Frequently asked questions for Sage 100 and Sage 300 customers

Online encryption security enhancements

Sage 100 and Sage 300 upgrade requirements

Overview:

Effective September 2023, Sage servers will stop accepting communication from Sage 100 and Sage 300 product versions using Transport Layer Security (TLS) 1.0 and 1.1.

TLS is a security protocol that creates encryption paths over computer networks to help ensure that online communications and information cannot be intercepted. Regulatory standards have increasingly required the adoption of TLS 1.2 and the subsequent deprecation of TLS 1.0 and 1.1 due to known security risks.

Any subscription customer on product versions using TLS 1.0 and 1.1 will require an upgrade to their Sage 100 and Sage 300 software to prevent a disruption in the use of their software.

If a customer does not upgrade their software by September 2023, they will begin receiving warning messages when accessing Sage 100 and Sage 300 due to the inability to communicate with Sage servers. The software will revert to read-only mode and restrict access.

We encourage all customers to remain on current software versions to ensure that you realize the full benefits from enhancements and updates, as well as to help prevent disruptions that may result from mandatory security updates.

1. **Q. What is Transport Layer Security (TLS)?**
   TLS is a security protocol that creates encryption paths over computer networks to help ensure that online communications cannot be intercepted.

2. **Q. What is a security protocol?**
   Security protocols are a set of operations or steps that occur when data is delivered or exchanged between parties (e.g., when sending an email, processing a credit card transaction, or when any data is shared between a web browser and website). Security protocols help protect the communication and shared data.

3. **Q. How does TLS work?**
   TLS uses security techniques to ensure that parties involved in an online communication are authenticated as the intended recipient, it protects the data being transferred, and encrypts the communication thereby protecting it from a breach.

Last update: August 12, 2022

DSD BUSINESS SYSTEMS

4. **Q. Why is an upgrade to TLS 1.2 important?**
   TLS 1.0 and 1.1 were replaced by TLS 1.2 starting in 2008 to provide improved data security and better protection for customer and application information communicated over the internet. Many companies and standards (e.g., HIPAA, PCI) require the use of TLS 1.2, as do many Sage ISVs. This move to TLS 1.2 will provide increased data protection and decreased risk for our customers and partners.

5. **Q. When was the requirement to upgrade to TLS 1.2 announced?**
   Since its launch in 2008, companies and regulatory standards have increasingly required adoption of TLS 1.2. Sage 100 and 300 began supporting the latest standard in our products several years ago, including announcements in product release notes and updates. However, until recently, Sage had not announced a mandatory upgrade.

6. **Q. Why is Sage informing Sage 100 and Sage 300 customers that an upgrade to a product using TLS 1.2 is required if this is already addressed in the product?**
   Many customers are on older product versions where TLS 1.2 is not used. Sage implemented support of TLS 1.2 in Sage 100 and Sage 300 starting with version 2019. Customers automatically adopt the new standard as part of their update to any recent Sage 100 and Sage 300 version. We are notifying customers now to help ensure they will have adequate time to upgrade before Sage stops supporting the old security protocol come September 2023.

7. **Q. What is required to prevent a software disruption?**
   Subscription customers will be required to be on a version that utilizes TLS 1.2. For Sage 100 this means 2019.4, 2020.1 and newer versions. For Sage 300 this is 2019.6, 2020.3 and newer versions. Customers not on one of these recent releases, must upgrade to a version that utilizes TLS 1.2.

8. **Q. How long will it take to update or upgrade to support TLS 1.2?**
   Upgrade time varies by customer and depends on several factors. Some customers will be able to apply product updates (PU's), while others will need to perform a full upgrade as they would when moving to any new product version.

   For customers that may also require a hardware upgrade, use of our hosted Sage Partner Cloud program may reduce or eliminate the need for a hardware investment. Contact your Sage Business Partner for more information.

   If your Sage Business Partner is unable to assist you or you don't have a partner, for Sage 100 contact Sage Expert Services at Sage100.expertservices@sage.com and Sage300.experservices@sage.com for Sage 300.

9. **Q. What will happen if an upgrade to TLS 1.2 is not completed?**
   For customers on subscription, the software will be unable to acquire an updated expiration date from our servers and will initiate subscription warning messages. If not addressed, the software will revert to read-only mode and restrict access after a grace period of approximately 45 days.

10. **Q. When will an upgrade to a version higher than TLS 1.2 be required (i.e., TLS 1.3)?**
    TLS 1.3 has not been implemented in our Sage 100 and Sage 300 products, and our internal systems do not require its use. While we do not have specific plans yet, partners and customers

Sage DSD BUSINESS SYSTEMS

will be notified once we update our software to support TLS 1.3 and notified well in advance of any required upgrade.

11. **Q. How can I determine if my system needs to be upgraded?**
    TLS 1.2 is already included in current and supported versions of our software. If you are not on one of the versions using TLS 1.2, you will need to upgrade.

    For Sage 100, you must be on 2019.4, 2020.1 or a more current version.

    For Sage 300, you must be on at least 2019.6, 2020.3 or a more current version.

    To identify what version of Sage 100 you are running, access Help from the menu bar and select About. The major release will be displayed. For Sage 300, select System Info.

    For Sage 100, the product update will be listed as part of the version number. For example, version 7.00.4.0 would mean you are using product update (PU) 4.

12. **Q. Does this impact third-party products that integrate with my Sage ERP?**
    Each ISV will use TLS differently and have their own support policies. It is best to check with each of the vendors you use to determine if their products are impacted and if any updates are required.

13. **Q. Do customers have any other options if they cannot upgrade?**
    The necessity to upgrade to TLS 1.2 is a requirement that has impacted many industries. Security has been increased in TLS 1.2 to help prevent personal information from being breached. It is important to discuss the options provided by Sage with your Sage Business Partner. If you do not have a business partner, please contact Sage directly for assistance.

14. **Q. Will subscription and annual maintenance and support (M&S) plan customers be impacted differently?**
    Yes. Customers not on a subscription plan may not experience a direct impact to software services but are highly encouraged to upgrade to a current version of Sage 100 and Sage 300 that supports TLS 1.2 to help mitigate vulnerabilities presented in the continued use of TLS 1.0 and 1.1.

    Subscription customers will be impacted as outlined in the Overview section. Please note that Sage 100 payroll and Sage 300 payroll are only available as a subscription and therefore are impacted even if your ERP is a perpetual/M&S plan.

15. **Q. What should I do if I do not have a Sage Business Partner, or my partner is not responding?**
    For Sage 100, please email our Sage Expert Services team for assistance at Sage100.expertservices@sage.com or call 1-888-721-8989.

    For Sage 300, please email our Sage Expert Services team for assistance at Sage300.expertservices@sage.com or call 1-877-336-4038.

Next Steps

Sage DSD BUSINESS SYSTEMS

- Check your software to determine what version you are on.
- Contact your Sage Business Partner to upgrade to a version that uses TLS 1.2.

Current product versions

- **Sage 100 versions 2022 - 2020**
- **Sage 300 versions 2022 - 2020**
    - Version 2023.0 of Sage 300 is planned to be available September 2022. Upon the release of 2023.0, customers are encouraged to upgrade to versions 2023 - 2021.