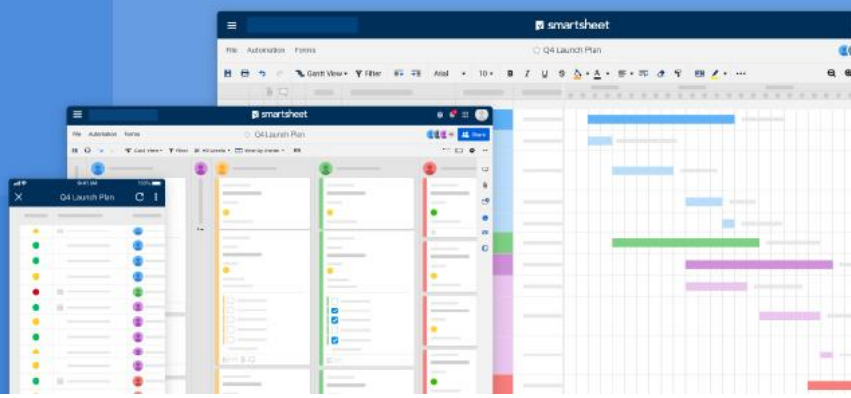
smartsheet



How IT Can Enable Collaboration With Enterprise-Grade Security Using Smartsheet

Smartsheet provides a secure work collaboration environment that meets the growing data governance and security needs of enterprise customers.

Executive Summary

As the adoption of cloud-based systems increases across organizations, the security of information and data contained in such systems becomes increasingly important for enterprise IT and leadership. Reliable security, compliance, and governance features have become the key capabilities needed for the wide-scale adoption of any modern software as a service (SaaS) system.

We at Smartsheet understand that an enterprise-grade SaaS platform must have built-in data security capabilities as well as the flexibility to seamlessly integrate with your organization's existing data security systems. Keeping this in mind we designed the Smartsheet platform's security controls and infrastructure to keep your data secure.

This guide is intended to share some of the existing best practices that Smartsheet administrators, customer IT departments, and enterprise users can adopt to maintain a secure, compliant, and well-governed Smartsheet work environment. The paper does not talk about yet-to-be-launched security capabilities under development. Please reach out to your sales account manager or get in touch with us at salesteam@smartsheet.com for more information on security capabilities under development.

Overview

This guide illustrates our proven best practices in managing a Smartsheet environment for the enterprise. For the purposes of this document, we have divided our security and account control best practices into three main areas of focus: identity and access management, data governance, and global account configuration.

- **Identity and access management** is controlling how your users gain access to Smartsheet and ensuring that each user's role and identity within the platform is in alignment with your organizational structure and policies. In addition, we'll cover how to properly address external collaborators, based on your security posture.

- **Data governance** is important at both a user level and organizational level. At the user level, we'll focus on the importance of giving users only the information that they need, when they need it, utilizing dynamic views and app-packaging solutions in Smartsheet. At the organizational level, we'll illustrate the best practices around permission settings and feature controls, such as enabling a safe sharing list as well as taking advantage of user and data reports available to System Admins.

- **Global account configuration** refers specifically to the ability to customize the aesthetics of your Smartsheet environment to match your organization's brand. Something as simple as a visual cue confirming to your users that they are within the organizations' account is important to a healthy and secure work environment, as is locking that branding and customization in place so each and every asset created will be in line with your brand.

Identity management

Managing a user's identity in Smartsheet and their access to the system is just as important as managing how they're utilizing the platform.

Early in your Smartsheet deployment, you'll decide what authentication method you want to use. Smartsheet offers different options: email and password, and Single-Sign On (SSO) methods from Google, Microsoft, SAML 2.0 providers, and Apple.

You can select one or more methods for your organization. The best practice is to **select one SSO authentication method** for all users and disable all other methods, but this may vary based on your organization's needs.

We recommend setting up **Multi-factor authentication (MFA)** to add another layer of security with your selected SSO method.

Smartsheet has a robust set of REST APIs. The Smartsheet API uses OAuth 2.0 for authentication and authorization. An HTTP header containing an access token is required to authenticate each request. For additional security and as a recommended best practice, you should use OAuth 2.0 for any integrations you build.

