SMBsecure™ Addin for Classic Microsoft® Outlook

Simple Mode User Guide

SMBsecure™
Document Version 1.1

Using SMBsecure Email Encryption SIMPLE MODE

A simple out-of-box experience for senders, made easy for recipients too!

Following the installation of the software and running the script to prevent Outlook disabling the Addin, the app will run in **Simple Mode** (by default) to quickly enable you to begin sending attachment files as password-encrypted **Secure PDF** *plus* allow you to send or resend the personal password by SMS to the recipient(s).

Simple Mode incorporates preconfigured settings to individually convert attachment files, including standard office and image files, to portable document format (**PDF**), encrypt them with a personal password, embed a password hint in the email body, and allow you to also send the actual password by SMS to the recipient(s). Simple Mode minimises the need to deliver the actual password to a recipient by always including a ***password hint*** in the body of the email for the recipient(s) to reference. This aligns to what recipients are familiar with, like when they receive encrypted correspondence from their Bank which usually includes a note in the email body of what info to use to open the password-encrypted PDF, for example, an ID Number. However, **SMBsecure™** further enhances the usability experience for the recipient with integrated sending of the actual password by SMS at the same time for more convenient unlocking of the **Secure PDF** making it very recipient-friendly!

Simple Mode requires minimal input. You only need to specify a **personal password** for the **Secure PDF**, a **hint for that password** to open the **Secure PDF**, and optionally you can **add the mobile number** for the recipient to receive the actual password by SMS which we highly recommend you do.

Simple Mode strikes a balance between *usability, productivity, and security* whenever emails with attachment files are sent as encrypted **Secure PDF** files.

If your admin allows, you can switch to **Custom Mode** to get full flexibility and granular settings options to have a tailored setup for your specific needs.

Defining a Password Standard for Your Organisation

Prior to using the app contact your Administrator to find out about the password standard used by your organisation. A **Password Standard** is the convention used to set passwords and hints for recipients, for example ID Number. It is important for all users in the same organisation to use the same standard when defining the password for the **Secure PDF** for a recipient to ensure that all recipients who receive correspondence from anyone in your organisation will have a good experience accessing the **Secure PDF**. *You do not want recipients to use different passwords for Secure PDF files received from different people in your organisation, so define a password standard for all to follow.*

The password should be something that the recipient will know *off-hand*, or have, and can be referenced without much effort by them but one that is not easily attained or attainable by an unauthorised device user if the email is intercepted, or if the recipient's mailbox is compromised.

A Password-Hint is *a descriptive reference for the actual password used to open the encrypted PDF and what the typed-in format should be (if any) for example:* ***Your Date of Birth in the format DDMMYYY.***

The password *Hint* embedded to advise the recipient what to use to access the **Secure PDF** should not be included anywhere in your email signature nor in the body of the email which you are sending. *For example, do not use your Practice Number if that number is listed with your email signature.*

Good Examples include an Account or Entity Number, a Practice or Registration Number, a Contact Number, Customer/Client/Patient ID Number, or a "secret" that you have discussed and communicated with the recipient, etc.

Using The Recipient's Mobile Number as Their Personal Password:

It may be a good idea (and easy) to use the Mobile Number (Cell Number) of the recipient as their personal password to open **Secure PDF** files as this is something they know and they can easily recall. However, it will be unwise to have the hint defined as "Your Cell Phone Number" in the body of the same email as anyone can obtain it and gain access to the **Secure PDF**.

Better example of a *Hint* to include when using their Mobile Number as the password could be:

"Your Customer Number"
"Your Contact ID"
"Your Contact Digits"
"Your MTN ID" *or* ***"Your Telkom ID"*** *-> swap* ***MTN/Telkom*** *with their mobile service provider.*

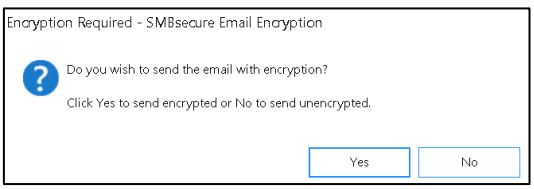
Refer to the ***SMBsecure™ Guidance Note*** *about password considerations and best practices which can be downloaded from:* https://smbsecure.co.za/guidancenotes/.

