Smartsheet Security

An in-depth view of Smartsheet security capabilities, practices, and protections

Executive Summary

At Smartsheet, we understand that enterprise-grade software as a service (SaaS) platforms must offer multiple layers of defense and a myriad of IT protections and controls to keep sensitive company data secure. It's also important for these solutions to be flexible and integrate with existing data security systems and processes.

This whitepaper is intended to showcase Smartsheet security and governance capabilities, protections, and practices. Primarily, we'll focus on the customer controlled capabilities that Smartsheet recommends implementing in order to maintain a secure, compliant, and well-governed work environment. Note: This whitepaper covers generally available capabilities only. Some features may require additional purchase or may not be included in all plan levels.

Overview

To best secure your organization, we recommend implementing controls around three main areas of focus: identity and access management, data governance, and global account configuration. In addition to these topics, this document includes high-level information regarding Smartsheet security, privacy, and compliance practices.

- **Identity and Access Management** focuses on controlling how your users gain access to Smartsheet, ensuring that each user's role and identity within the platform aligns with your organizational structure and policies. Additionally, we'll discuss how to ensure security when collaborating with external users, based on your security preferences.

- **Data Governance** must be enforced at both a user level and across the organization. For users, a least privilege approach is the default in Smartsheet, with additional controls available to further constrain and control visibility so users are only exposed to what they need, when they need it. At the organizational level, we'll cover both simple mechanisms like safe sharing and user reports, as well as optional advanced capabilities available like data egress policies.

- **Global Account Configuration** enables you to customize the aesthetics of your Smartsheet environment to match your organization's brand. Even something as simple as a visual cue confirming that users are within the organization's protected environment can help ensure your security. Enforce consistency by locking that branding and customization in place so each and every asset created will be in line with your brand.

- **Security, Privacy, and Compliance Practices** refer to the actions and protections Smartsheet maintains outside our platform, to help ensure customer data remains highly secure. Smartsheet has implemented industry leading, defense in-depth strategies through a combination of people, processes, and technologies to protect the confidentiality, integrity, and availability of Smartsheet environments and assets.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Table of Contents

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Identity Management

Managing a user's identity in Smartsheet — and, as such, their access to the system — is just as important as managing the data within the platform. Smartsheet provides a layered set of identity management capabilities designed to meet the needs of enterprises of all sizes, from authentication enforcement and automated lifecycle management to API security and continuous monitoring.

Authentication Methods

Early in your Smartsheet experience, you'll decide which authentication method you want to use. Smartsheet offers several options: email and password, and Single Sign-On (SSO) via Google, Microsoft, Apple, and SAML 2.0 providers.

Smartsheet's SAML 2.0 support is compatible with major enterprise identity providers (IdPs), including Okta, Microsoft Entra ID, PingIdentity, and others. This broad compatibility allows organizations to leverage their existing IdP investment and enforce consistent authentication policies across all SaaS applications.

We recommend enforcing a single SSO authentication method for all users, with all other login methods disabled. This eliminates weaker credential-based attack surfaces and centralizes authentication governance within your identity provider.

For organizations with multiple domains or federated IT structures, Smartsheet supports domain-level SSO enforcement. System administrators can specify that users from a given email domain — such as "@regionaloffice.com" or "@subsidiary.org" — must authenticate using a designated identity provider. This enables tailored identity policies across business units while strengthening governance and risk mitigation.

Multi-Factor Authentication (MFA)

We recommend implementing Multi-Factor Authentication (MFA) as an additional layer of security alongside SSO. MFA enforcement is best managed at the identity provider level, giving your security team centralized control over MFA policies across all connected applications.

For non-SSO users, Smartsheet supports authenticator-app-based MFA as an additional login security layer. The authenticator app pairs with either email and password or email-based one-time passcode (TOTP) as the primary sign-in method. System administrators on Enterprise plans can require authenticator-app MFA at the plan or domain level, with individual user exemptions available for edge cases.

Note: Authenticator-app-based MFA applies to the core Smartsheet login experience. Premium apps and add-on capabilities use the existing Smartsheet authentication methods configured for your organization.

Session Management

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Enterprise plan administrators can configure session inactivity timeouts, automatically signing users out after a defined period of inactivity — ranging from 15 minutes up to 30 hours — across web and desktop sessions. Establishing an appropriate timeout policy reduces the risk of unauthorized access from unattended sessions and should be part of your baseline security configuration.

User Lifecycle Management

Timely provisioning and deprovisioning of user accounts is one of the most critical controls in any SaaS security program. Smartsheet supports **System for Cross-domain Identity Management (SCIM)** integration via Directory Integrations with Microsoft Entra ID and Okta, enabling automated provisioning and deprovisioning of user accounts directly from your identity provider.

With SCIM enabled, when an employee is onboarded or offboarded in your IdP, their Smartsheet account is automatically created or deactivated — eliminating the risk of orphaned accounts retaining access after an employee departure. This also reduces administrative overhead and ensures access is always consistent with your authoritative directory.

Smartsheet also supports **Just-in-Time (JIT) provisioning** via SAML, which automatically creates a user account upon a user's first successful SSO login, without requiring pre-provisioning by an administrator. This is particularly useful for large organizations or those with high onboarding volumes.

Recommended practices:

- Enable SCIM via Directory Integration with your IdP as the primary mechanism for user lifecycle management.
- Use JIT provisioning as a complement for high-volume onboarding environments.
- Establish a regular access review cadence to identify and remediate stale or orphaned accounts.

API Security & Token Management

Smartsheet provides a robust set of REST APIs. The Smartsheet API uses **OAuth 2.0** for authentication and authorization, requiring an HTTP header containing a valid access token with each request. As a best practice, use OAuth 2.0 for all integrations you build to ensure secure, scoped API access.

