
Secure Your Community or Portal

Salesforce, Summer '19



CONTENTS

- [Secure Your Community or Portal](#) 1
- Give Secure Access to Unauthenticated Users with the Guest User Profile 2
- SEO Best Practices and Considerations for Guest Users 7
- Community User Visibility Best Practices for Guest Users 8
- Control Public Access to Your Lightning Community with Community Builder 9
- Object-Specific Security Best Practices for Guest Users 13
- Test Guest User Access in Your Community or Portal 15

SECURE YOUR COMMUNITY OR PORTAL

Communities and portals help you connect with customers and partners. When building your community or portal, you can use various settings and permissions to protect your data and your customers' data. Keeping your data secure is a joint effort between you and Salesforce. Get a printable version of the guide [here](#).

Get a [printable version of the security guide here](#).

EDITIONS

Available in: **Essentials**,
Enterprise, **Performance**,
Unlimited, and **Developer**
editions

[Give Secure Access to Unauthenticated Users with the Guest User Profile](#)

Public communities lend themselves well to business-to-consumer (B2C) type scenarios and help you to reach a broader audience. You can use a guest user profile to control public access to data, content, and objects in your community that don't require authentication. For example, you can create a customer support community where existing and potential customers can view public discussions, known issues, and solutions posted by other members or support without logging in.

[SEO Best Practices and Considerations for Guest Users](#)

To help end users discover publicly accessible content in your community through search engines, Salesforce provides you with several tools for search engine optimization (SEO). For Lightning communities, Salesforce generates a sitemap with a list of the publicly accessible pages based on the data that you made available to guest users through Community Builder and object access on the guest user profile. For communities built with Salesforce Tabs +Visualforce, customers are responsible for creating the sitemap and indicating which pages are included.

[Community User Visibility Best Practices for Guest Users](#)

Community and guest users often need to see one another in a public setting, especially when you implement a public forum, such as a self-service community, or build a public-facing app, such as ideas. Keep these guest user visibility best practices and considerations in mind when setting up your public-facing forum or site.

[Control Public Access to Your Lightning Community with Community Builder](#)

Set the public access level to your Lightning community, and set page-specific access to your community pages.

[Object-Specific Security Best Practices for Guest Users](#)

After you configure the guest user profile and the site guest user record, keep object-specific best practices in mind for guest user access.

[Test Guest User Access in Your Community or Portal](#)

After you've implemented the recommended security settings, take your community or portal on a test drive to see what guest users see.

Give Secure Access to Unauthenticated Users with the Guest User Profile

Public communities lend themselves well to business-to-consumer (B2C) type scenarios and help you to reach a broader audience. You can use a guest user profile to control public access to data, content, and objects in your community that don't require authentication. For example, you can create a customer support community where existing and potential customers can view public discussions, known issues, and solutions posted by other members or support without logging in.

Check out this video to learn more about how guest user profiles work: [Open Up Access to Your Community or Portal with the Guest User Profile](#).

When you create a community, Salesforce creates a profile, a user record, and sharing mechanisms that are available only to guest users, regardless of whether the community is configured for public access. Each public community or portal uses this guest user profile and record to let unauthenticated users browse the site. All guest visitors to a public site share the same guest user record (one per site) and have the same access level.

For instance, let's say you have three communities or portals set up in your Salesforce org. Each community or portal has its own guest user profile and guest user record.

Here's how it works.

- Community 1 —> Guest User Profile 1 —> Community 1 Site Guest User
- Community 2 —> Guest User Profile 2 —> Community 2 Site Guest User
- Community 3 —> Guest User Profile 3 —> Community 3 Site Guest User

A guest user has access to certain pages in your community as long as the community is active in your org. For example, guest users can always see login and login error pages in your community.

To secure your community for guest users, consider all the use cases and implications and implement security controls that you think are appropriate for the sensitivity of your data.

[Configure the Guest User Profile](#)

Before publishing your community with public access enabled, configure the guest user profile so that your customers can view and interact with your community without logging in.

