madcap software

USER GUIDE

MADCAP FLARE ONLINE

Security Whitepaper

Copyright © 2026 MadCap Software. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of MadCap Software.

MadCap Software
1660 17th Street, Suite 201
Denver, Colorado 80202
858-320-0387
www.madcapsoftware.com

THIS PDF WAS CREATED USING MADCAP FLARE.

Security and MadCap Flare Online

MadCap Flare Online leverages the security, power, and flexibility of the cloud to mitigate or eliminate many of the technical hurdles faced by both content creators and information technology professionals. The overhead traditionally associated with managing complex systems can hinder the ability to create content and deliver content efficiently. The goal of this document is to provide a high-level overview of the ways that Flare Online addresses these challenges.

Security and privacy are top priorities at MadCap Software, especially when providing customers with a cloud-based system in Flare Online. We are committed to keeping your files, data, and communications secure. Therefore, in choosing Microsoft® Azure as a partner, we focused on selecting a security center that understands the importance of privacy and complies with the highest international and industry-specific compliance standards and uptime guarantees. Microsoft Azure regularly undergoes rigorous third-party audits to ensure and verify the highest level of security controls.

For more information, see the following:

```
https://www.microsoft.com/en-us/TrustCenter/Security/default.aspx
```

This document discusses the following:

Server Regions 5

Data Centers and Disaster Recovery 8

Source Control Provider and Data Storage 9

Web Server Hosting and Management 11

Security Headers 13

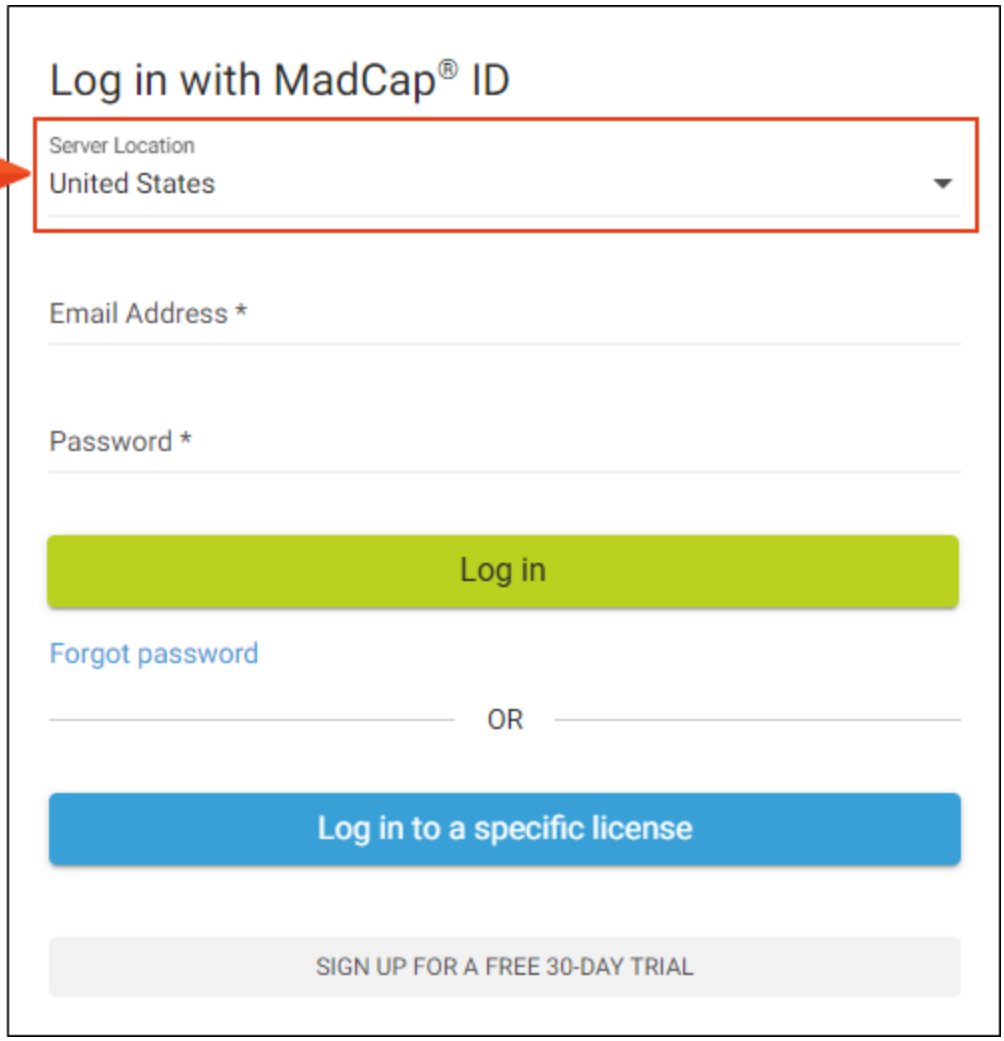
Service Level Agreement 14

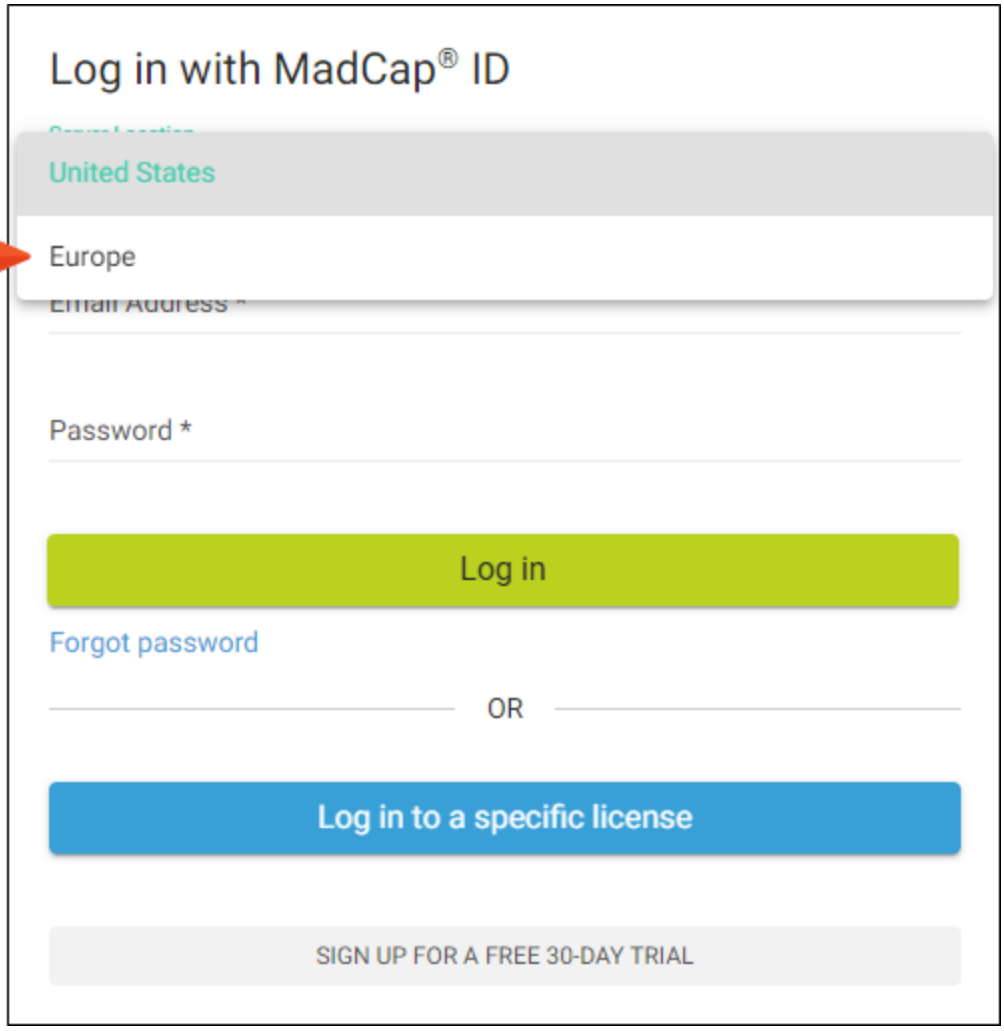
Application and Browser 15

Server Regions

New license subscriptions have the option a server region.

Depending on which region you chose when subscribing to a Flare Online license (United States or Europe), you can select the corresponding server when logging in to Flare Online.




Log in with MadCap® ID
United States
Europe
Email Address *
Password *
Log in
Forgot password
OR
Log in to a specific license
SIGN UP FOR A FREE 30-DAY TRIAL

- The European server is located in Germany.
- If you have an existing license (i.e., one that was created before the introduction of the European server), it will remain on the United States server.
- The server that you select will hold all of your data and hosted output for that license.
- Regardless of the server, the default MadCap domain is madcapflare.com (e.g., fictionsoft.madcapflare.com). Of course, you can still add your own host mapped domain (e.g., help.fictionsoft.com).
- Each server will have access to a global list of vanities, but will not contain any sensitive information. License vanity, region, and Flare Online key are the only pieces of data shared globally, so each server has access to that data.

