Outlook for iOS & Android – Info for IT Pros

Contents

Intro	1
Architecture of the app	1
Data storage	
Passwords and security	
Outlook first run	
Creating an account and protecting passwords	
Inactivity and flushing password from memory	
Flushing encrypted password and message cache from hard disk	
Putting it all together	3
Device identifiers and access control	
ActiveSync policies and mobile device management	5
PIN lock & device encryption	
Remote Wipe	8
Mobile device management	
Blocking the app	
Product Roadmap	

Intro

This document provides a deeper look into Outlook for iOS and Android for IT professionals including information from Microsoft engineers and answers to frequently asked questions we've received from customers. If you have additional questions, please reach out to your Microsoft Account Manager or contact our product team directly by posting in the Exchange IT Pro group on the Office 365 Yammer network.

Architecture of the app

Despite the smartphone becoming a primary screen for reading email, most of us perform only basic email triage on the phone, delaying many tasks until we are at a computer. <u>Outlook was designed</u> to bring together your email, calendar, contacts and files in a fast and feature rich app that helps you get more done while on the go.

In order to fulfill this promise of getting more done, Outlook needs two components - a rich, cloud-enabled native app as the front end, powered by a secure and scalable cloud service on the back end.

The Outlook cloud service (the back end) allows us to present email data in compelling ways and build great experiences for you. For example, our focused inbox feature's intelligence is controlled in this cloud. This cloud allows us to provide a 1-click unsubscribe feature from mailing lists, improve search speed and effectiveness and enable you to forward and send large files without first downloading them to your phone.

Processing information in the Outlook cloud service makes it possible for us to provide new services and capabilities that enhance your Outlook experience and improve performance and stability. Leveraging the power of the cloud, we can keep our application light on local code and rely on the cloud for intensive processing needed to enable our advanced

features. The combination of cloud service and local app gives us the ability to process, secure, and enhance data in ways that we think will delight you, both now and in the future.

Q: Does Microsoft ever plan to deliver a version of Outlook that does not leverage this cloud backend?

A: This cloud structure is a strategic part of the Outlook architecture that we plan to continue. It will allow us to continue to innovate and provide rich features and capability for both end-users and IT.

Data storage

For the benefit of the advanced features discussed above and to facilitate fast, secure delivery down to the device, we cache a subset of email, calendar and files data from your mailbox in our Outlook cloud service. Because the app is based on Microsoft's recent acquisition of Acompli, today that cloud service runs on Amazon Web Services (AWS). We are moving the cloud service to Azure and Office 365 and plan to have that move completed later this year (2015).

The information in Outlook cloud service is currently cached in the United States. As we move to Azure and Office 365, we will align the Outlook cloud service to the principles of the Office 365 Trust Center with a regionalized data center strategy. In Office 365 a customer's country or region, which the customer's administrator inputs during the initial setup of the services, determines the primary storage location for that customer's data.

Q: How much of my mailbox data is cached in the Outlook cloud service?

A: Approximately 1 month of email, calendar and contact data. This caching process is determined algorithmically, based on the size of the mailbox, importance of the folder (e.g. Inbox v. a folder created by the user) and how often you visit the folder. If your emails have attachments and you request to open them in Outlook, the service retrieves them from the mail server, securely stores them temporarily on our servers, and delivers them to the app. Data older than ~1 month is flushed out of our service and only available on your email server.

Q: Is Outlook's cloud service covered by the Office 365 Trust Center?

A: Outlook's cloud service is not currently covered under the Office 365 Trust Center. We are moving to Microsoft Azure and Office 365 later this year, to align to the principles outlined in the Office 365 Trust Center.

Note: The data privacy and security commitments of the Office 365 Trust Center apply to our online services that store data on servers we control. The native mobile apps (like Outlook, Word, PowerPoint, Excel, etc.) are not covered in the Office 365 Trust Center, as data stored locally on a user's device remains under the control of the end user.

For a list of specific services covered by the Office 365 Trust Center, click here.

Passwords and security

Outlook uses OAuth for the accounts that support it (Outlook.com, OneDrive, Dropbox, Box, and Gmail). OAuth provides Outlook with a secure mechanism to access those cloud services without ever touching your password. For accounts that don't support OAuth (Exchange ActiveSync for on-premises Exchange or Office 365, Yahoo, and iCloud), we have to take a different approach.

Note: Outlook will support OAuth for Office 365 in Q2 of CY2015.