Access management

Making sure only your organization's users are allowed access is absolutely paramount to maintaining a secure software environment.

Further, making user administration and management as simple as possible while maintaining granular controls such as user roles and permissions is a delicate balancing act that Smartsheet has put at the forefront of our administration console.

User administration

Ensuring consistent enforcement of your organization's security and compliance policies and streamlining user administration can be challenging when you have multiple Smartsheet plans.

In some scenarios, multiple teams in your company may independently adopt Smartsheet for their own needs. Mergers and acquisitions can also result in multiple Smartsheet plans — and a need to consolidate those plans.

To simplify the discovery of those plans, we recommend enabling **Account Discovery**. This allows any person from your organization's domain to see the list of Smartsheet plans in your organization, and request membership to join those plans.

If your organization centrally manages users and billing, consolidating these plans into a centralized Smartsheet plan can significantly reduce this overhead. With the **org merge** capability, you can easily consolidate two of your Smartsheet plans at a time. Customers with premium Smartsheet capabilities such as Dynamic View, Connectors, and Control Center can work with Smartsheet support for assisted consolidation.

User management

Smartsheet provides user management capabilities tailored to the needs of your organization. Adding users one at a time may not scale when adoption grows to dozens or even hundreds of users. We recommend leveraging the **bulk user import** feature in Admin Center to easily add up to 1,000 users at a time to your Smartsheet org. You can also use bulk update to edit roles en masse for existing users.

Mergers or acquisitions often result in rebranding, with users getting new email addresses as a result. In such situations, once you complete the consolidation, use **User Merge** to bulk update the primary email addresses of users and to clean up any duplicate accounts.

A consolidated Smartsheet plan takes advantage of two critical user management capabilities to streamline and automate user management:

- **User Auto Provisioning (UAP)** automatically imports any person whose email domain matches the one that you have verified with Smartsheet. You no longer have to manually add those users. We recommend enabling UAP so that any person who joins the account is automatically under the purview of your account's security and governance policies.

- **Directory Integration** allows you to directly sync your Microsoft Azure Active Directory (AD) users into Smartsheet. Plug Smartsheet into your existing automation in Azure AD to fully automate user onboarding AND offboarding, minimizing the risk of users overstaying in your Smartsheet account. As an added benefit, user-level AD attributes such as department/cost center/division are included in a Smartsheet **Chargeback Report**, which is available in Admin Center and can be used for internal chargeback. A recommended best practice is to sync all users in the Directory into your organization's Smartsheet account. This prevents the creation of user accounts

outside your Smartsheet account when a new person in your organization logs into Smartsheet for the first time. Optionally, you can, leave UAP enabled as a catch-all for users who are not synced from the Directory, and ensure that you periodically reconcile your existing Smartsheet user list with assignments in the Directory.

When a person leaves your organization, it is important to remove them from all sharing and transfer ownership of their Smartsheet items to a new owner in your organization. Directory Integration allows you to configure an escrow user account to which all items owned by an offboarded user are automatically transferred, eliminating the risk of permanently losing access to those items.

Roles and user types in Smartsheet

Regardless of your user provisioning method, you will need to determine Smartsheet roles for the people in your organization.

Note that a role assignment doesn't give the person access to Smartsheet assets in your organization. The assets must also be shared with those people. The person's role and their access permissions to the asset determine their level of access. Smartsheet supports the following primary roles:

- **Licensed User**: Use licensed features, such as creating sheets.
- **Group Admin** Create and manage Smartsheet groups.*
- **Resource Viewer**: See how people are allocated across projects.*
- **System Admin**: Manage users, account settings, and security controls.

*Group Admin and Resource Viewer roles must also be Licensed Users

We strongly recommend that at least two active system administrators be assigned for your organization's Smartsheet account so that there is no disruption if one System Admin is unavailable.

Group Admins can create Smartsheet groups, allowing users to share content to the group rather than to each member. Group Admins can *only* manage groups they *own*. If your policies require, you can restrict group membership to people in the organization to limit external collaboration.