If your organisation is not making use of a **Shared List**, we strongly recommend that your administrator defines a Personal Password standard (policy) that all users must follow for defining the personal password when sending a **Secure PDF** to recipients. This is to ensure a good recipient experience when they receive **Secure PDF** files from your organisation.

Sending Attachment Files as Password-Encrypted Secure PDF to a New Recipient for the First Time

1. Respond to the Send Encrypted prompt:

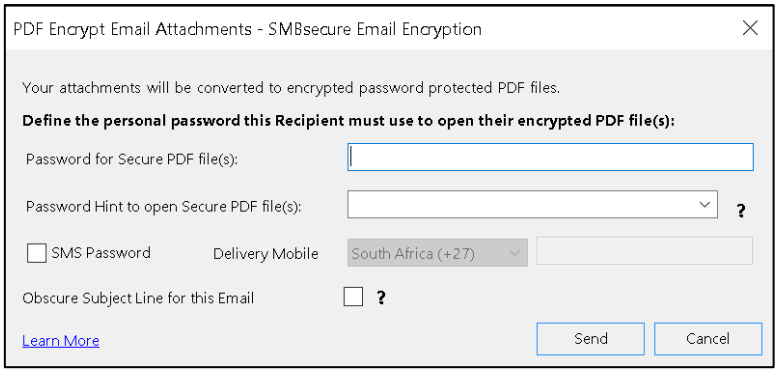
When composing and sending an email with attachment files, you will be presented with a prompt to automatically convert the attachment file(s) to portable document format (**PDF)** and send them as password-encrypted **Secure PDF** files. Select **Yes** to send with encryption.



Note that the above prompt will NOT appear when there are no files attached to your email or when sending emails internally (i.e. to a recipient of your internal email domain).

2. Set the password for the Secure PDF + a Hint for what info to use to open the Secure PDF:

When sending a password-encrypted **Secure PDF** for the first time to a recipient, you will be presented with a window to set the recipient's personal-password for the Secure PDF(s) and a Hint to embed in the body of the email (**as a tip**) for the recipient to know what to use to open the **Secure PDF**.



Read the above section "**Defining a Password Standard for Your Organisation**".

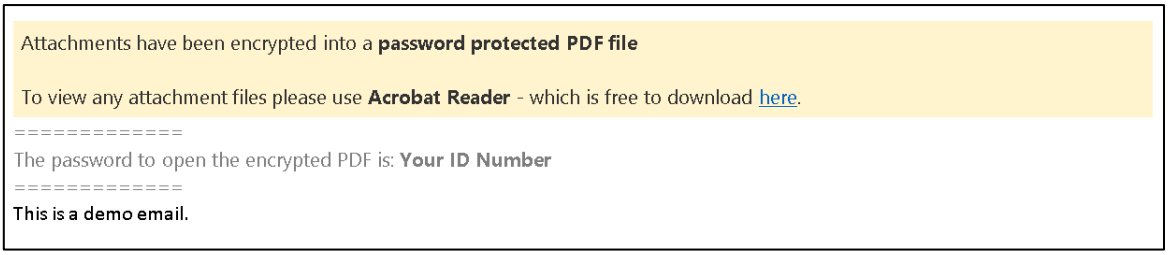
All future Secure PDF files for the recipient will automatically encrypt using these details!

3. Add the mobile number to send the actual password by SMS: This is a FREE service to you!

To make is easier for recipients to know the actual password to open the encrypted PDF file(s) when sending to them, the personal password can be easily sent by SMS to their mobile number at the same time. We **highly recommend** that you check this option and add the recipient's mobile number the first time you are sending them a password-encrypted **Secure PDF**. This will drastically improve the recipient's experience when receiving password-encrypted files from you. **There are zero charges to you as the sender to SMS the password to a recipient's mobile number.**

How Emails with Secure PDFs Look for Recipients

The email will have a highlighted header and a section and the Hint which you have defined for the corresponding password automatically embedded in the body of the email. Any text you have typed in your email and your email signature will be visible as normal (clear text) to the recipient i.e., **only attachments are password encrypted** with Simple Mode.



A **Secure PDF** can be opened and viewed using any PDF Reader on any device. Acrobat Reader is recommended by default which is free to download and use on any device.