In addition to OAuth 2.0, Smartsheet supports **personal API access tokens** for individual users. These tokens carry significant privilege and require careful management. System administrators can configure a plan-level token expiration period, ensuring personal API tokens do not remain valid indefinitely — reducing the exposure window from compromised, forgotten, or orphaned tokens tied to former employees or decommissioned integrations. The expiration period should be aligned with your broader credential lifecycle policies, balancing security requirements against the operational impact of periodic token rotation.

Beyond expiration, organizations should also:

- **Audit personal API tokens regularly** to identify unused, overly broad, or no longer needed tokens.
- **Rotate tokens periodically** and immediately upon any suspected compromise.
- **Apply the principle of least privilege** when configuring OAuth scopes for third-party integrations — request only the permissions the integration requires.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

- **Review third-party OAuth-connected applications** periodically to ensure only approved integrations retain access to your organization's data.

Access Management

Managing users and their access is a core administrative function that can impact both security and your organization's adoption of Smartsheet. Organizations must strike a delicate balance, encouraging collaboration while managing risks as data and teams become increasingly distributed. To support this, Smartsheet offers three distinct governance models in line with the primary ways our customers have looked to manage the application.

Smartsheet Governance Models

The first approach is our decentralized (federated) model, where individual business units control their own purchasing and plans directly. In this model, IT is typically not involved in administration, and plan billing, governance, and user management are left to departmental discretion. This model generally applies for companies earlier on in their Smartsheet journey.

Our second approach is the centralized (consolidated) model, where Smartsheet plans have all been consolidated into a single, IT-governed subscription. This provides direct control over spend, user management, and security controls. This model is best suited for IT teams that want to maintain close oversight over every aspect of their Smartsheet experience.

Finally, our shared (hybrid) model is meant to provide a middle-ground approach, where IT controls organization-wide settings using Enterprise Plan Manager, while license and user management are governed directly by line of business system admins. Billing is also separated by plan, supporting departmental billing, or a model where Smartsheet spend is incorporated into departmental budgets versus centrally billed to IT.

To ensure high standards for security, Smartsheet recommends our shared or centralized models, which provide more direct IT control over your plan(s).

User Administration

As various teams in your company independently adopt Smartsheet for their own needs, multiple, separate plans may be created. Mergers and acquisitions can contribute to an environment with multiple Smartsheet plans.

To manage users in these plans using the decentralized model, we recommend enabling Account Discovery for each of those plans. As new users are exposed to Smartsheet, that allows them or any person from your organization's domain to see a list of the Smartsheet plans associated with your company, providing a centralized means to request to join one of those existing plans, rather than starting a new one. Those requests are automatically routed to your system administrators (via the Smartsheet Admin Center) for review and approval.

If you have multiple separated plans and wish to manage users with the centralized model, you may have to complete an account consolidation. Note: customers with Advance capabilities such as Dynamic View, Connectors, and Control Center will need to partner with Smartsheet support for additional assistance with some aspects of consolidation.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

If you're using the shared model and Enterprise Plan Manager, a best practice is to organize plans around departments/teams/cost centers, enabling you to define a policy to automatically assign users to the relevant plans based on their affiliation to one of these entities.

Licensing/Subscription models

Most Smartsheet customers have transitioned to our current pricing model, which provides transparent, predictable pricing, faster value realization, and increased ease of management. However, some customers remain on our legacy collaboration model and you may find yourself working to understand the differences between these two models.

Legacy Collaborator Model

Our legacy collaborator model was built on the foundation of giving creators access to the product while enabling free collaboration as an Editor or Commenter. That resulted in significant growth through viral adoption, but also resulted in fewer users being able to take full advantage of the platform. Only users who needed to create sheets, reports, dashboards, or workspaces were required to pay. Under this model, System Admins faced challenges in understanding Smartsheet user types, effectively managing their users, assigning licenses appropriately, and demonstrating the platform's value to their leadership teams.

User Model

While creation is important, Smartsheet is a collaborative work management platform; collaboration is at our core. The power and value of the Smartsheet platform truly stand out in enabling teams to create processes, programs, and projects, and collaborate on critical business initiatives. The user model overcomes the challenges of our legacy model. It adapts to your evolving business needs, helping you achieve your goals as your organization grows, through the introduction of:

- New User Types.
- Provisional Use.
- Reconciliation Periods and True Ups.

Read the brief for more on our User Model.

User Management

Smartsheet understands that adding users one at a time may not scale as adoption grows to dozens, hundreds, or even thousands of users. As such, when getting started, we recommend leveraging the bulk user import feature in our Admin Center, which easily adds up to 1,000 users at a time to your Smartsheet organization. Similarly, you can also use bulk update to edit roles and user types en masse.

Mergers or acquisitions often result in rebranding, with users getting new email addresses. User Merge can help you bulk update the primary email addresses of users and clean up any duplicate accounts.