[Configure the Site Guest User Record](#)

Each time a community or portal is created, Salesforce creates a guest user profile and a site guest user record. The site guest user record is the only user record associated with the guest user profile. It works like other user records in Salesforce, so you can add it to assignment rules, queues, public groups, manual sharing, and permission sets.

EDITIONS

Available in: **Essentials**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To enable public access to community content:

- Create and Set Up Communities


AND

Is a member of the community

Configure the Guest User Profile

Before publishing your community with public access enabled, configure the guest user profile so that your customers can view and interact with your community without logging in.

For Lightning communities, access the guest user profile from Community Builder.

1. In Salesforce Setup, enter *communities* in the Quick Find box and select **All Communities**.
2. Next to the community that you want to access, click **Builder**.
3. In Community Builder, click the Settings icon  and select **General**.
4. Under Guest User Profile, click the profile name.



5. Click **Edit**.
6. Scroll to the Standard Object Permissions section, and change the object permissions to meet your business needs.
7. Click **Save**.

For Salesforce Tabs + Visualforce communities, access the guest user profile from Community Workspaces.

1. In Salesforce Setup, enter *communities* in the Quick Find box and select **All Communities**.
2. Next to the community that you want to access, click **Workspaces**.
3. Select **Administration > Pages > Go to Force.com**.
4. Click **Public Access Settings** and change the access levels based on your needs.

Best Practices and Considerations When Configuring the Guest User Profile

When configuring the guest user profile, keep these best practices and considerations in mind.

EDITIONS

Available in: **Essentials, Enterprise, Performance, Unlimited, and Developer Editions**

USER PERMISSIONS

To access Community Workspaces:

- Create and Set Up Communities

AND

Is a member of the community

To edit app and system permissions in profiles:

- Manage Profiles and Permission Sets

To edit object and field permissions in profiles:

- Manage Profiles and Permission Sets

AND

Customize Application

Best Practices and Considerations When Configuring the Guest User Profile

When configuring the guest user profile, keep these best practices and considerations in mind.

EDITIONS

Available in: **Essentials**,
Enterprise, **Performance**,
Unlimited, and **Developer**
Editions

General Best Practices and Considerations

- The guest user profile is specific to the particular community or portal. Check the guest user profile for each of your communities or portals to ensure data security.
- As long as the community is active, guest users can access a subset of community pages, such as login and error pages.

Sharing Settings

External org-wide defaults control which objects external users, including guest users, can see and what their base level of access is.

- Review your organization-wide defaults, and ensure that External Org-Wide Defaults are enabled.
- Set all external org-wide defaults to their most restrictive setting, preferably **Private**.
- Review the external org-wide defaults that are set to **Controlled by Parent**, and make sure that the parent sharing settings are set to **Private**.
- Securing external sharing settings starts with securing internal sharing settings. To ensure that guest users access only what they need, review your data sharing model.

Object Settings

- Review all default object permissions in the guest user profile, and apply the most restrictive permissions for the guest user. For almost all objects, we recommend that the guest user has no access. If your business case calls for object data to be exposed to the guest user, set a maximum Read permission where possible.
- When guest users create records, such as cases via web-to-case or other records created via flows, the site guest user is the record owner. If the record owner isn't changed, anyone who has guest access to your community or portal can see the record.
- Never assign the View All or Modify All permission to guest users.
- Never assign update or delete permissions to guest users.

System Permissions

- Review all system permissions, and deselect the permissions that aren't necessary for your use case.
- Disable the View All Users permission if you don't want guest users to see other community users.



Note: When you deselect View All Users, guest users no longer have access to user or topic feeds in a community.

- Disable the Run Flows permission if guest users aren't using flows. If guest users need flow access, disable the pause option on flows that guest users are accessing.

API Usage

The API Enabled permission in system permissions lets external applications or connectors use the API to authenticate or access Salesforce data. Some examples of API usage are Workbench, Dataloader.io, Jitterbit, Excel Connector, the Salesforce app, Mobile SDK apps, Salesforce IoT, and connected apps.

