAMP Requirement: When using OIDC, organizations MUST configure MFA at the external Identity Provider.

3.4 Single Sign-On Between App Types

Single Sign-On Between App Types is a pre-requirement for SAML 2.0 authentication. To enable it:

1. Open Service Center
2. Navigate to **Administration** > **Security**
3. Enable the following settings:
    - **Secure Connections** > **Enable HTTP Strict Transport Security (HSTS)**
    - **Cookies** > **Secure**
4. Click **Save**
5. Click **Applications Authentication**
6. Enable **Single Sign-On Between App Types**

7. Ensure **Max. Idle Time** matches session timeout for Traditional Web Apps
8. Click **Save and Apply Settings to the Factory**

Security Implications:

- SSO between app types requires HTTPS
- Logging out from one app logs out all apps in the same browser session
- Session timeout mismatches can cause authentication failures

---

4. Role-Based Access Control

This section addresses FedRAMP requirements R2 and S1 for privileged account management and security implications of access control settings.

4.1 Built-in Roles

OutSystems provides two built-in roles:

4.1.1 Developer Role

Default Permissions	**Description**
Development Environment	Deploy applications
QA Environment	Open applications
Production Environment	List applications

Note: Developer role permissions CAN be customized.

4.1.2 Administrator Role

Permissions	**Description**
Full Control	All environments
All Applications	Change and Deploy
Infrastructure Management	Full access
User Management	Create, modify, delete users

Note: Administrator role permissions CANNOT be modified.

4.2 Permission Levels

Permission levels are cumulative (each level includes permissions of lower levels):

Level	Capabilities	Security Implications
Full Control	Environment settings, infrastructure management	Highest privilege, administrative access
Change and Deploy	Publish applications, modify settings	Can deploy potentially malicious code
Open and Debug	Open modules in Service Studio, debug	Access to source code and runtime data
Monitor and Add Dependencies	View monitoring data, add module dependencies	Access to application performance data
List Applications	View applications in LifeTime/Service Center	Information disclosure of app inventory
Access	Log in to environment only	Minimal access, no application visibility
No Access	Cannot log in to environment	Complete access denial

4.3 Role Assignment Methods

Roles can be assigned through three methods, with the following precedence:

Priority	Assignment Method	Overrides
1 (Highest)	Application-specific role	Team role, Default role
2	Team role	Default role
3 (Lowest)	Default role	None

4.3.1 Default Role Assignment

- Assigned when creating a user
- Defines base permissions for all environments and applications
- **Security Best Practice:** Set default role to minimum required permissions

4.3.2 Team Role Assignment

- Assigned when adding user to a team
- Applies to applications owned by the team
- Overrides default role for team applications

4.3.3 Application-Specific Role Assignment

- Assigned directly to a user for specific applications
- Provides most granular control
- Overrides both default and team roles

4.4 Creating Custom Roles

To create a custom role:

1. Access LifeTime USER MANAGEMENT > ROLES
2. Click **New Role**
3. Enter Role Name
4. For each environment, configure:
    - Permission level (slider)
    - Specific permissions (toggles):
        - Create Applications
        - Add System Dependencies
5. Configure infrastructure-wide permissions:
    - Manage Users and Roles (Cloud only)
    - Manage Infrastructure and Users (self-managed)
    - Manage Teams and Application Roles
6. Click **SAVE**

4.5 Infrastructure-Wide Permissions

Permission	**Capability**	**Security Implications**
Manage Users and Roles	Add/edit/remove IT users, roles, teams; enable Technical Preview features	Full user management; can create admin accounts
Manage Infrastructure and Users	Add/switch environments, manage infrastructure settings, manage users	Complete infrastructure control
Manage Teams and Application Roles	Manage team membership, grant/revoke application roles	Can escalate privileges within assigned scope

4.6 Least Privilege Implementation

FedRAMP Requirement: Organizations MUST implement least privilege for all accounts.
Recommended Implementation:

User Type	**Default Role**	**Additional Access**
Developer	Custom minimal role	Team-based for project applications
QA Tester	List Applications	Application-specific Open and Debug
Operator	Monitor and Add Dependencies	Application-specific as needed
Administrator	Administrator	No additional (already full access)