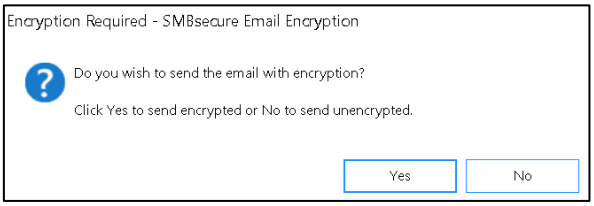
The **SMBsecure™** application also caters for attachments included in Outlook Calendar invites to be sent as password-encrypted **Secure PDF**, with all RSVP functions fully preserved to allow your recipient to Accept or Decline the meeting invite.

TIP: *Always put all correspondence which contain personal or sensitive information in the attachment file(s) which will be encrypted and secured with a password. Avoid including any personal or sensitive information as clear text in the body of your emails when using Simple Mode.*

Sending Password-Encrypted Secure PDF to an Existing Recipient

1. Respond to the Send Encrypted prompt:

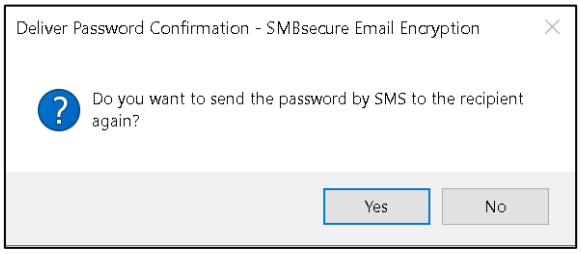
When composing and sending an email with attachment files you will be presented with a prompt to automatically convert the attachment file(s) to portable document format (**PDF)** and send them as password-encrypted **Secure PDF** files. Select **Yes** to send with encryption.



Note that the above prompt will NOT appear when there are no files attached to your email or when sending emails internally (i.e. to a recipient of your internal email domain).

2. Respond to the Send Password by SMS Prompt:

If you have added a mobile number for the recipient, the app will remember the Mobile Number and prompt if you would like to send the password again to the user in-case they have forgotten it or if they cannot easily recall it. Select **Yes** to re-send the password to the recipient by SMS. **There are zero charges to you as the sender to SMS the password to a recipient's mobile again.**



Sending Secure PDFs to Multiple Recipients

To allow correspondence (Reply and Reply-All functions) by ALL recipients included on your email, the app will employ a "***common-password***" to ensure that **ALL** the recipients can have access to the **Secure PDF** file(s) attached to that email.

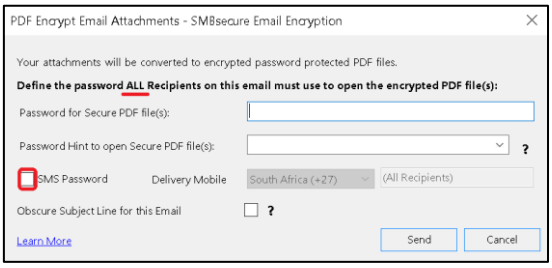
A "***common-password***" is required and is to be defined EACH TIME you send an email with attachments encryption to multiple recipients (i.e. **Multi-Recipient Emails**). Note that the app DOES NOT make use of the recipient's personal password in this case.

The password used should be known to **ALL** the recipients requiring access to the **Secure PDF**.

Good Examples include an Account or Entity Number, a Practice or Registration Number, a contact number or reception number, Customer/Client/Patient ID Number, or a "*secret*" that you have discussed and communicated with **ALL** the recipients included in the email, etc.

A Password Reference ID is also always noted at the bottom of each email containing a Secure PDF to enable you to search and retrieve the password using the Addin inside Outlook on your PC.

We highly recommend that you check the option to SMS the password to ALL recipients on the email when sending them a password-encrypted **Secure PDF**. This will improve the recipient experience when they receive the password-encrypted **Secure PDF** from you. **There are zero charges to you as the sender to SMS the password to the recipient's mobile.**

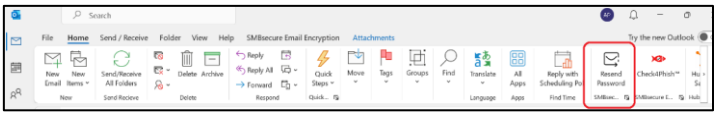


If any recipients are missing a Mobile Number or are not in your password list these will be displayed when sending. You will create a Personal Password record for them and add a Mobile Number. Note that the personal password defined in recipient record is for **Secure PDF** files sent only to them.