Outlook first run

A random AES-128 key is generated by Outlook the first time the application runs following its installation on a device. This key is known as the device key and is stored only on the device.

Creating an account and protecting passwords

When a user logs into Exchange and Office 365, the username, password and device key are sent to the Outlook cloud service over a TLS connection (<u>read more</u> about how TLS encrypts and protects data in transit) and held in runtime compute memory. Once our service verifies the password with your email server, it uses the unique AES-128 device key

to encrypt the password before storing the encrypted password in the Outlook cloud service. The device key is wiped from memory and never stored in the Outlook cloud service.

When a user wishes to connect to Exchange to fetch mailbox data, the device key is passed to Outlook's cloud service from the device over TLS-secured connection and used to decrypt the password in the service in runtime compute memory. The decrypted password is never stored in the service (i.e. written to local storage disk). The device key is wiped from memory.

Once Outlook's cloud service has decrypted the password at runtime, it can then connect to your email server to synchronize mail, calendar and other data. As long as the user continues to open and use Outlook periodically, the Outlook cloud service will keep a copy of your decrypted password in memory to keep the connection to your server active.

Inactivity and flushing password from memory

After 3 days of inactivity, Outlook's cloud service will flush the decrypted password from memory. At this point, Outlook's cloud service is unable to access your email server. It also has no ability to decrypt your password, since the device key necessary to decrypt the password is stored on the device itself and never in our service.

A user account can become inactive one of three ways

- 1. Uninstall Outlook
- 2. Disable background app refresh in Settings and force-quit Outlook
- 3. No internet connection is available on the device, which means Outlook cannot synchronize with Exchange

Note: Outlook will not become inactive simply because the user does not open the app (e.g. over a long weekend where you do not access Outlook to check email). If you keep background app refresh enabled (the default setting for smartphone apps), the push notifications that occur when new messages arrive in your mailbox and background synchronization of mail to the device count as activity.

Flushing encrypted password and message cache from hard disk

The Outlook cloud flushes inactive accounts on a weekly schedule. After a user account becomes inactive, the Outlook service will flush both the encrypted password and all the user's cached mailbox content out of the service.

Putting it all together

Your unique device key is never stored in the Outlook cloud service. Your password is never stored on the device. This architecture means that in order for a malicious party to gain access to your password, they would need unauthorized access to the Outlook cloud service and physical access to your device.

In addition, if you enforce PIN policies and encryption on your user's devices, the malicious party would have to defeat your device's encryption just to get access to the device key. And they would have to do this all before the user noticed that the device was compromised and had requested an administrator to initiate a remote wipe for the device.

Q: Are my users credentials stored in your cloud if I block Outlook from accessing my Exchange server?

A: If you have chosen to block Outlook's access to your Exchange server, the initial connection will be rejected by Exchange. User credentials will not be stored by the Outlook cloud service and the credentials presented in the failed connection attempt are immediately flushed from memory.

Q: How is the unique key and password encrypted in transit to Outlook's cloud service?

A: All communication between Outlook and the Outlook cloud service is done with via a TLS connection (<u>read more</u> about how TLS encrypts and protects data in transit). The Outlook app is only able to connect to the Outlook cloud service.

Q: How do I remove my user's credentials and information from Outlook's cloud service?

You have three options to remove your information from the Outlook cloud service.

- Option 1: Initiate a Remote Wipe for each user who has used Outlook to connect to Exchange.
- Option 2: Have all users delete Outlook. All data will be removed in approximately 3-7 days.
- Option 3: Have each user remove their account from the Outlook app, then delete the app. To remove an
 account, follow these steps: Settings > Account Settings > Select an Account > Remove Account > From Device &
 Remote Data.

Q: The app is closed (and/or is uninstalled), but I still see it connecting to my Exchange Server. How is this happening?

A: The Outlook cloud service decrypts your password in runtime compute memory and uses it to connect to Exchange. Since the Outlook service is connecting to Exchange on behalf of the device to fetch and cache mailbox data, it can continue for a short period of time until the service detects that Outlook is no longer requesting data.

If you uninstall the app without first using the "Remove Account" option, the Outlook cloud service will stay connected to your email server until your account becomes inactive, as described above in "Inactivity and password flushing from memory". To stop this activity, simply follow *Option 1* or *Option 3* from the above FAQ, or block the app (see "Blocking the app" section below).

Q: Is my password less secure in Outlook than when using other Exchange ActiveSync clients?