If you don't assign any of the above roles to a user, their access will be limited to only those Smartsheet assets (sheets, reports, or dashboards) shared to them. They must be Licenced Users to create Smartsheet assets — a role they can request via the app. System Admins can track and respond to requests individually or in bulk in the **Admin Center's License Request Management** section. If you already have an established process for managing license requests you should consider taking advantage of a **Custom Upgrade Screen** to redirect all license requests to these processes.

External collaborators

Any person who is not part of your organization's Smartsheet account but collaborates on assets owned by people in your organization is considered an external collaborator. Smartsheet empowers your organization to collaborate freely with any trusted entities or persons. We recommend leveraging three critical admin levers to manage collaboration with external collaborators:

- **Safe Sharing** lets you specify domains or email addresses that are trusted for external collaboration.
- **Sheet Access Reports** are for auditing the list of external collaborators who have access to Smartsheet items in your organization.
- **Revoke Access to Items**, available in Admin Center, lets you revoke access to Smartsheet items to external collaborators once they no longer need access.

Data governance

Effective data governance is indispensable for today's enterprise to ensure the information assets of the organization are created, used, shared, and protected in line with the applicable regulations and industry best practices.

Such information control is needed not only for regulatory purposes but also for efficiency and business confidentiality:

- **At the user level,** the organization needs to provide effective tools so only the minimum required information is shared with stakeholders and other collaborators.
- **At the organization level,** the enterprise needs mechanisms for effective policy creation, as well as ensuring the information systems have the capabilities to enforce such policies.

Dynamic View and WorkApps: Data governance at the user level

Most users are familiar with permission levels in Smartsheet (viewer, editor, admin, and owner). Dynamic View and WorkApps provide additional controls and flexibility to Smartsheet users, leading to effective data governance capabilities at the user level. Limiting access to only collaborator-relevant information makes the processes more efficient and secure.

Dynamic View

Not all business processes warrant full transparency. Many processes — order management, vendor collaboration, projects involving mixed internal and external teams — require tight control over what is shared with whom.

Dynamic View allows collaboration without compromising on confidentiality. Using Dynamic View, sheet owners can selectively share the relevant rows and fields with specific collaborators — without sharing the underlying sheets. This enables several use cases wherein specific business users can selectively share elements with vendors, mixed internal and external teams, or across organizations, inviting collaboration only on certain fields. Everyone has access to the information they need — and only the information they need.

WorkApps

WorkApps is a no-code platform for building intuitive web and mobile apps to streamline your business and simplify collaboration. You can tailor each app's experience for your team members based on each person's role, and work together from the same underlying datasets. Apps scale using the same enterprise-grade, multi-level security as the Smartsheet platform.

WorkApps eliminate the need to share the underlying assets that constitute the WorkApp. You can create a WorkApp with a filtered view of selected sheets and reports, but none of

those sheets or reports need to be shared with the end-user. They only see the "WorkApp" view of those assets.

Data governance policy controls at the organization level

Smartsheet empowers administrators to ensure functionalities of the platform are used within the organization's governance policies. These controls allow admins to implement good data governance guard rails to ensure data is handled correctly and by *only* those who need to interact with said data.

Administrators can pick and choose how they want users to interact with specific features such as **adding images to sheets**, web content control, automation permissions, publishing, and attachment options. Should sheet owners be able to publish their sheets and create new automations? Do you have a specific storage system that files must be attached from? These are examples of questions administrators should ask themselves to effectively set these controls.

In addition, policy controls extend to **safe sharing lists** as well. If you want to limit data and asset sharing to specific domains or email addresses, this is the tool to use. Safe sharing lists also determine whether your organization can share Smartsheet items with other organizations, such as vendors and partners.

Web content widget control

This widget allows you to embed interactive content (videos, charts, docs, and more) in your dashboards. You can enable or disable the feature and define the approved list of supported domains for the web content widget. As a best practice, limit this to internal company domains. For example, an internal Tableau server accessed through a vanity URL (smartsheet.tableau.com).