- Check if the API Enabled permission is enabled for the guest user profile.
- Salesforce strongly recommends that you disable the API Enabled permission unless guest users explicitly need API access.

- Disable the permission in a sandbox first to see how guest user access is affected.

Visualforce Page and Apex

- Review all whitelisted Visualforce and Apex pages. Remove pages that you don't want guest users to access.
- The following Salesforce-provided Visualforce pages are added by default to the guest user profile to provide common services, such as authentication flows or site maintenance.
 - BandwidthExceeded
 - CommunitiesLanding
 - CommunitiesLogin
 - CommunitiesSelfReg
 - CommunitiesSelfRegConfirm
 - CommunitiesTemplate
 - Exception
 - FileNotFound
 - ForgotPassword
 - ForgotPasswordConfirm
 - InMaintenance
 - SiteLogin
 - SiteRegister
 - SiteRegisterConfirm
 - UnderConstruction
- If your site doesn't offer self-registration, remove these self-registration pages from your guest profile:
 - CommunitiesSelfReg
 - CommunitiesSelfRegConfirm
 - SiteRegister
 - SiteRegisterConfirm
- Remove all other Visualforce pages unless they're needed to support specific business processes (ISV app, custom app).
- Restrict Apex classes for guest users. Allow Apex class access only for REST or SOAP API use. Apex classes that serve as Visualforce controllers don't need explicit access.
- In Apex class and subclass code, look for record updates or queries that don't check field-level security or object permissions or are in "without sharing" classes. Keep Apex and subclass code that runs without sharing or bypasses field-level security and object permissions to a minimum.
- If guest users can execute [Aura-enabled Apex controllers](#), such as a custom Lightning component, always use the "with sharing" keyword.

Data Category Settings

- If you have Classic Knowledge implemented in your org, check data category settings to ensure that guest users can access all the Salesforce Knowledge categories that you want them to.

Field-Level Security

- Review the field-level security of objects that guest users can access to ensure that they have access to the correct fields.
- Remove field-level access to fields that you don't want guest users to see.

Configure the Site Guest User Record

Each time a community or portal is created, Salesforce creates a guest user profile and a site guest user record. The site guest user record is the only user record associated with the guest user profile. It works like other user records in Salesforce, so you can add it to assignment rules, queues, public groups, manual sharing, and permission sets.

1. In the [guest user profile](#), click **Assigned Users**.
2. In the Full Name column, click the site guest user record link.
3. Make your changes, and click **Save**.

Best Practices and Considerations When Working with the Site User Record

Keep these best practices and considerations in mind when configuring the site user record.

EDITIONS

Available in: **Essentials**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

USER PERMISSIONS

To access Community Workspaces or Community Builder:

- Create and Set Up Communities

AND

Is a member of the community

To edit app and system permissions in profiles:

- Manage Profiles and Permission Sets

To edit object and field permissions in profiles:

- Manage Profiles and Permission Sets

AND

Customize Application

Best Practices and Considerations When Working with the Site User Record

Keep these best practices and considerations in mind when configuring the site user record.

General Best Practices and Considerations

- Enforce authentication where possible, and lock down access to the site guest user.

Record Ownership

- The site guest user must never own records.

EDITIONS

Available in: **Essentials**, **Enterprise**, **Performance**, **Unlimited**, and **Developer** Editions

- When a guest user creates a record, such as a case via web-to-case or a record created via a flow, the site guest user is the record owner. If the record owner isn't changed, anyone who has guest access to your community or portal can see the record. To remove the site guest user as the owner's record:
 - Set up your processes, flows, and Apex triggers to automatically change the record owner to a user or queue within your org.
 - For cases and leads, rather than processes, flows, and Apex triggers, you can set up assignment rules to change the record owner to a user or queue in your org.
 - Depending on your use case, you could set up one queue or several queues, for example, one queue for leads and another for cases.
- In some use cases, you might need to give Read access to guest users to newly created records (such as ideas created by guest users in a community).
 - Create a public group that includes only a community's guest user (one guest user per public group).
 - Create a criteria-based sharing rule on the object, and assign the rule to the public group previously created.