A: The traditional approach taken by EAS clients is to save user credentials locally on the device. This means a stolen device (if rooted and/or decrypted) could result in a malicious party gaining access to your password. With our approach, they would need unauthorized access to the Outlook cloud service and have physical access to your device.

Q: What is the experience of a user if they attempt to use Outlook after their data has been flushed?

A: If a user becomes inactive (either by disabling background app refresh or having their device disconnected from the internet as described above), Outlook will reconnect to the Outlook cloud service the next time the app is launched and restart the password encryption and email caching process. This is all transparent to the user.

Q: The <u>Privacy Policy</u> states "No person at our company will ever read any of your email or data except in the specific, narrow circumstances described in this Privacy Policy." You also state in this document "Outlook's architecture means that in order to gain access to your password, you would have to have access to both our cloud service and have physical access to the device." How do you access my information without my password?

A: As is the case with all cloud services, our development and support engineers have controlled access to troubleshooting tools that allow them to access data under the conditions described in the privacy policy. If a customer experiences problems with Outlook, the support tools allow us to look at the state of your account without your using your password. We will only do so at the user's request and with the user's explicit permission.

Q: How is the temporarily cached mailbox data secured while at rest in Outlook's cloud service?

A: You can read about how our data is currently protected at the <u>Amazon AWS Security Center</u>. As noted above, we are moving from AWS to Microsoft Azure and Office 365. You can read more about the security of these service as the <u>Azure Trust Center</u> and <u>Office 365 Trust Center</u>.

Device identifiers and access control

Due to our cloud service architecture, Outlook connections appear as a single mobile device identifier (ID) in Exchange. That means mobile device access controls for each user are applied to all devices connected to this device ID.

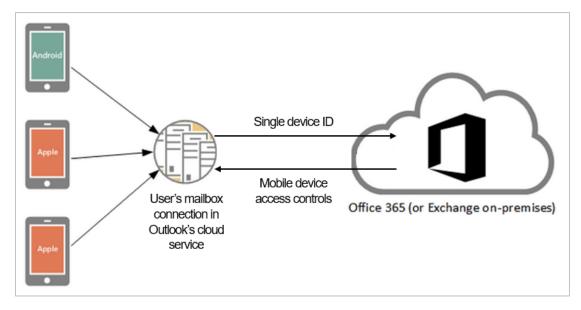


Image used with permission from http://exchangeserverpro.com.

This implementation creates two differences from how traditional Exchange ActiveSync device access controls work:

- Block: a block rule blocks Outlook on all devices and supported operating systems. You cannot block individual devices or operating systems.
- Quarantine: the quarantine process works on a per user basis, rather than a per-device basis. Once a user has a device released from quarantine, they can install and configure Outlook on as many additional devices as they like. Because the user has been released from quarantine, the new devices will not be quarantined.

When mobile device mailbox policies are in place, they apply to all associated devices (Outlook, OWA for iPhone/iPad/Android, other EAS mail clients, etc.). Therefore if you enforce a PIN lock for a specific mailbox, all devices that connect to that mailbox require a PIN.

We will deliver the ability to manage individual device access when we deliver support for Microsoft Intune.

ActiveSync policies and mobile device management

Outlook for iOS & Android supports the most common Exchange ActiveSync policy settings today. We are currently working to enable support for Microsoft Intune to enable mobile device management (MDM) and mobile application management (MAM) capabilities.

Read our recent blog about ActiveSync policy improvements here.

PIN lock & device encryption

If your company email policy requires that devices have a password in order to sync mail, Outlook will enforce this at the device level. How this works on iOS and Android devices varies slightly, based on the available controls provided by Apple and Google.

On iOS devices, Outlook checks to make sure a passcode is properly set. In the event a passcode is not set, Outlook prompts users to create a passcode in iOS settings. Until the passcode is setup, the user will be unable to access Outlook.

Outlook for iOS only runs on iOS 8.0 or later. These devices are shipped with built-in encryption, which Outlook uses once the passcode is enabled to encrypt all the data Outlook stores locally on the device. Therefore, iOS devices with a PIN will be encrypted whether or not this is required by an ActiveSync policy.



Passcode Lock Required

requires that a passcode be set on this device.