A consolidated Smartsheet plan can use three additional capabilities to further streamline and automate user management:

- User Auto Provisioning (UAP) automates the process of adding users to an enterprise account. As users sign up or sign in to Smartsheet with their company email address, they will automatically be added to your account. Additionally, you can choose whether users should be granted licenses versus automatically joining the account as Provisional Members.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

- If you've adopted our consolidated model, we recommend enabling UAP so employees automatically join the central, IT-controlled account.
- If using our shared model (and if your organization has documented department/cost-center information for your user list), we recommend turning on UAP, as that information can be imported to automatically associate users with the right plan when they request a license. It can also be used to automate the movement of unlicensed users between plans.
- Directory Integrations allow you to directly sync your Microsoft Entra ID or Okta Directory users into Smartsheet. Plug Smartsheet into your existing automation in Entra ID or Okta to fully automate user onboarding and offboarding, minimizing the risk of users lingering in or revisiting their Smartsheet accounts. As an added benefit, user-level attributes such as department/cost center/division are included in a Smartsheet Chargeback Report, which is available in Admin Center and can be used to facilitate internal chargeback. A recommended best practice is to sync all users in the Directory into your organization's Smartsheet account. This prevents those users from creating additional "shadow IT" Smartsheet accounts when logging in for the first time. As a second layer of defense, you can also leave UAP enabled as a catch-all for users who may not already be synced through the Directory.

When a person leaves your organization, it is important to remove their access to Smartsheet. Removing a user from your plan revokes their access to Smartsheet and removes them from shared assets owned by your plan. Note that assets owned by the departing user will remain in the system but may be left without an owner — system administrators should review and transfer ownership of those assets before or after removal to avoid broken automations or inaccessible content.

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 directly shared with those people. As such, both role and asset access permissions will determine what stakeholders can see and do in Smartsheet. Smartsheet supports the following primary roles:

- Credentialed User: Access and use the Smartsheet service subject to seat type and permissions.
    - Members: Users with full access – can create and manage assets, edit, or upload files.
    - Provisional Members: Users with full access for a limited time.
    - Viewers: Users with a free seat that can view information.
    - Guests: External users who may edit, comment on, or view information.
- Group Admin: Create and manage Smartsheet groups. (must also be a licensed user)*
- System Admin: Manage users, account settings, and security controls.

We strongly recommend assigning at least two active system administrators for your organization's Smartsheet account to ensure continuity of access and administrative control — including the ability to manage or recover an admin account in the event of compromise or other security incidents.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Group Admins can create Smartsheet groups, allowing users to share content with the group rather than requiring users to share with each member individually. Group Admins can only manage groups they own. As needed, to limit external collaboration, restrict group membership to only stakeholders within your organization.

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, dashboards, or workapps) shared to them. In order to create Smartsheet assets, stakeholders must be licensed users, and can request a license through the Smartsheet app directly. System Admins can track and respond to requests individually or in bulk through 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 direct users to submit their license requests via those internal processes.

Guests

Any user outside of your domain who is shared to your Smartsheet assets is considered a Guest. Smartsheet empowers your organization to collaborate freely with any trusted external parties, with no associated cost for these Guests. To ensure security when partnering externally, we recommend leveraging three central admin controls:

Safe Sharing lets you specify domains or email addresses that are trusted and authorized for external collaboration.

Sheet Access Reports provide a list of Guests who have access to your organization's Smartsheet content.

Revoke Access to Items, centrally through the Admin Center, so Guests are removed from content they no longer need to access.

Guest Authentication Controls

To further protect sensitive content when collaborating with users outside your organization, Smartsheet offers enhanced authentication verification for Guests, ensuring only authorized users are granted access to your content.

External Collaborator Single Sign-On (EC-SSO) allows system admins to **enforce the use of corporate identity providers**—ensuring that only users verified by SSO have the ability to access content shared. Additionally, External Collaborator Multi-Factor Authentication (EC-MFA) gives administrators the ability to **require MFA enforcement for external users as a condition of access**. When enabled, Smartsheet checks with the external user's identity provider at the time of login to confirm that MFA was used—blocking access if that requirement is not met.

These capabilities provide enterprise IT and security teams with the flexibility and confidence to scale collaboration securely, particularly in highly regulated or risk-sensitive environments.

Data Governance

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

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

These controls are needed not only for regulatory purposes but also to ensure efficiency, business confidentiality, and business continuity:

- At the user level, the organization needs to provide effective tools to constrain visibility; only showing relevant stakeholders relevant information.
- At the organization level, the enterprise needs to be armed with applicable tools for effective policy creation and enforcement.

Data Governance at the User Level

Most users are familiar with permission levels in Smartsheet (viewer, commenter, editor, admin, and owner). Dynamic View and WorkApps provide additional, more-granular controls and flexibility, helping provide effective data governance capabilities at the user level. Limiting access to only the most relevant content both helps ensure process efficiency (as users must necessarily focus on items needing attention), but also ensures security by extending the Smartsheet approach of least privilege by default to a more granular scale.

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 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 allow you to streamline your work and simplify collaboration using easy-to-navigate apps built directly from your sheets, forms, dashboards, reports, and more. 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 the capabilities of the platform are used within the organization's governance policies. These controls allow admins to implement good data governance guardrails 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. 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? Should external collaborators be able to download content

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

shared with them? These are examples of questions administrators should ask themselves to effectively evaluate the appropriate organization-wide controls to implement.

These policy controls also extend to safe sharing. If you want to limit data and asset sharing to specific domains or email addresses, this is the tool to use. As previously mentioned, safe sharing also determines whether your organization can share Smartsheet items with other organizations, such as vendors and partners.

Third-Party Integration security

Smartsheet provides a layered OAuth 2.0 security model where access tokens are bounded by the authorizing user's underlying sharing permissions, ensuring integrations can never exceed the data access of the person who authorized them. Enterprise admins can enforce plan-wide token expiration policies through Admin Center, automatically revoking all OAuth tokens after a configurable duration. Admins can also automate user offboarding via Okta or Entra ID directory sync (via SCIM), which neutralizes associated tokens when employees leave. For ongoing visibility, Smartsheet's Event Reporting captures over 100 types of administrative and user activity events in a six-month audit log, and integrates directly with Skyhigh Security CASB and Microsoft Defender for Cloud Apps for anomaly detection and trigger-based alerts.

