Downloads and Security

Customer Documents Documentation

Guide for Magento administrators, technical project owners, and implementation teams.

LAST UPDATED
2026-10-13

SOURCE
Open this article online

EXTENSION
Magento 2 Extension Customer Documents

Downloads and Security

Customer Documents serves local files through controlled download actions and redirects eligible external documents only after validation. Avoid linking directly to files in the media directory.

Local files

The configured upload path sits below `pub/media`. Allow only the file types the business needs and set a sensible upload-size limit. Web-server and PHP limits still apply.

Protect the upload folder from direct public browsing in the web-server configuration. A copied media URL should not bypass Customer Documents access checks.

External documents

External URLs are useful when files live in an approved document service. Configure **Allowed External Domains** with the exact trusted hostnames. An empty allowlist permits every domain, so it should not be used for a controlled production setup.

Only HTTP and HTTPS links should be used. The extension validates the external host before saving or redirecting.

Checks performed for a download

- customer or public access
- website scope
- validity dates
- password, when present
- download allowance
- local file availability or approved external destination

A failed check does not provide a valid file response. Successful downloads are recorded for reporting, and counters are updated only after an allowed response is prepared.

Download rate limit

The download endpoint allows five successful downloads per document and hour. The counter is tracked per document for each signed-in customer; guests are tracked by a hashed IP address. Once the limit is reached, further attempts return "Download limit exceeded. Please try again later." until the one-hour window expires.

Only requests that actually serve a file or an approved redirect count against the limit. The limit is fixed and cannot be configured; it applies on top of the separate per-document **Max. Downloads** allowance.

Signed download links

The `downloadCustomerDocument` GraphQL mutation returns a signed download URL that is valid for 30 minutes and works without a customer session — anyone holding the link can use it within that window. See GraphQL.

Download Report

Every recorded download appears under **Customers > Customer Documents > Download Report** with the document, customer, time and result. Use the grid to audit who downloaded a sensitive file. Its **Delete** mass action removes report rows — deleting a report row never touches the document itself.

Filenames

Enable **Obscure Filename** when customers should not receive the stored filename. This reduces accidental information exposure in downloaded filenames but does not replace access control.

Bulk downloads

ZIP downloads exclude password-protected and external documents. See ZIP Downloads.

For sensitive files, combine a private audience with a short validity period and, where appropriate, a password or download limit. Test the complete path using a customer account rather than only an administrator session.