Data Centers and Disaster Recovery

MadCap Software partners with Microsoft Azure to securely host mission-critical infrastructure, such as MadCap Flare Online. Depending on the server you choose when subscribing to Flare Online, the data residency and infrastructure are hosted in one of two locations:

- United States Azure WESTUS datacenters
- Europe Azure German datacenter

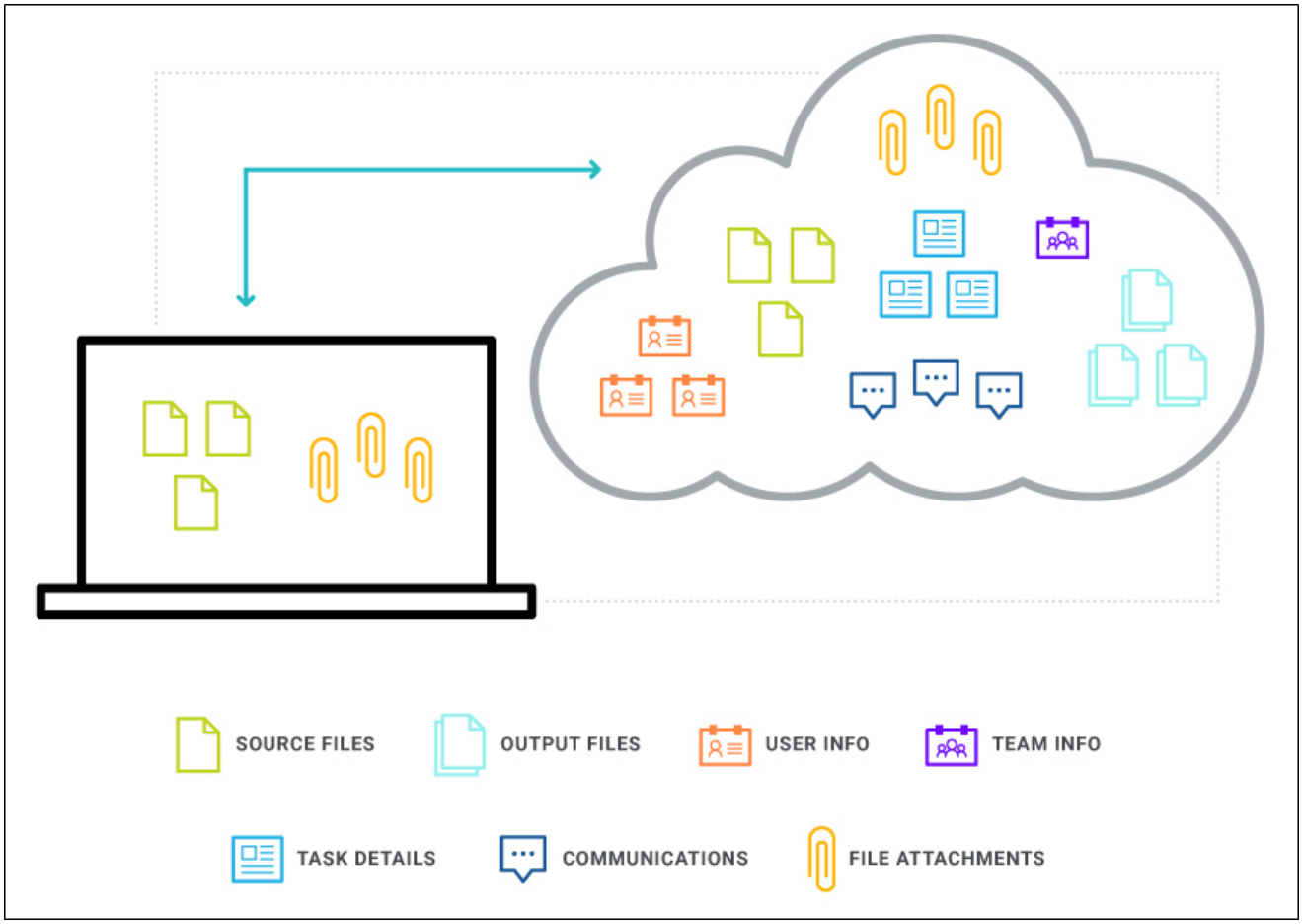
These Azure data centers are ISO27001 certified. For details, see:

```
https://www.microsoft.com/en-us/cloud-platform/global-datacenters
```

In addition to data stored in the database, the source control provider (Git) has the ability to failover in case of an outage. This is essential in handling mission critical data in the event of a catastrophe.

Source Control Provider and Data Storage

In addition to creating projects in Flare Online, projects can be uploaded locally from Flare Desktop to Flare Online, thus creating copies of those projects on the cloud. From the cloud versions of your projects, output files can be generated and published. In addition to project source and output files, Flare Online hosts many other types of data, including user and team information, task details, communications between individuals, and ancillary file attachments.



When local projects are uploaded from Flare Desktop to a Flare Online license, they are bound by a Git source control connection.