Microsoft InTune Mobile Application Management (MAM) controls

As organizations increasingly rely on mobile access to maintain workforce productivity, starting April 2026, Smartsheet offers Mobile Application Management (MAM) controls via Microsoft Intune, enabling IT administrators to enforce enterprise-grade security policies without requiring full device enrollment.

Organizations on the Pro, Business, Enterprise, and Advance Work Management plans can configure granular policies including PIN and biometric authentication requirements, data encryption, copy/paste and screenshot restrictions, third-party keyboard blocking, print prevention, minimum OS version enforcement, jailbreak and root detection, and automated data wipe after a defined offline period. This application-level approach allows organizations to secure corporate data on the Smartsheet Mobile App while preserving employee privacy on personal devices — balancing security compliance with user experience.

Web Content Widget Control

Dashboards support the ability to embed interactive content (videos, charts, docs, and more). Admins have the ability to enable or disable this feature and define an approved list of supported domains for the web content widget. As a best practice, we recommend limiting this to internal company domains.

Automation Permissions

Control who can receive automation from sheets. Options are organized from Restricted (only enables actions for users shared to the sheet) to Unrestricted (where automation is applicable to 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

Determine 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 internal policies.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Publish Controls

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.

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 generally allow publishing, but limit access to published items to people within their account.

Safe Sharing

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). Safe sharing enforcement extends beyond direct sharing actions — embedded content in dashboards will also only display to viewers who are authorized under your organization's safe sharing settings. **Smartsheet strongly recommends implementing safe sharing to control external collaboration**. Additionally, to simplify updates and maintenance of your safe sharing list, we recommend that you manage your safe sharing list via requests collected through a Smartsheet webform.

Offline Form Submission Controls

When using the mobile app, Smartsheet automatically enables forms to be submitted while offline, to support use cases where users may not have a consistent connection (e.g. on a construction work site). This control provides admins the ability to turn offline form submissions off (or back on) to control whether a user is able to launch the mobile app without a connection, to submit forms.

Communication Integration Controls

Smartsheet supports Google Chat, Microsoft Teams, Slack, and Cisco Webex as supported communication services. Account administrators can enable one or multiple services, at your discretion.

Logging and Reporting

You can download reports covering different aspects of Smartsheet usage across your organization for ongoing visibility into Smartsheet usage, users, content, billing and access:

Sheet Access Report

Generates a CSV listing the names of all sheets, reports, and dashboards owned by the plan on the account, the name of the workspace these items are saved in (if applicable), the collaborators shared on 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 who published specific items.Use this report to inform the configuration of the Publish control as needed.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

User List Report

Generates a CSV listing all members (both invited and active) on the plan, a timestamp for when they were added to the plan, their access levels (System Admin, Group Admin, etc), the number of sheets they own, and the timestamp of their last login to Smartsheet.

Login History Report

System Admins on multi-user accounts can use Admin Center to receive a report with a list of recent login history via email.

Chargeback Report

Available in Admin Center, customers using directory integration can use Chargeback Reports to facilitate internal chargeback. This adds columns for division, department, and cost center to the existing report created when customers download their user list, providing the data needed to perform internal chargeback reporting.

Other logging/Monitoring Mechanisms

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

- **Cell History:** Displays a log of changes made on the cell level, detailing who made the changes, what they were, and when they were made. Users can easily use copy-paste from cell history to restore previous information that may have been improperly deleted or changed.

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

- **Security Score:** Helps SysAdmins assess and strengthen their Smartsheet security posture by providing a data-driven score based on implemented security capabilities. Rooted in industry best practices, the score includes a categorized policy breakdown and an intuitive metric to track security strength and improvements over time. Accessible within the admin center.

- **Event Reporting:** An advanced capability that provides visibility into over 100 types of security and user activity events for a comprehensive audit trail. (See more about Event Reporting below)

Advanced Data Governance Controls

Smartsheet offers a number of advanced capabilities that provide data governance control for clients with particularly stringent data security needs. These capabilities are included in Smartsheet Advance Platinum and Smartsheet Safeguard.

Data Egress Policies

Sharing data always involves some level of risk, but when dealing with particularly confidential content, ensuring that company data remains only in your account and in your control is paramount.

System administrators can use data egress policies to protect confidential information through granular control over how data can be exported both within and outside your organization.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Data egress policies can be implemented to prevent internal and external collaborators from taking the following actions on sheets, reports, and dashboards:

- Save as new
- Save as template
- Send as attachment
- Publish.
- Print
- Export

Users that attempt a restricted action will receive notification that the behavior is prohibited due to the data egress policy your organization has implemented.

These limits are designed to prevent collaborators from saving or sharing confidential information for malicious purposes.

Event Reporting

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

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

Event Reporting 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 you can more tightly enforce organizational security and compliance policies.

Event Reporting provides a JSON 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.

To benefit from that feed, Event Reporting data is typically integrated with other security systems that provide monitoring, notification, policy creation and enforcement, and data loss prevention (DLP). These apps are sold by third parties — typically Cloud Access Security Broker (CASB) systems, Security Information and Event Management systems (SIEMs), or a combination of CASB and SIEM working together. Sometimes enterprises develop their own monitoring and response systems, instead of relying on those provided by third parties.

Event Reporting key use cases:

- Data loss prevention
- Personally identifiable information (PII) data handling
- Data governance
- Gain insights on collaboration

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Data Retention Controls

The more content your organization has in any SaaS application, the more risk your business takes on.

Smartsheet Data Retention Controls give organizations the ability to create a policy that dictates when content should be deleted, based on the criteria they elect to enforce.

