



ENGAGE

# Legal

Certain information set forth in this presentation may be “forward-looking information.” Except for statements of historical fact, information contained herein may constitute forward-looking statements. Forward-looking statements are not guarantees of future performance and undue reliance should not be placed on them.

Such forward-looking statements necessarily involve known and unknown risks and uncertainties, many of which are and will be described in Smartsheet’s filings with the US Securities and Exchange Commission, and these risks and uncertainties may cause actual performance and financial results in future periods to differ materially from any projections of future performance or results expressed or implied by such forward-looking statements. Although forward-looking statements contained herein are based upon what Smartsheet management believes are reasonable assumptions, there can be no assurance that forward-looking statements will prove to be accurate, as actual results and future events could differ materially from those anticipated in such statements. Smartsheet undertakes no obligation to update forward-looking statements except as required by law.

This presentation is proprietary to Smartsheet and the content herein is confidential and intended for permitted internal use only. This content shall not be disclosed to any third party that is not under an obligation of confidentiality to Smartsheet.

Smartsheet is a registered trademark of Smartsheet Inc. The names and logos of actual companies and products used in this presentation are the trademarks of their respective owners and no endorsement or affiliation is implied by their use.

SEA32Inter

# Smartsheet Security

Essential controls for safer collaboration

 smartsheet  
ENGAGE





**Pawan Shukla**  
Senior Product Manager



**Drew DeCounter**  
Senior Software Engineer



# About this session

By the end of this session, you will be able to describe how to...

## 1 Secure your data

*Protect company data with secure login policies and access controls*

## 2 Enable flexible management

*Understand common data security threats and choose the Smartsheet governance model that best fits your organization's needs*

## 3 Ensure safe collaboration

*Collaborate confidently with protected data sharing and role-based access*

## 4 Manage advanced security settings

*Acknowledge the additional Smartsheet security capabilities intended for customers working with sensitive data or in regulated industries*

# Table of contents

**1**

Why security is important

**2**

Smartsheet governance models

**3**

Login security

**4**

Collaboration security

**5**

Taking security to the next level

# 1

## Why security is important

Common threats to your data and how to be a good corporate citizen

smartsheet

ENGAGE

# Why is security important?

## Common threats to your data



### Social engineering

Cybersecurity threats use deception to trick people into revealing sensitive information or performing an action that they wouldn't normally do.

Example: Phishing



### Third-party exposure

Clients must be confident that partners and collaborators are handling information securely and sensitively.

Example: Sharing assets outside of permitted domains



### Data exfiltration

Clients need to protect against theft and unauthorized removal or movement of sheet data and assets.

Example: Assigning privileges that allow data to be removed from the environment.



### Other data vulnerabilities

Cyberattacks can take place through any weakness in the system.

Example:  
Behaviors/actions that put client data at risk - intentionally or unintentionally.



# Integrating Smartsheet into your corporate environment

Security begins with being a good corporate citizen



## Reduce risk

Smartsheet implements a variety of controls to reduce the risk of exposure to different types of cyber attacks.



## Security is a shared responsibility

Security should never be the sole responsibility of the app owner.

External teams have the expertise for corporate security policies and configurations .



## Engage your IT partners

External teams have the expertise for certain security configurations:

- Integration into Identity Provider solution
- SSO configurations
- Corporate cloud storage solutions for attachments
- Safe sharing

# 2

## Smartsheet governance models

Flexible plan management options to support your company's needs

 smartsheet  
ENGAGE

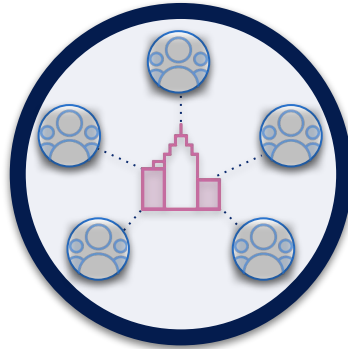
# Smartsheet governance models



## Decentralized model

Independent management by BUs

- Enables business units to administer, manage, and govern Smartsheet individually & independently
- Each business unit pays directly for their subscription



## Centralized model

Centrally managed by IT

- Enables IT to administer, manage, and govern Smartsheet subscriptions company-wide
- IT centrally governs the subscription



## Shared model

Shared management by IT and BUs

- Enables IT to centrally manage and govern multiple Smartsheet subscriptions
- Each business unit maintains control over their plan and billing