The following objectives are important for this relationship:

- Easy Access Projects are hosted in the cloud, which means they can be accessed from anywhere.
- Security Projects are stored securely in the cloud. Communication between your local desktop and the cloud is over HTTPS (HTTP over SSL). This is an encrypted, secure channel of communication. Source control data is secured by user name and security token. It is also possible to configure a license so that authentication is based on single sign-on (SSO) from the company's identity provider, thus adding another level of security.
- Data Transference Users can synchronize the local and cloud versions of projects after changes are made to files. In addition, you can retrieve files to a local machine whenever necessary. Uploaded projects can be imported and generated output files can be downloaded from Flare Online.
- Storage MadCap Flare Online stores user data in different ways depending on the nature of the data. Some examples of data storage include encrypted SQL databases, source control repositories (GIT), and Azure blob storage.
    - Sensitive data—such as user credentials and company information in the database tier—are stored using encryption to mitigate unauthorized access to data, and ensure your information is stored securely.
    - The methods of storing data follow industry security standards and offer a highly scalable solution to ever expanding storage management tracking needs.
    - If you choose to cancel your subscription, hosted data can be wiped at your discretion.
- Backups All data is backed up daily. All user data in Flare Online database backups are encrypted, transmitted remotely, and stored securely. This helps prevent unauthorized access.

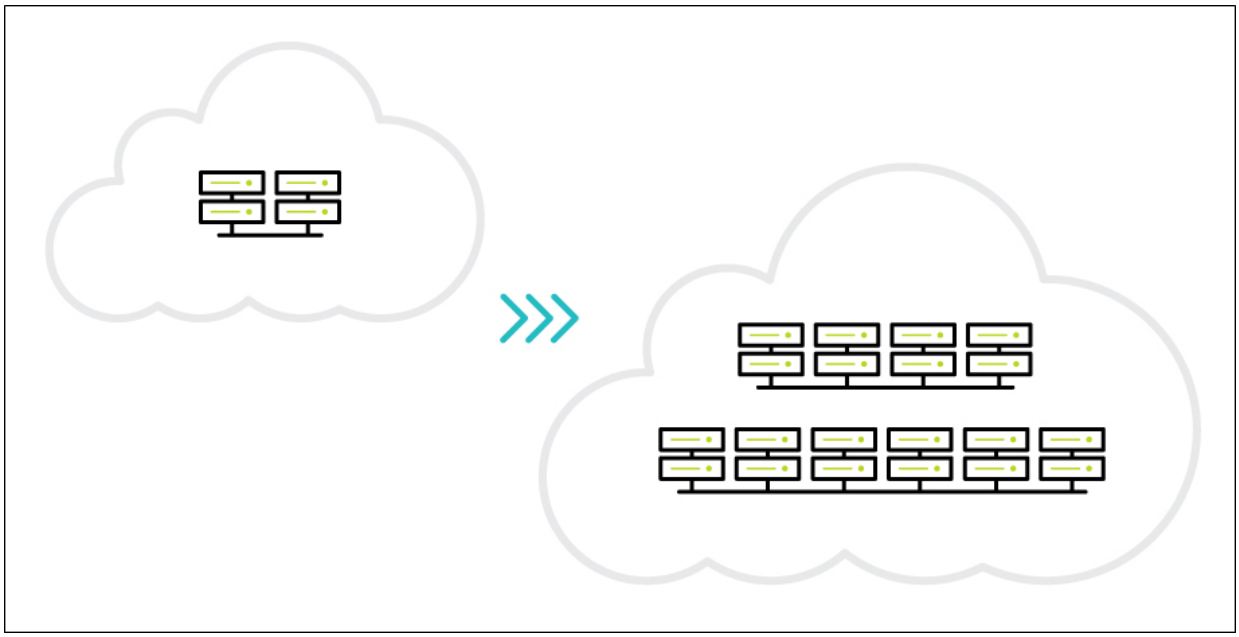
Web Server Hosting and Management

Every MadCap Flare Online subscription includes access to our highly scalable cloud-based build server. Because MadCap Flare Online is a cloud-based solution, content creators can rapidly generate and publish their content with minimal effort while benefiting from a high level of security, scalability, and durability, something that would otherwise require skilled IT resources to implement. Published output is hosted on a robust, secure, geographically redundant web application server.

