Contents

RADIANT Authentication Overview

Version: 5.52.29 | **Last Updated**: January 25, 2026 | **PROMPT-41C**

RADIANT provides enterprise-grade authentication with multi-layer security, supporting everything from individual users to large organizations with complex security requirements.

Key Features

Feature	Description
Multi-layer authentication	End users, tenant admins, and platform admins
Enterprise SSO	SAML 2.0 and OIDC integration
Two-Factor Authentication	Required for admin roles
OAuth 2.0 Provider	Third-party app integrations
18 Language Support	Full internationalization including RTL
Multi-language Search	CJK (Chinese, Japanese, Korean) support

Authentication Layers

RADIANT implements three distinct authentication layers, each designed for specific use cases:

```
graph TB
    subgraph "Layer 1: End Users"
        EU[End Users] --> UP[User Pool]
        UP --> TT[Think Tank]
        UP --> CU[Curator]
        UP --> TA[Tenant Admin]
    end

    subgraph "Layer 2: Platform Admins"
        PA[Platform Admins] --> AP[Admin Pool]
```

```
    AP --> RA[RADIANT Admin]
end

subgraph "Layer 3: Services"
    SV[Services & Apps] --> AK[API Keys]
    SV --> M2M[M2M Tokens]
    AK --> API[RADIANT API]
    M2M --> API
end

style EU fill:#e1f5fe
style PA fill:#fff3e0
style SV fill:#f3e5f5
```

Layer 1: End-User Authentication

For users of Think Tank, Curator, and Tenant Admin applications.

Feature	Description
Sign-in Methods	Email/password, Google, Microsoft, Apple, GitHub
Enterprise SSO	SAML 2.0 and OIDC for organization-wide sign-in
Passkeys	WebAuthn/FIDO2 passwordless authentication
MFA	Optional for standard users, required for tenant admins
Languages	18 languages including Arabic (RTL)

Layer 2: Platform Administrator Authentication

For RADIANT platform operators and support staff.

Feature	Description
Access	Invitation-only (no self-registration)
MFA	Always required, cannot be disabled
Session Timeout	30 minutes (shorter than end users)
Audit	All actions logged with full context

Layer 3: Service Authentication

For programmatic access and third-party integrations.

Feature	Description
API Keys	Long-lived keys for server-to-server communication
OAuth Tokens	Short-lived tokens for third-party apps acting as users
Scopes	Fine-grained permissions for each token/key

Supported Languages

RADIANT authentication screens are available in 18 languages:

Language	Code	Direction	Search Method
English	`en`	LTR	PostgreSQL FTS
Spanish	`es`	LTR	PostgreSQL FTS
French	`fr`	LTR	PostgreSQL FTS
German	`de`	LTR	PostgreSQL FTS
Portuguese	`pt`	LTR	PostgreSQL FTS
Italian	`it`	LTR	PostgreSQL FTS
Dutch	`nl`	LTR	PostgreSQL FTS
Polish	`pl`	LTR	PostgreSQL `simple`
Russian	`ru`	LTR	PostgreSQL FTS
Turkish	`tr`	LTR	PostgreSQL FTS
Japanese	`ja`	LTR	`pg_bigm` bi-gram
Korean	`ko`	LTR	`pg_bigm` bi-gram
Chinese (Simplified)	`zh-CN`	LTR	`pg_bigm` bi-gram
Chinese (Traditional)	`zh-TW`	LTR	`pg_bigm` bi-gram
Arabic	`ar`	**RTL**	PostgreSQL `simple`
Hindi	`hi`	LTR	PostgreSQL `simple`
Thai	`th`	LTR	PostgreSQL `simple`
Vietnamese	`vi`	LTR	PostgreSQL `simple`

See Internationalization Guide for details on changing your language.

Security Features

Multi-Factor Authentication (MFA)

```
flowchart LR
    subgraph "MFA Methods"
        TOTP[Authenticator App<br/>TOTP]
        BC[Backup Codes<br/>10 one-time codes]
    end

    subgraph "Device Trust"
        DT[Remember Device<br/>30 days]
        DM[Device Management<br/>Up to 5 devices]
    end

    TOTP --> DT
    BC --> DT
```

Method	Description
TOTP	Time-based codes from authenticator apps (Google, Microsoft, 1Password, Authy)
Backup Codes	10 one-time recovery codes for emergency access
Device Trust	Skip MFA verification on trusted devices for 30 days

Enterprise SSO

```
flowchart LR
    User --> App[RADIANT App]
    App --> |"Redirect"| IdP[Identity Provider]
    IdP --> |"SAML/OIDC"| App
    App --> |"Session"| User

    subgraph "Supported Providers"
        Okta
        AzureAD[Azure AD]
        Google[Google Workspace]
        OneLogin
        Custom[Custom SAML/OIDC]
    end

    IdP -.-> Okta
    IdP -.-> AzureAD
    IdP -.-> Google
    IdP -.-> OneLogin
    IdP -.-> Custom
```

OAuth for Third-Party Apps

Third-party applications can request permission to access RADIANT on behalf of users:

```
sequenceDiagram
    participant User
    participant App as Third-Party App
    participant RADIANT

    User->>App: Click "Connect to RADIANT"
    App->>RADIANT: Authorization request
    RADIANT->>User: Show consent screen
    User->>RADIANT: Approve
    RADIANT->>App: Authorization code
    App->>RADIANT: Exchange for tokens
    RADIANT->>App: Access token
    App->>RADIANT: API requests (as user)
```

Application Matrix

Application	User Types	MFA	SSO	OAuth	Languages
Think Tank	Standard users	Optional (hidden)		N/A	18
Curator	Standard users	Optional (hidden)		N/A	18
Tenant Admin	Tenant admins/owners	Required		N/A	18
RADIANT Admin	Platform admins	Required		N/A	18

Quick Links

Document	Audience	Description
User Authentication Guide	End Users	Sign-in, password, passkeys
Tenant Admin Guide	Tenant Admins	SSO, user management, MFA policies
Platform Admin Guide	Platform Admins	System-wide auth configuration
MFA Setup Guide	All Admins	Two-factor authentication setup
OAuth Developer Guide	Developers	Building third-party integrations
Internationalization Guide	All	Language settings, RTL support
API Reference	Developers	Technical API documentation
Search API Reference	Developers	Multi-language search
Security Architecture	Security Teams	Compliance and architecture
Troubleshooting	All	Common issues and solutions

Related Documentation

- RADIANT Admin Guide - Platform administration
- Think Tank Admin Guide - Tenant administration
- Think Tank User Guide - End-user documentation
- Engineering Implementation Vision - Technical architecture