# 3

## Login security

Ensure only the right individuals can access your Smartsheet items

 smartsheet  
ENGAGE



# Meet Daniel

## IT Security Specialist

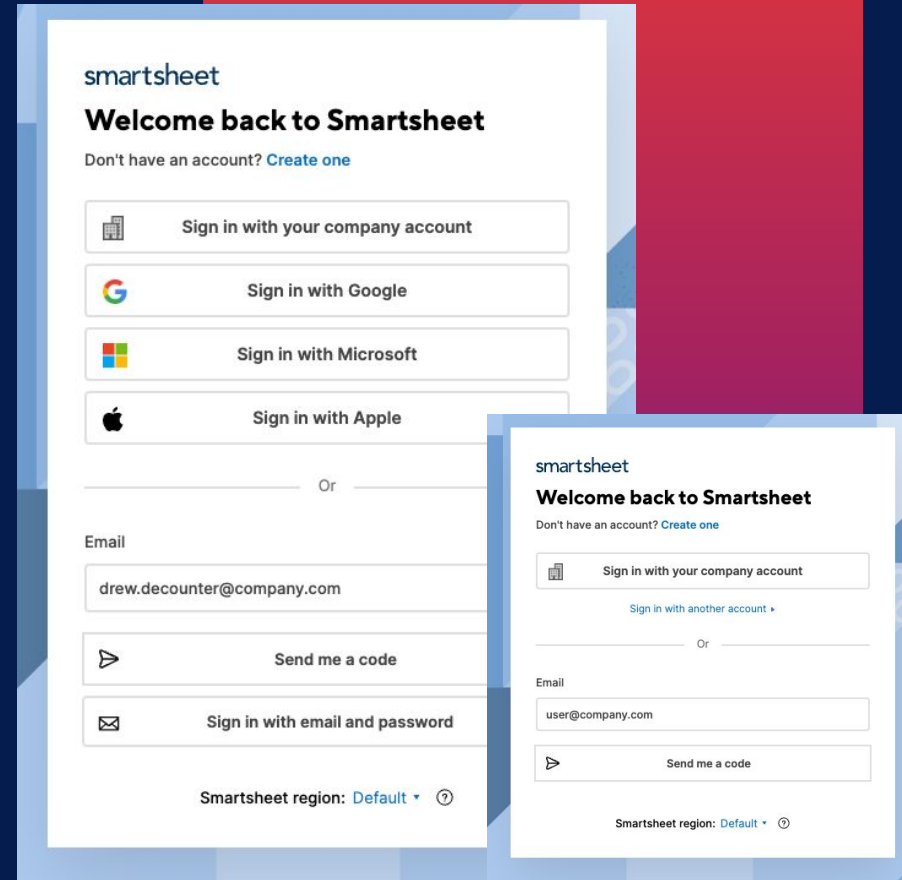
- Managing user authentication methods
- Ensuring secure access to company systems
- Implementing and enforcing sign-on policies
- **Needs to:**
  - Ensure that all users are using secure login methods like TOTP
  - Integrate SSO/SAML for seamless user experience
  - Push for domain validation to strengthen login security

# Supported authentication types

## Control how users can login to Smartsheet

Smartsheet supports a variety of methods for authentication.

- Only Enterprise plans can define specific authentication types for their plan or domain
- System Admins should consider HOW their users should authenticate into Smartsheet
- Consider removing authentication types that are not part of your company's best practices



# Domain-level login policy

## Centralize control, standardize login, and secure your users and data

Centralize login methods across plans by enforcing SAML-based Single Sign-On (SSO) at the domain level.

- Already launched:
  - Domain-level SAML SSO configuration
  - Simplified Okta-based SAML setup
  - Strict domain-level SAML SSO enforcement
- Coming soon:
  - Domain-level Google & Microsoft SSO login options
  - Automatic ISP user redirection to Google/Azure SSO pages

The screenshot shows the 'Authentication' section of the Smartsheet Admin Center. It includes a header 'Smartsheet Admin Center' and a main title 'Authentication'. Below the title is a brief description: 'Manage authentication options for users in your organization's domain. An active domain is required to configure authentication options.' The page is divided into several sections: 'Domain strict', 'Fallback option for System Admins', 'SAML Identity Provider (IdP)', and 'One-time password via email'. Each section contains a 'Select domain' dropdown menu. The 'SAML Identity Provider (IdP)' section is currently active, showing a '+ Add a SAML IdP' button and a configuration card for 'Okta'. The 'Okta' card has a toggle switch turned on and a dropdown menu with 'disney.com' selected. The 'One-time password via email' section has a checkbox checked and a 'Select domain' dropdown menu.