With that in mind, the following are important considerations:

- Reduced Hosting Costs You can host all of your projects within Flare Online and never worry about managing or scaling costly web servers. Whether you have a small, single project or several large projects, you can host and manage all of your content in one place.
- Automation and Convenience From Flare Online, you generate and publish output with minimal effort. You also have the ability to quickly roll back published outputs when necessary, with the click of a button. Builds can be initiated manually or they can be scheduled. All of this can be done from any device supporting the browser-based interface.
- Availability and Monitoring Your content is vital to your company, so 24-hour availability of the web server is crucial, as is constant uptime monitoring. All components of MadCap Flare Online are monitored 24 hours a day, 7 days a week, 365 days a year using remote monitoring systems. MadCap Software has staff on hand to respond to outages and security breaches.
- Security Management Data in MadCap Flare Online is secured in the various ways.
    - Web services have built-in load balancers to stave off most DOS (Denial-Of-Service) attacks.
    - We provide unauthorized access monitoring and incident response. Any breaches in data security will be reported to affected customers.
    - User portal and API endpoints (i.e., the connection between Flare Desktop and Flare Online) are secured via user authentication.
    - All data endpoints are secured using SSL. The user portal, API endpoints, source control provider (Git), and all backend system communications are all encrypted.
    - Published sites that are not set to “live” are secured by user authentication.

- Scalability As your content management needs grow, so will your demands for a system that dynamically scales as well. Over time, the builds that you generate in Flare Online will consume more and more space. Flare Online offers ease with scalability for your output, which helps to eliminate worries about CPU, memory, and disk-intensive projects.



Security Headers

MadCap Flare Online has implemented the following security headers for website security and the prevention of malicious attacks, such as clickjacking:

- Content Security Policy Useful for protecting your site from cross-site scripting (XSS) attacks that can load malicious assets.
- Permissions Policy Useful for controlling which features and application programming interfaces (APIs) can be used in the browser.
- Referrer Policy Useful for controlling how much information the browser includes with navigation away from a document.
- Strict Transport Security Useful for enforcing the use of HTTPS.
- X Content Type Options Useful for preventing a browser from trying to MIME-sniff the content type, forcing it to stick with the declared content type. The only valid value for this header is "X-Content-Type-Options: nosniff."
- X Frame Options Useful for allowing frames on your site. By preventing a browser from framing your site you can defend against attacks like clickjacking.

On the Sites page, you can create your own security policies, adding directives to security headers.

Service Level Agreement

The full Service Level Agreement (SLA) for MadCap Flare Online (and other MadCap Software products) can be found here:

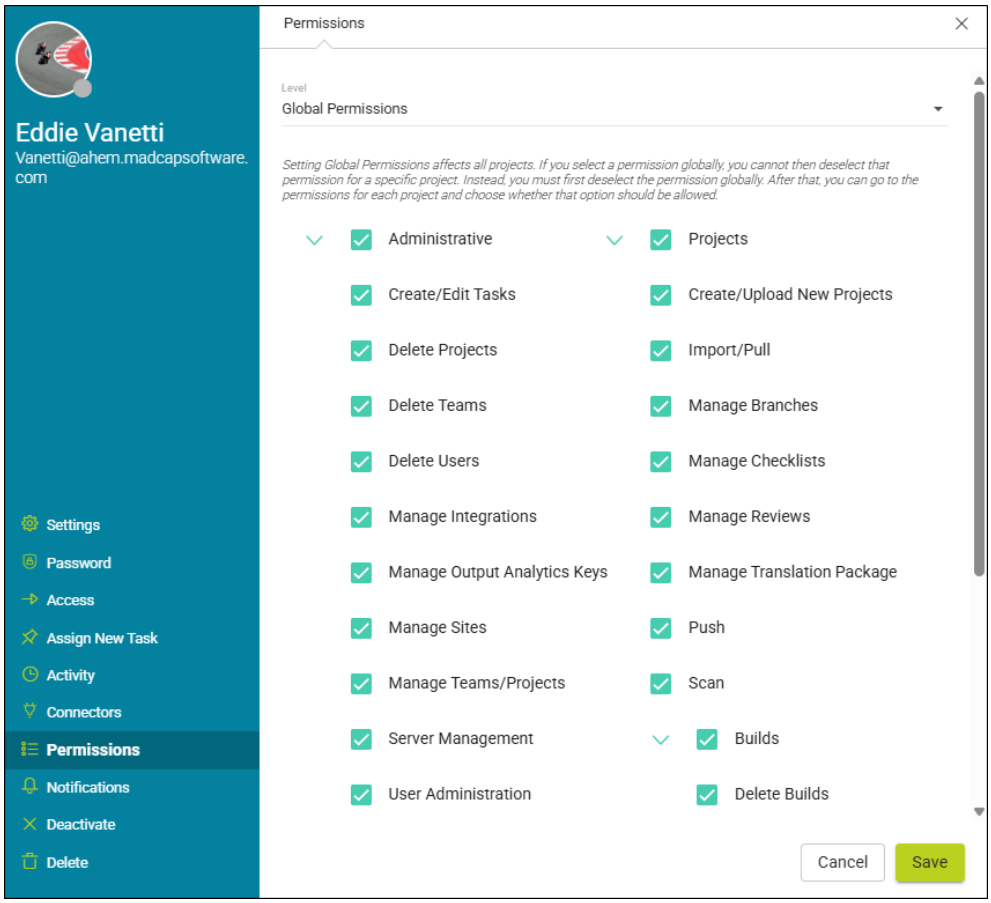
```
https://www.madcapsoftware.com/company/service-level-agreement/
```

