eHealth Ontario

ONE® Mail Direct for Mobile Devices

Guide

Version: 2.2

Document ID: 3292

Document Owner: ONE Mail Product Team

Ontario
eHealth Ontario

Table of Contents

1 About This Guide

1.1 Introduction

This guide describes how users of eHealth Ontario's ONE Mail Direct secure e-mail system can configure mobile devices to access ONE Mail.

Privacy and security tips for mobile devices are also included.

This guide covers iOS (Apple), Android, BlackBerry, and Windows Phone, and it may also be useful for other types of devices.

For information on accessing ONE Mail Direct through a web browser or desktop e-mail software, see the guides on the ONE Mail resources web site.

1.2 Audience

This guide is intended for people who wish to integrate mobile devices with Microsoft Exchange ActiveSync in order to access ONE Mail Direct accounts.

1.3 Terms of Use

Users choosing to access ONE Mail through mobile devices must ensure that they understand and adhere to all privacy, security, and legal declarations in the ONE Mail Direct Services Schedule as well as organizational policies concerning use of Exchange ActiveSync and other connection methods.

This document does not override legal schedules. In the event that there is a difference between information contained here and information contained in the ONE Mail Direct Services Schedule, the ONE Mail Direct Services Schedule is deemed correct.

1.4 Support

The ONE Mail Direct Services Schedule describes support provided by eHealth Ontario.

The first line of support is the client's own help desk. Beyond that, the eHealth Ontario service desk is available 24/7:

1-866-250-1554
ServiceDesk@ehealthontario.on.ca

For support for the mobile device itself, including connectivity issues, contact the device vendor or the network provider.

2 ONE Mail Overview

2.1 Background

ONE Mail is a secure e-mail system provided and paid for by eHealth Ontario, an agency of Ontario's Ministry of Health and Long-Term Care.

ONE Mail ensures fully encrypted e-mail transmission from source to destination whenever both sender and receiver are using ONE Mail.

Ontario's health care providers use ONE Mail to securely transmit personal health information (PHI), personal information (PI), and other data within Ontario's health care community. ONE Mail links thousands of health care professionals using state-of-the art encryption and malware (malicious software) filtering.

ONE Mail is the preferred secure e-mail system for a large and growing number of clients, including all major hospitals in Ontario.

Clients can subscribe to ONE Mail through one of two related services: ONE Mail Direct or ONE Mail Partnered. ONE Mail Direct (running on Microsoft Exchange) provides users with mailboxes housed in eHealth Ontario's secure data centres. ONE Mail Partnered securely connects organizations' existing e-mail systems to eHealth Ontario's centralized, secure infrastructure while ensuring end-to-end encryption.

This document covers ONE Mail Direct.

For more information, see the ONE Mail web site.

2.2 ONE Mail Compared to Other E-Mail Services

ONE Mail ensures fully secure e-mail transmission from source to destination whenever both sender and receiver are using ONE Mail.

Basic e-mail, including the various free services available on the Internet and accounts provided by ISPs, is unprotected. Mail can be intercepted and read by unauthorized people and machines as it moves across the public Internet. Basic e-mail is like a physical postcard: contents can easily be viewed by people other than the intended recipient. Never send personal information or personal health information over unsecured e-mail.

In contrast to basic e-mail, ONE Mail is highly protected by layers of security at the operating, technical, and software levels. Messages sent via ONE Mail are encrypted in transit and remain illegible until decrypted by the recipient. As well, servers for ONE Mail are located at eHealth Ontario's secure data centres.

Both sender and receiver must be using ONE Mail to ensure security of e-mail transmission.

2.3 ONE Mail Security

The ONE Mail infrastructure was designed and built with security and privacy in mind. ONE Mail provides spam and virus filtering, IP reputation handling, spoof protection, and end-to-end e-mail encryption.

2.4 Identity Confirmation: ONE ID

ONE ID is the name of eHealth Ontario's identity and access management service. ONE Mail Direct users receive ONE ID user names after successfully completing an identification process which ensures that they are indeed who they say they are. Access to ONE Mail (and listing in ONE Pages, the ONE Mail directory) is granted only after positive confirmation of identity.

A ONE ID account can also provide access to other eHealth Ontario services. For more information, see the ONE ID web site.

3 A Note on User ID, E-Mail Address, and Password

Each ONE Mail Direct user has a ONE ID user name as well as a ONE Mail e-mail address.

ONE ID user names have the format "firstname.lastname@oneid.on.ca," and they are the keys to accessing various eHealth Ontario services (including ONE Mail Direct).

ONE Mail e-mail addresses end in either "@one-mail.on.ca" or in a custom domain name like "@OntarioMedClinic.ca."

This terminology may be confusing because the identifiers can look very similar:
"dewey.rahim@oneid.on.ca" is a ONE ID user name (also called account name and user ID);
"dewey.rahim@one-mail.on.ca" is a ONE Mail Direct e-mail address.

Using the examples above, Dewey Rahim would use the user name "dewey.rahim@oneid.on.ca" to log in to the e-mail account that has the address "dewey.rahim@one-mail.on.ca."

Note that **a single password applies to both the ONE ID user name and to the ONE Mail Direct e-mail account.** That is, users enter the same password whether they are logging in to the eHealth Ontario portal or to a ONE Mail Direct account.

To change a password or perform other account maintenance, log in to the ONE ID account maintenance site.

4 Microsoft Exchange ActiveSync Description

Microsoft Exchange ActiveSync is a connection protocol that, in this case, allows users to access eHealth Ontario's ONE Mail Direct service using mobile devices. The protocol allows functions such as sending and receiving e-mail messages and calendar entries.

5 Quick Setup: Exchange ActiveSync Settings for Advanced Users

This section summarizes the configuration required to connect a mobile device to the ONE Mail Direct service using Exchange ActiveSync.

Following sections of this document provide step-by-step instructions for Apple iOS, Android, Blackberry, and Windows Phone devices.

Domain	[leave blank]
E-mail Address	ONE Mail Direct e-mail address (for example, Dewey.Rahim@one-mail.on.ca)
User ID	Full user ID (which differs from e-mail address; for example, Dewey.Rahim@oneid.on.ca)
Password	The password corresponding to both the user ID and the e-mail address
Server	mail.one-mail.on.ca
Port	443
Security type	SSL

If prompted to accept security settings during configuration, agree to the settings.

For information on features for a particular device, refer to the manufacturer's documentation.