# Email-based TOTP (time-based one-time passcode) login

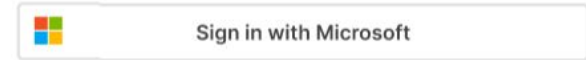
“Send me a code”

Secure access to Smartsheet with stronger email TOTP authentication.

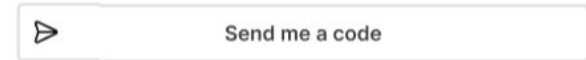
- **Enhanced Security:**
  - Each login requires a unique TOTP sent to the registered email
  - Reduces unauthorized access; no passwords to manage
- **Compliance:**
  - Aligns with industry best practices
  - Meets higher compliance standards

smartsheet

**Welcome to Smartsheet**



Or



[Sign in with another account](#) ▶

Smartsheet region: [Default](#) ▼ ⓘ

(example)

TOTP emails will come from: [system@system.smartsheet.com](mailto:system@system.smartsheet.com)

smartsheet

ENGAGE

Default, EU

All Plans

Adv: N/A



# Why Password are unsafe

Embracing a safer future by moving away from passwords



## Easy to guess

Common passwords are widely used and easily cracked by advanced algorithms



## Phishing vulnerability

Even strong passwords are compromised if users fall for phishing scams



## Reuse across many sites

Reusing passwords across platforms means one breach can compromise multiple accounts.

# Directory services integration

## Automate user management in Smartsheet

Save time and increase data security by automating user provisioning, deprovisioning, and profile updates by connecting to your organization's existing directory service.

- Microsoft Entra ID (*formerly Azure Active Directory*)
- Okta

For customers with Okta, group support via SCIM enables you to sync user groups from your directory to Smartsheet, simplifying group management.



okta

smartsheet

ENGAGE

Default, EU

Enterprise

Adv: N/A

# POP QUIZ #1

**Which Smartsheet feature can help reduce the risk of weak passwords by requiring a unique code sent to a user's registered email during login?**



**a. Single Sign-On (SSO)**



**b. Send me a Code (Email TOTP)**



**c. Password complexity rules**

# POP QUIZ #1

Which Smartsheet feature can help reduce the risk of weak passwords by requiring a unique code sent to a user's registered email during login?



a. Single Sign-On (SSO)



b. Send me a Code (Email TOTP)



c. Password complexity rules

## POP QUIZ #2

How can Smartsheet domain-level login feature help protect against phishing attacks?



**a. By ensuring users in verified domains use their corporate authentication policy**



**b. By sending security alerts to users**



**c. By offering password recovery options**

## POP QUIZ #2

**How can Smartsheet domain-level login feature help protect against phishing attacks?**



**a. By ensuring users in verified domains use their corporate authentication policy**



**b. By sending security alerts to users**



**c. By offering password recovery options**

# 4

## Collaboration security

Ensure worry-free collaboration with trusted internal and external stakeholders

 smartsheet  
ENGAGE

# Meet Alice

## Collaboration Tools Administrator

- Overseeing use of collaboration tools within the org
- Managing permissions and access control for internal and external users
- Ensuring secure data sharing practices
- **Needs to:**
  - Ensure only authorized access to sensitive information
  - Align with industry regulations
  - Balance security with user-friendly collaboration

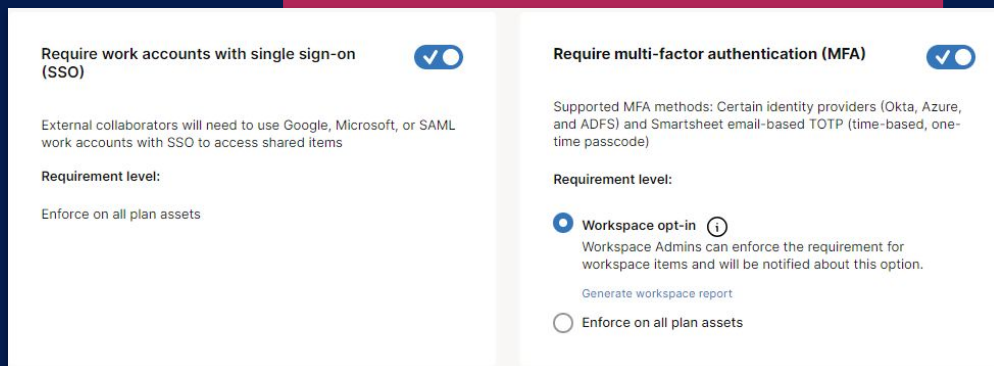




# Secure External Access

## Extra security when working with external collaborators

Enables System Admins to enforce work accounts and/or multi-factor authentication (MFA) policies for external collaborators wanting to access your plan's Smartsheet items.