Automation permissions

Control who can receive automation from sheets based on their sheet access and relationship with your organization. Options are organized from Restricted (only users shared to the sheet) to Unrestricted (any email address and third-party integration, such as Slack). We recommend that you review this control to ensure that its configuration matches your organization's desired level of internal and external collaboration.

Attachment controls

Control whether plan members can upload files from their own computers, by attaching a link (URL) to a site, or from third-party cloud storage services including Google Drive, OneDrive, Box, Dropbox, Evernote, or Egnyte. To prevent the ingestion of data from unapproved sources, enable only those attachment providers that are approved for use based on your organization's policies.

Publish controls

You can disallow the publishing of sheets, reports, dashboards, and iCal — the Publish button no longer appears on the Smartsheet asset. You also can restrict access to published items to only people within your Smartsheet organization. We have observed that security-conscious customers allow publishing, but limit access to published items to people within their account.

*Publishing a sheet, report, or dashboard generates a unique URL that anyone can access without logging in to Smartsheet and iframe code that you can embed within the source code of a website to display the sheet or report.

Safe sharing list

Use this capability to restrict sharing by domain or by specific email addresses (e.g. to ensure that sheets are shared only to people with a company email address). To ensure that your organization is only collaborating with trusted parties, we recommend using this control to list external domains or email addresses approved for collaboration. Additionally, set up an intake form to gather input from users on any updates to this list.

Chat integration controls

Smartsheet supports Google Hangouts and Skype for Business as supported chat services. Enable one of these providers that are approved for use based on your organization's policies so that all Smartsheet users in your organization can communicate with collaborators in real-time as they manage work together.

Logging and reporting

You can download reports covering different aspects of Smartsheet usage across your organization as described below. Such capabilities can be leveraged for e-discovery:

- **Sheet Access Report**: Generates an Excel file listing the names of all sheets, reports, and dashboards owned by licensed users on the account, the name of workspace these items are saved in (if applicable), the collaborators shared to each sheet, and the timestamp of last modification. We recommend reviewing this report periodically to audit the list of external collaborators who have access to assets owned by people in your organization.

- **Published Items Report:** Generates an Excel file listing all items that have been published. Great for data security or tracking down the source of the published version of an item. Use this report to inform the configuration of the Publish control. For example, if you notice that
-
- **User List Report:** Generates an Excel file listing all members (Invited and Active) on the account, a timestamp for when they were added to the account, their access levels (System Admin, Group Admin, Resource Viewer, and so on), the number of their owned sheets, and the timestamp of their last login to Smartsheet.

- **Login History Report:** System Admins on multi-user accounts can use Admin Center to receive an Excel file with Login History via Email to view which users listed in your account have logged in recently.

- Chargeback Report: Available in Admin Center, you can use Chargeback Reports for internal chargeback. A recommended best practice is to sync all users in the Directory into your organization's Smartsheet account. This prevents the creation of user accounts outside your Smartsheet account when a new person in your org logs in to Smartsheet for the first time. Optionally, you can, leave UAP enabled as a catch-all for users who are not synced from the Directory, and ensure that you periodically reconcile your existing Smartsheet user list with assignments in the Directory.

For further granular tracking of user actions at the sheet, dashboard, and cell level, you can use Activity Log, system columns, and cell history.

- **Activity Log:** See an audit trail of edits made to an item, who made them, and when they were made. This includes changes such as row deletion (with the data that was deleted), who has viewed the item and sharing permission changes.

- **Cell History:** See a log of changes made on the cell level, who made the changes, and when they were made. You can also use copy-paste from cell history to restore the previous information back in a cell.

- **System Columns:** Show the time that each row was last edited and the collaborator who made the change, for each row in the sheet.

Event Reporting - Org-wide monitoring of user behavior

To ensure information security many Enterprises require insight into how their business applications, like Smartsheet, are being used. It is prudent for the enterprises to maintain visibility into:

- Who is creating sheets
- Who is creating workspaces
- Who is deleting objects
- Who shared a sheet with whom

Event Reporting is a premium feature that provides granular visibility into user behavior and activity within your organization's Smartsheet account. This feature enables you to monitor data loss and identify anomalous patterns in usage, so they can more tightly enforce organizational security and compliance policies.