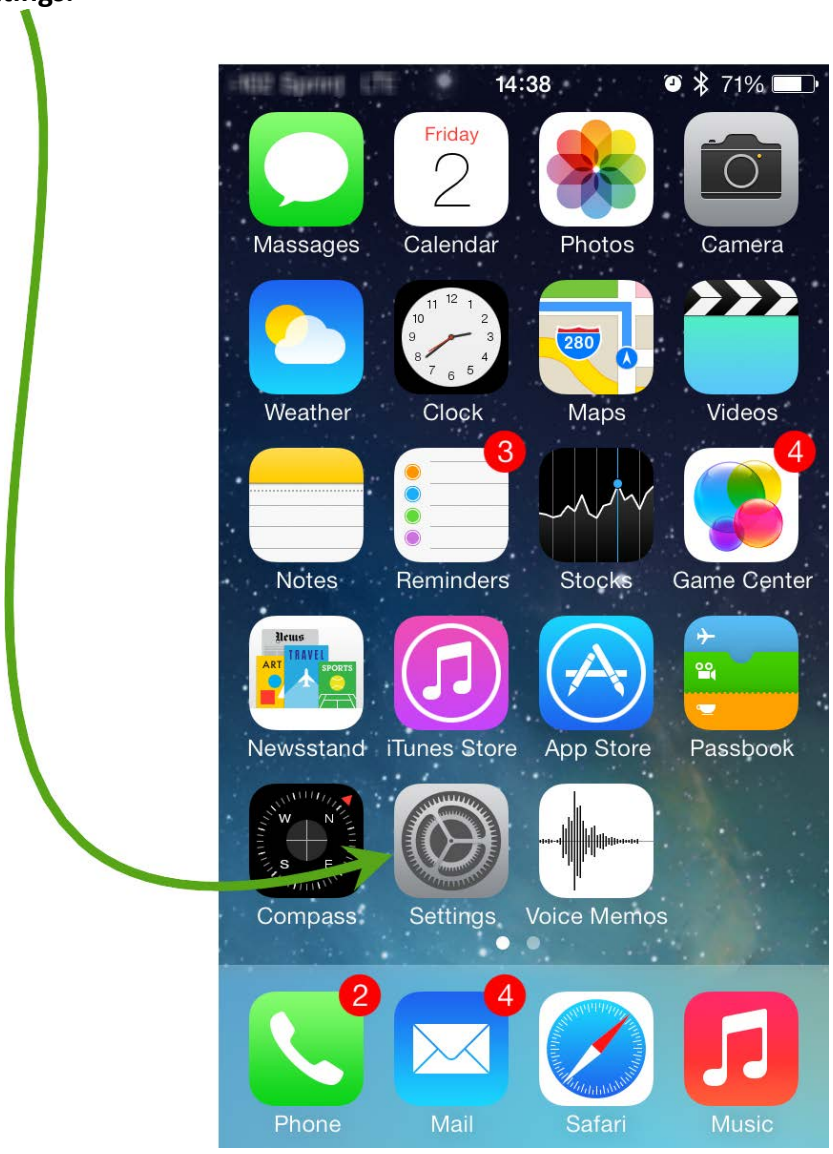
6 Exchange ActiveSync Setup for Apple iOS

6.1 Preamble

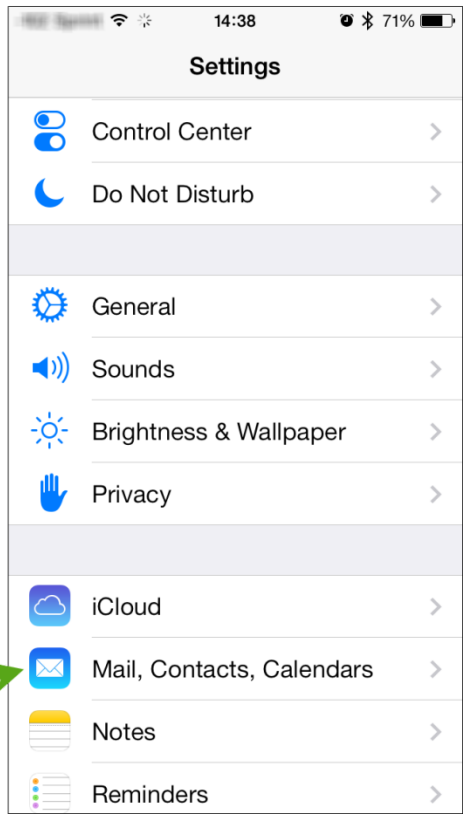
The following procedure applies to Apple iPhone, iPad, and iPod devices running iOS 4.0 or higher.

