Magento
An Adobe Company

Magento Open Source 1 – Formerly Community Edition – End of Software Support FAQ

The following FAQ is intended to help merchants, developers, and partners understand the implications of Magento's published End of Support date for all versions of Magento Open Source.

GENERAL

Q. Where can I find the software support dates for all versions of Magento Open Source?
Magento publishes its software lifecycle policy, which contain the dates for software support: https://magento.com/sites/default/files/magento-open-source-software-maintenance-policy.pdf

Q. What does it mean when support ends for a version of Magento Open Source software?
When Magento ends the support for Magento Open Source software, you can expect the following:

- Magento will cease creating further product changes, including functional, quality, security, and PCI compliance updates.
- Community pull requests will no longer be accepted or merged for said version.
- Extensions in the Magento Marketplace compatible only with unsupported versions of Magento Open Source will be removed.
- Documentation for the unsupported versions will be removed from magento.com, e.g. Dev Docs materials.

Q. What are the implications to merchants for using unsupported Magento Open Source software?
If you continue to use unsupported Magento Open Source software, you'll likely see negative impacts including – but not limited to – the following areas:

Providing Secure, Differentiated Shopping Experiences

Once a version of Magento Open Source software is no longer supported, it falls out of PCI compliance (https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard) and it's your responsibility to re-certify compliance. You may be subject to fines or removal of credit card processing ability if you're unable to update vulnerabilities from regular scans and penetration testing.

- General security vulnerabilities tend to increase the longer software remains unsupported as hackers apply new exploitation technologies and techniques. This raises the risk of attacks and security breaches over time, increasing the possibility of exposing personally-identifiable customer data.

- There exists a tangible risk to your brand and business if your site is perceived to be insecure, eroding the trust you've grown with your customers.

- In the event of a personal information data breach, merchants may be required to notify their customers while facing potential fines and penalties.

Operating Efficiently and Effectively

- Merchants who continue using unsupported versions of Magento Open Source software will need to allocate resources towards evaluating and employing third-party vendors who can enable security support, fixes, and updates. Furthermore, the merchant – or their security provider – will need to monitor continuously for ongoing security risks and related issues.

- As unsupported versions of Magento Open Source software age, the developer and partner pool providing support for outdated versions will diminish as they align towards newer technologies. Overall, qualified resources for software maintenance decrease, while the cost to maintain the software increases.

    - Note on Magento 1: Development on the Magento Open Source platform is a legacy skill and is becoming rarer – and often pricier – as a larger percentage of the Magento community shifts to Magento 2 development. For partners and developers, it's difficult to sustain legacy platform developers for only security maintenance.

- For Magento Open Source software, peripheral technologies and dependencies also reach their own end of life cycle such as PHP, MYSQL, REDIS, and SOLR. This makes it increasingly difficult – and sometimes impossible – to manage and maintain a fully secure and compliant site using unsupported versions of Magento Open Source.

- Extension developers also increasingly focusing their efforts on the latest technologies and compatible platforms. As a result, it's unclear whether the extensions themselves will be supported in the future if they break or become a security risk.

- Using unsupported versions of Magento Open Source software often leads to spending more money and resources maintaining a dated platform instead of applying those resources towards continued business innovation and growth.

Growing Aggressively

- Magento continues investing in new technologies and capabilities. By continuing to use older, unsupported software versions, you're unable to take advantage of newer features which could enable strategic advantages for your business, allowing it to grow faster.

Q; How can I move to a current and supported version of Magento Software?

As a Magento Open Source merchant, you already know about the power of the Magento platform and ecosystem. However, upgrading to Magento Commerce 2 not only provides additional customer and software support, but also provides your business many advantages, including:

- Improved Sales – boost conversions with quick two-step checkout, responsive themes, and virtually limitless marketplace of certified third-party add-ons.

- Streamlined Operations – work efficiently and reduce development time with enterprise-grade business intelligence, drag-and drop content creation with page builder, and resilient architecture for improved code quality.

- Peace of mind – A modern, cloud-based infrastructure optimizes performance and scales with your business while keeping data secure.

Yes, you do have the option to update your software and move to Magento Open Source 2, but you would be missing all the powerful features available through Magento Commerce 2.

Q. What should I do to avoid software end of support issues?
Your commerce platform is an essential business system and keeping its functionality current is an important, ongoing investment. While there are always ways to stretch the budget for your digital storefront, there's no excuse to cut corners on back end technology and security. Staying on the latest platform version is critical, helping you avoid complications associated with end of software support.

- **Migrate Ahead of Time**
  Plan your migration to the latest version of Magento Commerce or Magento Open Source as far ahead of the end of support date as possible. This will ensure you have adequate time and resources available to achieve strategic goals on-schedule while staying within your budget.

- **Book Your Talent**
  Another important consideration is to reserve developer and partner resources as early as possible since they're frequently booked up well ahead of the end of support date. This can result in significantly fewer alternative resources to assist with migration projects. Plan early to avoid scrambling for assistance at the last minute.

Q. Can I use a 3rd party service provider to provide software support?
Yes, you can look for security firms, developers, or partners who will provide support for Magento Open Source. It will be the merchant's responsibility to evaluate these providers, re-certify compliance as necessary, and identify and resolve on-going security threats which may impact their business and customers.

Q. Can Magento recommend a 3rd party service provider for extended support beyond the end of support date?
No, Magento does not recommend or endorse any providers for software support beyond our end of support date.

Q. Does a software version "shut down" when it reaches and passes its end of support date?
No, Magento Commerce or Magento Open Source software doesn't "shut down" once the end of support date is reached or passed. However, you will shoulder additional responsibility for PCI compliance re-certification and unable to update vulnerabilities uncovered by regular scans and penetration testing. This could potentially create liability for security breaches linked to the unsupported versions. Additionally, you will no longer receive security patches or upgrades which protect your digital storefront from bad actors on the internet.

Updated September 2019