These policies can be based on the date a sheet was created or the last time it was modified, ensuring only active or recent content is maintained within your Smartsheet instance and limiting your risk profile.

Customer Managed Encryption Keys (CMEK)

Smartsheet uses encryption to secure customer data and help customers maintain control over it. For standard customers, data resides in multi-tenant architecture encrypted with default keys managed and rotated on schedule via AWS KMS.

Customer managed encryption keys (CMEK) are intended for organizations that have sensitive or regulated data that requires them to manage their own encryption key. CMEK allow enterprise organizations to use cloud SaaS applications while maintaining data control comparable to that of an on-premises installation, adding a customer-managed layer of encryption to Smartsheet data storage to support advanced data security and governance policies.

For CMEK customers, data resides in single-tenant, physically isolated Aurora clusters encrypted with a KMS key hosted in the customer's own AWS account — Smartsheet has no access to the root key material. To use CMEK, customers must have access to Amazon Web Services Key Management Service (AWS KMS), as customer keys are set up and managed directly within AWS.

Smartsheet uses CMEK to encrypt your organization's data such that it remains under your control at all times. Specifically, Smartsheet does not store or control these encryption keys and Smartsheet must request and retrieve the keys from our customer's AWS KMS whenever Smartsheet needs to access your sheet data.

As your organization controls the CMEK stored in AWS KMS, you can revoke Smartsheet access to the CMEK and, thereby, access to your data at any time. By destroying the master keys in the AWS KMS, your organization can effectively lock down your data. A malicious party with a copy of the Smartsheet database, source code, and cloud encryption keys could still not read any of the data encrypted with CMEK. CMEK is available to purchase as a standalone offer for customers who meet the purchase criteria.

Global Account Configuration

Account security isn't limited to technical features such as data encryption, classification 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 logos globally to bring your Smartsheet deployment in line with organizational 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

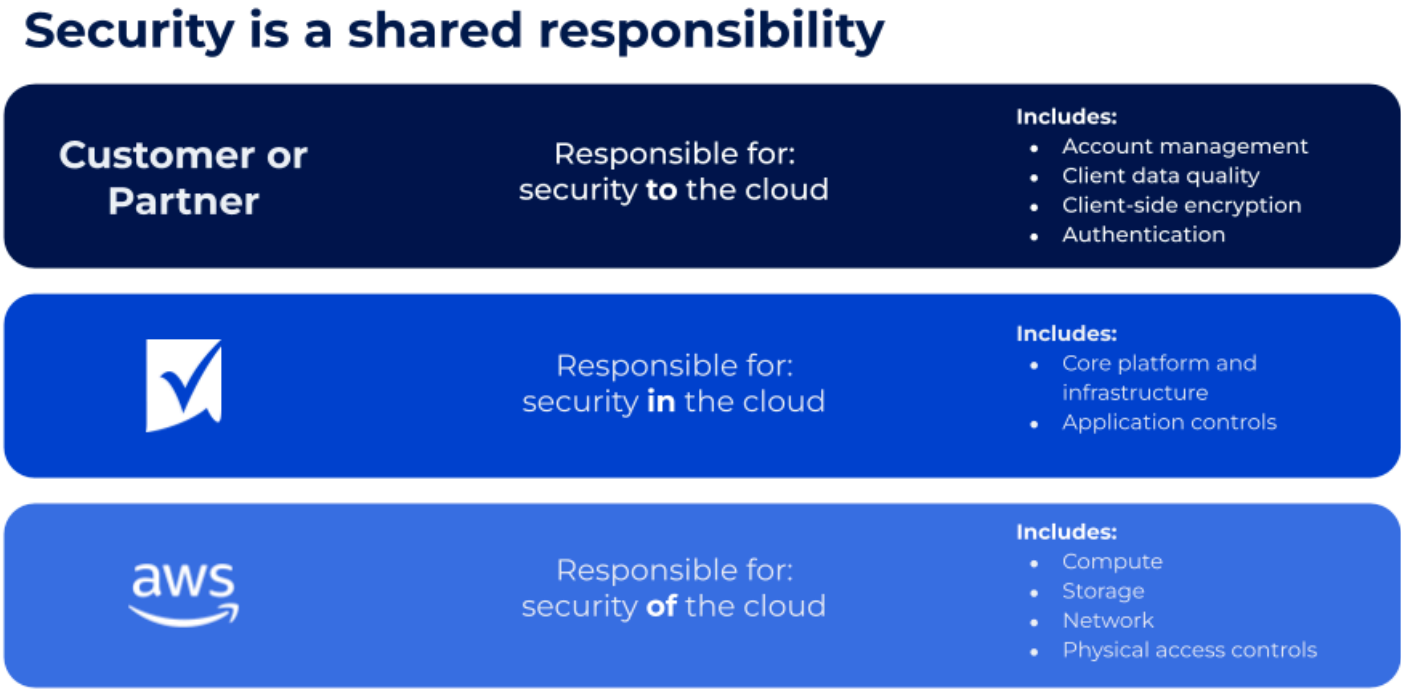
©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

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.

Smartsheet Security, Privacy, and Compliance Practices

Utilizing a holistic approach, the cybersecurity, privacy, and data protection programs at Smartsheet begin with strategic information security policies defined and supported by our executive leadership team. These policies are designed to align with the organization's strategic risk management practices, proactively manage and monitor security risks, promote security through process maturity and effective system architecture, and enable users to make prudent decisions about security risks through training and awareness.