4.7 Privileged Account Security Implications Table

Configuration	Security Risk	Mitigation
Default Administrator role	Excessive privileges, audit complexity	Use custom roles with minimum required permissions
Shared privileged accounts	Loss of individual accountability	Create individual accounts for each administrator
Excessive Full Control assignments	Broad attack surface	Limit to designated infrastructure administrators
Change and Deploy without code review	Malicious code deployment	Implement deployment approval workflows
Manage Users and Roles for non-admins	Privilege escalation	Restrict to designated user administrators
No role-based separation	Violation of separation of duties	Create distinct roles for development, testing, operations

---

5. Security Configuration Settings

This section addresses FedRAMP requirement R2 for security configuration with documented implications.

5.1 Session Management

Session settings control user authentication persistence and security.

5.1.1 Configuration Location

Service Center > **Administration** > **Security** > **Applications Authentication**

5.1.2 Session Settings

Setting	Description	Recommended Value	Security Implications
Cache Time In Minutes	Time before server validates authentication against database	5 minutes (or ~20% of Max Idle Time)	Higher values reduce database load but delay session invalidation
Single Sign-On Between App Types	Enable SSO across Web and PWA	Enabled (required for SAML 2.0 support)	Logout from one app logs out all apps

Setting	Description	Recommended Value	Security Implications
Max Idle Time (Persistent)	Days before requiring re-authentication for persistent sessions	30 days (adjust based on policy)	Longer values increase window for session hijacking
Cookie Expiration	Days before authentication cookie expires	30 days (match Max Idle Time)	Longer values increase session persistence risk
Max Idle Time (Session)	Minutes before session authentication expires	20 minutes	Shorter values improve security but impact usability

5.1.3 Authentication Key Management

To regenerate authentication and encryption keys:

1. Navigate to **Service Center** > **Administration** > **Security**
2. Locate **Authentication and Encryption Keys**
3. Click **Generate**

Security Implications:

- All users MUST re-authenticate after key regeneration
- Use for suspected key compromise or policy rotation requirements

5.2 Brute Force Protection

OutSystems provides built-in protection against password guessing attacks.

5.2.1 Protection Mechanism

User-Level Protection:

- Blocks login attempts for a specific user from attacker's IP
- Legitimate user can still log in from other IP addresses

IP-Level Protection:

- Blocks all login attempts from an IP after threshold
- Prevents user enumeration and DoS attacks

5.2.2 Backoff Mechanism

Stage	User-Level Trigger	IP-Level Trigger	Block Duration
First Backoff	3 failed attempts	20 failed attempts	~5 minutes
Second Backoff	6 failed attempts	50 failed attempts	~60 minutes

5.2.3 Configuration for Application Users

Service Center > **Factory** > **Modules** > **Users** > **Site Properties**

Site Property	Default	Security Implications
EnableBruteForceProtection	Enabled	Disabling removes user-level protection
MaxUsernameAttemptsFirstBackoff	3	Lower = more protection, higher = less lockouts
MaxUsernameAttemptsSecondBackoff	6	Lower = stronger protection
UsernameAttemptsFirstBackoffDelayInSeconds	30	Shorter = more attempts possible
UsernameAttemptsSecondBackoffDelayInSeconds	1800	Shorter = faster retry after lockout
EnableBruteForceProtectionPerIP	Enabled	Disabling allows unlimited IPs to attack
MaxIPAttemptsFirstBackoff	20	Lower = faster IP blocking
MaxIPAttemptsSecondBackoff	50	Lower = longer IP blocking
IPAttemptsFirstBackoffDelayInSeconds	300	Shorter = faster unlock
IPAttemptsSecondBackoffDelayInSeconds	3600	Shorter = faster unlock
InvalidLoginCheckWindowInMinutes	60	Shorter = faster counter reset

5.2.4 Configuration for IT Users

Configure via **Factory Configuration** application in all environments:

1. Download and install Factory Configuration from OutSystems Forge
2. Access `https://<environment>/FactoryConfiguration`
3. Configure Brute Force Protection settings
4. Click **Apply**

Important: Settings MUST be consistent across all environments.

5.3 Content Security Policy (CSP)

CSP protects against XSS and other injection attacks.

