FAQs for Sage 100

The Deprecation of TLS 1.0 & 1.1 AND Microsoft Basic Authentication

How your Sage 100 software may be impacted.

Items Covered in This Document:

1. The Deprecation of TLS 1.0 and TLS 1.1

Effective September 1st, 2023

Q. What is TLS 1.0 and TLS 1.1?

A. TLS (Transport Layer Security) is a security protocol that enables privacy and data security for internet-based communications. TLS plays a crucial role in preventing data breaches arising from insecure web applications by encrypting communications between web applications and servers.

TLSv1.0 and 1.1 were released in 1996 and 2006, respectively, so it is no surprise that they have reached end-of-life status. Neither protocol supports modern cryptographic algorithms, and both unnecessarily increase the attack surface and the opportunities for misconfiguration.

Q. Where is TLS 1.0 and TLS 1.1 used within Sage 100?

A. TLS 1.0 and TLS 1.1 is used to connect Sage's Subscription Server with Sage 100 Instances to ensure that their version of Sage is licensed properly. That connection leverages a TLS connection with older Sage versions using TLS 1.0 and 1.1 and newer Sage versions using TLS 1.2+.

Q. What version do I need to be on to ensure I'm not leveraging a less secure TLS 1.0/TLS 1.1 version?

A. All subscription customers must upgrade to a current supported version of Sage 100 (2020, 2021, 2022).

Q. How can I determine which version of Sage 100 I have installed?

A. Please see instructions on pg. 3

Q. I am on a perpetual license. Am I affected?

A. Perpetual licenses are not affected.

Q. Does it matter if I am deployed in a hosted environment, or deployed on my local servers?

A. The TLS Deprecation issue is not dependent on the deployment model.

Q. What will happen on September 1st, 2023, if my Sage 100 version is not at the supported version releases of 2020.5, 2021.4 or 2022.1?

A. Your Sage 100 instance will attempt to connect with the Sage Subscription Server to validate your license. If it is unable to connect due to being on an older version, your Sage 100 instance will give a 45-day countdown warning. After 45 days, your Sage 100 instance will be read-only until your Sage 100 is upgraded.

Q. Is there any chance the effective date of September 1, 2023 will change?

A. Based off the recommendations from the Sage Data Security Team, the September 1, 2023 date is firm.

Q. Are other solutions affected by the TLS 1.0 and TLS 1.1 deprecation?

A. Many solutions have made it mandatory to transition off TLS 1.0 and TLS 1.1 already. The ones that have NOT transitioned off TLS 1.0/1.1 will be doing it shortly, like the Avalara connector between Sage 100 and Avalara. Most credit card processors have moved off TLS 1.0/TLS 1.1 due to the extreme sensitivity with credit card data.

2. The Deprecation of Microsoft Basic Authentication

As Early as January 1st, 2023

Q. Why is Microsoft deprecating Microsoft Basic Authentication?

A. Microsoft Basic Authentication is an outdated industry standard protocol where an application sends a username and password with every request, and often, that username/password is stored or saved on a device. It is simple to setup, but is easier for hackers to capture user credentials, which increases the risk of those stolen credentials being reused. Furthermore, enforcement of multifactor authentication (MFA) is not simple or in some cases, not possible when Basic Authentication is being used. Because of the high security risk, Microsoft is deprecating Microsoft Basic Authentication and recommending using more secure protocols, like oAuth.

Q. Is Sage 100 the only application affected?

A. No. Many of our customers will see the biggest change coming from any email client. For example, Basic authentication will be disabled in Exchange Online for Exchange, POP, and Outlook. In other words, every email user may be affected if they are using older email clients or if Basic Authentication is

still being used.

Q. How does this affect Sage 100?

A. With Sage 100, the most predominant place where Basic Authentication is used is with Paperless Office, where emails are leveraged for document automation.

Q. If I use Sage 100 and send automated emails via Paperless, how do I know if I am affected?

A. If you are using a version of Sage 100 older than 2020, Basic Authentication is the only way Sage 100 sends emails. If you are on Sage 100 2020 or newer with that versions recent Product Update release, Basic Authentication MUST be turned off and a more secure method must be used (i.e. oAuth). This affects users who leverage Microsoft based email systems for sending emails.

