

Guest User Access Report



As of: Summer '21

Authored By: @George Abboud

First Published: 08/07/2019

Last Updated: 08/25/2021

Reviews and Contributions:

@Manish Aggarwal @Yelena Kamyshina

Description:

The Guest User Access Report gives you a visual overview of all objects and permissions that the community guest users have access to. Additionally, it outlines which public groups, if any, the guest user is a part of - which might impact sharing and record visibility

After you install the managed package, you can quickly check your org's data security when it comes to community guest users.

Note: This report can be run for force.com sites and Communities, but not [sites.com](https://www.salesforce.com/sites/) sites.

AppExchange Listing URL

<https://appexchange.salesforce.com/appxListingDetail?listingId=a0N3A00000FR6GaUAL>

Instructions for Use:

1. Install managed package into org with active communities. Select 'Install for Admins Only' during installation.
2. As a System Administrator, navigate to a Lightning App called "GUAR Admin". The app provides a list of all of your Communities and [force.com](https://www.salesforce.com) sites with instructions on how to configure and run the report for each.
 - a. **Grant the Guest User access to the Visualforce page called "guar.guestaccessreport"**, inside the installed package. You can click on the Profile Name in the Guest User Profile Name column of the "GUAR Admin" app. Alternatively, see [Locate the Guest User Profile](#).
 - i. In the Visualforce Page Access section, add the guar.guestaccessreport page to the Enabled Visualforce Pages section.
 - b. **From a private browsing session, or one that you are not logged into the org where the package is installed, navigate to the report link provided in the "Guest User Access Report Link column"**. You must use a private browser or not be logged into the org to ensure you are running the report as Guest User.
 - i. Alternatively, you can construct the url to the report yourself as such: [https://\[communityDomain\]/\[communityPrefix\]/apex/guar__guestaccessreport](https://[communityDomain]/[communityPrefix]/apex/guar__guestaccessreport) where the [communityDomain] is your community's [force.com](https://www.salesforce.com) and [communityPrefix] is the path of your site, if you have one configured, and that is the part that comes after the .com/.

- c. **Optionally Bypass Apex Info Calculations:** If your org has a high volume of apex classes and is not completing, you can pass the url parameter **“bypassApexInfo=true”** to bypass the apex class info calculations. This would prevent the report from displaying the apex info section, so you would have to manually ensure that the guest user profile has access to the proper apex classes they require, and not access to further classes they don't need to have access to.
- d. **Optionally include specific objects by API name:** The report by default shows objects that may be exposing data, if you want to include objects that may not be exposing data necessarily or just are not on the report, you can pass in a url parameter with comma-separated values of object API Names, like this **“includeObjects=Account,Custom_Object_1__c”**, to force include these objects in the report.
- e.
- f. **IMPORTANT:** Once you are finished running the report, revert the changes done for the guest user / public access on your community/communities to revoke access to the “GuestAccessReport” visualforce page.

Screenshots:

IMPORTANT: Remember to immediately revoke public access to this page for all your communities' Guest User profiles once you finish running the reports.

Note: Use this tool to check your security settings after you've read the security updates and recommendations by Salesforce. Ensure you have a good understanding of any upcoming changes and their potential impact. Do not use this tool as your only security check - it is meant to offer some guidance / insights throughout your assessment of your org, but it is NOT a definitive assessment of your org.

It is recommended to run this report before and after activating security updates and making any security modifications in your org, so you can compare impact.

A separate report should be run for each Community Guest user.

For help in using this report or securing your org, please post to the trailblazer community group [Securing Community Cloud](#) using the topic [#SecureMyGuestUser](#)

Have you completed implementing the best practices and resolved any and all impact of these security updates?

Give us the Green Light!

NOTE 1: In the above screenshot, the “Securing Community Cloud” group has been renamed to “Securing Experience Cloud”.

NOTE 2: In the above screenshot, the “Give us the Green Light” button is an optional way to report to Salesforce that you've secured your org and remediated any impact from these security updates. It does not affect the functionality of the report in any way.

