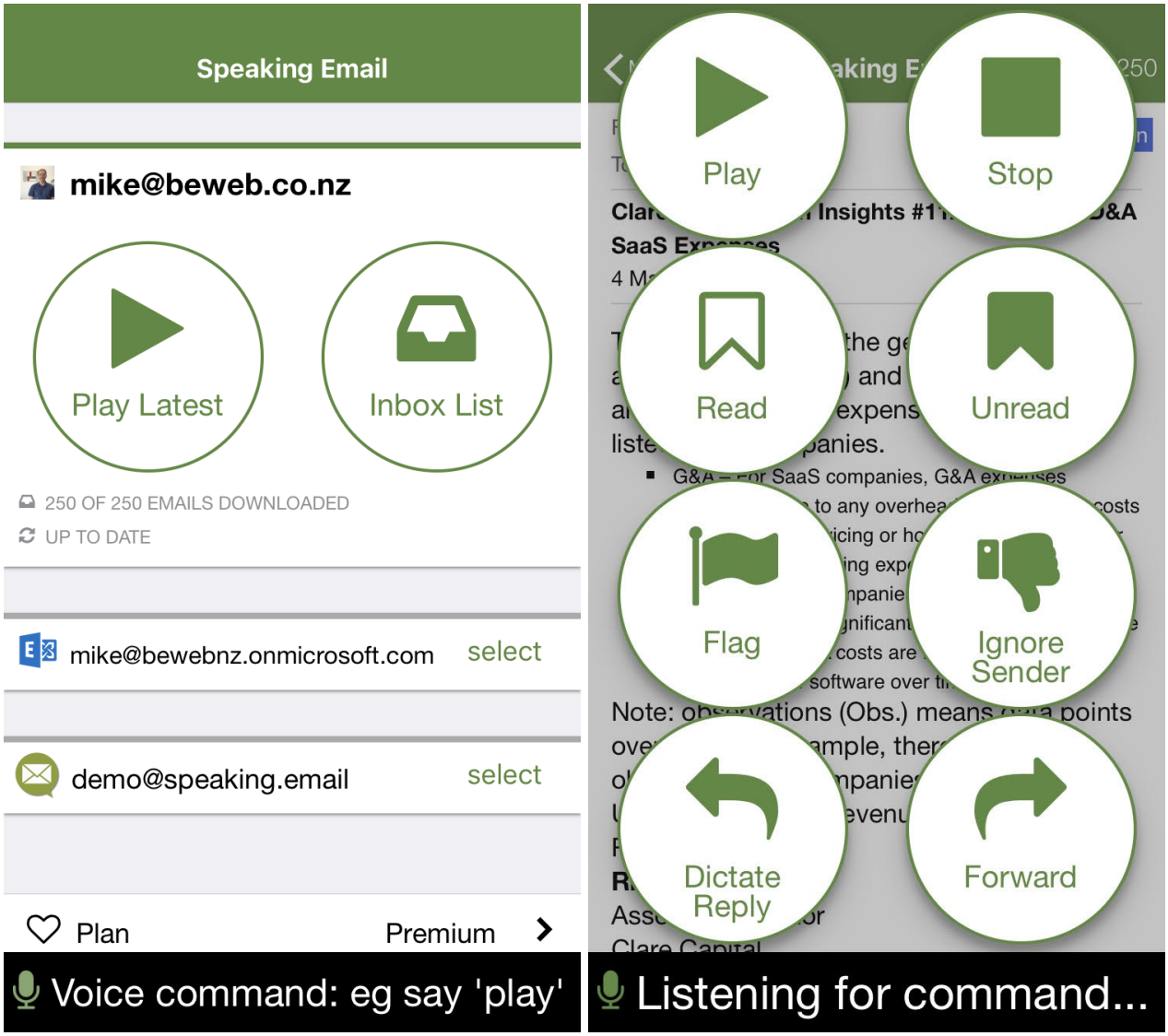
Enterprise Guide to Speaking Email

IPHONE & ANDROID APP

Last updated: 19 Jan 2022



Speaking Email enables distraction-free listening to your inbox

About this document

This document is aimed at IT security and infrastructure specialists evaluating Speaking Email for use by employees in their organisation. It covers all platforms and goes into depth about Microsoft 365 and Exchange server, which are the most common enterprise email platforms.

This document goes into detail about the current implementation. Please note that implementation details are subject to change. Please contact us if you have any specific concerns or questions.

Requirements

To run Speaking Email effectively users need an iOS 11+ or Android 8+ device. Voice recognition uses native device SDKs and as such iOS devices are more reliable for speech recognition.

