Anaplan

Anaplan security overview brief

Enterprise-level security for simplified user access, management, and control

Executive summary

Your planning decisions' success hinges on fast access to critical data to keep pace with market trends. At the same time, it's important to make sure your data is secure—and that only approved users can access particular data to comply with security protocols and mandates.

Some security methods can feel like productivity roadblocks to your users. Security requiring multiple steps to grant users access is also difficult for security administrators to manage and control. It's simply not conducive to workspace agility. That's why Anaplan security offerings provide enterprise-level protection for your company's most critical planning data that doesn't get in the way of business.

Security that protects your next move

Anaplan security offerings include Self-Service SAML (SS SAML) to simplify single-sign on (SSO) and Central Identity Management (CIM) to streamline user management, all managed with a unified administration console that provides security administrators with everything they need in a centralized place. Together, Anaplan security ensures that end users can easily access Anaplan.

In addition, administrators gain greater visibility and control of who is accessing the platform and when, all with a single pane of glass. Integration developers can also build processes that automatically update and manage user access based on the latest business needs. Compliance officers can rest assured their data is secured and meets the compliance and regulation mandates of their organization.

Key benefits of Anaplan security offerings

Simple secure access

End users gain fast and easy access to the Anaplan data they need with SSO.

Visibility and control

Greater visibility and control of useraccess, permissions, and events with a centralized interface.

Manageable and compliant

Easily adhere to the compliance best practices within your organization

Sleek, streamlined administrator experience

Security functions within Anaplan start with the administrator console, which delivers a seamless way to navigate users, workspaces, and events within the UX. Think of it as your one-stop-shop for configuring and managing your Anaplan security needs, including SS SAML and CIM. The administrator console is built for administrators across all stages of their Anaplan journey. Whether you're one administrator managing users, or part of a mature center of excellence (CoE), the console is designed to expedite processes through a centralized console.

The administrator console is a single point of entry to administer Anaplan for users and provides visibility with a single view across all tenant-level resources, such as models and workspaces, so administrators can gain a strong understanding of who's accessing what parts of the platform and when. This type of transparency also helps audit user activity across the organization to ensure that compliance needs are met.

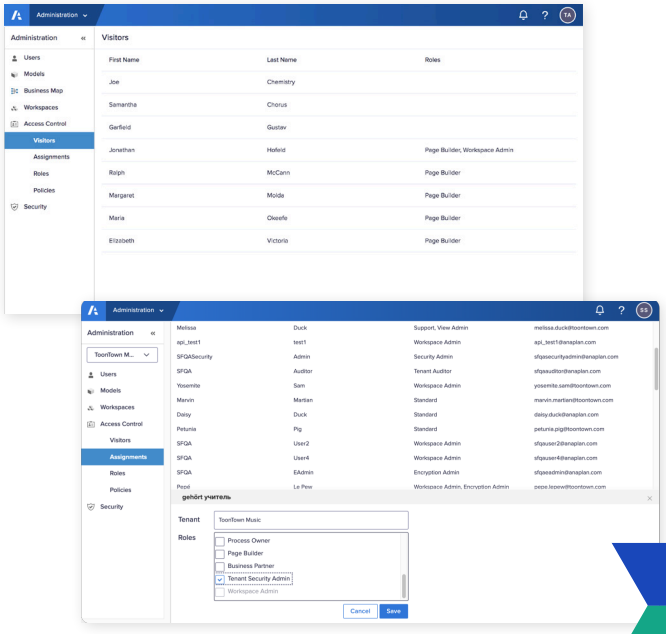
Access control helps ensure separation of duties and divides the administrator experience across different roles. Users with the following roles assigned can access the administrator console:

- The tenant admin role is the gateway to the administrator application and can assign roles to other users. They can also view and manage tenant-level configurations, assign and export roles, as well as view who has access to models within their tenant and enable/disable access.
- Tenant auditors can access audit functionality from the console.
- Tenant Security admin can access and deploy SS SAML, as well as update their identity provider (IDP) configurations.
- User admins can create, manage, and delete users, as well as assign them to workspaces.
- The Workspace admin can assign users to a model role within a workspace and define selective access for users.
- The View admin can see models and workspaces at the tenant level in their organization but cannot perform updates or changes.
- Integration admins can add or delete connections such as CloudWorks configurations.
- Page builders can configure pages in the UX.
- Encryption admins manage bring-your-own-key (BYOK) configurations and are typically part of IT.