6.2 Procedure

Select **Settings:**

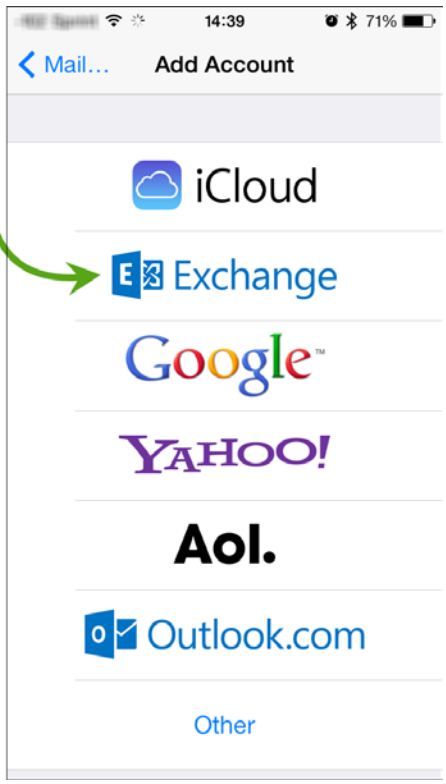


Select **Mail, Contacts, Calendars:**

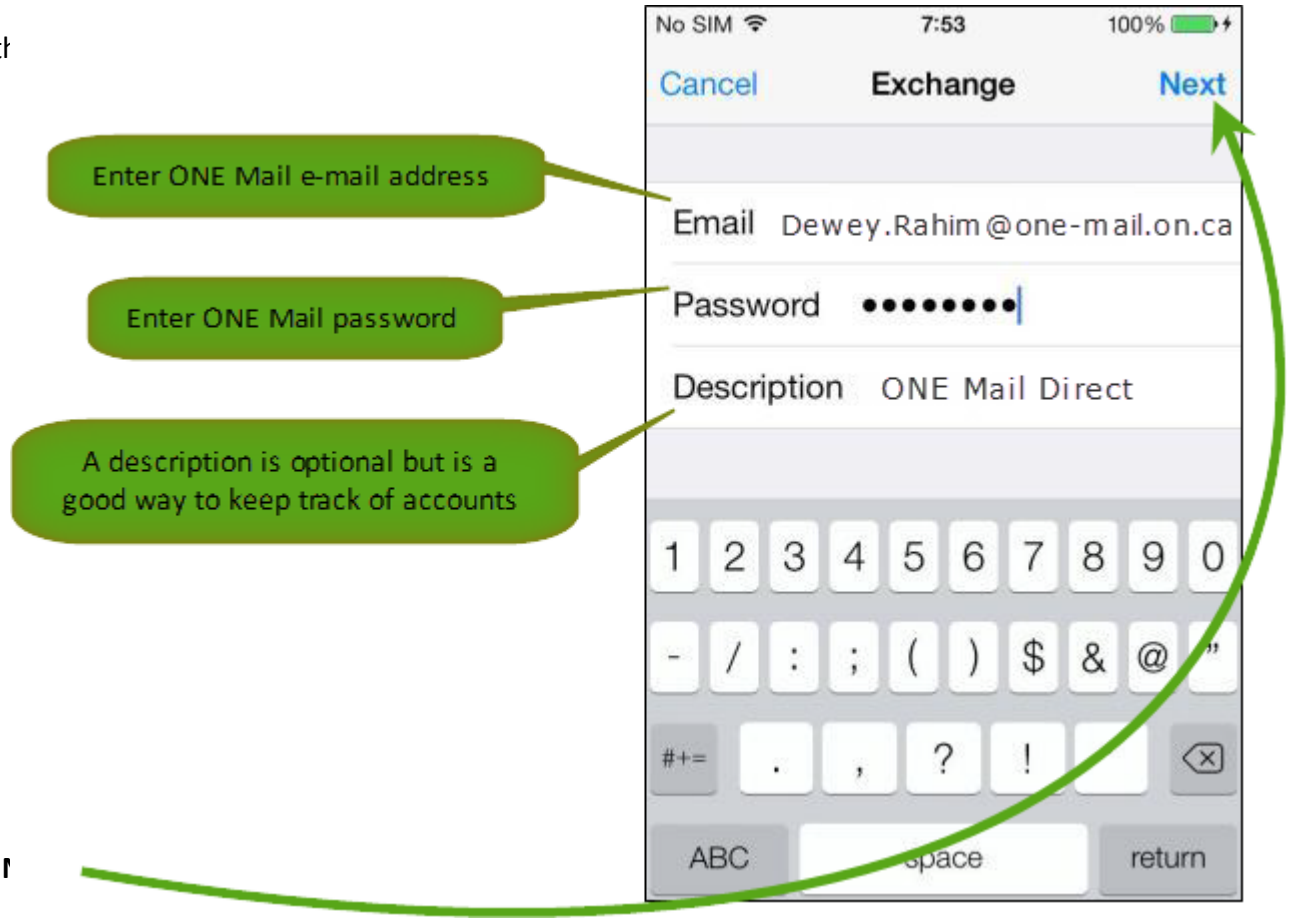


Select **Add Account:**

Select **Exchange:**

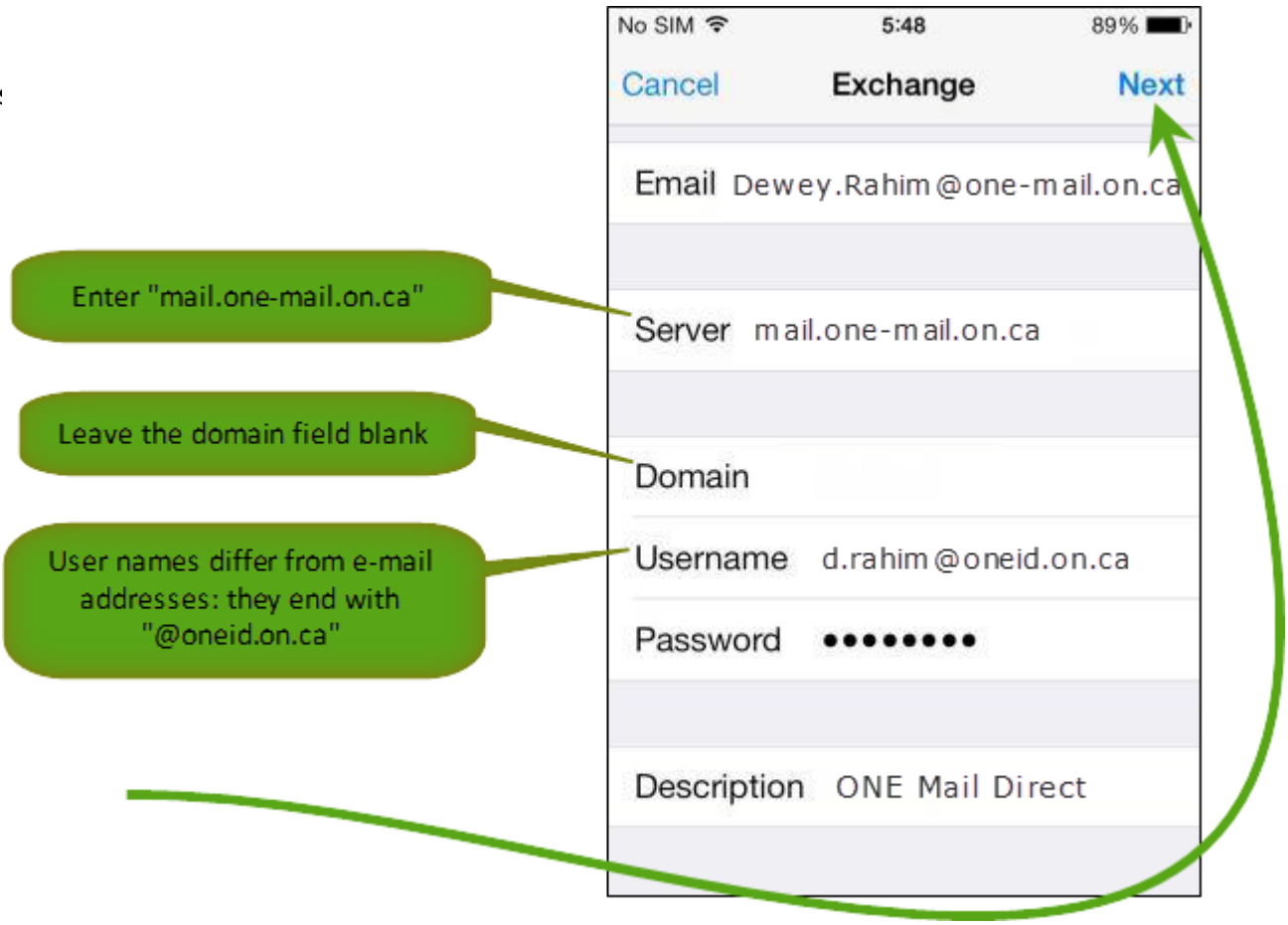


Fill in th



Select M

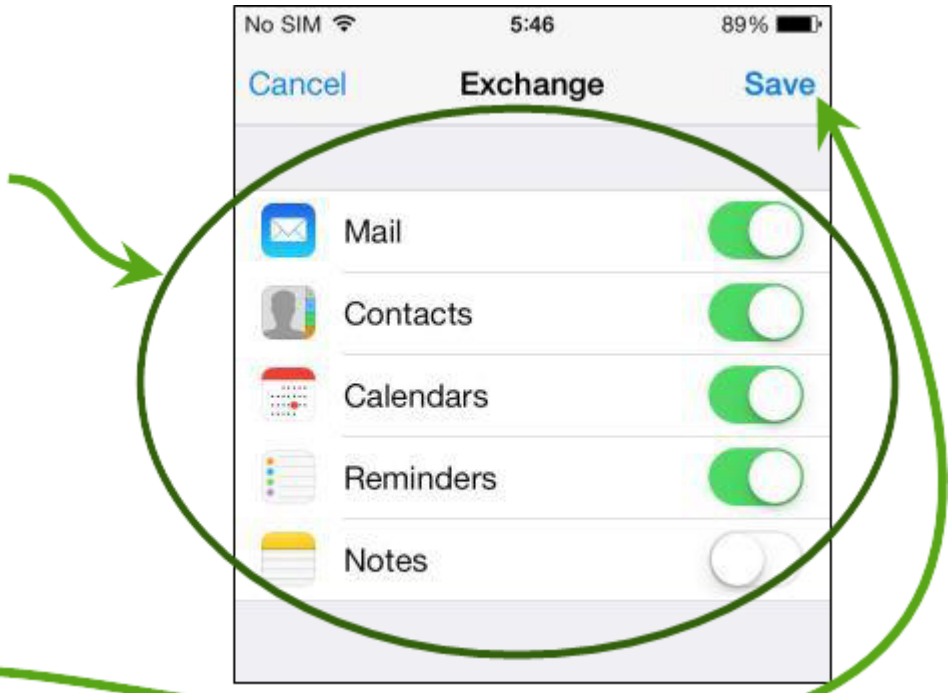
Fill
as :



Sel

The system will attempt to verify the new account's configuration.
If the device asks for confirmation, select **yes.**

Select which combination
contacts, etc. to synchroni



Select **Save** when finished:

The device is now configured for ONE Mail access.

6.3 Handling Multiple E-mail Accounts on the Same Device

When composing an e-mail message on an iOS device configured for multiple e-mail accounts, be sure to select the appropriate account from which the message should be sent.

To change the “from” account while composing a message, select the “Cc/Bcc, From:” field to make it expand, and then select the “From” field to display a selectable list of available accounts.

6.4 Wipe Device

It is possible to delete (“wipe”) all data from an iOS device by remote control. This feature is useful if the device is lost or stolen.

A wipe removes data and configuration information from the device. A wipe permanently deletes all data and restores the device to factory settings.

For lost or stolen devices, contact the eHealth Ontario service desk to have the device remotely wiped. The service desk is available 24/7:

1-866-250-1554
ServiceDesk@ehealthontario.on.ca

See the Security section of this document for more information.