Shared Responsibility Model

Effective security requires coordination across every layer of the technology stack. Smartsheet operates a three-tiered model in which AWS secures the underlying cloud infrastructure, Smartsheet secures the platform and application layer, and customers maintain responsibility for their own account management, data, and authentication practices.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Infrastructure and Architecture

Smartsheet's platform is built entirely on Amazon Web Services (AWS) and Google Cloud Platform (GCP) and is designed with strict environment boundaries to protect the integrity and confidentiality of customer data at every stage of the software lifecycle.

Environment Segmentation. Each environment — including development, staging, and production regions across the US, EU, Australia, and GovCloud — operates within its own dedicated AWS account and organizational unit or GCP Project, ensuring non-production workloads are completely separated from systems that handle customer data. For network connectivity across regions, Smartsheet uses AWS CloudWAN, which enforces logical routing segments — dedicated network lanes assigned to each isolated environment. Traffic between environments must pass through inspection infrastructure powered by AWS Network Firewall, which applies rule-based controls and logs all inter-environment traffic. Redundant inspection nodes are deployed in every region to ensure this protection remains continuously available.

Tenant Isolation. Every Smartsheet customer is assigned a unique tenant identifier applied consistently across all data storage, querying, and retrieval operations, ensuring no process can access data belonging to another customer. At the infrastructure level, containerized workloads are governed by network and security policies that restrict lateral communication between tenant contexts, and the dedicated-account-per-environment model ensures environmental isolation and development or test activity never touches live customer data.

Secure Development Lifecycle (SDLC). Security is embedded at every phase of product development. Before code is written, security engineers review architecture and design to identify flaws at the lowest possible cost. This is followed by structured threat modeling — using Data Flow Diagrams to enumerate attack vectors and log every finding for tracking — and targeted code review to verify mitigations are correctly implemented. Continuous Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) are integrated into CI/CD pipelines, automatically scanning every code change before it can reach production.

Penetration Testing. Smartsheet conducts penetration testing as a standard component of the security review process, applied based on risk classification. Engagements are performed by Smartsheet's internal security team or qualified external third-party firms. Testing typically follows a gray-box methodology — providing testers with both source code access and a staging environment — to surface vulnerabilities that purely external testing may miss. Continuous automated vulnerability scanning complements these point-in-time assessments across all infrastructure, including compute instances, containers, functions, and compute images.

Vulnerability Tracking and Remediation. Vulnerabilities identified through scanning or testing are tracked end-to-end with SLA-based remediation targets defined in Smartsheet's Vulnerability Management Policy.

Cloud Security Posture Management (CSPM). Smartsheet utilizes Wiz CSPM for its Cloud Security Posture Management tool for detection, tracking, and remediation of Cloud Security related concerns.

Smartsheet utilizes **Wiz CSPM** as its primary Cloud Security Posture Management solution to ensure comprehensive visibility across its multi-cloud environment. By providing a unified "graph-based" view of

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

the infrastructure, Wiz enables Smartsheet to identify complex attack paths and prioritize risks based on actual exposure rather than isolated vulnerabilities.

Key Security Benefits:

- **Continuous Compliance Monitoring:** Wiz automatically maps Smartsheet's cloud configurations against industry-standard frameworks (such as SOC2, ISO 27001, and FedRAMP) to ensure ongoing alignment with our regulatory commitments.
- **Real-Time Detection & Remediation:** The platform provides persistent scanning of cloud resources, alerting security teams to misconfigurations, overly permissive identity roles, or exposed secrets in real-time.
- **Reduced Attack Surface:** By correlating software vulnerabilities with network reachability, Smartsheet can rapidly remediate high-impact risks, ensuring that infrastructure remains hardened against external threats.

Data Security

We build security into our platform to ensure that your most valuable asset — your data — is protected. Smartsheet contracts with third parties to complete audits of our security practices, including a SOC2 Type II (or substantially equivalent) assessment and attestation, and third-party technical security assessments with penetration test firms. Furthermore, the Smartsheet vulnerability management program automates the identification and remediation of network and system vulnerabilities across Smartsheet corporate and production environments. Smartsheet uses encryption to secure your data and help you maintain control over it.

Customer data is hosted on Amazon Web Services infrastructure. Data stored at rest is encrypted using the industry-standard AES-256 encryption algorithm, as provided by Amazon RDS encryption. Data in transit is protected using TLS 1.2 technology. Encryption keys are managed through AWS KMS using a two-layer model: a Key Encryption Key (KEK) protects Data Encryption Keys (DEKs) that encrypt actual customer data. For standard plans, Smartsheet manages the KEK on your behalf with automated rotation. For organizations requiring direct control, Customer Managed Encryption Keys (CMEK) are available as a standalone add-on — see the CMEK section above.

Privacy

Privacy is core to how Smartsheet operates. Depending on the type of data involved, we play two different roles. We're a data controller for personal data we collect directly — like account, usage, and billing information — and a data processor for Customer Content, meaning the data customers upload or submit to the platform. As a processor, we only handle that data as directed by the customer, who stays in control.

We consider privacy one of our core principles; it's part of how we design features and make decisions, not something we bolt on. To that end, we don't use Customer Content for our own purposes — including marketing or training third-party foundation models.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Smartsheet follows a global approach to privacy that's designed to meet or exceed requirements under major regulations, including the GDPR, UK GDPR, and CCPA. See below for a list of and certifications. Here's a quick summary of our key commitments:

- **Data Processing Agreement (DPA)** — our DPA is automatically part of the Smartsheet User Agreement for all customers and includes EU and UK Standard Contractual Clauses (SCCs). Customers who want a separately signed copy can request one through the Smartsheet DPA page — the terms don't change.
- **Data Residency** — customers can choose where their Customer Content is hosted. See the Smartsheet Regions section for more.
- **Privacy by Design and Default** — we embed the principles of privacy by design and default into our application features. Ensuring privacy is a core capability, not an afterthought.
- **Subprocessors** — we publish a list of the subprocessors used by Smartsheet and we vet and apply contractual safeguards to any third party that processes Customer Content. See the Vendor and Supply Chain Risk Management section for more.
    - **Transfer Impact Assessments** — to assist our customers with their privacy compliance activities, we have completed transfer impact assessments available in the Smartsheet Security Packet. Please contact your sales representative or submit this form to obtain a copy.