Find out who has access to the model at a glance with identity management. View a dashboard with a list of model users and associated profile information within your tenant. Administrators can also enable and disable platform access to users at this level, as well as remove dormant users no longer accessing the platform.

With workspace management, administrators can view near real-time usage across all workspaces in the tenant, gaining valuable insight on the percentage of workspace being used. Easily view a list of workspaces and status across the organization, as well as the number of all models held within a certain workspace. This knowledge helps administrators forecast and prepare for upticks in usage during critical planning periods.

Administrators also gain visibility into the workspace usage for visitors from another tenant. The workspace administrator role provides a holistic view of all visitors with dedicated sections where they can view who has access and permissions levels. In addition, administrators can assign in which areas visitors and users can view and build pages.



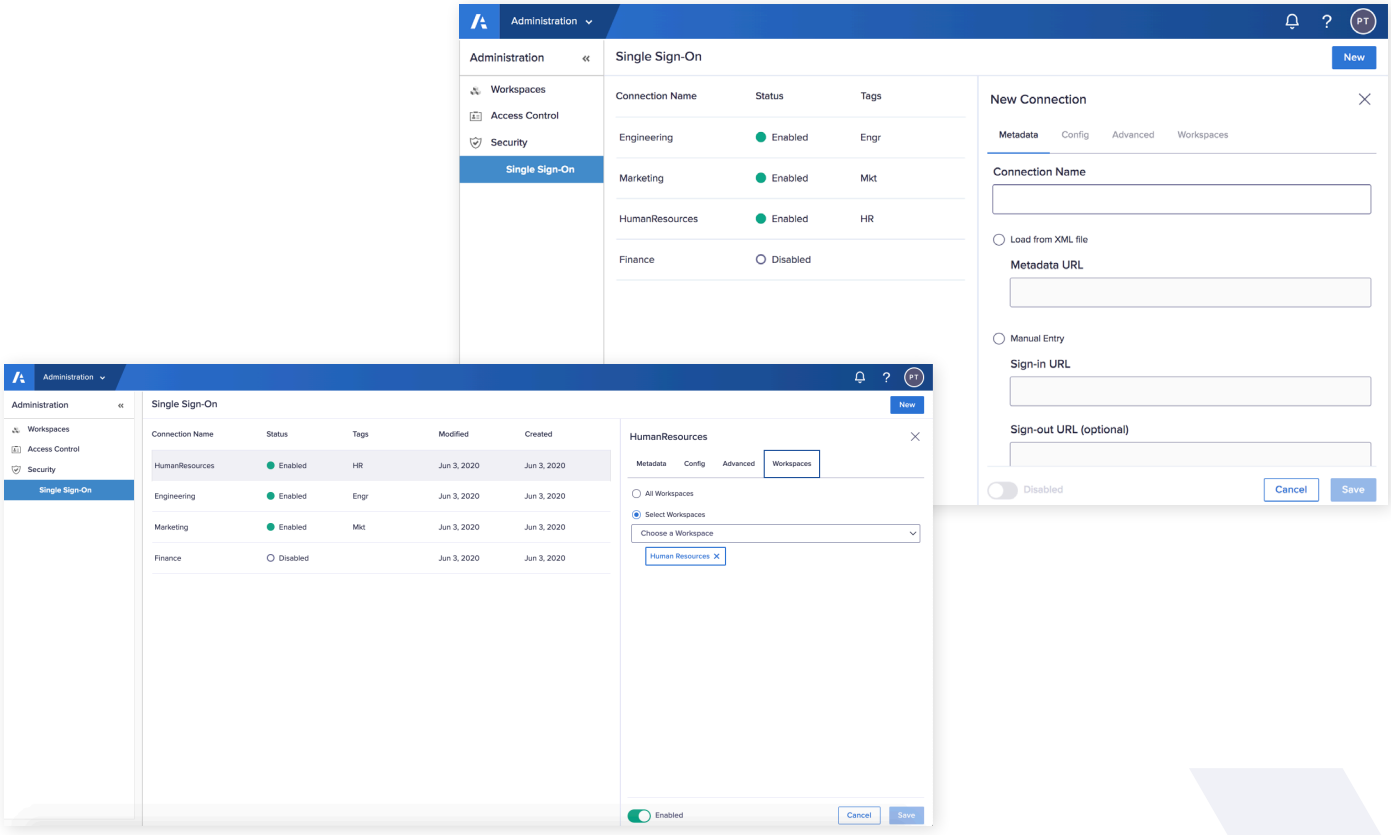
Self-Service SAML: Simple SSO, strong visibility