Sharing Settings

 **Important:** External org-wide defaults apply to guest users and authenticated users in a community or portal.

- Review your external org-wide defaults on all standard and custom objects and keep them private if possible.
- Set external org-wide defaults to private, and open up access with sharing rules.
 - Create one public group, and add the site guest user (repeat for each site guest user record).
 - Create a criteria-based sharing rule and assign it to the public group associated to the guest user.
- Never share data with guest users with owner-based sharing rules.
- Never add the site guest user to queues. If a guest user is part of a queue, you could accidentally grant visibility into records owned by the queue.
- Never add guest users to a public group other than one created for the sole purpose of driving guest user record visibility.
- Create a trigger or process that disables manual sharing for guest users.

SEO Best Practices and Considerations for Guest Users

To help end users discover publicly accessible content in your community through search engines, Salesforce provides you with several tools for search engine optimization (SEO). For Lightning communities, Salesforce generates a sitemap with a list of the publicly accessible pages based on the data that you made available to guest users through Community Builder and object access on the guest user profile. For communities built with Salesforce Tabs + Visualforce, customers are responsible for creating the sitemap and indicating which pages are included.

Lightning Communities

- To control which objects are included in your sitemap, whenever possible use generic object pages rather than creating specific object pages.
- Use Community Builder to review which objects and records are available to the guest user profile and therefore included in your sitemap.
- Use robots.txt for more control over which data is available for search engines to index when they crawl your community.
- Submit your sitemap to search engines, such as Google Search Console, only after completing the previous steps.

Salesforce Tabs + Visualforce Communities

- In your sitemap, include only publicly accessible Visualforce pages and objects that you want discoverable by search engines.
- Use robots.txt for more control over which data is available for search engines to index when they crawl your community.
- Submit your sitemap to search engines, such as Google Search Console, only after completing the previous steps.



Note:

- The generation of your sitemap.xml file is limited to production environments. The file isn't created in sandbox.
- All standard and object pages that require authentication as part of a publicly accessible community aren't included in the sitemap file and therefore aren't exposed to search engines for indexing.

SEE ALSO:

[Create a Custom robots.txt File for Your Community](#)

[Best Practices for Using SEO in Your Community](#)

Community User Visibility Best Practices for Guest Users

Community and guest users often need to see one another in a public setting, especially when you implement a public forum, such as a self-service community, or build a public-facing app, such as ideas. Keep these guest user visibility best practices and considerations in mind when setting up your public-facing forum or site.

- Protect the identity of your most active users by hiding the Knowledgeable Users and Reputation Leaderboard components using audience targeting in Community Builder.
- Never use the View All Users permission to give guest users visibility to other users.
- The Community User Visibility setting in Sharing Settings is org-wide. Never use this setting to grant visibility to other users.
- To give user visibility to community users, enable **See other members of this community** on a [community-by-community basis](#).
- If your community or forum needs to remain private, don't use the Community User Visibility setting. This setting shows authenticated users to guest users. Instead, use sharing rules or sharing sets on the user record to open up user visibility where needed.
- Consider using nicknames to protect the identity of your community members.
- Review the user profile page layout, and restrict exposed fields to a minimum.

Control Public Access to Your Lightning Community with Community Builder

Set the public access level to your Lightning community, and set page-specific access to your community pages.

If you allow public access, your community pages are accessible to the public, including unlicensed users. If don't allow public access, members must log in to access the community.

1. To enable public access in a Lightning Community, open Community Builder.
 - From the All Communities page in Setup, click **Builder** next to the community name.
 - From a community, click **Community Builder** in the profile menu.
2. Click **Settings**.
3. Select **Public can access the community**.