How to Resend Password Directly from Sent Items in Outlook

There will be times where recipients may contact you to ask for the password again for an email which contained a password-encrypted **Secure PDF**. To make this easy we have included a one-button function to accomplish this directly from inside your Send Items folder in Outlook on your PC.

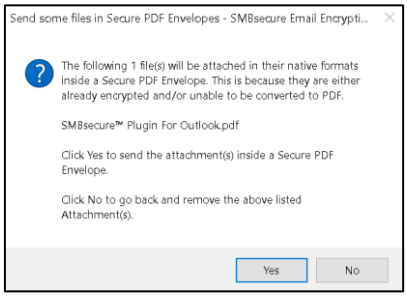
Simply find the relevant email in your **Send Items** and click the **Password Resend** button on the Outlook ribbon to SMS the password to the recipient(s). If the recipient(s) do not have a Mobile Number added for their record, you can simply click **Add Mobile Number** and have the app SMS the password directly to their mobile number.



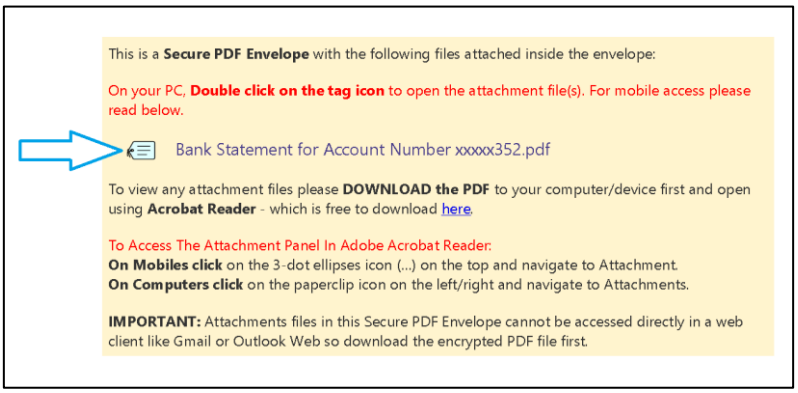
Sending Files Inside a Secure PDF Envelope

Files which are already encrypted or files which cannot be converted to PDF (for example already encrypted bank statements or non-standard office files), can still be secured and emailed. These files will be placed inside a **Secure PDF Envelope** as attachments inside the PDF.

You will be presented with a prompt should the application encounter such files. Each file will be individually secured inside its own **Secure PDF Envelope** so it can be separately accessed.



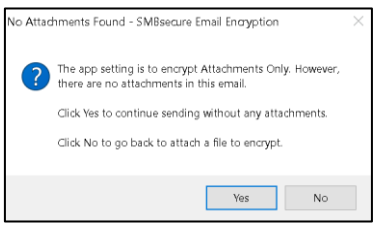
If you send a file inside a **Secure PDF Envelope**, the recipient will be provided with instructions on how to access the attachment file inside the PDF Envelope. A recipient may contact you for instructions on how to access the attachment file inside the PDF so it's worthwhile trying this for yourself.



Note: Password encrypted PDFs containing any file attachments (**Secure PDF Envelopes**) MUST be downloaded onto the device first and opened using Adobe Acrobat Reader to view attachments files. A web view cannot display attachment files contained inside a Secure PDF Envelope and will therefore limit access to any attachment files inside the PDF.

Pressing Send Encrypted When No Files Are Attached

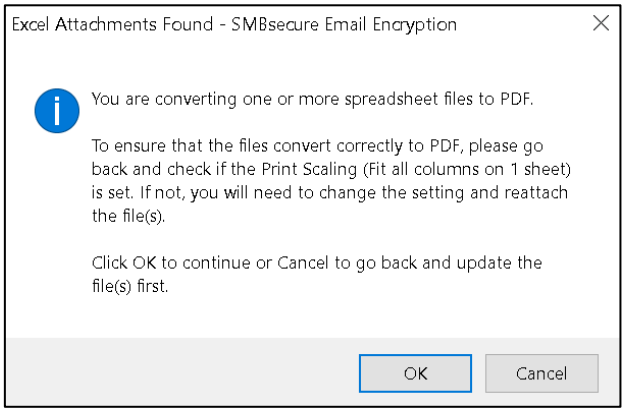
If no files are attached to your email and you press the **Send Encrypted button** on the Outlook ribbon, the app will warn you and allow you to take the appropriate action.