Q. What happens if I use a Microsoft Email system (i.e., Exchange, Office 365) and my Sage 100 attempts to send emails via Paperless Office and I am still using Basic Authentication after the depreciation?

A. Your Sage 100 solution will try to connect to the Microsoft Email system and since Microsoft no longer supports Basic Authentication, the connection will not work. Automated emails will fail and not be sent out, unless processed manually through a supported email client.

Q. What type of functionality does Paperless Office provide that I should look for?

A. Paperless Office's email functionality is normally used by our clients who want automated emails with attachments to go out to their vendors or customers. The most common use case consists of invoices or statements that get automatically sent to customers. Other use cases include Purchase Orders that go out to vendors, or custom documents that go out to any recipient leveraging Paperless Office.

Q. If I am on Sage 100 2020, 2021, or 2022, am I safe?

A. Not necessarily. It is also imperative you are on the right Product Update ("PU"). Version 2020 must be on PU5. Version 2021 must be on PU4 and v2022 must be on PU1. Furthermore, Basic Authentication cannot be used as successful authentication to the email server will require oAuth or use of other supported protocols. oAuth must be configured by your IT (we can also help) and requires the configuration of tokens.

Q. I don't have an IT department. Can Blytheco help with the oAuth configuration?

A. Blytheco has resources that can help on an hourly project basis, though we recommend leveraging your IT team who has configured your company email.

Q. If I am on a perpetual license, and not subscription, am I affected?

A. Yes, all license types are affected.

Q. If I am deployed on my servers, or hosted with a hosting provider (i.e., blyCloud), does that change anything?

A. No, deployment methods do not change who is affected.

Q. Do I need to upgrade to a supported version of Sage 100?

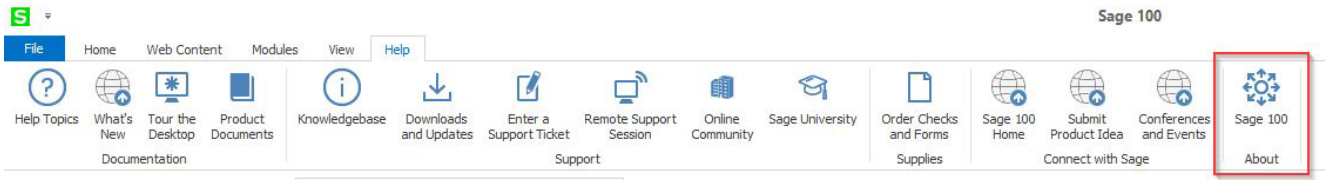
A. Yes. It is highly recommended that all customers upgrade to 2022 to avoid heightened security risks and/or business and process disruption.

Q. How can I learn more about the Basic Authentication deprecation?

A. Microsoft has published multiple articles, including the following - https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/deprecation-of-basic-authentication-exchange-online

Q. How can I determine which version of Sage 100 I have installed?

A. Select Help menu from the Sage 100 Launcher and locate the Sage 100 About and the version is listed first in the About window.



Note: If you are unable to find this option, please go to the Library Master module and select the Reports menu and launch the Installed Module Listing task. This report will show all modules and the version of the Sage 100 software.

Q. How do I tell if I am using Paperless Office and Microsoft Basic Authentication?

A. Select Library Master module and from the Main menu select Company Maintenance. From the Email tab, locate the SMTP (Mail) Server section and confirm if any of the following email domains are listed in the Address field: office.com, outlook.com or microsoft.com. If the above domains are listed and your Sage 100 version is 2020 (6.20) or prior then your system will be impacted.

3. SAGE 100 Versions and Upgrades

Q. How can I determine which version of Sage 100 I have installed?

A. Please see instructions on pg. 3

Q. If I need additional help understanding if I am affected, what do I do?

A. Please contact the Sage 100 Upgrade Team at Sage100Upgrade@Blytheco.com. As a free service, one of our experts will help walk you through understanding if you are affected or not.