EDITIONS

Available in: Salesforce Classic (not available in all orgs) and Lightning Experience

Available in: **Enterprise, Performance, Unlimited,** and **Developer** Editions

USER PERMISSIONS

To create, customize, or publish a community:

- Create and Set Up Communities AND View Setup and Configuration

Settings

General

Theme

Languages

CMS Connect

Advanced

Security

Developer

Updates

General

View and edit the main properties of your community.

Community Details

Community Template

Customer Service

Public Access ⓘ

☐ Public can access the community

Community Title

Guest Portal

Published Status

Not published

You can also set page-level access to specific Lightning community or portal pages in Page Properties.

Community Default Setting

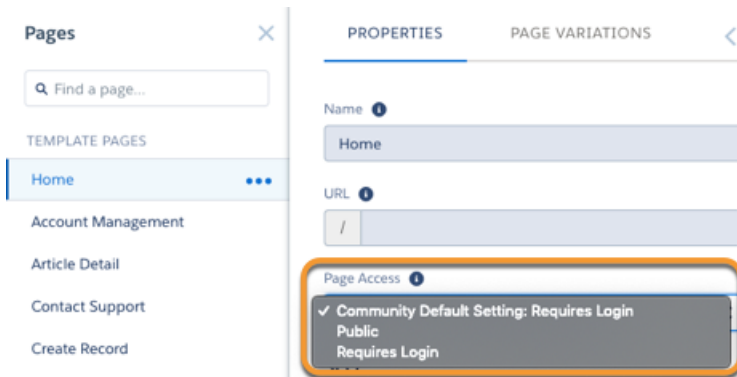
Reflects your choice for public access under General Settings.

Public

Makes the page public regardless of the community's default setting.

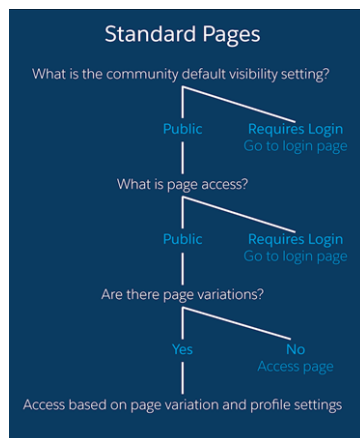
Requires Login

Makes the page private and requires members to log in, regardless of the community's default setting.

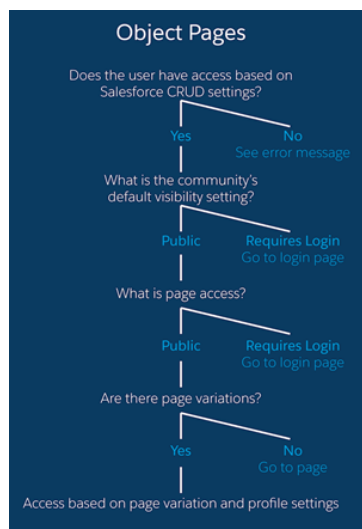


How do these settings work with [audience criteria-based page visibility in Community Builder](#)? When a member is trying to access a page, Salesforce first checks the community's default setting. Is it public or does it require users to log in? Then Salesforce looks at the page access. When that's cleared, Salesforce checks that the audience criteria-based visibility that you set in Page Variations.

How does this logic work for standard pages?



And what's the logic behind pages that show object data?



You can also set privacy settings for some components, such as the Tabs and the Navigation Menu components. To make a component on a public page visible to guest users, select **Publicly available** in the component's properties.



Important:

- Regardless of the settings, some pages are always public, and others are always private. Public pages include login-related pages (Login, Register, Forgot Password, Login Error, Check Password). The Messages page for direct messages is always private.
- If public access is enabled in Community Builder at the page or community level, the **Let guest users view asset files on public pages** preference is enabled in **Administration > Preferences** in Community Workspaces or Community Management. This preference lets guest users view asset files shared with the community on publicly accessible pages. It remains enabled as long as the page has public access enabled.

[Best Practices and Considerations for Page-Level Access in Community Builder](#)

Community Builder is a powerful tool for keeping your Lightning community or portal secure. Keep these best practices and considerations in mind when working with access levels in Lightning communities.