SS SAML allows users to easily access Anaplan with minimal effort, so they can get to the data they need fast. With an easy-to-use interface, administrators can deliver the power of SAML security, minus the complexity. Security administrators can easily automate UI configuration for SSO access to expedite user authentication. They can also harden protection for Anaplan security domain access and deliver a layered approach to their security configuration. SS SAML is available for both web and mobile, and mobile can authenticate users using native biometric options.

In addition, SS SAML drives strong compliance that enables administrators to leverage best practices that encrypt and configure settings to meet your organization's highest standard of security and compliance. SS SAML complies with SAML standards while interoperating with SAML 2.0 IDPs. It includes a Tenant Security Admin role to ensure separation of duties, and supports digitally signed artifacts, encrypted responses, and assertions.

Security administrators can also gain visibility into their SSO configurations with a robust framework that supports multiple authentication flows and configurations specifically. The framework can scale to address large volumes of users as well as the number of users per customer accessing the platform. Administrators can leverage flexible IDP policy enforcement as well as additional security beyond the standard SAML flow as needed.

SS SAML is highly customizable. It includes multiple configuration options for tight control over user behavior and authentication. Administrators can flexibly address use cases and meet compliance with their organization's authentication policies. Enhanced security options allow administrators to encrypt SAML requests, customize entity IDs and user identities, delivering higher assurance levels. See the SS SAML data sheet for more information.