Q. What is the cost of upgrading my instance?

A. The cost of upgrading is based on a various factors including database size, number of companies, modules, 3rd party solutions and any customizations. Blytheco's team can collaborate with you to provide a quote.

Q. How long does it take to perform an upgrade?

A. Most upgrades can be scheduled and completed in 1-2 months. As we get closer to the deprecation effective date, we expect to be engaging on a higher volume of upgrades, which can impact our ability time to complete yours safely within the deadline. We highly recommend scheduling an upgrade as soon as possible.

Q. What is required to configure the Microsoft email service for the new OAuth SMTP Server settings?

A. Blytheco can provide professional services to complete these required configurations.

Sage 100 Paperless Office Email configuration will require maintenance as early as January 1st, 2023 for all Sage 100 versions currently using Microsoft Basic Authentication. To avoid automated email interruption for Paperless Office, follow these instructions:

1. Work with your Blytheco consultant to upgrade to Sage 100 v2021 or v2022.
2. Purchase Azure Active Directory Basic or Premium licensing for Office 365 (Premium or Enterprise subscription, details here:

Supported Subscriptions

The following subscriptions are supported for Sage 100cloud integration with Office 365.

Your Microsoft account must include one of these subscriptions:

- Azure Active Directory Basic
- Azure Active Directory Basic (Government Pricing)
- Azure Active Directory Premium P1
- Azure Active Directory Premium P1 (Government Pricing)
- Azure Active Directory Premium P2
- Office 365 Enterprise Mobility +Security E3
- Office 365 Enterprise Mobility +Security E3 (Government Pricing)
- Office 365 Enterprise Mobility +Security E3 (Nonprofit Staff Pricing)
- Office 365 Enterprise Mobility +Security E3 (Nonprofit Staff Pricing) (50 Seat Donation)
- Office 365 Enterprise Mobility +Security E3 for Government
- Office 365 Enterprise Mobility +Security E5
- Office 365 Enterprise Mobility +Security E5 (Government Pricing)
- Office 365 Enterprise Mobility +Security E5 (Nonprofit Staff Pricing)
- Office 365 Enterprise Mobility +Security E5 for Government
- Office 365 Enterprise Mobility +Security E5 Trial

Supported Subscriptions

The following subscriptions are supported for Sage 100cloud integration with Office 365.

Your Microsoft account must include one of these subscriptions:

- Office 365 Business Premium
- Office 365 Business Premium Trial
- Office 365 Enterprise E1
- Office 365 Enterprise E1 (Government Pricing)
- Office 365 Enterprise E3
- Office 365 Enterprise E3 (Government Pricing)
- Office 365 Enterprise E3 Trial
- Office 365 Enterprise E5
- Office 365 Enterprise E5 (Government Pricing)
- Office 365 Enterprise E5 Trial

3. Configure an Application Connector for Sage 100 and update Sage 100 Company Maintenance with new OAuth connection settings, as seen below. The eight (8) variables listed in the bottom grid (starting with User ID) are specific to your Office 365 configuration and the dependency on purchasing the Microsoft subscriptions listed in #2 above are needed to complete this configuration (required by Microsoft to use this feature).


SMTP (Mail) Server
Select the Authentication Method used to connect to the SMTP mail server.
Authentication Method
OAuth
Enter the DNS address (for example, mail.example.com) or IP address (for example, 128.0.0.102) of the SMTP server you are using to send e-mail. The address is needed to generate e-mail. Enter the port number the SMTP server is using if it is not configured to use the default port.
Address
Port
587
Select the type of encryption to use between the SMTP client and SMTP server to send e-mail.
SMTP Encryption
TLS
Enter the user ID and client credentials that will be used to obtain an access token from the authorization server. While not always required, it is a good idea to only send 'authenticated' mail. This user does not have to be the one the mail is from; it is only used to log on to the e-mail server when sending mail.
User ID
Client ID
Client Secret
Auth End Point
Token End Point
Scope
Redirect URI
Code Challenge Method
S256