[Lightning Communities Search Best Practices and Considerations for Guest Users](#)

When setting up your search pages and components for communities and portals, keep these best practices and considerations in mind to keep data secure from guest users.

[Set Up Web-to-Case for Guest Users](#)

When you set up Web-to-Case along with a case quick action, guest users can create a case without having to log in.

Best Practices and Considerations for Page-Level Access in Community Builder

Community Builder is a powerful tool for keeping your Lightning community or portal secure. Keep these best practices and considerations in mind when working with access levels in Lightning communities.

- Don't create object pages for objects that aren't exposed to external users. If you have object pages that aren't being used, delete them.
- Use generic record pages when possible.
- If you set up object pages for authenticated users, test the pages to ensure that guest users can't see them.

Lightning Communities Search Best Practices and Considerations for Guest Users

When setting up your search pages and components for communities and portals, keep these best practices and considerations in mind to keep data secure from guest users.

Search Page

- Review page access settings for the search page to ensure that you want the search page accessed by guest users.
- To limit access to the search page, consider creating a search page variation with a guest audience.

Global Search Results Component

The Global Search Results component is the main component on the Search page in any community. The component allows admins to select the objects shown in search results.

- Guest users only see results on objects they have access to.
- Actual record access for the guest user isn't limited to the objects the admin configures in the Global Search Results component. The guest user can have access to other objects based on org sharing configurations.
- Always check the org's sharing model (including org-wide defaults and sharing rules) to ensure that the guest user doesn't have access to your org's sensitive data.

Search Box Component

- As with the Global Search Results component, the admin sets up which objects to show in searches. However, record access for the guest user isn't limited to the objects the admin configures in the Global Search Box and Global Search for Peer-to-Peer Communities components. The guest user can have access to other objects based on org sharing configurations.
- Always check the org's sharing model (including org-wide defaults and sharing rules) to ensure the guest user doesn't have access to your org's sensitive data.

Set Up Web-to-Case for Guest Users

When you set up Web-to-Case along with a case quick action, guest users can create a case without having to log in.

To let guest users create cases, first create a case page layout for unauthenticated users. This allows you to capture and create basic information that would already be associated with a registered user.



Tip: Assign case field-level security and guest user actions appropriately so guest users have access to what they need but can't see your company private information.

1. From Setup, enter *Web-to-Case* in the *Quick Find* box, then select **Web-to-Case**.
2. Select **Enable Web-to-Case**.
3. To ensure that guest users can log cases through contact support, from Setup, enter *Communities* in the *Quick Find* box, then select **All Communities**.
4. Select **Builder** next to the community you want your guest users to log cases via contact support.
5. Click the drop-down arrow next to your community name and select **Community Management**.
6. On the left-hand panel, click **Administration**.

7. Click **Pages**.
8. Click **Go to Force.com**.
9. On the Sites Detail page, click **Edit**.
10. Enable **Guest Access to the Support API**.
11. Add **NewCase**, or a custom quick action to add cases, to the Selected Quick Actions.
12. Click **Save**.



Note: When using a self-service template, it's unnecessary to set up the other options on the Web-to-Case Settings page.

Object-Specific Security Best Practices for Guest Users

After you configure the guest user profile and the site guest user record, keep object-specific best practices in mind for guest user access.

[Chatter and Discussions Best Practices and Considerations for Guest Users](#)

Turning on Chatter for communities and portals enables discussions among your portal and community users. Keep these best practices and considerations in mind when you're setting up Chatter and discussions.

[Files Best Practices and Considerations for Guest Users](#)

To view a file on a record, community users need access to the record, and record file visibility must allow community users. Files shared with users, Chatter groups, and topics follow the same sharing model as the objects that the files are shared on. Files in Libraries can be exposed to community users, but the community user must be added as a member of the library.

Chatter and Discussions Best Practices and Considerations for Guest Users

Turning on Chatter for communities and portals enables discussions among your portal and community users. Keep these best practices and considerations in mind when you're setting up Chatter and discussions.