7 Exchange ActiveSync Setup for Android

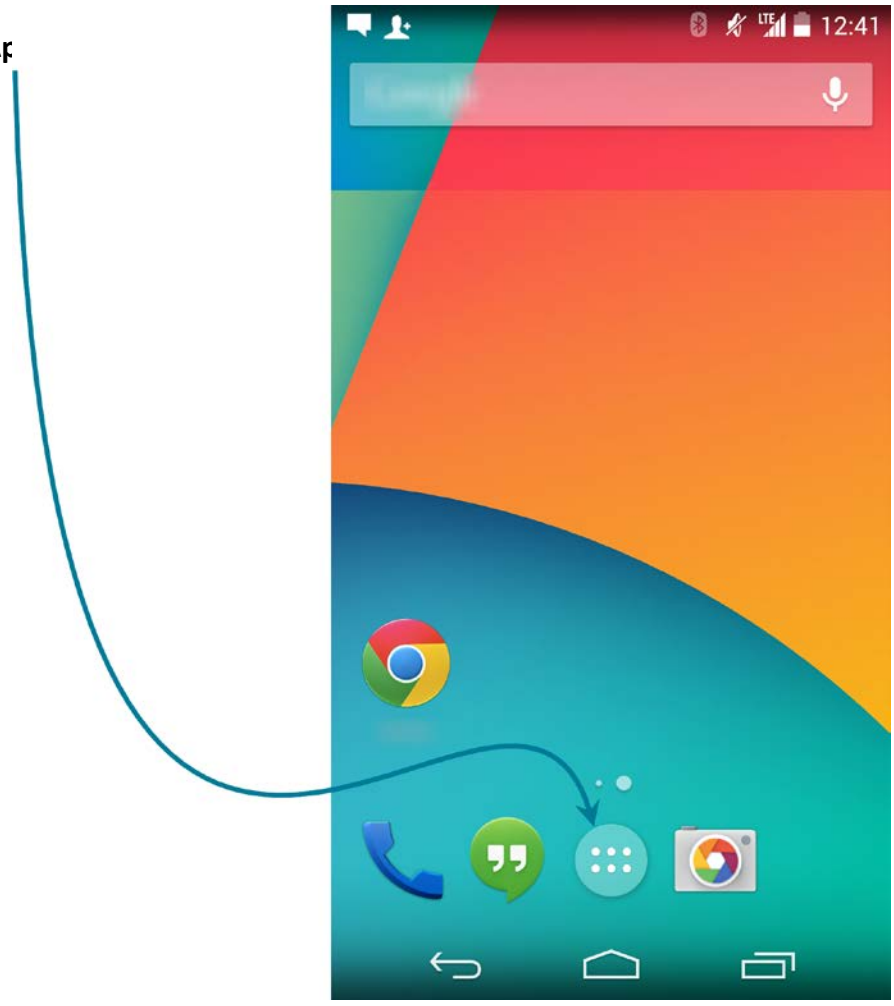
7.1 Preamble

The following procedure applies to mobile devices running the Android operating system.

Because there are a variety of Android devices available, screenshots in this document may differ somewhat from screens on other devices, but the procedure for setting up ActiveSync is similar on all varieties of Android software.

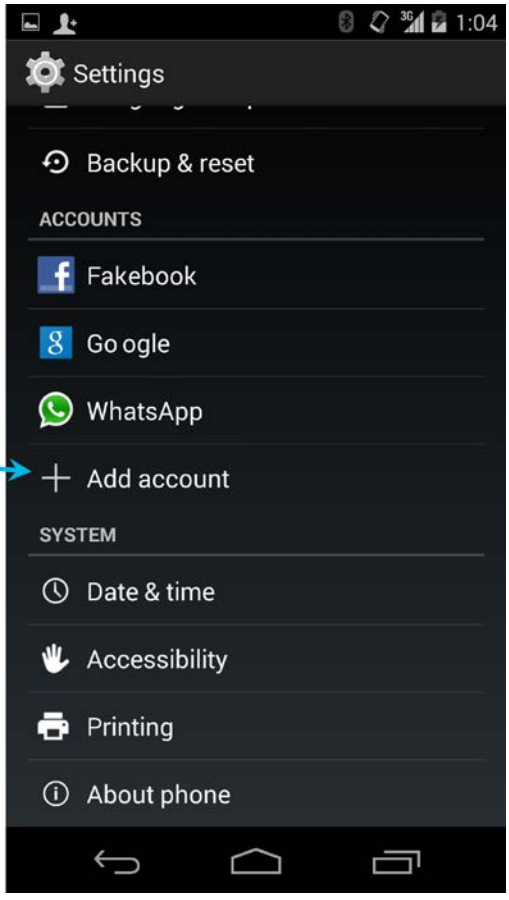
7.2 Procedure

Select the **Ap**

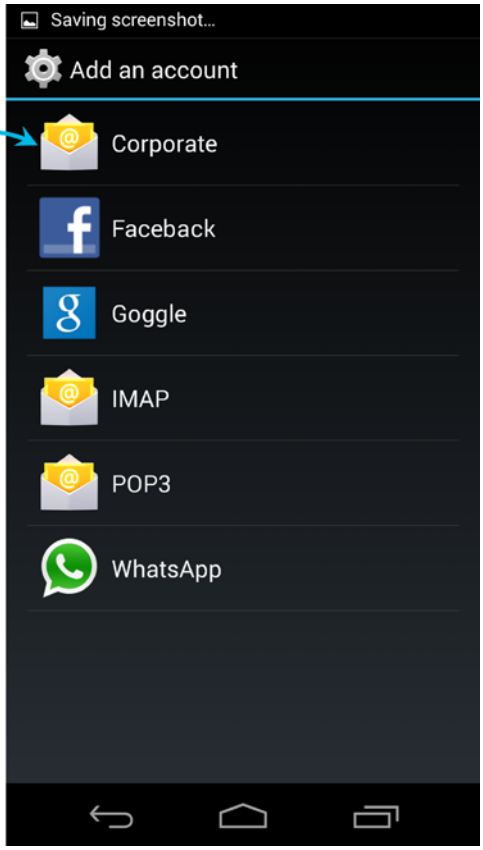


Select **Set**

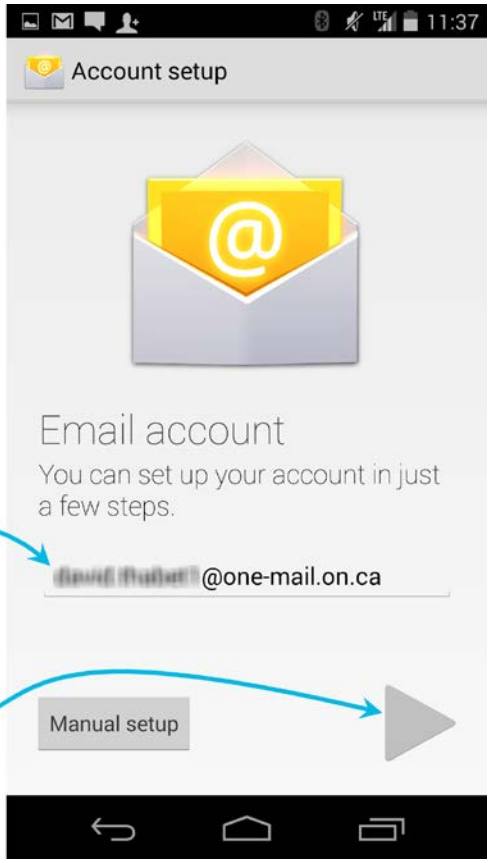
Select **Add account.**



Select **Corp**

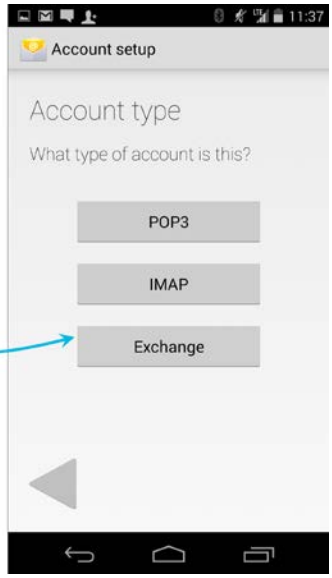


Enter ONE M
(probably er



...then selec

Select **Exch**



Fill in the fields as shown:

This field may default incorrectly

User names differ from e-mail addresses: they end in "@oneid.on.ca"