Users can connect to their on-premise or externally hosted email account assuming it is accessible on:

- Microsoft 365 (aka Office 365)
- ActiveSync (including Exchange server, Microsoft 365 with MFA, Amazon WorkMail)
- Gmail / G-Suite
- IMAP
- POP3 (least preferred)

Setup

Install Speaking Email from the App Store or Google Play. Links are available from www.speaking.email

Once installed, follow the prompts to connect to the user's mailbox. You will need their username, domain if applicable, and password.

If your organisation has configuration settings published using the Microsoft Autodiscover standard, the protocol and hostname should be automatically configured. In this case you may be able to leave the setup to the user. The user enters only their own email address and password, and the remaining settings are discovered. If this is the first install you have done it is recommended to do this yourself to check the autodiscover works as intended.

If the user email address is identified as Microsoft 365 (by the MX records you have published), you will be given the choice of which Microsoft protocol to use for the connection. Generally you should choose the highest security level that is compatible with your systems. The best are the first two options - Microsoft 365 Direct and Intune.

If your mail server is not automatically configured, tap Account Setup to set up manually by choosing the mail server type (under the "manual connection setup" heading). We support Gmail, Microsoft 365, Exchange, Hotmail/Outlook.com, Yahoo, iCloud, AOL, IMAP, POP.

Once connected, go to the "Plan" screen to upgrade to Premium Edition. This gives access to all Speaking Email features. Users can pay via the App Store or Google Play or enter an enterprise key.

Contact us if you would like to purchase an enterprise license and be invoiced instead of paying via the store.

Security and mail servers

All connections from the device are encrypted and go either directly to the mail server or to our private cloud using a valid public CA certificate.

In all cases user details, specifically name and email address, are sent to our cloud server, for analytics and marketing purposes, where they are stored in our private cloud database.

The following describes more detail about security implementation, depending on the mail protocol selected.

Microsoft 365 Direct

The login process goes directly to Microsoft servers using Microsoft Identity v2 and OAUTH (also known as Modern Authentication). This takes the user to their enterprise sign-in page if applicable, or the Microsoft sign in page. It enables MFA (multi factor authentication) and password entry directly to Microsoft servers.

Connections go directly from the device to Microsoft 365 in the cloud over secure HTTPS connections.

Speaking Email uses Microsoft Graph API. For this to work, IT admins must enable logins via Exchange Web Services (EWS).

Intune - part of the Microsoft Enterprise Security + Mobility suite

Speaking Email is an official Microsoft Partner for Microsoft Enterprise Security + Mobility. If your corporate environment is using Microsoft MDM then this will be the way to connect.

Intune including access via Company Portal, Microsoft Authenticator, and using Microsoft Conditional Access (CA) rules are supported and have been road tested in large enterprise environments.
(See https://docs.microsoft.com/en-us/intune/apps-supported-intune-apps for InTune support)

When choosing Intune, the security is completely handled by the Microsoft Intune SDK, so Speaking Email never sees your password.

Speaking Email's Intune integration is currently supported on iOS only.

ActiveSync / Exchange server

If not using Microsoft 365, or not having Microsoft Identity v2 or Exchange Web Services enabled, you can use our ActiveSync client.

Connections go directly from the device to the ActiveSync server over secure HTTPS connections for endpoints signed with valid certificates from public Certificate Authorities (including Microsoft 365 / Exchange Online).

ActiveSync with Modern Authentication

If you have Microsoft 365 but don't have Microsoft Identity v2 or Exchange Web Services enabled, you may want to use ActiveSync with Modern Authentication. This uses Microsoft Identity v1 to create a secure OAUTH token and then connects via ActiveSync.

ActiveSync with Standard Authentication
If you are not using Microsoft 365, your server will not support OAUTH, so you need to use ActiveSync standard security. The user enters their email address and password into Speaking Email and Microsoft Autodiscover is run directly from the device.

If the mail server is not found a discovery process is performed by our API (running on our private cloud). If not found, the user must enter their mail server address, domain and username. This is then verified by our API.

This involves sending credentials, to check the connection, certificate validity, and username / password validation. User credentials are sent encrypted and passwords are not stored in our database.

Support for Exchange MDM

In addition to Intune (see above), Exchange Online MDM (mobile device management) is supported. This is where you use the Exchange Online security module (set up within Exchange Admin Center) to apply policies. You can disable individual clients and an appropriate error message will display in Speaking Email.

Other MDM systems may not be supported or may be partially supported. Please contact us if you would like us to develop support for other providers. There would likely be some development costs involved.

Support for Exchange server self signed certificates

If you use a self-signed certificate, or have an expired certificate, we establish the trust relationship from our cloud server to your endpoint, and then proxy all data back to the device via our public CA HTTPS SHA2 certificate. This means there is no onus on the user to install or accept certificates. This also enhances security by avoiding reliance on the device's current DNS service (which could change with wifi or cell connections). We do not log any content in this proxy connection and it is entirely transmitted over HTTPS end to end.