Org Community Information:

This section lists all communities in the org and provides a link to run the report for each of the communities.

Report for this Community?	Site Name	Guest User Name	Guest User Profile Name	Run Guest Access Report
☐	Aloha App Launcher	Aloha App Launcher Site Guest User	Aloha App Launcher Profile	Run Report
☐	Partner	Partner Site Guest User	Partner Profile	Run Report
☒	Customer Service - POC 1	Customer Service - POC 1 Site Guest User	Customer Service - POC 1 Profile	Run Report
☐	Customer	Customer Site Guest User	Customer Profile	Run Report
☐	POC 2	POC 2 Site Guest User	POC 2 Profile	Run Report

Report for Community ([GuestTest](#)) with Guest User ([GuestTest Site Guest User](#)). Ran on [Fri Sep 27 20:46:15 GMT 2019](#):

Potential Impact of Security Updates on your org:

Learn More	Security Update	Impact	Details
Release Notes #GuestDefaultOWD-Mar'20	Guest Default OWD Settings (Secure Guest User Record Access setting)	potential risk	The report will attempt to detect one or more objects' records being exposed to the guest user. Review your External OWD sharing settings and avoid Public Read Only and Public Read/Write configuration.
Release Notes #GuestUserSharingRules-Mar'20	Guest User Sharing Rules	potential risk	The report will attempt to detect if the guest user profile has access to one or more objects.
Release Notes #GuestUserVisibility-Winter'20	Guest User Visibility	potential risk	The report will attempt to detect one or more User records being exposed to the guest user.
Release Notes #GuestPermsRetirement-Spring'20	Guest Profile Changes	potential risk	The report will attempt to detect one or more enabled permissions on the Guest user profile that are either being retired or defaulting to false / unchecked.
Release Notes #ViewAllUsers-Mar'20	View All Users	no risk	The report will attempt to detect if the "View All Users" permission on the Guest user profile is enabled and exposing User records to the Guest user. Changes to this permission may impact this configuration.
Release Notes #DefaultRecordOwner-Mar'20	Guest Cannot Own Records	no risk	The report will attempt to detect one or more objects' records that are owned by the Guest user.
Release Notes #AuraEnabledApex-Spring'20	AuraEnabled Apex	potential risk	The report will attempt to detect if there are some AuraEnabled methods in Apex controllers which the Guest User profile does not have access to. If an apex class is part of a managed package, it will be flagged as a risk for review.
Release Notes #SelfRegOnStandardProfiles-Dec'19	Standard Profiles for Self Registration	no risk	The report will attempt to detect if there are any external users assigned a standard (non-custom) profile.

Object Access Information (6):

Object Name	Is Custom?	Is Exposing Data?	Total Number of Records with Access To	Total Number of Records Owned	Total Number of Records due to Manual and/or Apex Sharing	Total Number of Records due to Non-Guest Sharing Rules	Total Number of Records due to Guest Sharing Rules	Profile Read Access?	Profile Create Access?	Profile Edit Access?	Profile Delete Access?	Profile View All Access?	Profile Modify All Access?
account	false	no risk	0	0	0	0	0	potential risk	no risk	no risk	no risk	no risk	no risk
contact	false	no risk	0	0	0	0	0	potential risk	no risk	no risk	no risk	no risk	no risk
custom_object_1__c	true	potential risk - Help me secure this	3	0	1	1	0	potential risk	no risk	no risk	no risk	no risk	no risk
custom_object_2__c	true	potential risk - Help me secure this	3	N/A	N/A	N/A	N/A	potential risk	no risk	no risk	no risk	no risk	no risk
custom_object_3__c	true	no risk	0	0	0	0	0	potential risk	no risk	no risk	no risk	no risk	no risk
custom_object_4__c	true	potential risk - Help me secure this	1	0	0	0	0	potential risk	no risk	no risk	no risk	potential risk	no risk
user	false	potential risk - Help me secure this	16	N/A	0	0	0	no risk	no risk	no risk	no risk	no risk	no risk