Properly Format Spreadsheet Files When Sending as Secure PDF

When emailing attachment files which are spreadsheets, **it is important to set the print format** prior to converting it to a **Secure PDF** so that all columns appear on a single page. This is to ensure that the PDF document appear neat, presentable, and is easily readable for your recipient(s).

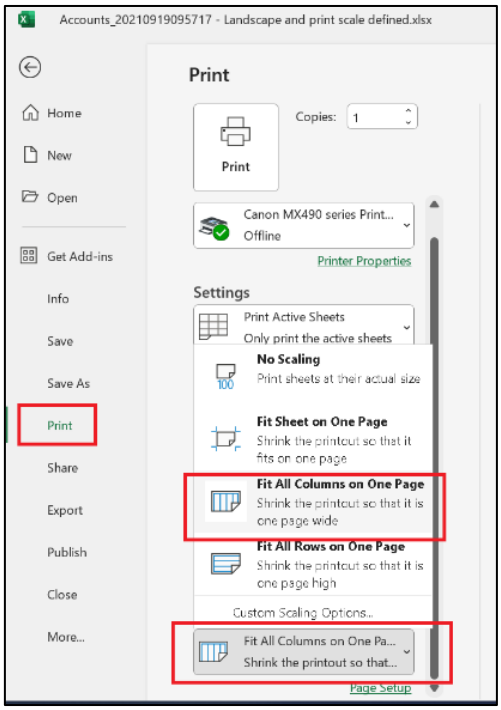
The app will automatically detect spreadsheet files and will warn you. It will allow you to go back and set the print format if you have not done so already.



To format your spreadsheet file for proper PDF conversion, open it in Excel directly from your composed email and click on **File**.

Click on **Print** and navigate to the bottom of the print settings window to set the **Print Scaling** option to **Fit All Columns on One Page**. You can also set the page to be portrait or landscape.

Save the changes, close the file and hit **Send** in Outlook.



Obscuring The Subject Line

When you compose a new email and click on the **Send Encrypted button**, you can launch the interactive window and choose to obscure the subject line for the email. Selecting the option will change the Subject Line to whatever is default or what is set by your administrator. Obscuring Subject Line can enhance the privacy of the email to help conceal what the correspondence (and the contents of the Secure PDF) relates to, in case the email is intercepted or accessed by an unauthorised person.

This option can be used whenever very sensitive information is being emailed, for example payment remittance advice (bank details) for large amounts.

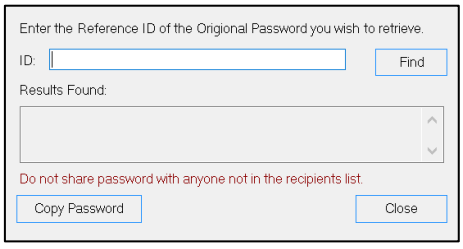
Emailing Recipients on the Mandatory List

The app will automatically detect any recipient or domain on the mandatory list defined in the app or by your administrator. The app will warn you and allow you to go back to take the appropriate action.

Retrieving Historic Passwords

All emails sent with password-encrypted **Secure PDF** files are *tagged* with a **Password Reference ID** at the bottom of the emails. This will be viewable in your own **Sent Items** folder in Outlook, or the recipient can view it on the email in their Inbox. It will appear like this at the bottom of emails:

Open the app on your Outlook ribbon and select "**Retrieve Password**" from the menu. A window will open to allow you to paste or type the Password Reference ID number to find the original password from your password history database. You can call the recipient to advise them of the password to use to open the **Secure PDF** file. Avoid emailing the password to the recipient for security reasons.



Thank you for using SMBsecure™ Email Encryption Software.
For any training, help or assistance please contact your Service Provider or IT Administrator.
For more information, please visit https://smbsecure.co.za