G-Suite / Gmail for Business

For this server type Speaking Email uses Gmail REST API directly from the device to Google servers. Security is using OAUTH so your users passwords go directly to Google servers via secure HTTPS connections.

We upgraded this in 2017 to the latest Google Sign In technology, which uses credentials already stored on the device if available. On Android this is built into the operating system and on iOS it uses a Safari instance to connect to Google servers.

In 2019, we passed Google Cloud Platform/API Trust & Safety official approval. This means Speaking Email is compliant with the Google API User Data Policy and the Additional Requirements for Restricted Scopes.

IMAP and POP

For both these protocols we use a server-to-server approach, which involves caching mail on our private cloud servers and sending it down to the device when requested. This means that the password is sent via HTTPS from the app to our servers, once, and encrypted (double salted AES256 rijndael encryption). From that point on, the password is decrypted in memory, then used to connect directly from our cloud servers to the IMAP or

POP mailboxes in question. For outgoing mails (replies and forwards) the app calls a service endpoint on our cloud servers which initiate the SMTP connection (with valid authentication) to send mail using the user's mail server if possible, or otherwise we send users' mail from our servers. All mail sent from our own servers have "from" header of "no-reply@speaking.email" and "reply-to" header set to user email address, to avoid spoofing (authenticated with DKIM and SPF).

Device security

Data on the device is protected by the operating system. Both iOS and Android enforce application isolation, meaning that malicious apps cannot access your data. We recommend corporate devices are protected by operating system biometric or PIN code.

For iOS devices, email data is stored in a secure database on the device, encrypted with AES256.

Revoking access

If an employee loses their phone or leaves the organisation, you need to be able to revoke access.

ActiveSync / Exchange server

"Remote Wipe" is a feature of Microsoft 356 and all Exchange servers and is supported by Speaking Email. If an administrator sets the account to Remote Wipe, the next time Speaking Email contacts the server all mail and the account credentials will be deleted.

If you are using Microsoft 365 with Modern Authentication (which is the default in Speaking Email), you can see which apps have access to your mail using Microsoft 365 / Azure Portal. Clicking the button to revoke access means that the account can no longer send or receive mail.

You can also disable accounts in Exchange, or change their passwords, which will have the same effect.

G-Suite / Gmail for Business

Google mail is secured by OAUTH. You can revoke access to any app in your Google account settings, here: https://myaccount.google.com/permissions

IMAP and POP

Change the password or disable the account in your mail server to disconnect it from Speaking Email.

Privacy and GDPR

Data is stored on the user's device and some data, such as account details, is stored on our private cloud servers located in New Zealand. Data sovereignty of that data is subject to New Zealand law, which has a track record of upholding user privacy.

We maintain user profiles which we associate with payment history and usage data for analytics, error reporting and support. The only personally identifiable information (PII) included are name and email address which we use for transactional communications (for example onboarding and assistance emails), occasional marketing

communications (email newsletters, no more than 6 times a year) and statistical analysis. Marketing communications can be opted out of by clicking an unsubscribe link present on all marketing emails.

We record telemetry data for use in usage analytics. Telemetry data does not include any personal data or user content.

By their nature, error reporting logs may include fragments of personal data or user content. This is used by employees of Beweb, who are bound by strict confidentiality contracts, for the sole purpose of diagnosing and resolving any errors.

Our policies are compliant with GDPR. You may request permanent deletion of your data by emailing us on feedback@speaking.email.

See our full privacy policy online.

Employee Safety & Compliance

Accessibility policies

If your company has policies about providing equal access for people with disabilities, you ought to be providing Speaking Email as an alternative mobile email client.

Mobile phone usage policies

We recommend providing a policy on mobile phone use and giving employees the tools to engage more safely with technology in cars. By supplying Speaking Email to employees and encouraging its use, employers are providing safer alternatives to commonly used communication tools.

We suggest such a policy could include:

- Enable work communication be done as safely as possible - voice calls using Bluetooth and emails using Speaking Email
- Supply employees with hands free kits and mandate their use, including a cradle to enable safely touching the phone
- Supply apps designed for in-vehicle use and suggest using these instead of standard apps

Distracted driving laws

There are no counties, states or territories we know of which have banned mobile phone usage in cars outright, except Quebec. Everywhere else it is legal to use a mobile phone in a safe manner while driving.

In most places, handheld mobile phone usage is banned, meaning you are not allowed to hold your phone while using it. While all jurisdictions have different laws, this appears to be the common denominator, applying to most US states and most of Europe, the UK, New Zealand, Australia, and Canada.