The screenshot shows two configuration panels for 'Secure External Access'. The first panel, 'Require work accounts with single sign-on (SSO)', has a toggle switch turned on. Below the title, it states: 'External collaborators will need to use Google, Microsoft, or SAML work accounts with SSO to access shared items'. Under 'Requirement level:', the option 'Enforce on all plan assets' is selected. The second panel, 'Require multi-factor authentication (MFA)', also has a toggle switch turned on. It lists supported MFA methods: 'Certain identity providers (Okta, Azure, and ADFS) and Smartsheet email-based TOTP (time-based, one-time passcode)'. Under 'Requirement level:', the 'Workspace opt-in' option is selected, which includes a tooltip icon (i) and a description: 'Workspace Admins can enforce the requirement for workspace items and will be notified about this option.' Below this, there is a link 'Generate workspace report' and the 'Enforce on all plan assets' option is unselected.

**Require work accounts with single sign-on (SSO)**

External collaborators will need to use Google, Microsoft, or SAML work accounts with SSO to access shared items

**Requirement level:**

Enforce on all plan assets

**Require multi-factor authentication (MFA)**

Supported MFA methods: Certain identity providers (Okta, Azure, and ADFS) and Smartsheet email-based TOTP (time-based, one-time passcode)

**Requirement level:**

**Workspace opt-in** ⓘ  
Workspace Admins can enforce the requirement for workspace items and will be notified about this option.

[Generate workspace report](#)

Enforce on all plan assets

# Secure External Access

Extra security when working with external collaborators

## Require corporate accounts:

- Corporate account or Single Sign-On (SSO) is enforced at the entire plan level
- Enforcement verification box appears when external collaborator attempts to access items in your plan



## Corporate account required

Sign in with a corporate account to access this asset or contact your IT administrator. [Learn more](#)

- Corporate account (SSO) supports: SAML(any IDP), Google work account and Microsoft work account

Sign in with corporate account

smartsheet

ENGAGE

Default, EU

Enterprise

Adv: N/A

# Secure External Access

Extra security when working with external collaborators

## Require MFA:

- MFA can be enforced at plan or workspace level
- Enforcement verification box appears when external collaborator attempts to access items in your plan
- Email-based MFA will be requested if Identity Provider (IdP) based MFA completion cannot be completed



## Enter your verification code

We sent a verification code to:  
annelle.charles@mbfcorp.com

 Resend code

# Identity provider (IdP) managed access

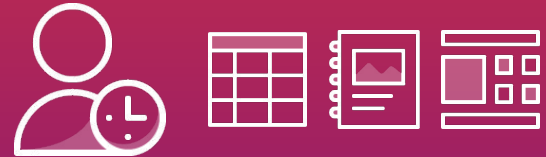
## Streamline and secure user asset management

Smartsheet Administrators will soon be able to **map Identity Provider (IdP) user roles** with **IdP managed groups** within Smartsheet at the domain level.

This is a highly **adaptable system** that supports easy modifications to IdP user role-based access rights as the company's needs evolve.

Customers can **manage user asset access** in Smartsheet based their user role based from their own IdP.