CIM: Centralized management and security

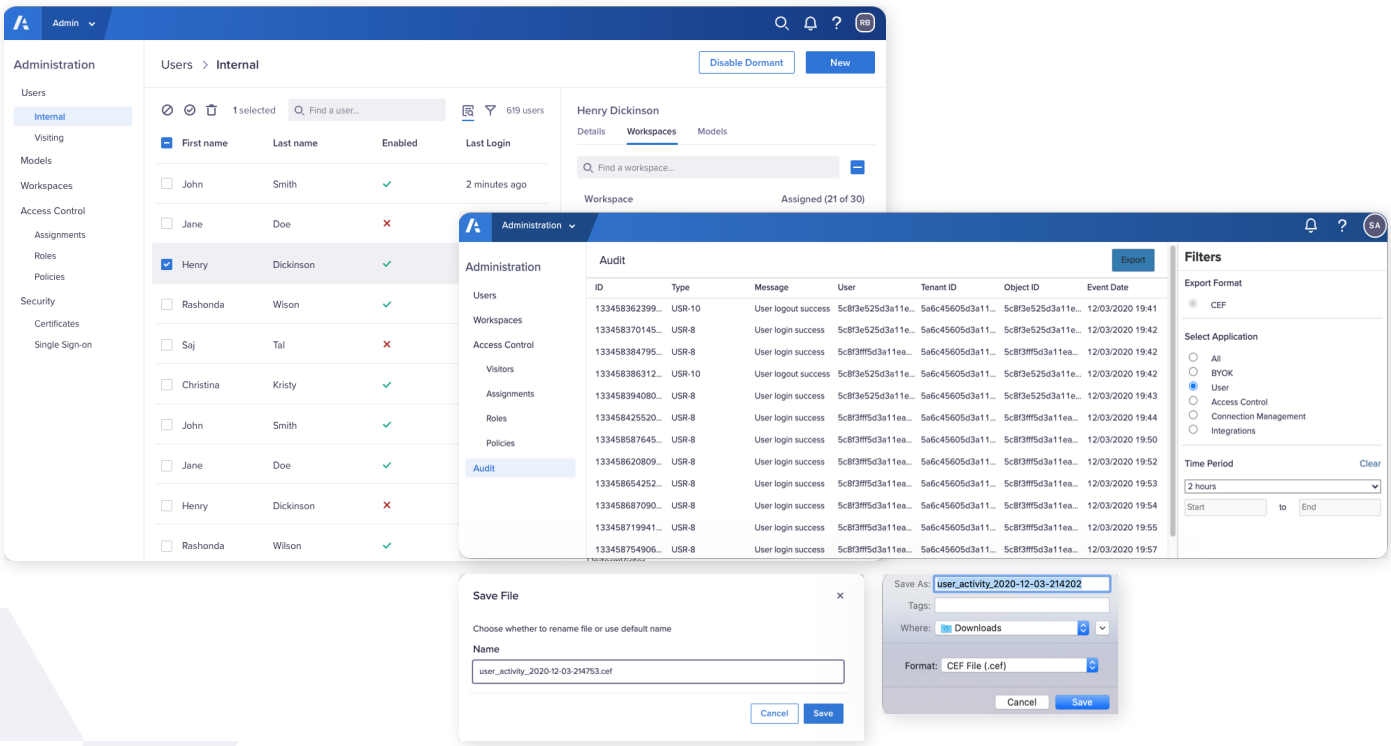
CIM is designed to empower administrators to manage all of the users in their tenant from a single pane of glass dashboard, providing a high level of security and trust for users, data, and the environment.

Administrators can leverage CIM to easily manage enterprise-wide compliance requirements. With CIM, they can support segregation of duties with a user administrator role and enable audit tracking within the user interface with robust tools, APIs, and third-party integrations. Users will also be able to be quickly de-provisioned from the platform with a single step to protect against unauthorized access.

The CIM unified interface provides granular visibility and control, so administrators can gain a complete and accurate view of the entire tenancy of all users and access. Administrators can create, provision, and manage users across multiple workspaces with one unified interface. In addition, they can see all users, their status, and the workspaces they have access to at a glance and add or remove temporary visitors within a centralized UI.

The ability to simplify and streamline user access management with CIM helps save time, costs, and boost productivity. Administrators can create a user once and assign them to multiple workspaces, eliminating user creation at the workspace level. Upcoming features such as three-step user configuration across one or more workspaces and two-step user de-provisioning and deletion will streamline user management, and it will be simple to auto-populate users into Anaplan with in-house directories and provisioning systems via integrated APIs. These capabilities will significantly reduce the number of administrative resources and overhead needed for traditional manual administration.

Anaplan System for Cross-Domain Identity Management (SCIM) APIs are the next step in the evolution of CIM. These REST-based APIs may be used in data integrations between the Anaplan tenant and a SCIM-compliant identity source. SCIM APIs will allow customers to more easily create users in Anaplan, assign workspaces, and apply simple changes. Customers can simplify user management by integrating directly with their primary sources of user identity so they can use their existing application provisioning policies, tools, and specialists. SCIM APIs will make user management in Anaplan faster, easier, and more economical.