Application and Browser

Much of the work in MadCap Flare Online (e.g., management of users, teams, tasks, projects, and builds) requires user interactions to be performed through a browser. In addition to Flare Desktop requiring end-to-end encryption, all traffic from your web browser to the MadCap Flare Online portal is also secured using industry standard security practices such as SSL.

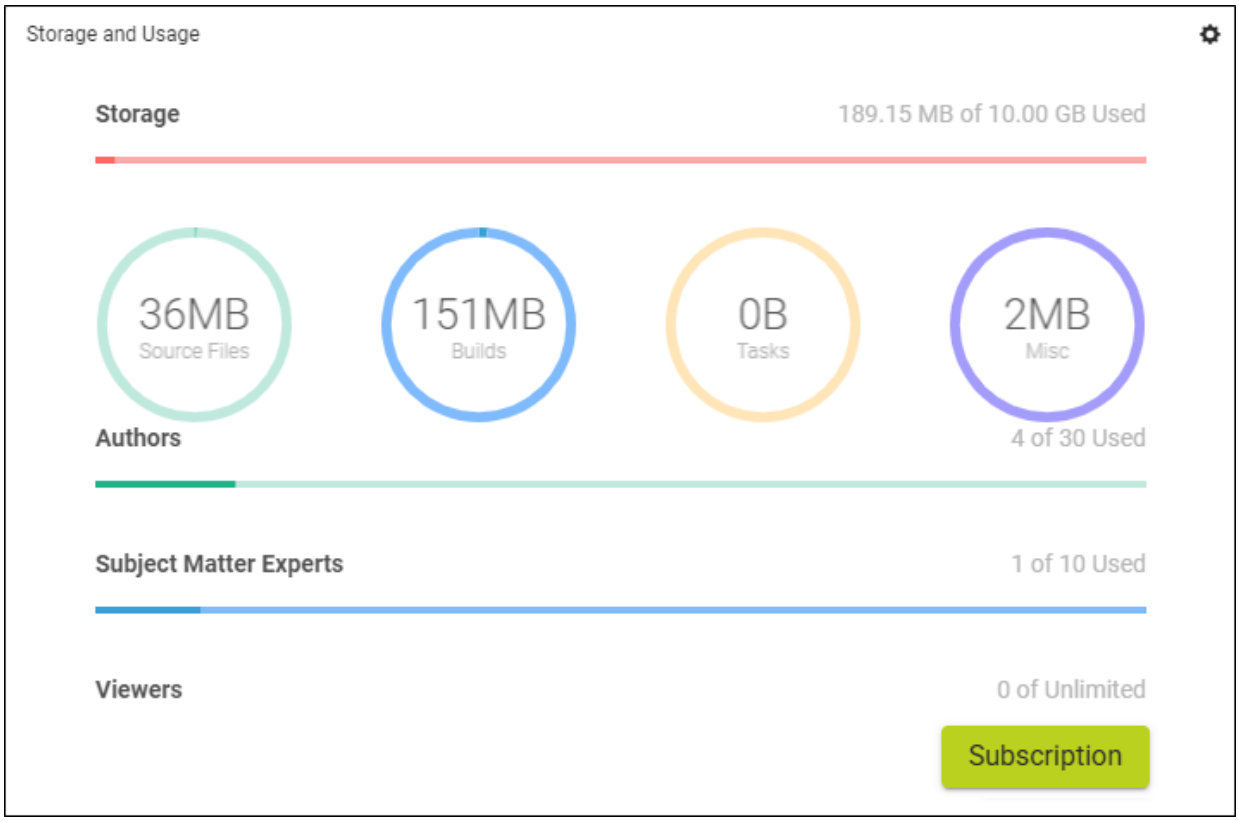
Following are some of the notable features in Flare Online that contribute to a secure, accessible work experience:

- Permissions In Flare Online, permissions allow you to dictate which users can see certain information and perform a variety of functions. In addition to basic permissions, there are several administrator-level rights that can be set, giving you the most flexibility to control how your data and files are being managed and distributed.