Event Reporting is a data feed of Smartsheet usage events ("Events") within a plan (org) accessed via the Event Reporting API. The service reports on more than 120 events in Smartsheet and stores up to six months of data, beginning with the date when the feed is enabled.

Event Reporting data needs to be integrated with other security systems that provide monitoring, notification, policy creation and enforcement, and data loss prevention (DLP). Such apps are available from third parties (at additional cost) and could be of different types such as Cloud Access Security Broker (CASB) systems, Security Information and Event Management (SIEMs), or a combination of CASB and SIEM working together depending on the enterprise security stack deployed by your corporate IT/InfoSec department. Sometimes enterprises develop their own monitoring and response systems, instead of relying on those provided by third parties.

Reach out to your IT/InfoSec team to see if they have a system through which your organization's cloud security policies are created and administered. Once integrated with your CASB/SIEM system, Event Reporting provides visibility (via a data feed) and the other system provides monitoring, forensics, and policy creation.

Event Reporting key use cases

Data loss prevention: Your corporate assets need protection against loss, accidental or intentional. You also want alignment with organizational compliance and governance policies. For example, you don't want an internal marketing campaign or project schedule made available outside your org via email as an attachment or via send row. As another example, a disgruntled employee may indulge in disruptive actions such as deletion or export of a large number of sheets. Event reporting provides visibility into such user actions and so can take corrective action.

Personally identifiable information (PII) data handling: With the data feed from Event Reporting, CASB/DLP apps recognize patterns of data (e.g. credit card or social security numbers) when entered into a sheet and encrypt them or restrict sharing. Event Reporting provides the data of an event (Sheet Update, Share Sheet), and these apps provide data handling capabilities.

Data governance: Leveraging Event Reporting data and a third-party app, IT and Compliance can set boundaries for the usage of data in Smartsheet, identifying users who have high-risk behaviors and reaching out to them about data governance policy. Using the built-in forensics in DLP or CASB apps, IT and Compliance teams can enforce policy and provide the appropriate safeguards.

Gain insights on collaboration: Event Reporting enables a customer to identify the impact of Smartsheet on their organizations: power users, groups that collaborate and share, and processes that are improved and accelerated. It is also possible to identify total usage (licensed users, collaborators, anonymous visitors) for sheets, dashboards, forms, and other Smartsheet items.

Global account configuration

Account security isn't limited to technical features such as data encryption or authentication options. Security can be something as simple as including your organization's logo on each and every item that belongs to it.

Global account configuration controls allow you to implement visual branding (and other restrictions) so your users know they're accessing the right information.

System Admins can add your logo to bring your Smartsheet deployment in line with your organization's branding requirements. Use the **branding lock** to ensure each new asset is branded the same.

Smartsheet customization controls and account configurations also allow you to set up custom welcome screens. You can create **custom help screens** with descriptions on how to get started, **license request screens** to help your users contact you, or **customized and branded welcome screens** that appear when a user logs in. Screens can include a requirement that a user approves the terms of service before they access more information.

Combining consistent visual identity along with custom information helps users know they're accessing the right tools and information and enhances your security.

Conclusion

In summation, Smartsheet offers not just a best-in-class work collaboration experience, but also the capabilities and tools to keep your information secure. This cloud-based system integrates with your existing tools and processes and scales as you grow. Additionally, we have a number of security-enhancing features currently under development that we will be launching in the near future.

If you'd like to learn more about Smartsheet security and how it can help your work environment become more efficient while maintaining industry standards for security, contact your sales account manager or get in touch with us at salesteam@smartsheet.com.

For additional information and resources pertaining to security, privacy policies, availability, and more visit the additional web pages listed below.

Additional Resources

- Smartsheet Information Security and Data Governance
- Smartsheet Trust Center
- Smartsheet Admin Center Online Help
- Smartsheet features by plan
- 5 steps for getting started with the Smartsheet API
- API Security Best Practices