Report for Community (Customer Service - POC 1) with Guest User (Customer Service - POC 1 Site Guest User):

Profile Permission Information:

Permission Name	Permission Value
permissionemailsingle	no risk
permissionemailmass	no risk
permissionsedittask	no risk
permissionseditevent	no risk
permissionsexportreport	no risk
permissionsimportpersonal	no risk
permissionsdataexport	no risk
permissionsmanageusers	no risk
permissionseditpublicreports	no risk
permissionseditpublicfilters	no risk
permissionseditpublictemplates	no risk
permissionsmodifyalldata	no risk
permissionsmanagecases	no risk
permissionsmassinlineedit	no risk
permissionseditknowledge	no risk
permissionsmanageknowledge	no risk
permissionsmanagesolutions	no risk
permissionscustomizeapplication	no risk
permissionseditreadonlyfields	no risk
permissionsrunreports	no risk
permissionsviewsetup	no risk
permissionstransferanyentity	no risk
permissionsnewreportbuilder	no risk
permissionsmanagecssusers	no risk
permissionsactivatecontract	no risk
permissionsactivateorder	no risk
permissionsimportleads	no risk
permissionsmanageleads	no risk
permissionstransferanylead	no risk
permissionsviewalldata	no risk
permissionseditpublicdocuments	no risk
permissionsviewencrypteddata	no risk
permissionseditbrandtemplates	no risk
permissionsedithtmltemplates	no risk
permissionschatterinternaluser	no risk
permissionsmanagedashboards	no risk
permissionsmanagettranslation	no risk
permissionsdeleteactivatedcontract	no risk
permissionschatterinviteexternalusers	no risk
permissionsendsitrequests	no risk
permissionsoverrideforecasts	no risk
permissionsviewallforecasts	no risk
permissionsapiuseronly	no risk
permissionsmanageremoteaccess	no risk
permissionscanusenewdashboardbuilder	no risk
permissionsmanagecategories	no risk
permissionsconvertleads	no risk
permissionspasswordneverexpires	potential risk
permissionsuseteamreassignwizards	no risk
permissionseditactivatedorders	no risk
permissionsinstallmultiforce	no risk
permissionspublishmultiforce	no risk
permissionsmanagecontact	no risk

This section lists all the permissions for the Guest User Profile and indicates potential risk (permission enabled) or no risk (permission disabled).

AuraEnabled Apex Profile Permission Information:

Apex Class Name	Apex Class Namespace Prefix	Has AuraEnabled Methods?	Is Accessible by Guest Profile?
AssignMultipleUsersController	trailheadapp	maybe	potential risk
AssignMultipleUsersController_Test	trailheadapp	maybe	potential risk
Badge	trailheadapp	maybe	potential risk
BadgeDedupe	trailheadapp	maybe	potential risk
BadgesComponentController	trailheadapp	maybe	potential risk
BadgesComponentController_Test	trailheadapp	maybe	potential risk
BadgesErrorMock	trailheadapp	maybe	potential risk
BadgesUpsertErrorMock	trailheadapp	maybe	potential risk
Badge_Test	trailheadapp	maybe	potential risk
ChannelManagerProfileController		yes	potential risk
CommunitiesPackageInstall	ca_collab_2_0	maybe	potential risk
CommunitiesPackageInstallTest	ca_collab_2_0	maybe	potential risk
DownloadBadgeIcons	trailheadapp	maybe	potential risk
DownloadBadgeIcons_Test	trailheadapp	maybe	potential risk
DownloadTrailIcons	trailheadapp	maybe	potential risk
DownloadTrailIcons_Test	trailheadapp	maybe	potential risk
FeatureSearchController		yes	potential risk
GuestAccessReportController	guar	maybe	potential risk
GuestAccessReportControllerTest	guar	maybe	potential risk
GuestAccessReportHelperWS	guar	maybe	potential risk
LightningForgotPasswordController		yes	potential risk
LightningLoginFormController		yes	potential risk
LightningSelfRegisterController		yes	potential risk
Logger	trailheadapp	maybe	potential risk
Logger_Test	trailheadapp	maybe	potential risk
LoginCalloutExceptionMock	trailheadapp	maybe	potential risk