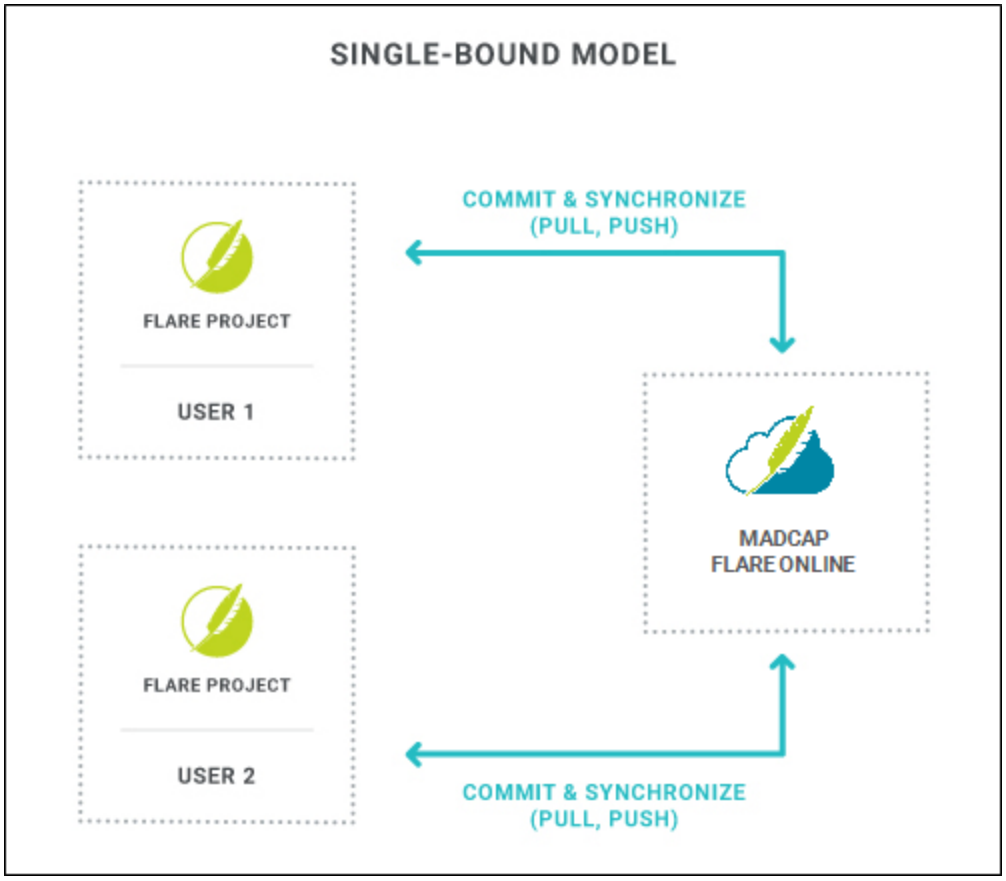


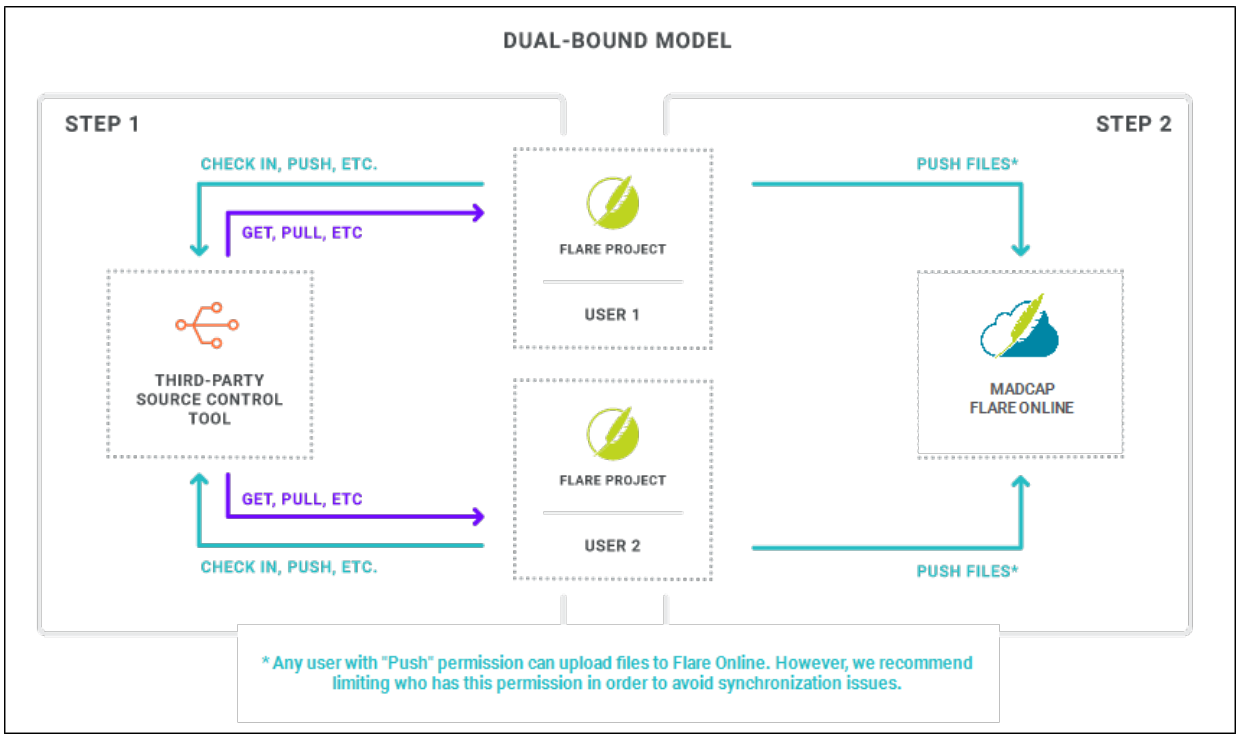
- Importing Projects If another user uploads a project locally from Flare Desktop to your MadCap Flare Online license and you do not yet have that project on your computer, you can import it. You can do this from the Flare Online window pane in Flare Desktop.