AI Security and Privacy

Smartsheet AI features are built on the same security and privacy principles that govern the rest of our platform.

Your data never mixes with other customers' data. It never trains third-party foundation models. It never leaves your control. Every AI action or recommendation can be explained, audited, and traced back to its source.

Input prompts and generated outputs are stored for support and abuse monitoring purposes only, and are automatically deleted after 180 days.

For organizations with specific policy requirements that necessitate disabling AI capabilities entirely, this option is available by contacting Smartsheet Support. Disabling AI capabilities will negatively impact a customer's ability to fully utilize the Smartsheet service.

For a full overview of how Smartsheet AI tools handle your data please see our AI Security Whitepaper or Responsible AI webpage.

Operational Management

We have implemented policies and procedures designed to ensure that your data is secure and backed up to multiple physical locations. Our teams are continually evaluating new security threats and implementing updated countermeasures designed to prevent unauthorized access or unplanned downtime of the subscription service. Access to all Smartsheet production systems and data is limited to authorized members of the Smartsheet Technical Operations team based on the principles of least privilege and need-to-know.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

The Smartsheet cloud infrastructure is architected to be redundant and reliable, with a guaranteed uptime SLA of 99.9% or better. Real-time service availability and performance information is published on the Smartsheet Status Page. Customers who have signed up for automatic updates will be notified of significant incidents by email and/or text message.

Incident Response and Breach Notification

Smartsheet maintains documented incident response plans that are reviewed and tested annually. In the event of a security incident, our response process covers preparation; detection and analysis; containment, eradication and recovery; and post-Incident activity. Where required by applicable law or contract, Smartsheet will notify the contacts provided by our customer within legally mandated timeframes. Customers should escalate all security concerns via Smartsheet support. For full details on our availability commitments, see our Service Level Agreement.

Vulnerability Disclosure and Bug Bounty

Smartsheet operates an active bug bounty program that invites independent security researchers to identify and responsibly disclose vulnerabilities in our platform. This program is a deliberate extension of our security posture — providing an additional layer of scrutiny beyond our internal testing and enabling us to discover and resolve issues before they can be exploited. Responsible disclosure is rewarded with monetary compensation based on the severity of the finding.

Program Scope. The bug bounty program covers Smartsheet's core platform and enterprise capabilities, including the primary Smartsheet application, enterprise access controls, Dynamic View, Event Reporting, and platform integrations such as Salesforce and Jira connectors. Brandfolder and Outfit are also included as in-scope targets. The program is managed through Smartsheet's in-house bug bounty platform, and researchers are provided with dedicated test accounts to conduct their work safely. Out-of-scope activities include testing against accounts researchers do not own, automated scanning and denial-of-service testing, phishing, and any testing that could impact live customer data.

Severity Classification. All reported vulnerabilities are evaluated and classified using a four-tier severity model:

- **Critical (S1):** Issues that allow server or account takeover, unauthorized access to or modification of customer data, or denial of service — without requiring any existing credentials or user access. Examples include SQL injection, exposed secrets, or missing access controls on insecure object identifiers.
- **High (S2):** The same classes of impact as Critical, but requiring authenticated access or existing user credentials to exploit. Examples include cross-site scripting vulnerabilities that allow session hijacking, or the ability to permanently delete content by bypassing standard controls.
- **Medium (S3):** Issues limited in impact to other users within the same organization or to shared assets. Examples include privilege escalation within a shared sheet or the use of insecure cryptographic primitives.
- **Low (S4):** All other security issues that do not meet the above criteria.

Remediation SLAs. Once a vulnerability is confirmed and triaged, Smartsheet commits to the following remediation timelines:

- **Critical:** Remediated or mitigated as soon as possible, not to exceed **15 days.**
- **High:** Remediated or mitigated within **30 days.**

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

- **Medium:** Remediated or mitigated within **90 days.**
- **Low:** Remediated or mitigated within **180 days.**

These SLAs apply from the date of discovery or external disclosure. For Critical severity issues, all required team members are expected to prioritize remediation to the exclusion of other work until the issue is resolved.

Responsible Disclosure. Smartsheet is committed to working collaboratively with security researchers throughout the disclosure process. Researchers are asked to report findings privately, refrain from testing against customer accounts, and avoid any actions that could disrupt service availability. In return, Smartsheet commits to timely acknowledgment, transparent communication, and appropriate recognition and compensation for valid findings. Organizations wishing to report a potential security issue outside of the bug bounty program can contact Smartsheet directly at bugbounty@smartsheet.com. Smartsheet reserves the right to stop or suspend any bug bounty program at any time.

Vendor and Supply Chain Risk Management

Smartsheet conducts due diligence on all subprocessors before they are onboarded, with closer scrutiny applied to any vendor that will access, process, or store Customer Content. These reviews include checking relevant security documentation such as SOC 1 and/or SOC 2 Type II reports, penetration and vulnerability testing results, PCI-DSS audits, and third-party security assessments. Subprocessors are reevaluated each year to confirm that their security controls still meet Smartsheet's standards.

Every subprocessor is required to sign contracts that reflect Smartsheet's security and privacy expectations. These agreements cover data processing requirements, security standards, incident notification obligations, and rules that extend those same expectations to any additional vendors the subprocessor may use.