Steps for setting a passcode:

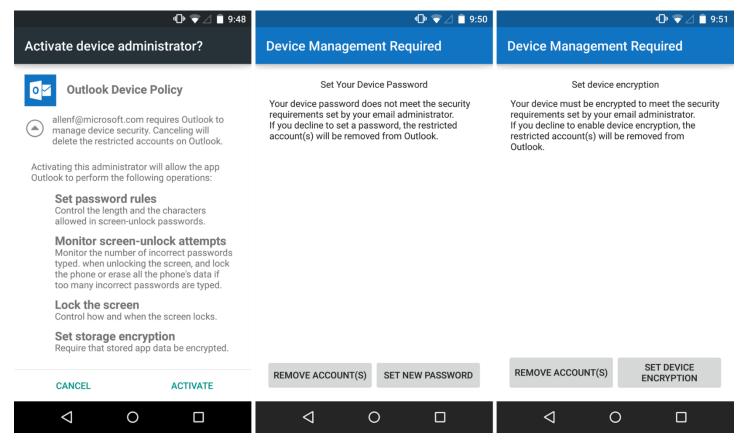
- 1. Go to your system settings
- 2. Select passcode option
- 3. Turn passcode on
- 4. Enter a passcode of your choice

You will not be able to access your mail until a passcode is set. If you do not want to create a passcode on this device, you can delete the account

Delete Account

On Android devices, Outlook will enforce screen lock rules. Further, Google provides controls that allow Outlook to honor additional Office 365 and Exchange policies regarding password length and complexity requirements and the number of allowable screen-unlock attempts before wiping the phone. It will also encourage storage encryption if it is not enabled. Outlook will guide users through this process with a step-by-step walkthrough.

Devices that do not support these security settings will not be able to connect to an account.



Q. The native Mail application on iOS enforces Office 365 and Exchange policies for password length and complexity requirements. Why doesn't Outlook?

A. Outlook takes advantage of the controls available to Microsoft as a third-party application developer. We will continue to improve this capability as we enable support for Microsoft Intune mobile device management and as Apple makes more controls available to developers.

Why does Outlook enforce PIN at the device level, rather than the app level?

A. After talking with customers and evaluating the capabilities available in iOS and Android, we believe a device-level PIN delivers the best experience for customers for both convenience and security. An app-level PIN means you often have to enter two different PINs in order to access your email, which is cumbersome. Further, a device level PIN means we can take advantage of features like native device encryption, TouchID on iOS and Smart Lock on Android. Remote Wipe is still implemented at the app-level, which means your personal applications and data will be unaffected when Outlook is wiped. We will continue to evaluate this approach in response to your ongoing feedback and as we enable support for Microsoft Intune mobile device management.

Q: I was able to cancel out of Android device encryption. How come?

A: If requested by the mobile device mailbox policy, encryption on Android devices will be encouraged and the step-by-step walkthrough will ask the user to set device encryption. Due to differences in availability and implementation by Android OS version and manufacturer and instability in the encryption process, we allow the user to cancel out during the encryption process.

Even if the Android device is unencrypted and an attacker is in possession of the device, the Outlook database is inaccessible with a PIN enabled. This is true even with USB debugging enabled and the Android SDK installed. If an attacker attempts to root the device to bypass the PIN to gain access to this information, the rooting process wipes all device storage and therefore removes all Outlook data.

If the device is unencrypted and rooted by the user prior to being stolen, it is possible for an attacker to gain access to the Outlook database by enabling USB debugging on the device and plugging the device into a computer with the Android SDK installed.

Remote Wipe

The remote wipe command is supported. This is an app-level wipe (not a device wipe). The Outlook app will reset and all Outlook email, calendar, contacts and files data will be removed from the device, as well as from the Outlook cloud service. The wipe will not affect any of the user's personal apps and information outside of Outlook. The wipe happens within seconds of Outlook's next connection to Exchange after the remote wipe command is requested.

Note: Since Outlook for iOS and Android appears as a single mobile device association under a user's mobile devices in Exchange, a remote wipe command will remove data and delete sync relationships from all devices running Outlook (iPhone, iPad, Android).

Q: I notice in testing Remote Wipe is successful, but stays in 'pending' state in Exchange. What is happening?

A: Due to our cloud architecture, the result of the device wipe is not reported back to Exchange. We are working on a solution.

