



THINKTRENDS AI PLATFORM

Intelligent Infrastructure. Trusted by Design.

SECURE CONFIGURATION GUIDE

ThinkTrends AI Platform — For Customer Administrators

Document ID	TT-GDE-SCG-001
Version	1.0
FedRAMP Package ID	FR2634659079
Classification	PUBLIC — CUSTOMER-FACING
Effective Date	October 22, 2026
Review Cycle	Quarterly, or upon any change to the platform's security-relevant configuration
Document Owner	ISSO

PUBLIC — CUSTOMER-FACING | FOR TENANT ADMINISTRATORS



TABLE OF CONTENTS

1. Authentication (In Progress)
2. Password Requirements
3. Session Behavior
4. Access Management (In Progress)
5. Data Protection
6. Support and Questions
7. Obtaining and Using This Guide



This guide describes the security-relevant behavior of the ThinkTrends AI Platform that is relevant to your organization, and states plainly what is and is not currently configurable by a tenant administrator.

1. AUTHENTICATION (IN PROGRESS)

User identity is managed through AWS Cognito, fronted by the platform's load balancer, with cryptographic signature verification (ES256) on every request.

Users sign in with a passkey (WebAuthn / FIDO2) — a phishing-resistant credential stored on their device and unlocked with Face ID, a fingerprint, or a device PIN. This combines something the user has (the device) with something they are or know (biometric or PIN). **Every passkey sign-in is multi-factor.** The platform requires user verification on every use: a passkey only works after the user unlocks it on their device with Face ID, a fingerprint, or a device PIN. This combines two factors in a single step, the device the user has and the biometric or PIN only they can provide, and the platform's identity service is configured to treat passkey sign-in with user verification as MFA. Because each passkey only works on the ThinkTrends domain, this MFA is also phishing-resistant: a look-alike site cannot capture or replay it. The platform does not use SMS or authenticator-app codes.

Supported devices. Built-in authenticators (Face ID, Touch ID, Windows Hello, Android fingerprint or screen lock) and hardware security keys. A security key must have a PIN set, because user verification is required.

2. PASSWORD REQUIREMENTS

The platform enforces the following password policy for all users. This is a fixed, platform-wide baseline — it is not currently configurable per tenant:

- Minimum length: 12 characters.
- Requires uppercase, lowercase, numeric, and symbol characters.
- Temporary (first-login) passwords are valid for 7 days.

3. SESSION BEHAVIOR

Session and token lifetimes are explicitly configured and enforced platform-wide, identically across all environments:

- Access token validity: 1 hour.
- ID token validity: 1 hour.
- Refresh token validity: 24 hours.

These values are codified in infrastructure with hard limits (access and ID tokens cannot exceed 1 hour; refresh tokens cannot exceed 24 hours) and are not customer-configurable per tenant — they are a fixed, enforced platform baseline. There is currently no customer-facing setting to force-terminate an individual active session before its token expires.



4. ACCESS MANAGEMENT (IN PROGRESS)

The platform enforces role-based permissions internally to control what actions a user can take within the platform. Organization-level self-service role management is not yet available. Today, changing a user's role requires a support ticket and a ThinkTrends administrator or developer to make the change directly. There is currently no ThinkTrends-side admin console or API for this, for ThinkTrends staff or for administrators. If you need a user's role changed, contact your ThinkTrends account representative rather than looking for a settings page.

ThinkTrends plans to implement organization-level RBAC, giving your organization's own administrators the ability to assign and adjust roles for your users directly, without requiring ThinkTrends to make the change on your behalf. Each organization will have an administrator with full control over role and team assignment within that organization. Users within an organization will be organized into teams. Each user will hold one of four roles — admin, team lead, builder, or user. Anyone holding a role above user will be able to create and configure resources; a user may only invoke and use resources that have been shared with them by another role holder.

Administrators will manage team membership and role assignment directly, through a dedicated administration interface, without contacting ThinkTrends. Resource sharing will extend beyond direct, person-to-person sharing: administrators will be able to share a resource with a specific person, a specific team, or the entire organization.

As of October 22, 2026, this is not yet live in production. Role assignment today requires a ThinkTrends support ticket, as described above. Resource sharing today is self-service and person-to-person: the creator of a resource can share it directly with another user in the same organization, but there is no team- or organization-wide sharing, and no administration interface for team or role management. Once implementation is completed and verified against the live system, this section will be updated to describe the delivered configuration.

Access to your organization's top-level administrator accounts is currently protected by the same passkey sign-in described in Section 1. The security-relevant settings that apply to administrator and privileged accounts (sign-in method, password policy, and session and token lifetimes) are fixed platform-wide and described in Sections 1–3. They cannot be changed by tenant administrators, which means no tenant action is needed to keep them secure. Role assignment is the only administrator-relevant control that changes who can act in your organization, and it is currently performed by ThinkTrends on request. Because elevated roles carry broad access, we recommend granting them only to people who need them and reviewing role assignments at least quarterly. To remove an administrator or revoke elevated access, for example when someone leaves your organization, contact your ThinkTrends account representative. Request removal on the day the person leaves or changes role.

5. DATA PROTECTION

Data is encrypted at rest and in transit throughout the platform. No additional customer configuration is required to enable this baseline protection.



6. SUPPORT AND QUESTIONS

For questions about your tenant's security configuration, or to report a suspected security issue, contact your ThinkTrends account representative or the security contact listed in ThinkTrends' Trust Center.

7. OBTAINING AND USING THIS GUIDE

- The current versions of both this document and its companion machine-readable copy are available at <https://trust.paramify.com/thinktrends/thinktrends-ai-platform/deliverables>. Additionally, this guide is included in ThinkTrends' FedRAMP Certification Package.
- The machine-readable companion lists each security-relevant setting described in Sections 1–3, with its recommended value, and carries the same version number as this document. Compare it against the settings you observe in your tenant.
- Versioning: the version number increases with every substantive change. Each change is recorded below.

Version	Date	Summary of Changes
1.0	October 22, 2026	Initial release.

DOCUMENT APPROVAL

This guide (TT-GDE-SCG-001, Version 1.0) has been reviewed and approved by the ISSO, the Document Owner, and is effective as of October 22, 2026. Content is verified directly against existing infrastructure.

Role	Name	Date
ISSO	Dikshyant Rai	October 22, 2026

Version 1.0 — October 22, 2026. Prepared for FedRAMP CR26 20x Class C certification. Content verified directly against existing infrastructure. © 2026 ThinkTrends AI Platform. All rights reserved.

— End of Document —