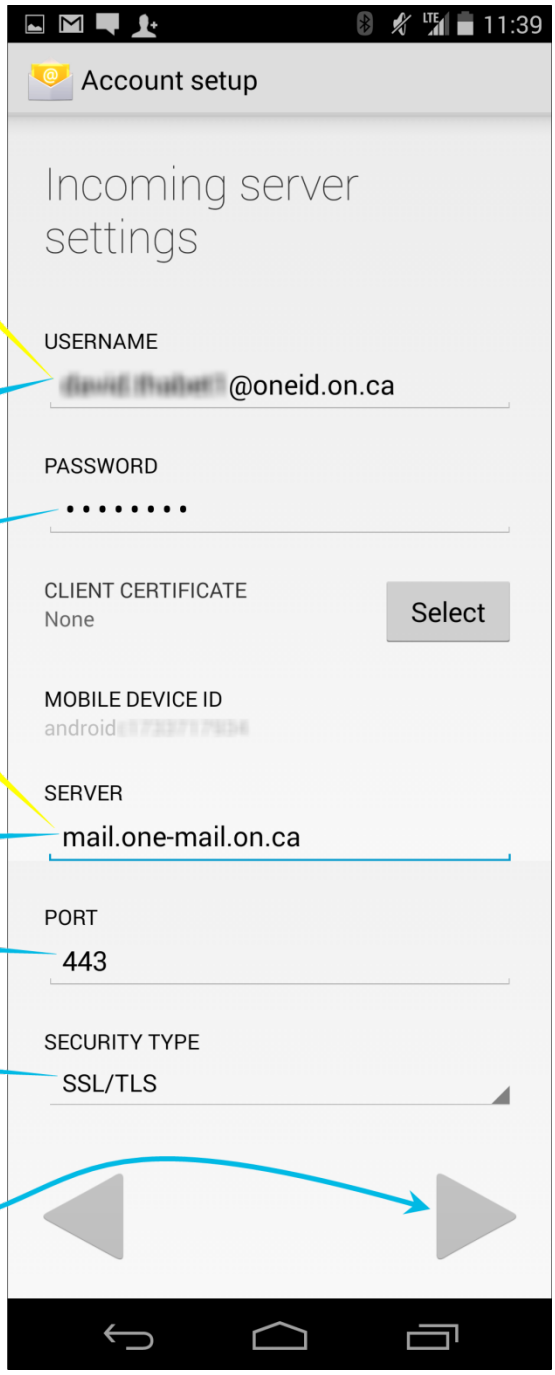
Enter ONE Mail password

This field may default incorrectly

Enter "mail.one-mail.on.ca"

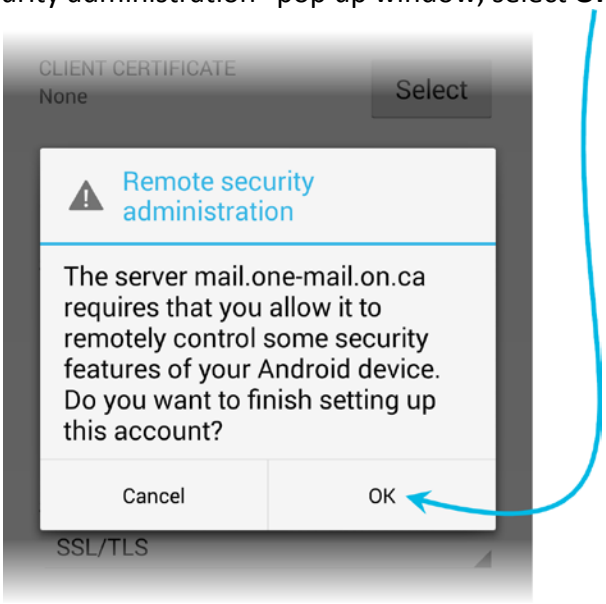
The default value of "443" is correct

Security type "SSL/TLS" is correct

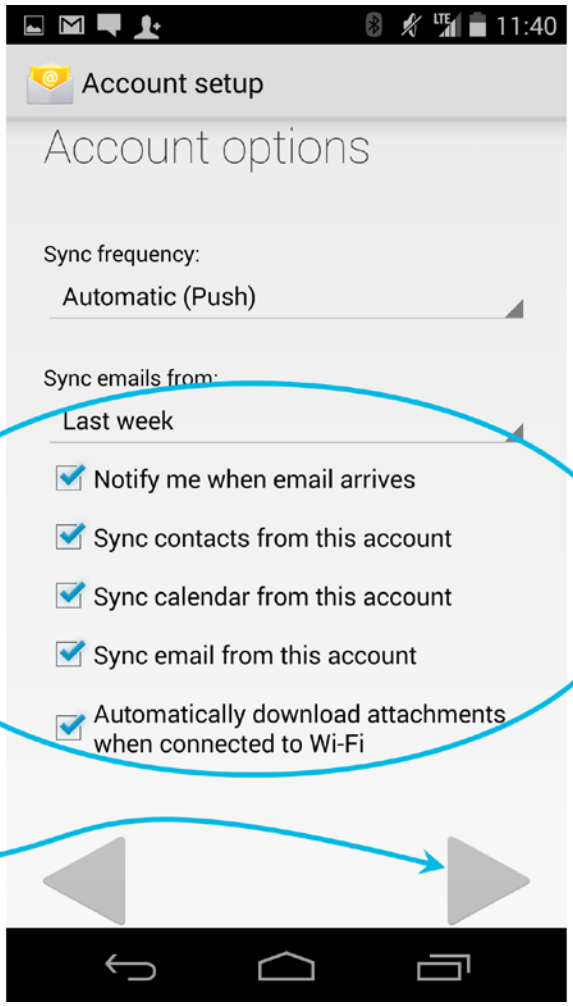


Select the right arrow:

At the “Remote security administration” pop up window, select **OK.**

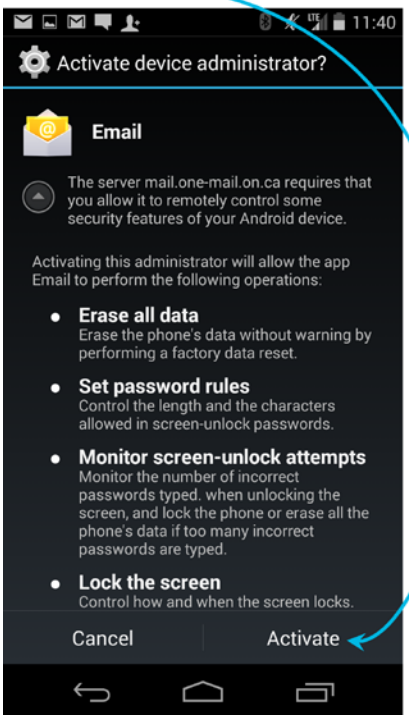


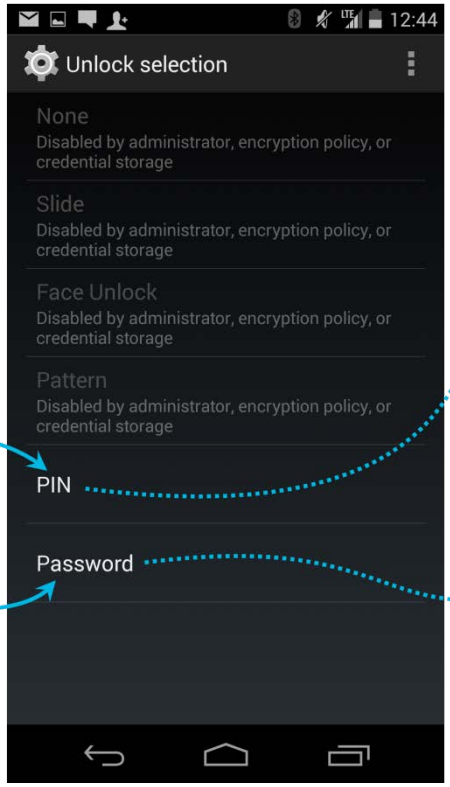
Select synchronization



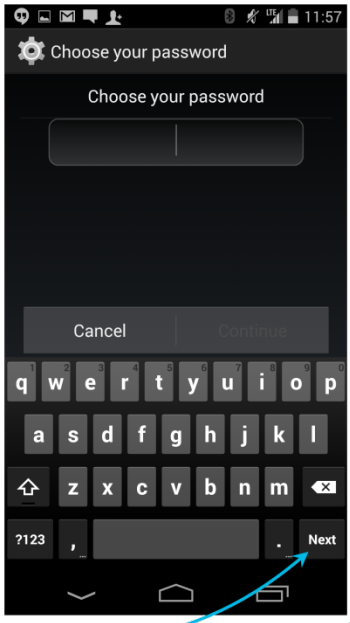
Select the right arrow:

Select **Activate:**



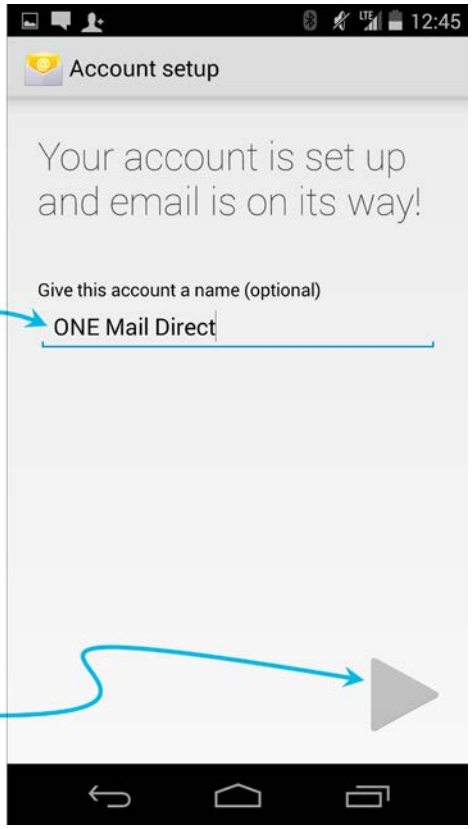


Select **PIN** or **Password:**



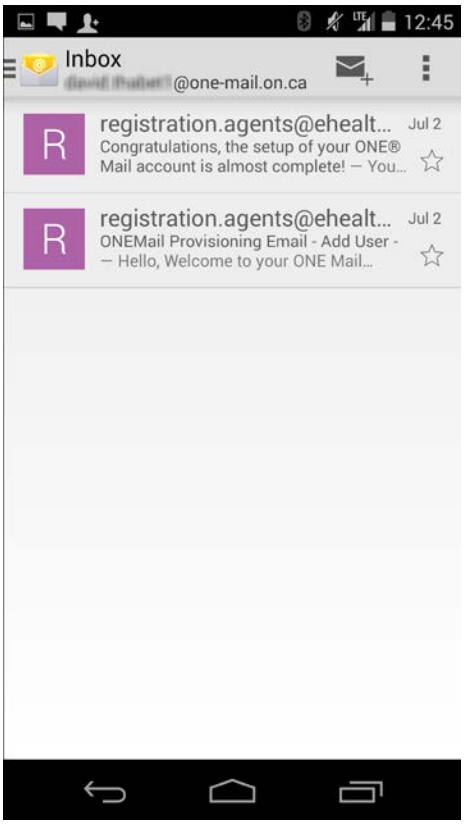
Enter either PIN or password, and then select **Next:**

Enter a name for the acc



Select the right arrow:

The device opens the newly-connected ONE Mail account and displays the mailbox contents:

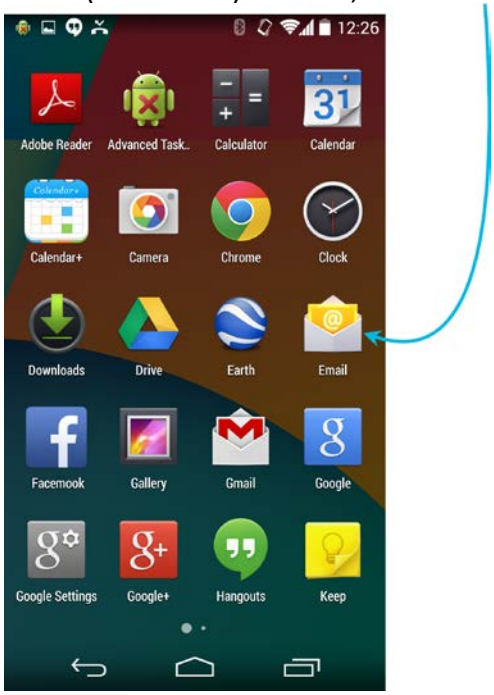


The device is now configured for ONE Mail Direct access.

7.3 Handling Multiple E-mail Accounts on the Same Device

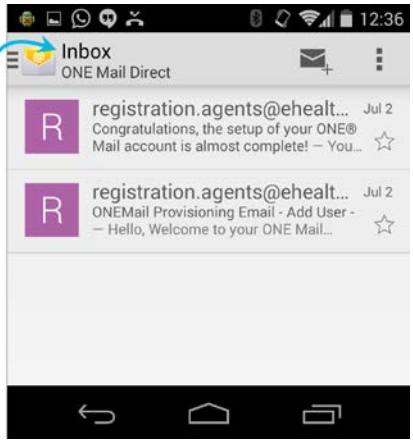
It is possible to have multiple e-mail accounts configured on the same Android device. Aside from Gmail accounts, which have their own icon, most accounts are grouped together under “Email.”

To access the ONE Mail (or another) account, select **Email:**

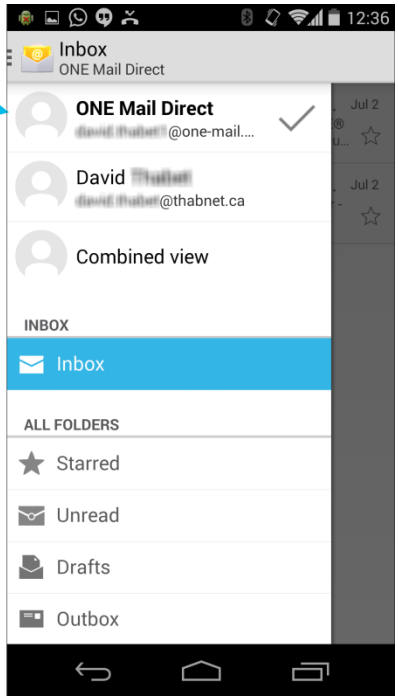


The device displays the contents of one or more mailboxes:

To see conter of a different select **Inbox..**

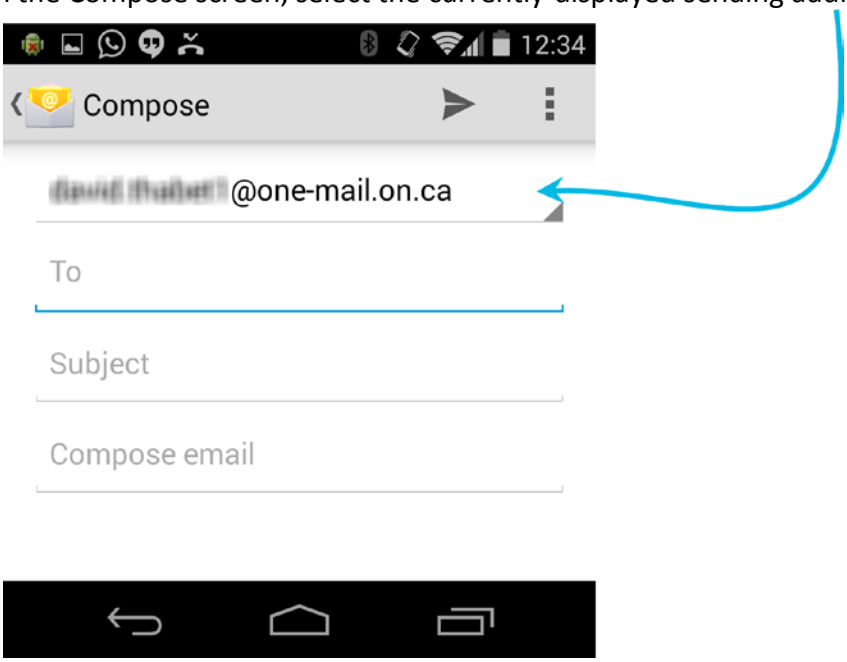


...and then select the preferred mailbox:

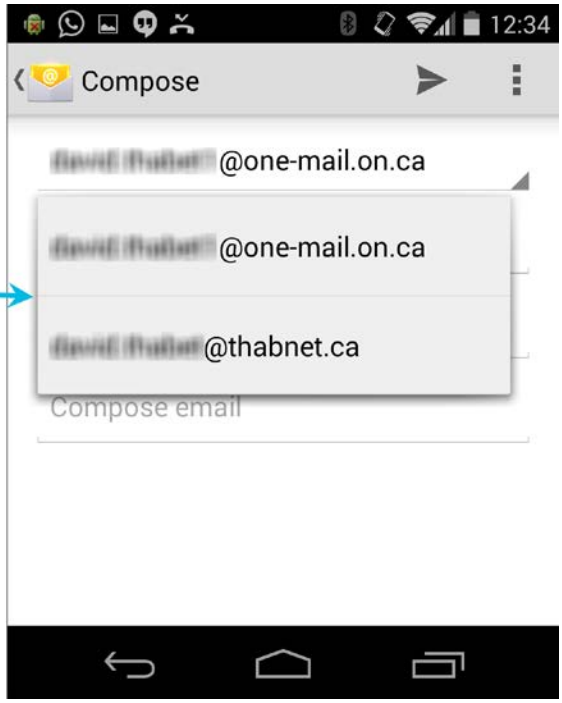


When composing a message on an Android device configured for multiple e-mail accounts, be sure to select the appropriate account from which the message should be sent.

From the Compose screen, select the currently-displayed sending address:



Select the preferred s
from the list of availa



7.4 Wipe Device

It is possible to delete ("wipe") all data from an Android device by remote control. This feature is useful if the device is lost or stolen.

A wipe erases all data from the device (and its SD card) including e-mail, calendar, contacts, photos, music, and users' personal files.

For lost or stolen devices, contact the eHealth Ontario service desk to have the device remotely wiped. The service desk is available 24/7:

1-866-250-1554
ServiceDesk@ehealthontario.on.ca

See the Security section of this document for more information.

8 Exchange ActiveSync Setup for BlackBerry 10

8.1 Preamble

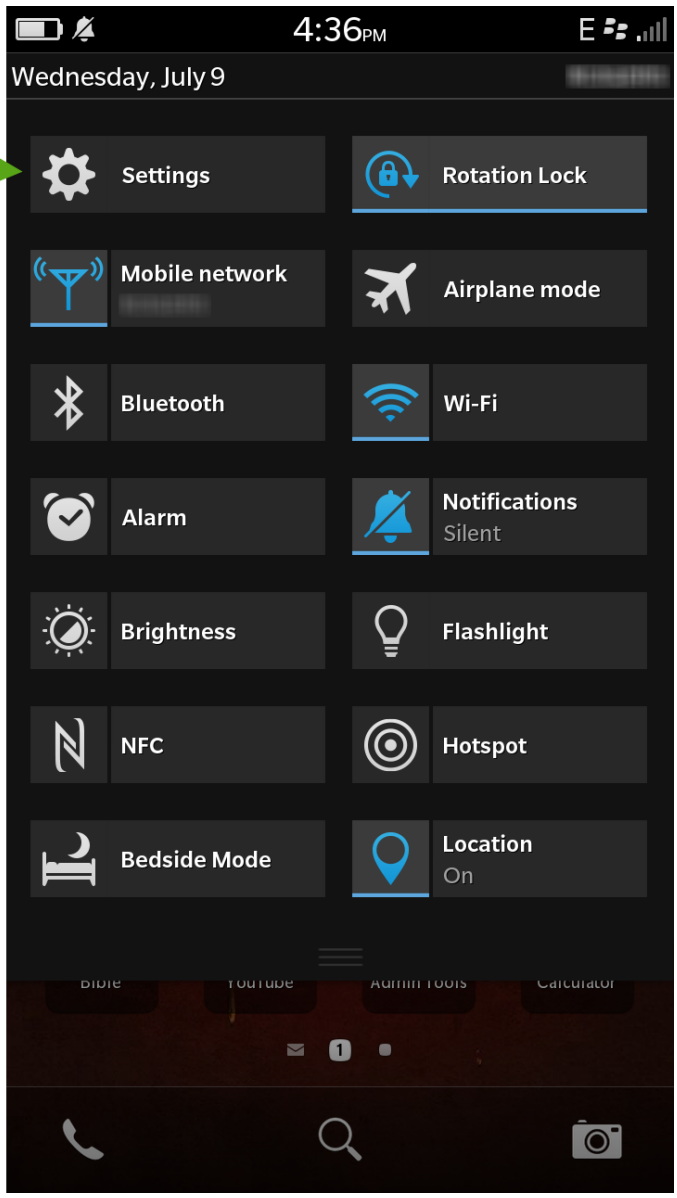
The following procedure applies to devices running BlackBerry 10 OS.

Devices running operating systems earlier than BlackBerry 10 OS are no longer supported.

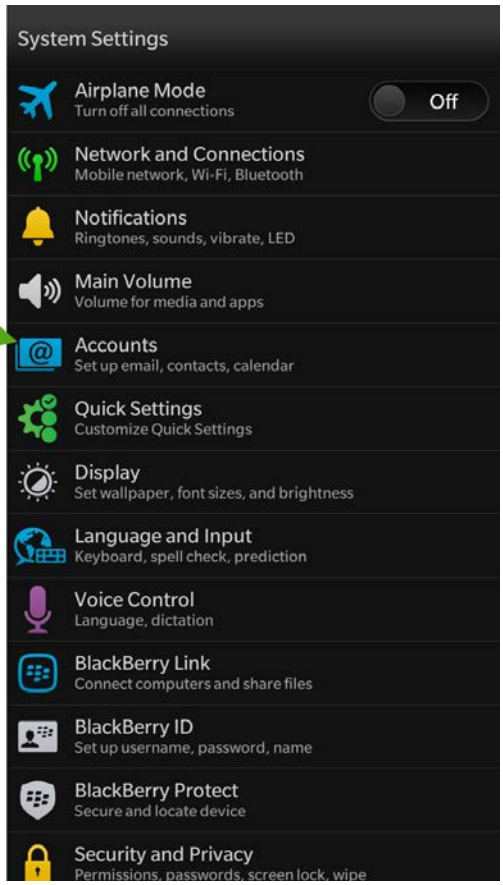
8.2 Procedure

On the BlackBerry device, from the Home screen, swipe down from the top of the screen. The Quick Settings menu appears.