Mobile device management

We understand that mobile device management support is a must-have capability at many businesses today, and supporting these capabilities is high on the Outlook priority list. We are committed to delivering support for Microsoft Intune in Q2 CY2015. The capabilities we will release first are:

- Mobile Device Management (MDM) controls above and beyond what is provided by Exchange ActiveSync (e.g. blocking jailbroken/rooted devices, disabling Bluetooth, preventing screenshots, etc.).
- ◆ Mobile Application Management (MAM) control how Outlook interacts with other corporate managed and unmanaged applications (e.g. ability to restrict copy/cut/paste/save-as actions, only enabling between managed applications, control which cloud storage accounts a user can save to in Files, etc.).
- Conditional Access Policies secure and manage corporate resources by requiring enrollment of devices in Intune before email can be synced. This will enable the ability to restrict email access to individual devices.
 - Note: Conditional Access will only work for customers using Office 365 at launch. We are evaluating how we can deliver this for Exchange on-premises customers.

We will share additional details on timing for these capabilities as soon as we can. Third-party MDM support is still an open discussion as we focus on delivering support for Intune.

Q: Will Outlook work with the mobile device management features coming to Office 365?

A: We <u>announced that built-in mobile device management</u> (MDM) capabilities are coming to Office 365 in the first quarter of 2015. That work remains on track. We will be updating Outlook to support those capabilities when we deliver support for Microsoft Intune. In the meantime, organizations can use Exchange ActiveSync policies to manage the Outlook app.

Blocking the app

Each organization has different policies regarding security and device management. If the current version of Outlook does not meet your needs, you can block the app using Exchange ActiveSync device management policies. The Outlook app is identified in Exchange ActiveSync management screens with the DeviceModel: 'Outlook for iOS and Android' or DeviceType: 'Outlook'. See Controlling Device Access in the TechNet for specific steps.

Office 365 and Exchange Server 2013 customers can continue using the OWA for iPhone/iPad/Android apps, or the built-in mail apps on iOS and Android, while we deliver additional security and management features.

Below is an example of what a device rule looks like in PowerShell after creating with the Exchange Admin Center.

```
C:\windows\system32> Get-ActiveSyncDeviceAccessRule
                   : 0077dc8f-780e-474a-904e-0ac1c467bd86
RunspaceId
QueryString
                  : Outlook
Characteristic
                 : DeviceType
AccessLevel
                  : Quarantine
                   : Outlook (DeviceType)
AdminDisplayName
                  : 0.10 (14.0.100.0)
ExchangeVersion
DistinguishedName : CN=Outlook (DeviceType),CN=Mobile Mailbox Settings,CN=Conf
                     guration,CN=contosogroup.onmicrosoft.com,CN=ConfigurationUn
                     its,DC=NAMPR03A003,DC=prod,DC=outlook,DC=com
                  : Outlook (DeviceType)
: e9a404b5-fbb7-4f10-af82-5a5bba4a9ec1
Identity
Guid
ObjectCategory
                   : NAMPRO3A003.prod.outlook.com/Configuration/Schema/ms-Exch-D
                     evice-Access-Rule
                   : {top, msExchDeviceAccessRule}
ObjectClass
                  : 2/6/2015 3:49:11 PM
: 2/6/2015 3:49:06 PM
whenChanged
WhenCreated
WhenChangedUTC
                 : 2/6/2015 11:49:11 PM
                  : 2/6/2015 11:49:06 PM
WhenCreatedUTC
OrganizationId
                   : NAMPRO3A003.prod.outlook.com/Microsoft Exchange Hosted
                     Organizations/contosogroup.onmicrosoft.com - NAMPRO3A003.pr
                     od.outlook.com/ConfigurationUnits/contosogroup.onmicro
```

Product Roadmap

To bring features to customers faster, Outlook uses a rapid development model and new versions of the app will be available every few weeks. We'll focus on the capabilities that help users get things done on the go, as well as those that help IT secure and manage devices and be compliant with their corporate policies and industry regulations.

The best ways to stay up to date with the new features of Outlook are:

- ◆ Roadmap.office.com see what is coming in future updates
- iOS/Android release notes when we push updates to Outlook on iOS and Android, the app will notify you what has changed
- <u>Blogs.office.com</u> for the most important and requested updates, we will provide additional detail on the Office blog (e.g. PIN lock and other updates to Outlook).

Coming IT controls:

- Support for Microsoft Intune mobile device management (including support for managing individual device access)
- Moving Outlook's cloud service from Amazon Web Service to Microsoft Azure
- Improvements to reporting and execution of remote wipe

Have a feature request? Let us know right from Outlook by navigating to **Settings > Help > Contact Support**, as this will help us triage and prioritize.