General Best Practices

- Check System Permissions in the guest user profile to assign or remove Chatter-specific permissions to guest users.

Groups

- Give only internal and trusted members the ability to create groups. Consider a group creation workflow with an approval process.
- Keep the number of groups to a minimum, and audit your community's groups on a regular basis.
- Keep groups private whenever possible.
- Consider a process on who can manage groups.
- Review the content in the group detail page to make sure it meets your community's content standards.
- Review files that are publicly accessible and associated to groups to make sure that they meet your community's content standards.

User-Generated Content

- Set up [moderation rules](#) for all content created by users.

Topics

- Enforce a minimum access policy for topics.
- Never assign guest users Create Topics or Assign Topics user permissions.
- Carefully choose who can create topics in a community.
- Deselect **Suggest topics in new communities posts** in **Community Workspaces > Administration**.

Enabling API Access to Chatter for Guest Users

The following Lightning and Visualforce pages and components in communities need access to underlying Chatter capabilities to load correctly for guest users. Enabling public access through the guest user profile and the API exposes data for guest users through Chatter in Apex, which is helpful when you're building your own community pages from scratch.

- Case
- Featured Feeds
- Feed
- Group
- Group Detail
- Headline
- Record Information Tabs
- Related Lists
- Reputation
- Search & Post Publisher

To enable access to Chatter functionality, access [Community Workspaces](#) or [Community Management](#).

1. Select **Administration > Preferences**.
2. Select **Give access to public API requests on Chatter**.
3. Click **Save**.


Files Best Practices and Considerations for Guest Users

To view a file on a record, community users need access to the record, and record file visibility must allow community users. Files shared with users, Chatter groups, and topics follow the same sharing model as the objects that the files are shared on. Files in Libraries can be exposed to community users, but the community user must be added as a member of the library.

The logic for sharing files with community users also applies to guest users. If guest users have access to an object, they can have access to files shared with that object if the file visibility allows community users.

Use this community preference to give guest users access to files: Give access to public API requests on Chatter.

- Review permissions for who can create content deliveries and public links to make sure that they align with your business needs.
- Review library membership and permissions to make sure that they meet your business needs.
- You can add both users and public groups as members of a Content Library. Public groups pose a risk of extending access beyond who you want to have access.
 - Review who are library administrators. Admins have the power to add more library members.
 - Don't add a public group to a library unless you know who is in the group and the type of members who will be added in the future.

- Review which [library permissions grant the ability to create content deliveries](#) (the Deliver Content permission).
 - Make sure that unintended files aren't public.
 - [Query ContentAsset](#) to check for the field `isVisibleByExternalUsers`.
 - [Query documents](#) to check for the field `IsPublic`.
 - [Query StaticResource](#) to check whether the `CacheControl` field is set to `Public`.
 - Audit file visibility on records.
 - Export `ContentVersion` to get a list of all files in the org. Export [ContentDocumentLink](#) to see all the records that the files are shared with and what the file visibility is for the share to the record.
-  **Note:** For each file, you see multiple shares, such as one share to the owner and multiple shares to different records. Some rows, such as a share to the owner could have the visibility set to `AllUsers`, but this setting doesn't grant access to community users. Only shares to records that have the visibility set to `AllUsers` mean that community users who have access to that record have access to its related files.

Test Guest User Access in Your Community or Portal

After you've implemented the recommended security settings, take your community or portal on a test drive to see what guest users see.

- Access your community or portal using an incognito window to make sure that you're logged out.
- Browse to each public page to make sure that your guest user has the correct access level.
- Browse to object pages to see what the guest user can see.
- Do a global search in the community for specific records to see a search results page.
- Access the community from a mobile device to see the mobile guest user experience.
- Access direct links to various object detail pages as a guest user to ensure that there's no access.
- Access `[www.domain.com]/[siteprefix]/sitemap.xml` to view what is listed in your community sitemap to guest users. The `sitemap.xml` shows what information is exposed to search engines.