5.3.1 Environment-Level Configuration

LifeTime > **Infrastructure** > **Environment Security**

1. Select environment
2. Enable CSP

3. Configure directives (one value per line)
4. Click **Save**
5. Republish all applications using "All Components" solution

5.3.2 Application-Level Configuration

LifeTime > **Applications** > [Select App] > **Security Settings**

1. Select environment from dropdown
2. Enable CSP
3. Configure directives
4. Click **Save**
5. Republish application

Note: Application-level CSP overrides environment-level CSP.

5.3.3 CSP Directives Reference

Directive	Purpose	Required Values	Security Implications
default-src	Default resource sources	`self`	Controls all unspecified resource types
script-src	JavaScript sources	`self`	Overly permissive allows XSS attacks
style-src	CSS sources	`self`	Inline styles may require `unsafe-inline`
img-src	Image sources	`self` `data:`	`data:` needed for embedded images
connect-src	AJAX/WebSocket sources	`self`	Restricts data exfiltration vectors
frame-ancestors	Embedding restrictions	`self`	Prevents clickjacking

5.3.4 Removing Unsafe Directives

For enhanced security in Reactive Web apps (Platform Server 11.28.0+):

1. Access Factory Configuration
2. Navigate to **Platform Configurations** > **Runtime**
3. Uncheck **Enforce Unsafe Eval Reactive**
4. Uncheck **Enforce Unsafe Inline Reactive**
5. Restart OutSystems Deployment Controller Service
6. Republish all applications

Security Implications:

- Removing `unsafe-eval` prevents dynamic code execution
- Removing `unsafe-inline` prevents inline script execution
- May break applications using dynamic JavaScript

5.4 Data Encryption at Rest

5.4.1 OutSystems Cloud Encryption

Front-End Server Encryption:

- AES-256 encryption on AWS EBS volumes
- AWS KMS key management
- Available by default on Sentry edition

Database Server Encryption:

- AES-256 encryption
- Dedicated encryption keys per customer
- Available by default on Sentry edition
- Enterprise/Universal requires request to OutSystems Support

5.4.2 Application-Level Encryption

For sensitive data (PII, PHI), implement application-level encryption:

1. Use **CryptoAPI** Forge component
2. Implement envelope encryption:
    - Generate Data Encryption Key (DEK)
    - Wrap DEK with Key Encryption Key (KEK)
    - Store wrapped DEK with encrypted data
3. Use AES-256-GCM for data encryption
4. Store KEK in external key management system (AWS KMS, HSM)

Security Implications:

- Application-level encryption provides defense in depth
- Key management is customer responsibility
- Consider performance impact on high-volume data

5.5 Transport Security

5.5.1 HTTPS Configuration

Service Center > **Administration** > **Security** > **Secure Connections**

Setting	**Recommended Value**	**Security Implications**
Enable HTTP Strict Transport Security (HSTS)	**Enabled**	Forces HTTPS, prevents downgrade attacks
Cookies > Secure	**Enabled**	Cookies only transmitted over HTTPS

5.5.2 TLS Requirements

FedRAMP Requirement: Use TLS 1.2 or higher for all connections.
OutSystems Cloud uses AWS-managed TLS termination with current security standards.

---

6. Audit Logging and Monitoring

This section covers logging capabilities for security monitoring and incident response.

6.1 Audit Log Types

6.1.1 Infrastructure Audit Logs (LifeTime)

Logs all IT user actions in infrastructure management:

Log Type	**Contents**
User Activity	Actions performed by each IT user
Application Changes	Deployment and configuration changes
Deployment Plans	Deployment approvals and executions
User Management	User creation, modification, deletion
Team Changes	Team membership and permission changes
Role Changes	Role creation and modification
Environment Changes	Environment configuration changes
Infrastructure Changes	Infrastructure-level modifications

Retention: 365 days (default), configurable via `TimeToKeepAuditsInDays` site property

6.1.2 Environment Logs (Service Center)

Log Type	**Contents**	**Retention**
Errors	Application and system errors, security exceptions	9 weeks
General	Application activity, slow queries, deployments	9 weeks
Traditional Web Requests	Request timing for Traditional Web Apps	9 weeks
Screen Requests	Request timing for Mobile/Reactive Apps	9 weeks
Service Actions	Service action execution details	9 weeks
Integrations	REST, SOAP, SAP integration logs	9 weeks