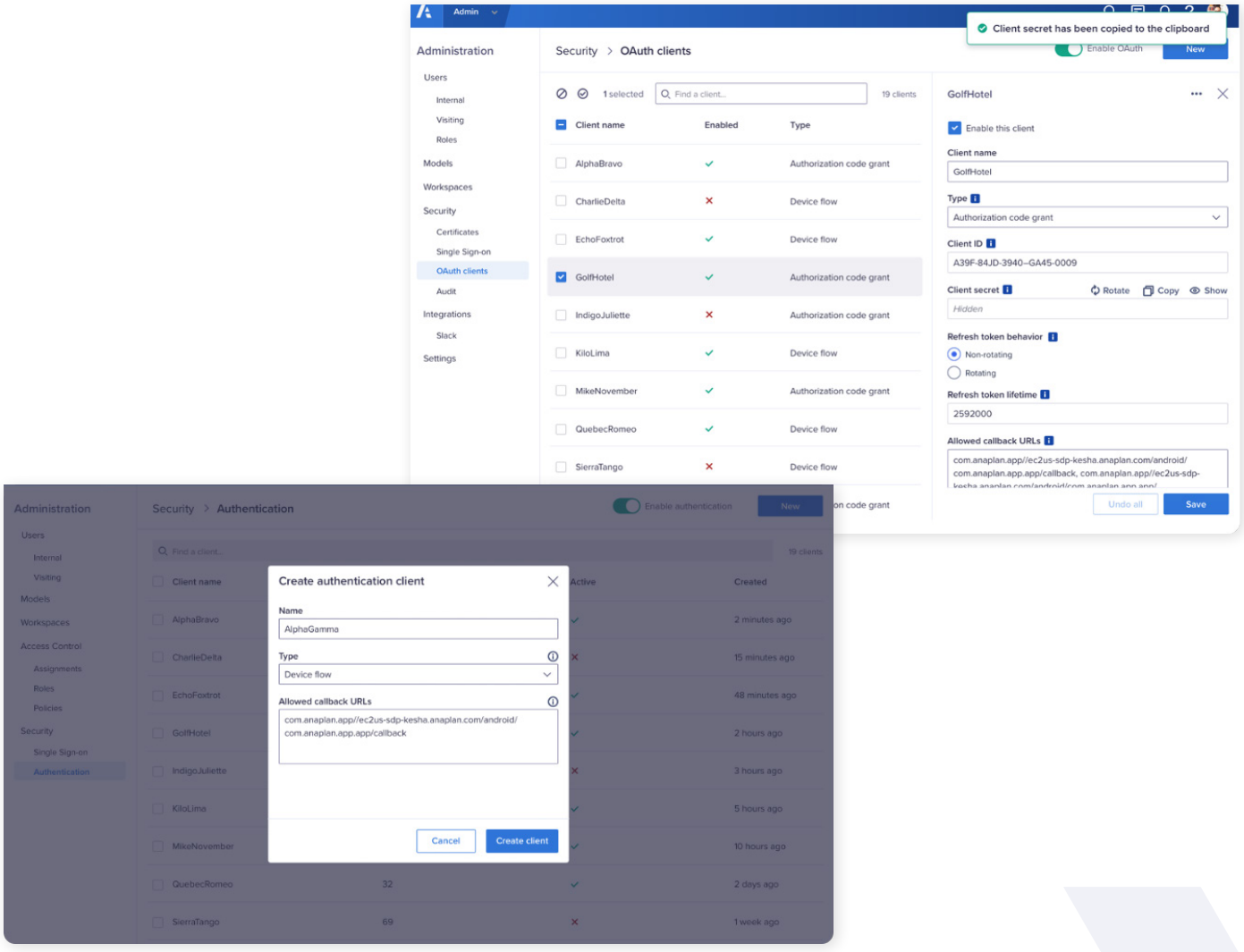


Self-service OAuth

With self-service (SS) OAuth, customers have even more options to align APIs and integrations with their organization's authentication, authorization, and access (AAA) policies. An industry-standard protocol for authorization delegation, tenant security administrators can enable SS OAuth to establish secure integrations to third-party applications without maintaining certificates or exposing privileged credentials.