- Downloading Builds After generating a target, you can download the output to your computer. This is an optional step, in case you want to have a local copy of the build (e.g., you want to view your Microsoft HTML Help output, which is an output format that you cannot view from Flare Online).
- Subscription Built-in widgets inform you when space or user count becomes a concern. You can click the Subscription button to get into contact with MadCap Sales directly.

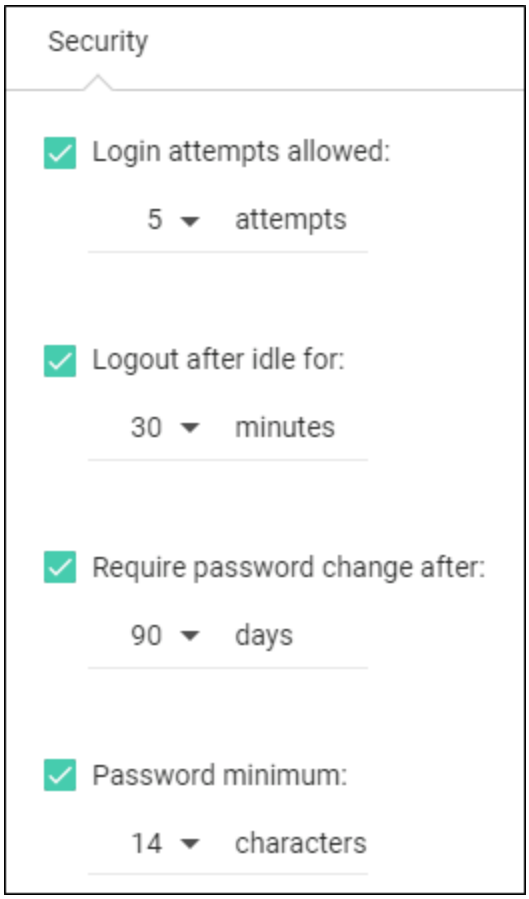


- Single-Bound and Dual-Bound Projects When you upload a project to Flare Online, the files are connected to Flare Online via an integrated source control system (Git). Your interaction with source control can follow one of two models—single-bound (recommended) or dual-bound. Single-bound projects are not bound to an additional third-party source control provider; they only use Flare Online's source control system. Dual-bound projects, on the other hand, are already bound to another source control provider, and therefore are bound to both the original third-party source control provider and to Flare Online.




DUAL-BOUND MODEL
STEP 1
STEP 2
CHECK IN, PUSH, ETC.
GET, PULL, ETC
THIRD-PARTY SOURCE CONTROL TOOL
FLARE PROJECT
USER 1
FLARE PROJECT
USER 2
PUSH FILES*
MADCAP FLARE ONLINE
GET, PULL, ETC
CHECK IN, PUSH, ETC.
PUSH FILES*
* Any user with "Push" permission can upload files to Flare Online. However, we recommend limiting who has this permission in order to avoid synchronization issues.

- Security Options On your license, you can set the maximum login attempts, automatic logout settings when the system is idle, as well as password change and minimum requirements.



PDFs

The following PDFs are available for download from the Help system.

AI Assist Guide

Analytics Guide

Authoring Guide

Branding Guide

Building Output Guide

Checklists Guide

Conditions Guide

Getting Started Guide

Images and Multimedia Guide

License Management Guide

Links Guide

Projects Guide

Reports Guide

Reviews Guide

Security Whitepaper

Sites Guide

Snippets Guide

Source Control Guide

Styles Guide

Targets Guide

Tasks Guide

TOC Guide

Topics Guide

Translation Guide

Users and Teams Guide

Variables Guide

What's New Guide

Widgets Guide