



SendGuard for Outlook

Understanding Security and Data Protection

Last Updated: October 18, 2024

Contents

Introduction.....	1
Versions of SendGuard	1
Areas of Emphasis	2
Security and Data Protection Matrix.....	3
Standss License Management System.....	5
Conclusion.....	5

Introduction

This document provides an overview of the various versions of SendGuard with special emphasis on security including what information is communicated with Standss servers, the server architecture, where data is processed, and what data (if any) is saved.

Depending on your requirements, SendGuard can be configured so that everything is saved and processed on users' local computers and/or your own servers.

This document is intended for decision-makers to assess the impact of SendGuard on their existing systems. The document does not contain information on features or functionality. Please contact us at sales@standss.com if you wish to learn more about the software and/or schedule a demo.

Versions of SendGuard

SendGuard is currently available in two main versions built using different technology. Security in the two versions is handled differently.

Outlook COM Add-in (Outlook Desktop for Windows)

The add-in is physically installed on each computer (can be deployed centrally) and all processing is also carried out on the local computer.

This provides the most secure user experience as no data is transferred away from the user's computer.

COM add-ins are only supported for users using the full version of Outlook on Windows.

Outlook Web Add-in (New Outlook for Windows & Mac, Outlook Web Access, Classic Outlook on Windows and Legacy Outlook on Mac)

This is a new style of Outlook add-in that is only available to Microsoft 365 users.

Unlike COM add-ins, Outlook Web add-ins don't have any code physically installed on the user's device or Outlook client. Outlook reads a manifest file and then loads JavaScript and HTML from our servers. The loaded JavaScript and HTML are the application. The web components run in the context of a browser in a sandbox with access only to the email currently being worked on.

Most of the processing is still carried out on the user's computer with no data being passed back to any servers.

The only exception is if you want the actual contents of attachments to be scanned and checked (This is an optional feature and can be turned off). If this feature is turned on, then attachments are passed to our servers for processing. No data is saved by the application on our servers.

Microsoft Azure is used to host the application. With HTTPS requests and TLS settings, it offers secure endpoint connections. The app only has access to client data through restricted permissions that the customer's Microsoft 365 Admins can grant.

This ensures that we meet the requirements of GDPR (including Article 28).

Note: We recommend that Microsoft 365 users install the Outlook Com Addin version if they are using Outlook Desktop for Windows. This can co-exist with the HTML/JavaScript version with the correct version being activated based on the Outlook client being used.

Areas of Emphasis

The matrix in the next section has details on each of the following key areas for the two versions of SendGuard.

Installation: What gets installed and if any code needs to be downloaded after installation.

License and Activation: Does the software need to activate against any licensing server?

Settings: Where are the settings for the software saved?

Email/Attachment Processing: Are the emails transmitted away from the users' computers for processing?

User Action Logging: Administrators can optionally activate logging. When this is activated, logs are maintained of basic details of the email as proof that the user was prompted for confirmation before an email was sent. These logs are in a standard format and can be used with PowerBI/Splunk etc for compliance reporting, impact assessment, etc.

Security and Data Protection Matrix

	Outlook COM Addin	Outlook Web Addin
Installation	The full software is physically installed on each computer (It can be centrally deployed using GPO etc).	The software is deployed by the user or admin using a manifest file and Microsoft 365. Outlook reads a manifest file and then loads the application (JavaScript and HTML) from our servers.
License and Activation	This information is stored in the registry. <i>We can provide a customized MSI with the settings prefilled so that no communication is necessary with our servers.</i> Alternatively, activation can be done using the Standss License Management System. This system allows admin control over the licenses/users. The license information is checked against our server every 7 days for validity.	The license information is contained in the manifest file and/or the Settings file. <i>We can provide a manifest so that no communication is necessary with our servers.</i> Alternatively, activation can be done using the Standss License Management System. This system allows admin control over the licenses/users. The license information is checked against the server every 5 days for validity.

<p>Settings</p>	<p>This is saved directly to users' registries on their local computers.</p> <p><i>If client does not want any settings on the servers, we can provide ADMX files for the centralized management of settings via GPO (using your own Windows Servers).</i></p> <p>Alternatively, the settings can be centrally managed via the Standss License Management system.</p> <p>The settings will be saved on our server OR on the client's own servers (only requires HTTPS endpoints).</p>	<p>This needs to be hosted on a server accessible with HTTPS endpoint for secure connections.</p> <p><i>The settings will be saved on our server OR on the client's own servers (only requires HTTPS endpoints).</i></p> <p>The settings can be centrally managed via the Standss License Management system.</p>
<p>Email/Attachment Processing</p>	<p>All processing is carried out on the local machine.</p> <p>No data is transmitted away from the user's computer.</p>	<p>Most of the data is processed on the client's local computer.</p> <p>If attachments needed to be scanned for sensitive/DLP content, then this is done on Microsoft Azure based servers.</p> <p>HTTPS requests and TLS settings ensure secure transmission.</p> <p>No data is saved after processing.</p>
<p>User Action Logging</p>	<p>The data can be logged to the Windows Event Log, a folder on the local computer or a network drive.</p> <p>No logs are saved on any Standss computers or servers.</p>	<p>The data can be logged to Azure Tables in the organization's own Azure account.</p> <p>No logs are saved on any Standss computers or servers.</p>

Standss License Management System

This system lets Office 365 Global Admins log in and handle user/license information. It ONLY stores email addresses for users registered under the license, and no data about sent emails is kept. Additionally, the system can store SendGuard settings for both COM add-in and Outlook web add-in.

The email addresses of the users can only be viewed by the authorised Account Manager at Standss. The respective client's Office 365 Global Admin will be able to view the data and no other parties will be able to view the data. During the onboarding process the Office 365 admin will need to provide consent to the Standss License Management System to save the users email addresses.

Note: This system is OPTIONAL. If IT admins prefer not to use it, they can contact Standss for guidance on obtaining licenses to host settings on their own servers.

Conclusion

We recommend that organizations deploy the version of SendGuard based on the environment (Outlook version) that users will be working with.

Windows users should install the Outlook COM/VSTO version of the add-in. This provides for a more powerful user experience as it is based on more mature technology.

It also provides the most secure user experience as no data is transferred away from the user's computer.

For M365 (Outlook for Windows, OWA and MAC) the newer style Outlook Web Add-in can be used. This can be configured for the level of security that you need.

For Windows users, both can also be installed to co-exist with the correct version being activated based on the Outlook client (Desktop or OWA) being used. Different settings can be done for each version if needed.

Please contact your account manager at Standss or email us at sales@standss.com if you need further information.