Tenant security administrators also secure perpetual access to protected resources, aligning token rules and behaviors with organizational requirements. Simple to use and easy to configure, tenant administrators can select from different flow types, such as the authorization code grant and device grant, to create the appropriate OAuth client for each use case.

Refresh and access tokens are used to securely connect to Anaplan APIs to manage AAA policies, and tenant security administrators can control and align token lifecycles in accordance with organizational security policies. Alongside these governance and access controls, tenant security administrators can disable clients to deny services or prevent undesirable user activity at any time for greater peace of mind.



Maintain compliance with audit tracking

Anaplan Audit allows you to track audit events from your Anaplan tenant into your auxiliary technology such as a Security Information and Event Management (SIEM) system for alerting and tracking purposes. Within Anaplan Audit, you can track a variety of audit logs including encryption, user activity, access control, and connection management.

Easily see who is logging in and out of workspaces, along with the specific actions they took while using Anaplan. This helps expedite the internal audit process by helping administrators easily identify which internal and external users are using the platform most frequently, if their roles have been changed, as well as track their activity across the platform in near real time.

Users can access audit logs via an API or the administrator console for up to 30 days of logs. In addition, they can filter logs by time period and application, as well as insights about specific events. This helps tenant administrators perform internal audits based on usage. They can also leverage this data with some of their SIEM systems. Administrators can initiate a download of this data from the assignments page and save it to a CSV.

Plus, CIM can further meet compliance needs with audit tracking. Administrators can increase compliance visibility and enrich SIEM system analysis. They can get a granular view of audit logging across user creation, deletion, updates, and workspace assignments, and then generate audit logging in Common Event Format (CEF) as well as leveraging the UI to easily identify events in the console.

Protect critical planning data

Anaplan also has capabilities you can leverage to ensure that your most important planning data in the cloud is protected. With Anaplan's BYOK service, you can define and manage unique encryption keys for your Anaplan workspaces. Encrypt your most proprietary and confidential data in the cloud for an additional layer of protection, so you can run your business with peace of mind. In addition, BYOK helps meet compliance and regulation requirements all while leveraging your data
in the cloud.

Dynamic cell access protects cell data by providing the ability to control access to cell data at a granular level. For example, workspace admins can make the contents of individual cells, rows, or columns read-only, editable, or completely invisible to certain users. For example, dynamic cell access would be particularly useful in headcount planning that requires user access to employee data. Particular data such as personally identifiable data (PII) or compensation may not want to be revealed based on the user accessing the data. In these cases, a workspace admin can hide sensitive information, or make particular columns read-only to adhere to compliance and protect employee data.

Meet compliance across any environment

Easily ensure compliance and monitoring across any environment with a defense-in-depth approach. Anaplan has a full-time team of security and compliance experts to perform SOC 1 and 2 audits, are aligned with ISO 27001 and 27018, TRUSTe certified, and IAPP members.

In addition, Anaplan has ISO 27k certified Equinix IBX data centers and provides encryption for data at rest and in transit. With our approach to continuous monitoring across applications and infrastructure coupled with regular vulnerability scans, we're committed to keeping data secure.

Conclusion

Maintaining secure user access and granular visibility while meeting company compliance standards doesn't have to feel like a burden. With an intuitive administrator console, SS SAML, and CIM, Anaplan security offerings empower administrators to configure SSO and manage user access, ensuring that only approved users have access to workspaces and data.

In addition, integrations and APIs can further help to effectively and easily manage user data. By putting security in the hands of your own administrators, you can ensure smooth, secure access to Anaplan that, instead of stifling productivity, bolsters it.

About Anaplan

Anaplan (NYSE: PLAN) is a transformative way to see, plan, and run your business. Using our proprietary HyperblockTM technology, Anaplan lets you contextualize real-time performance, and forecast future outcomes for faster, confident decisions. Because connecting strategy and plans to collaborative execution across your organization is required to move business FORWARD today. Based in San Francisco, we have 20 offices globally, 175 partners and more than 1,750 customers worldwide.

To learn more, visit **anaplan.com**