Release Log

V3.16

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002KmrB>

Notes:

- Added the Event, Task, and EventRelation objects to display as part of the report
- Added the ability to optionally pass in object API names (comma separated) to include in the report: Example:
guar__guestaccessreport?includeObjects=Account,Custom_Object_1__c

V3.14 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002XFK9>

Notes:

- Removed green light flow
- Added help me secure this disclaimer
- Added apex info bypass to bypass apex info calculations in the report for orgs that have high volumes of apex classes

V3.13 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002XFJu>

Notes:

- Added section to show permission set / permission set group assignments, and some copy text updates (same code as V3.12)

V3.12 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002utoX>

Notes:

- Added section to show permission set / permission set group assignments, and some copy text updates

V3.11 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002utoS>

Notes:

- Fix for issue while getting share counts for big objects that do not support aggregate functions

V3.8 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002maik>

Notes:

- Fix for errors when querying a large volume of apex classes. Capped at < 11K classes.

V3.7 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002macW>

Notes:

- XHR Timeouts error handling fix

V3.6 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002maNn>

Notes:

- XHR Timeouts error handling
- Added instructions for profile permission updates

V3.5 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002maMp>

Notes:

- Fixed issue in GUAR Admin app in construction of report url

V3.4 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002maMV>

Notes:

- Fixed issue in GUAR Admin app in construction of report url

V3.3 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000002maMQ>

Notes:

- Fixed issue with guest user name / profile not populating for force.com sites.
- Fixed issue with force.com sites not displaying in the table of communities.
- Added a LEX app “GUAR Admin” to help construct the URL for the report for each site, with links to guest user profiles to grant/revoke access to the VF page for the report.

V3.0 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000A5qz>

Notes:

- Fixes to address orgs with higher number of Objects / Apex Classes that were causing Apex CPU Limits
- Support for up to 1000 Objects, thousands of Apex Classes
- Added spinner overlay with progress logs to allow for asynchronous calls to complete.

V2.6 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000A5e3>

Notes:

- Added count for total records shared by ownership vs total records owned
- Updated AuraEnabled-related yellow potential risk legend
- Added display of package version on report
- Updated user flow parameters

V2.3 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000A5QD>

Notes:

- Bug fix for guest sharing rule counts

V2.2 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000A5PU>

Notes:

- Removed the Community feature requirement for installing the package.

V2.1 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000A5Oq>

Notes:

- Resolved Apex List limitation of 1000 records for large volumes.

V2.0 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000A5OI>

Notes:

- Updated copy text at the top of the report
- Added links to trailblazer group and topic
- Added Green Light Flow for customers to notify Salesforce of addressing all impact of security updates in their production orgs and adhering to best practices
- Added Legend section to explain color-coding
- Added timestamp on report
- Added section for impact of security updates
- Under object access information section, added columns for manual/apex sharing counts, non-guest user rule share counts, guest user rule share counts
- Under object access information section, added “help me secure this” link to step-by-step flows for helping users secure specific object configurations in their org
- Added AuraEnabled apex class section to show impact of AuraEnabled apex class access check enforcement security update

V1.8 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000A5GH>

Notes:

- Re-ordered sections: Object Access, Public Groups, Profile Permissions
- Under Object Access, re-arranged columns. Is Exposing data moved up for more visibility.
- Under Object Access, added a count of total number of records with manual share.
- Under Public Groups, added “Groups / Queues” and a “type” column to show regular group vs queue.

V1.2 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000yC3I>

Notes:

- Minor visual/cosmetic tweaks for when counts are 0

V1.1 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000yBqp>

Notes:

- Updated bug with “Run Report” link to include namespace for visualforce page

V1.0 (DEPRECATED)

URL: <https://login.salesforce.com/packaging/installPackage.apexp?p0=04t4P000000xhJs>

Notes:

Initial Release