To help customers understand who is involved in processing their data, Smartsheet publishes a publicly available subprocessor list. Additional information regarding our use of subprocessors is available in the Smartsheet Security Packet. Please contact your sales representative or submit this form to obtain a copy.

Data Center Security, Continuity, and Redundancy

We work with industry-recognized hosting partners to ensure that you can deliver services to your organization confidently on a platform you can trust. We have multi-site data redundancy, hosting at AWS facilities, and our facilities are SOC 1, SOC 2, ISO 27001, and FedRAMP/DISA IL5 examined and certified. Our monitoring includes continuous surveillance and 24x7 production environment management. Smartsheet maintains internal processes and plans in order to address business continuity events and disaster recovery scenarios. These plans are reviewed and tested on an annual basis and are distributed to applicable staff throughout the organization. Through our AWS hosting we utilize multiple data centers with independent power, HVAC and fire suppression to prevent data centers from being impacted simultaneously in the event of a large-scale natural disaster.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

Smartsheet Regions

Smartsheet Regions gives you control over where your data is hosted, making it easier to address your organization's regional privacy and governance requirements. Three regional instances are available: United States (US), European Union (EU), and Australia (AU).

The EU instance is hosted on AWS in Frankfurt, Germany. The AU instance is hosted on AWS in Sydney, Australia. Data created in a regional instance remains in that region — content cannot be transferred or accessed across regional boundaries.

To learn more about Smartsheet Regions options, visit the Smartsheet Trust Center and our Data Residency page.

Audits and Certifications

ISO & SOC 2 Compliance

Smartsheet validates its security posture through a combination of Trust Services Criteria and the ISO/IEC family of standards (or substantially equivalent standards). These certifications provide independent assurance of our commitment to operational excellence.

- **SOC 2 Type II:** Smartsheet undergoes an annual examination by a third-party CPA firm to test the design and operating effectiveness of our controls.
    - **Scope:** This report encompasses the complete Smartsheet application environment, including the core platform and infrastructure throughout our hosted data centers.
    - **Trust Criteria:** Security, Availability, and Confidentiality.

- **ISO/IEC 27001, 27017, & 27018 (Security & Cloud):** This suite of certifications validates our Information Security Management System (ISMS). While 27001 is our foundational security framework, we also adhere to 27017 for specific cloud service security controls and 27018 for the protection of Personally Identifiable Information (PII) in public clouds.

- **ISO/IEC 27701 (Privacy):** An extension of our security framework, this standard focuses on our Privacy Information Management System (PIMS), ensuring we meet global data protection requirements like GDPR, UK GDPR, and CCPA as a data controller and a data processor.

- **ISO/IEC 22301 (Continuity):** This certification ensures we have a robust Business Continuity Management System to remain resilient and available during unforeseen events.

- **ISO/IEC 42001 (AI Management — *In Progress*):** We are currently pursuing this certification to establish a formal Management System for Artificial Intelligence, ensuring our AI-driven features are developed and deployed ethically and securely.

- **EU-US Data Privacy Framework (DPF):** Smartsheet and its affiliates participate in the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce (collectively,

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com

the Data Privacy Framework). We are committed to complying with the Data Privacy Framework Principles with respect to personal data transferred to the United States from the European Economic Area (EEA), the United Kingdom (UK), and Switzerland. To learn more about the Data Privacy Framework, and to view our certification, please visit the DPF program website. Smartsheet's commitments under the Data Privacy Framework Principles are subject to the investigatory and enforcement powers of the United States Federal Trade Commission (FTC).

- **HITRUST Readiness**: Smartsheet has achieved HITRUST Readiness status, reflecting our alignment with the HITRUST CSF framework and commitment to robust security and privacy controls. This designation underscores our ability to support customers with rigorous compliance requirements, including those in healthcare, finance, and other highly regulated sectors.

- **FedRAMP (moderate):** Smartsheet was selected for the FedRAMP Connect program by the Joint Authorization Board (JAB), which prioritized Smartsheet Gov for certification based on demand from federal government agencies. Smartsheet Gov is a separate Smartsheet environment with FedRAMP authorized status and is assessed at DoD Impact Level 4 (IL4), making it easier for the U.S. government defense, and civilian agencies to use Smartsheet for managing their work while helping them meet their security and compliance requirements.

- **Sarbanes-Oxley Act of 2002:** As a formerly public company, Smartsheet was previously required to comply with the Sarbanes-Oxley Act (SOX). While we are no longer subject to this regulatory requirement, Smartsheet has elected to maintain SOX-aligned internal controls to support strong financial governance and ongoing audit readiness. This continuity reflects our commitment to operational excellence and organizational integrity.

As noted on our legal webpage, Smartsheet uses infrastructure provided by Amazon Web Services, Inc. ("AWS") to host customer data. Information about security and privacy-related audits and certifications received by AWS, including ISO 27001 certification and SOC reports, is available from the AWS Security website and the AWS Compliance website.

For a full list of our certifications and additional information, visit the Compliance page in the Smartsheet Trust Center. **For direct access to key security documentation such as our CAIQ and SOC 2 report, please contact your account representative or CSM to request a "security pack".**

Conclusion and Additional Resources

Work today (and tomorrow) needs a modern work management platform that is easy to use and secure. Through ongoing focus and investment, we've built Smartsheet from the ground up with strict data confidentiality requirements and capabilities. In addition to what's available today, we have a number of additional security features currently under development.

For real-time system status, visit the Smartsheet Status Page. For security documentation, certifications, and compliance resources, visit our Trust Center.

©2026 All Rights Reserved Smartsheet Inc.
smartsheet.com