Log Type	Contents	Retention
Extensions	Extension action execution	9 weeks
Timers	Timer execution and scheduling	9 weeks
Emails	Email delivery status	9 weeks
Security	Blocked IP addresses, brute force attempts	9 weeks

6.2 Accessing Audit Logs

6.2.1 User Activity Logs

1. Access LifeTime USER MANAGEMENT > USERS
2. Select user
3. Click **View Activity Log**

6.2.2 Infrastructure Change Logs

1. Access LifeTime INFRASTRUCTURE (or ENVIRONMENTS for Cloud)
2. Click **View Audit Logs**
3. Filter by date, user, or action type

6.2.3 Security Event Logs

1. Access Service Center > Monitoring > Errors
2. Filter by **Source** = **Login**
3. Review blocked user/IP information

6.3 Log Permissions

Log Type	Required Permission
User Activity	Manage Infrastructure and Users
Application Logs	List permission for specific application
Deployment Logs	List permission for applications in deployment
User Management Logs	Manage Infrastructure and Users
Team Logs	Manage Teams and Application Roles
Role Logs	Manage Infrastructure and Users
Infrastructure Logs	Manage Infrastructure and Users

6.4 Security Event Monitoring

6.4.1 Events to Monitor

Event Type	Log Location	Severity
Failed login attempts	Errors (Source: Login)	Medium
User/IP blocked	Errors (Source: Login)	High
Privilege escalation	Audit Logs	Critical
Role changes	Audit Logs	High
User creation/deletion	Audit Logs	High
Environment configuration changes	Audit Logs	High
Application deployment	Audit Logs	Medium
CSP violations	Errors (Source: CSPReport)	Medium

---

7. Customer Configuration Quick Reference

7.1 Configuration Summary Table

Setting	Location	Recommended Value	NIST Control
Admin Password Complexity	LifeTime/Users App	Min 12 chars, mixed case, numbers	IA-5
SSO/SAML Configuration	Users App	Enabled with signed assertions	IA-2, IA-8
MFA	External IdP	Required for privileged users	IA-2(1), IA-2(2)
Session Timeout	Service Center	20 minutes (session), 30 days (persistent)	AC-12
Brute Force Protection	Service Center/Factory Config	Enabled (defaults)	AC-7
HTTPS/HSTS	Service Center	Enabled	SC-8, SC-13

Setting	Location	Recommended Value	NIST Control
Content Security Policy	LifeTime/Service Center	Configured per application	SC-18
Audit Log Retention	LifeTime	365 days	AU-4, AU-11
Data Encryption at Rest	OutSystems Cloud	Enabled (Sentry default)	SC-28
Log Streaming	LifeTime	Configured to SIEM	AU-4, SI-4
Role-Based Access	LifeTime	Least privilege roles defined	AC-2, AC-3, AC-6

7.2 Pre-Deployment Checklist

Item	Status	Notes
[ ] Users App administrator configured		Strong, unique password
[ ] All privileged accounts use SSO with MFA		Via external IdP
[ ] Custom roles created following least privilege		Avoid default Administrator
[ ] Brute force protection verified		Both user and IP level
[ ] Session timeouts configured		Align with security policy
[ ] HTTPS and HSTS enabled		All environments
[ ] CSP configured		Environment and application level
[ ] Audit logging verified		Retention meets policy
[ ] Break-glass procedures documented		Emergency access plan

7.3 Periodic Review Checklist

Review Task	Frequency	Notes
Privileged account review	Quarterly	Verify need-to-have

Review Task	Frequency	Notes
Role and permission audit	Quarterly	Check for privilege creep
Audit log review	Weekly/Daily	Security event analysis
Session timeout alignment	Annually	Policy compliance
CSP directive review	After deployments	Validate no regressions
Encryption key rotation	Per policy	Document rotation

Document History

Version	Date	Description
1.0	March 2026	Initial release

Contact Information

For questions regarding this guide:
Knox Systems https://knoxsystems.com/secure-configuration-guides
OutSystems Support https://success.outsystems.com/Support