### Example roles



Finance Manager



HR Manager

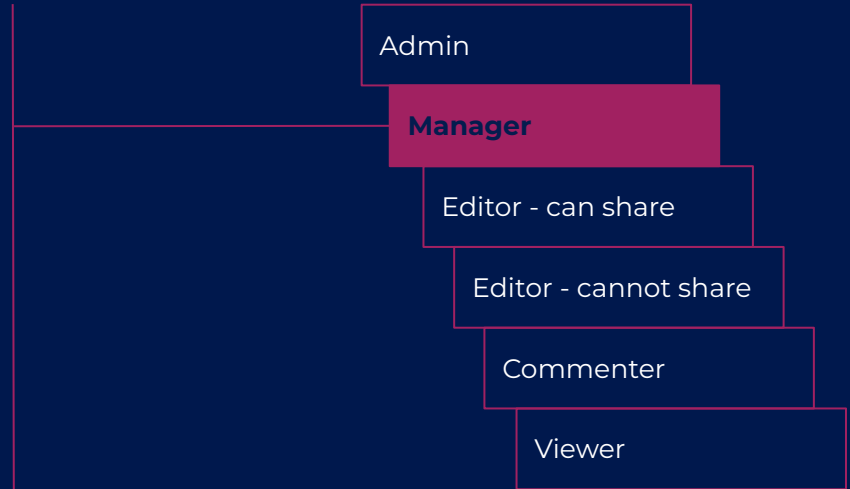
# New Manager permission set

Offering more flexibility and security for your core Smartsheet assets

New permission level **between “Admin” and “Editor - can share”** creates a "trusted second-in-command" role that may effectively assist the asset Admin in most building and maintenance functions.

Managers will be able to:

- Hide/unhide columns
- Edit conditional formatting rules
- Create and edit shared filters
- Create and edit automated workflows
- And more...



## POP QUIZ #3

**How does Smartsheet IdP managed access enhance collaboration security?**



**a. It assigns permissions based on user roles, limiting access to only what is necessary**



**b. It disables access to all external collaborators**



**c. It allows everyone full access to all data.**

## POP QUIZ #3

How does Smartsheet IdP managed access enhance collaboration security?



**a. It assigns permissions based on user roles, limiting access to only what is necessary**



**b. It disables access to all external collaborators**



**c. It allows everyone full access to all data.**

5

## Advanced security measures

Be safe. Sleep well.

 smartsheet

ENGAGE



# Meet Chris

## Information Security Manager (CISO office)

- Defining and implementing the organization's security strategy
- Overseeing advanced security measures and compliance
- Ensuring data protection and regulatory adherence
- **Needs to:**
  - Streamline and automate security processes
  - Align security policies with overall business goals
  - Reduce the likelihood of data breaches and unauthorized access
  - Meet regulatory standards and avoid penalties



# Data egress

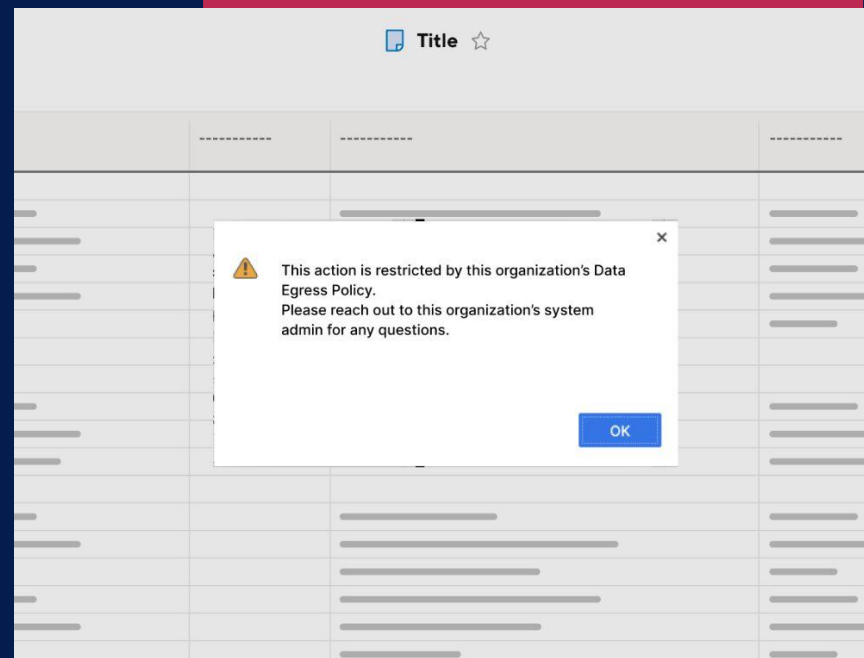
Prevent confidential data from leaving your Smartsheet ecosystem

SysAdmins define company egress policies for users with control over the following actions:

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

Data egress policies applicable to:

- Sheets, reports, and dashboards
- Internal and external users



# Data retention

Ensure only current, relevant data is stored in your Smartsheet account

SysAdmins can set organisation-wide data retention policies to automatically remove unused Smartsheet sheets.

