Recognize

Technology | Security Overview

Overview

Preserving the confidentiality and integrity of your information is one of Recognize's highest priorities. This document summarizes the key measures we take in ensuring your data is always protected. Please consult your Recognize contact for the latest security overview.

How Recognize is Protected

Recognize utilizes an iterative approach in designing and improving security procedures and controls. We continuously analyze the effectiveness of our security policies to ensure we are providing optimal protection for our customers.

- Data Center Security: Recognize's servers are located in Amazon web service's world-class, highly secure data centers utilizing state-of-the art electronic surveillance and multi-factor access control systems. Data centers are staffed 24x7 by trained security guards, and access is authorized strictly on a least privileged basis. Environmental systems are designed to minimize the impact of disruptions to operations.
- Secure Connections: All connections to Recognize are secured via SSL/TLS. Any attempt to connect over HTTP is redirected to HTTPS.
- Application Security: Recognize utilizes secure development best practices that integrate security reviews throughout design, prototype and deployment.
- Customer Data Protection: All data is classified as confidential and treated as such. Inbound and outbound low-level logical firewalls ensure that data is protected from unauthorized access.
- Hardened Operating System: Recognize runs on hardened Linux servers. Externally exposed critical patches are addressed within 24 hours.
- Internal and Third Party Testing: Recognize routinely runs internal and external vulnerability scans and penetration tests. Third party firms are utilized to perform daily application testing.
- Business Continuity: Recognize customer data is backed up daily, protected with strong encryption on disk, and distributed geographically via the AWS RDS service. The backup retention period is 7 days.

© Recognize 2018

Recognize

Authentication and Authorization

Access to Recognize is restricted to employees within your organization. We provide robust features and integrations to manage your users and control your data. The browser extensions connect via OAuth.

- User Provisioning: User Provisioning is accomplished via manual invite, bulk invite, automatic login via OAuth 2.0 or User Sync. User sync can be accomplished via Yammer, Office 365, or ActiveDirectory(LDAP) via standard queries from their respective apis.
- Password Policies: Recognize implements industry standard password policies by requiring minimum length (eight characters) and are stored with a salted one-way 256 bit encryption algorithm. Brute-force password attacks are mitigated with CPU and memory bound computational constraints.
- OAuth 2.0 Authentication: Access to Recognize can be granted via an OAuth 2.0 flow. Recognize supports Google, Yammer, and Office365 OAuth. Passwords are never transmitted to Recognize via OAuth 2.0. Upon successful authentication, an api token is provided to make api requests on behalf of the authenticated user. See technology references below for more information.
- Single Sign On (SAML v2): Please see our SAML Security Document - https://recognizeapp.com/recognize-security-saml.pdf

Personal Information

We store the following personal user information in our database:

- Name (first, last, display)
- Email
- Hire date (optional for service anniversary recognitions - month, day, and year)
- Birthday (optional for birthday recognitions - month and day only)
- Phone (optional - for SMS notifications)
- Password (unless 3rd party authentication such as Google, Yammer, Office365, or SSO)
- Job title (optional)
- Display name (optional)
- Manager (optional)
- Avatar / Profile image (optional)
- Recognition messages, comments, approvals and other data generated via Recognize platform

Recognize

Additional Privacy Information

Yammer feed data and Office 365 data will never be stored, however, aggregate information may be collected or analyzed.

More information at: https://recognizeapp.com/privacy

General Data Protection Regulation (GDPR) Compliance

Recognize intends to comply with the European Union's General Data Protection Regulation requirements. Users may request their personal data to be removed at any time. Recognition data involves multiple people and will remain in the platform. However, any identifying data such as name, email or display name, to those who request so will be removed from the platform.

Technology References

- https://developer.yammer.com/v1.0/docs/oauth-2
- https://developer.microsoft.com/en-us/graph/graph-explorer
- https://msdn.microsoft.com/en-us/office/office365/howto/common-app-authentication-tasks
- https://developers.google.com/identity/protocols/OAuth2