Identity and Access Management

Intapp Identity and Access Management puts firms in control

When you select Intapp solutions to help your professional services firm remain competitive and profitable, you're assured of tightly managed access to your user, client, and matter data. Intapp Identity and Access Management (IAM) puts you in control of managing individuals' access rights while a centrally managed single sign-on (SSO) approach provides frictionless access across all applications. Intapp IAM harnesses the latest technology to provide a unified view into security policies across an organization.

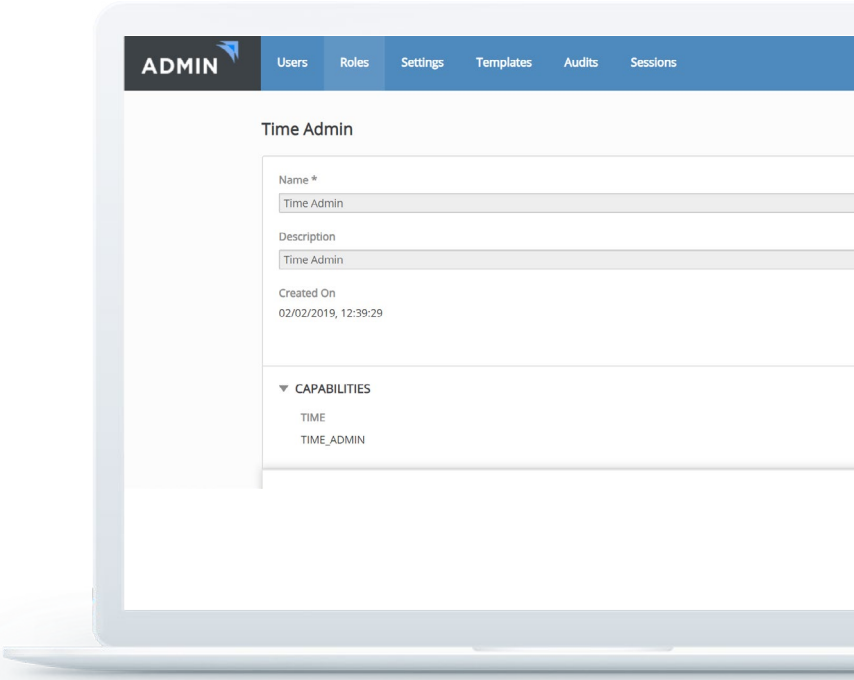
Professional services firms need to be able to manage the authentication of identities provided to employees, contractors, or lateral hires. They must also secure access to client information, especially between business units within the same practice, to prevent any conflicts of interest between staff of two or more business units serving the same client.

Intapp IAM allows client collaboration by managing the access of external users at your firm's discretion via a single integrated solution.

Global control enabled by a central portal

Intapp IAM provides a unified global view into security policies across your entire organization. Admins can easily grant default permissions to entire groups or users.

The administrator has fine-grained access control over the definition and management of standard and custom roles, privileges, and the assignment of roles to users with synchronization to external systems.



CONTACT @intapp | sales@intapp.com | intapp.com

Third-party authentication support

Intapp supports industry standard providers for exchanging authentication and authorization data between security domains, such as Intapp certified Azure AD, Active Directory Federation Services (ADFS), OKTA and OptimalCloud.

Mature local-user management

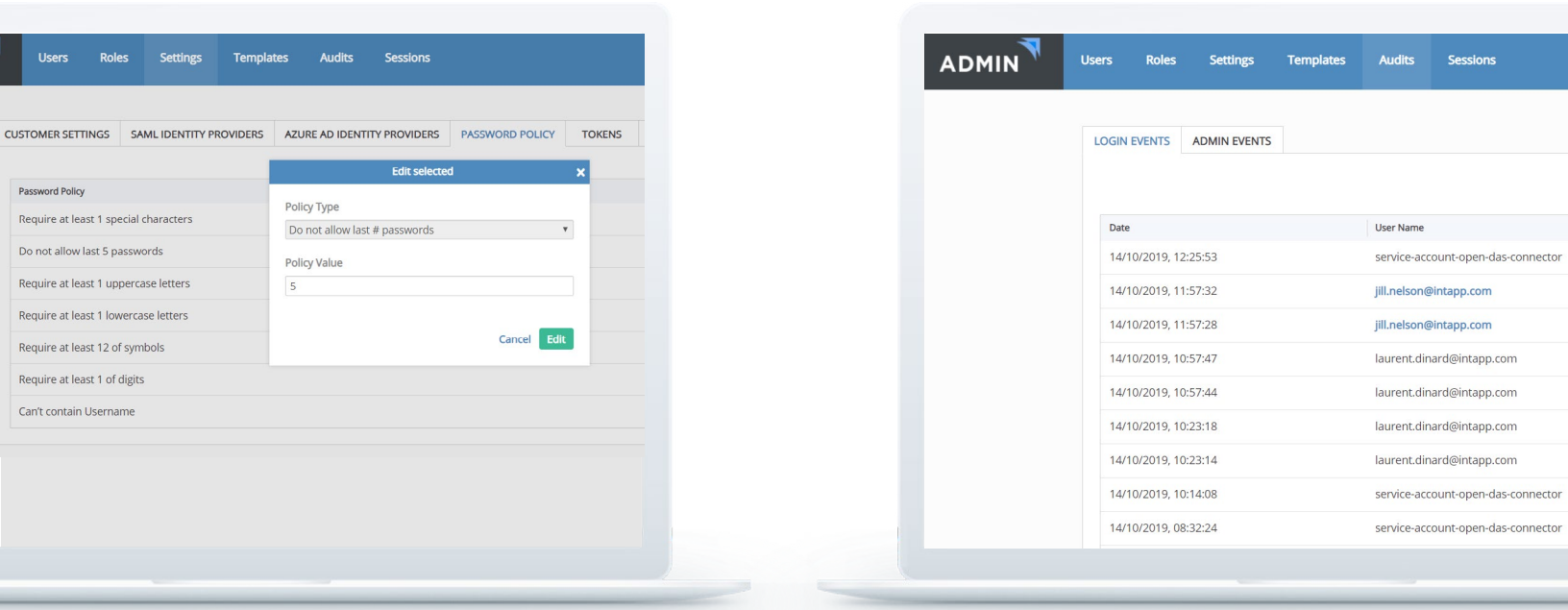
Intapp IAM offers mature local-user management with customizable password complexity requirements. It can also provide a mobile-based, multifactor authentication option.

Mobile user administration

Intapp allows mobile users to stay logged in without having to reauthenticate every time. The admin portal provides oversight by displaying all logged-in users at any point of time and includes the ability to revoke offline access on a per-user basis, such as in case of a lost device.

Audit logging

Intapp provides a full audit trail of user-related login information, including a history of permissions authorization, removal, and delegation, to the admin.



Secure access

SSO and multifactor authentication enable secure access to your common data store as well as Intapp products and solutions whether via computers, tablets, or smartphones.

Frictionless sign-on

Intapp lets users remember just one user name and password to sign in to any Intapp product or solution, or any other third-party system integrated with Intapp OnePlace.

Managed users

You can easily provision and manage users — including local users, such as lateral hires or external identities — for Intapp products and solutions, and Intapp OnePlace.

Centralized management

The Intapp administrative UI provides a unified view into a security policies across your entire organization. The same interface lets you define and manage roles and privileges.

intapp

CONTACT @intapp | sales@intapp.com | intapp.com