We recommend supplying employees with cradles to enable them to see and touch the phone legally. As long as the tasks are not distracting, this usage is legally acceptable. Most apps, however, are distracting to use, with small buttons, small text, typing or complex interactions.

In 2019 Maine introduced new legislation which is slightly tighter - not allowing users to hold or even tap the phone. One Maine user told us “Outstanding attention to the details! This application is saving me from myself and lots of tickets”.

Productivity

To illustrate the potential for economic benefit, let's take a whole country the size of New Zealand where 22% of its 5 million people drive to work. Given an average of 30 mins each way, this is an hour per day in traffic. Taking 200 working days, and the average wage, this equates to $5 billion worth of lost productivity.

In the US, 80% of workers drive to work. That's 16 billion hours a year of commuting. Imagine if some of that time could be used productively...

So how do you get this benefit for your company? There are three main uses: commuting, work related driving, and accessibility.

1. Commuting

Many senior level, engaged and committed employees want to be up to date on their communications and maximise their productivity. All you need to do is provide them with the tools to empower them achieve this. Speaking Email is the next natural evolutionary step - from PC, to web, to mobile, to voice. Users can now check mail without looking, opening up a range of possible ways to consume email and stay ahead. The primary use case is driving to and from work, where a commuter would traditionally listen to the radio, they can now listen to their inbox, flag, archive and reply to emails.

Some employees resisted getting a BlackBerry because they didn't want their work to take over their home lives. It is certainly important to have a good work/life balance. Surprisingly we have found the same employees who don't like having work email on their phone, with the notifications and temptation to check in, actually like being able to have their email read to them at a time of their choosing such as on the way to work. For these people Speaking Email provides a more preferable alternative tool to consume email outside of the office. Basically, more options are better.

Examples:

- Taking a legal firm with 100 lawyers, say one in 10 use the app while commuting, they would save at least half an hour a day each. At a charge out rate of $250 an hour this would enable the firm to bill an extra $287,000 annually.

- At a firm of 5000 consultants, if only 1% used the app daily, they could see an increase in billable hours of $2 million annually.

2. Work Related Driving

If employees are driving as part of work, they can be contactable and productive at the same time.

If you have sales reps on the road, the more time they can be enabled to be out and about the better. By keeping on top of their email inbox, agents or sales reps can spend more time visiting customers and less time

at their desk. There are no surprises lurking in their inbox compelling them to go into the office just to “catch up” on emails.

Even employees who occasionally drive to meetings might spend a couple of hours a week driving during work time. This uninterrupted quiet time is the perfect opportunity to listen to their inbox and review any emails not yet dealt with.

Example:

- Let's say you have 10 sales reps on the road and each spends an hour a day at their desk doing emails. By using Speaking Email you could likely cut this down to half an hour a day. If your reps are paid $50 an hour that's a saving of $50,000 a year. This is a conservative estimate: we are not even taking into account opportunity costs, reduced number of trips back to the office, or increased sales resulting from better responsiveness to emails.

3. Accessibility

If you have staff with disabilities, Speaking Email can help them be more productive. Speaking Email is a godsend for users with blindness, vision problems, dyslexia, motor dysfunction, stroke victims, and any condition that makes regular mobile or desktop email apps difficult to use.

Licensing Options

For enterprise customers, we can provide direct invoicing, support SLAs and sign supplier agreements as required by your IT security and procurement policies.

For enterprise customers, we can provide direct invoicing, support SLAs and sign supplier agreements as required by your IT security and procurement policies. Volume discounts and customisation are available.

Contact us if you would like to purchase an enterprise license and be invoiced instead of paying via the App Store / Google Play.

Troubleshooting

ActiveSync / Exchange server

Speaking Email uses ActiveSync to connect to Exchange Server.

It appears with the User Agent name “Speaking Email SE” so you can clearly identify clients.

Speaking Email supports most ActiveSync features, including autodiscover, provisioning and remote wipe. It supports Basic Authentication and Modern Authentication.

Exchange Online MDM (mobile device management) is supported. You can disable individual clients and an appropriate error message will display in Speaking Email.

If you are having trouble connecting see the troubleshooting section below. In many cases you can see the client quarantined or blocked and will just need to unblock or whitelist the user agent “Speaking Email SE”. Our device IDs start with “speakingemail”.

Speaking Email includes an “done” command which can be set up by the user to archive, trash, move or mark-as-read. The “archive” action moves mail items to a folder named “Archive”.. If the folder does not exist it will be created automatically.

More information

Our website has more info and comprehensive FAQs at www.speaking.email

For a quick video overview see:

https://www.youtube.com/watch?v=88FYC0qT_cI