- Run on a defined schedule, based on your criteria of when assets were created or last modified
- Reports showing impacted sheets and their attachments are generated automatically
- Email notifications are sent to non-compliant sheet owners so they can take action

The screenshot displays the Smartsheet Admin Center interface. The main content area is titled "Governance Controls" and features two policy cards: "Data Egress Policy" and "Data Retention Policy". The "Data Retention Policy" card is selected and expanded, showing configuration options for "Apply to these items" (set to "Sheets"), "Policy conditions" (with "Created" set to "More than 10 months ago" and "Last modified" set to "More than 180 days ago"), and a "Next" button at the bottom right. The top navigation bar includes a menu icon, the text "Smartsheet Admin Center", and user profile information.

## POP QUIZ #4

### Why is controlling data egress important in Smartsheet?



**a. It speeds up the processing of large data sets.**



**b. It prevents unauthorized data from being exported or shared outside the organization**



**c. It allows unrestricted sharing of data across all platforms.**

## POP QUIZ #4

### Why is controlling data egress important in Smartsheet?



a. It speeds up the processing of large data sets.



b. It prevents unauthorized data from being exported or shared outside the organization



c. It allows unrestricted sharing of data across all platforms.



## Session recap

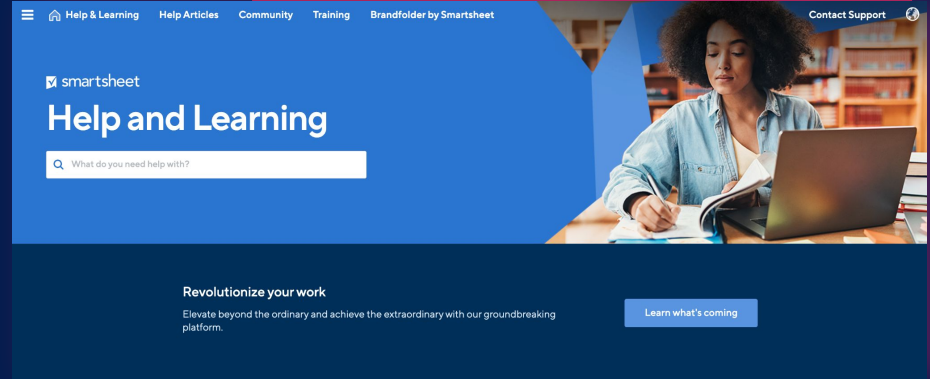
You now know how to...

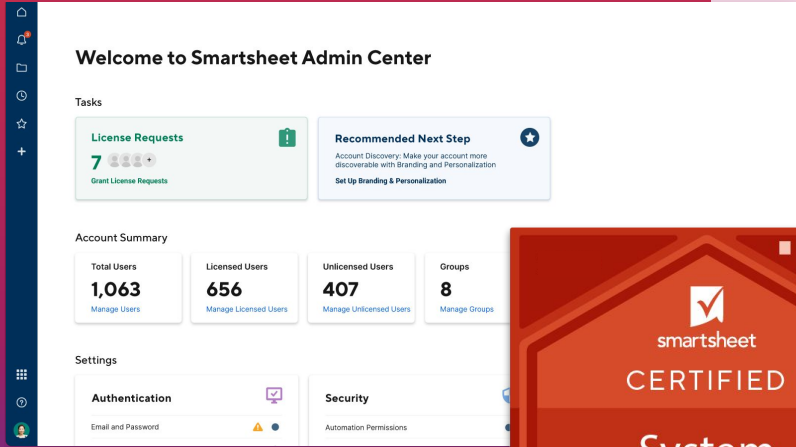
1. Enable flexible management of Smartsheet
2. Secure your data
3. Ensure safe collaboration
4. Manage advanced security settings

# Online resources

## Smartsheet Help & Learning Centre

- Knowledge base
- Help Center Articles
- Free tutorials and webinars
- Community forums
- Smartsheet University





## Test your knowledge

- Take our eLearning path; System Admin
- Get SysAdmin certified!
  - Minimum of 3-6 months of experience as a SysAdmin recommended
- Earn Professional Development Units (PDUs) with the Project Management Institute (PMI)



# Next steps...

- **View recordings of:**
  - *SEA33: Smartsheet Administration: Creating an efficient experience for everyone*
  - *SEA34: How to talk to your IT and security teams about Smartsheet*

## Take the survey

We'd love to hear your thoughts on the session.

**Open this session in the mobile app, click "Survey,"  
and answer two questions — it's that easy!**

# Thank you.

 smartsheet

# ENGAGE