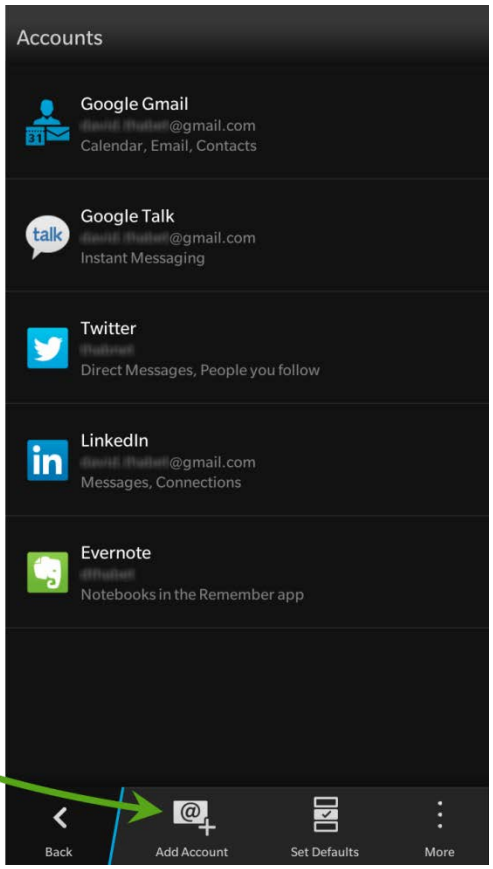
Select **Settings:**



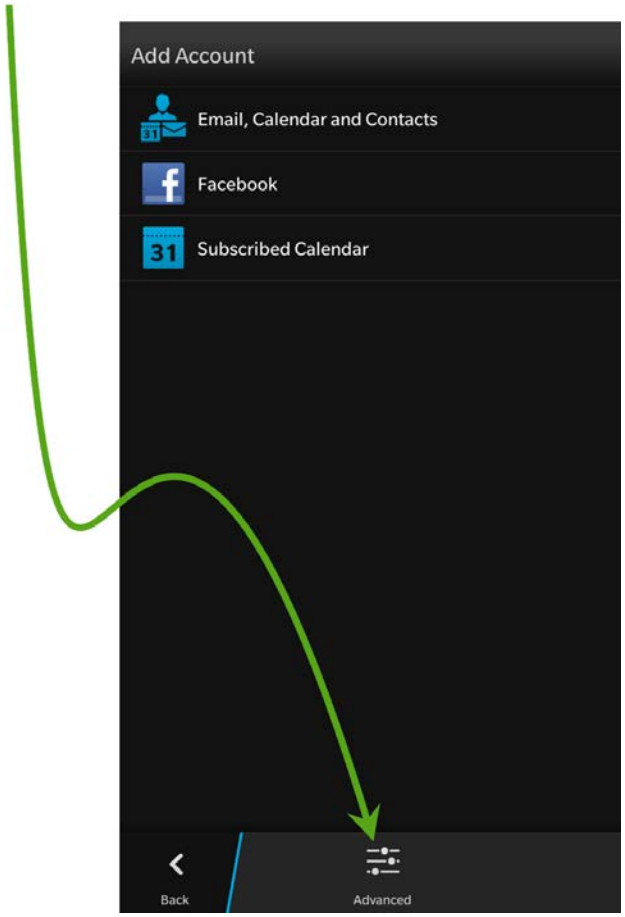
Select **Accour**



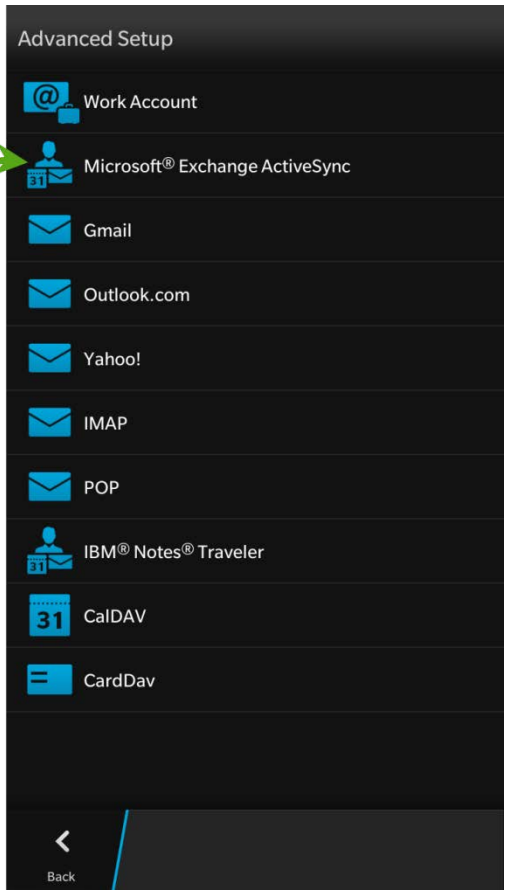
Select **Add Account:**



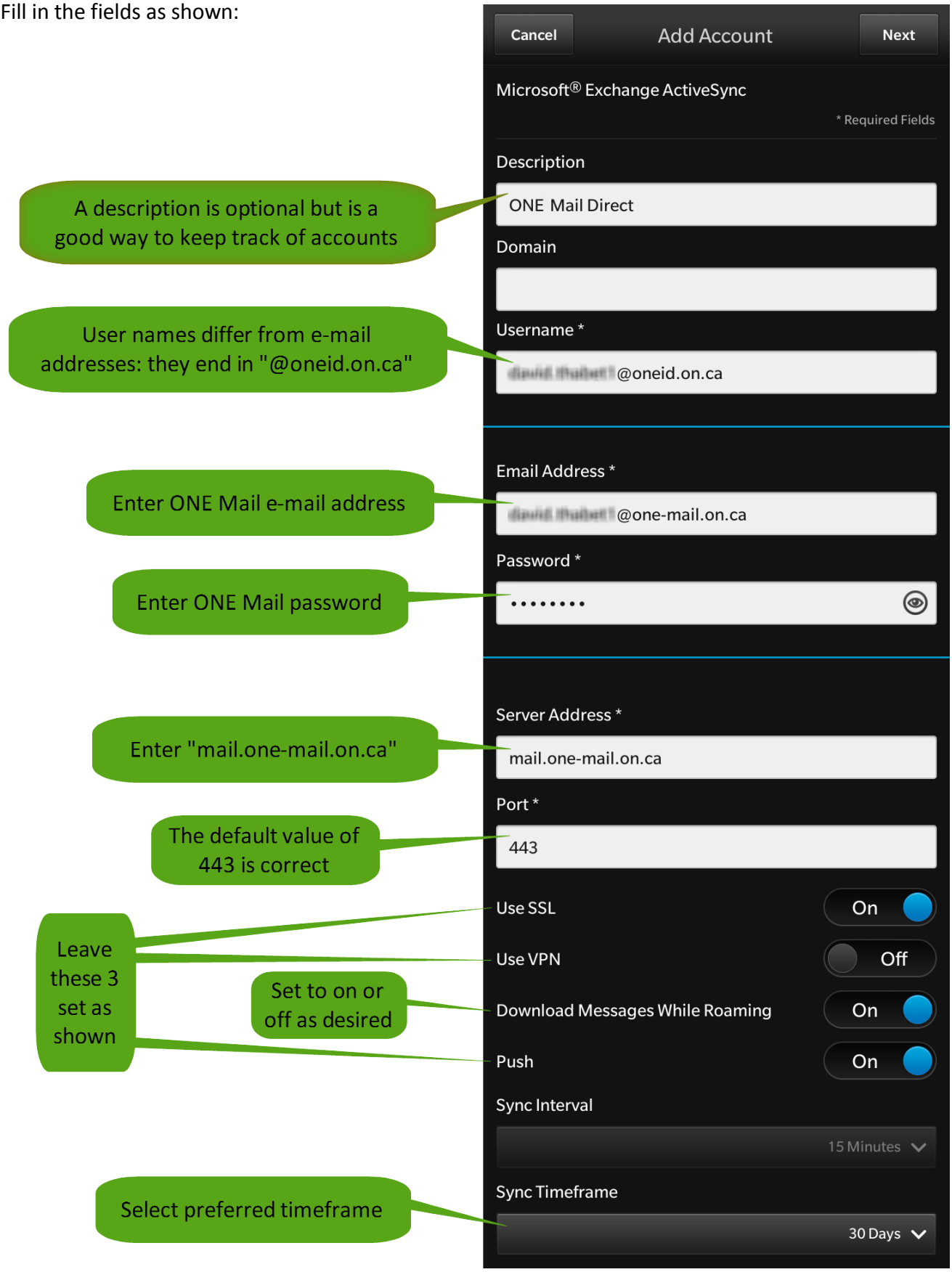
Select **Advanced:**



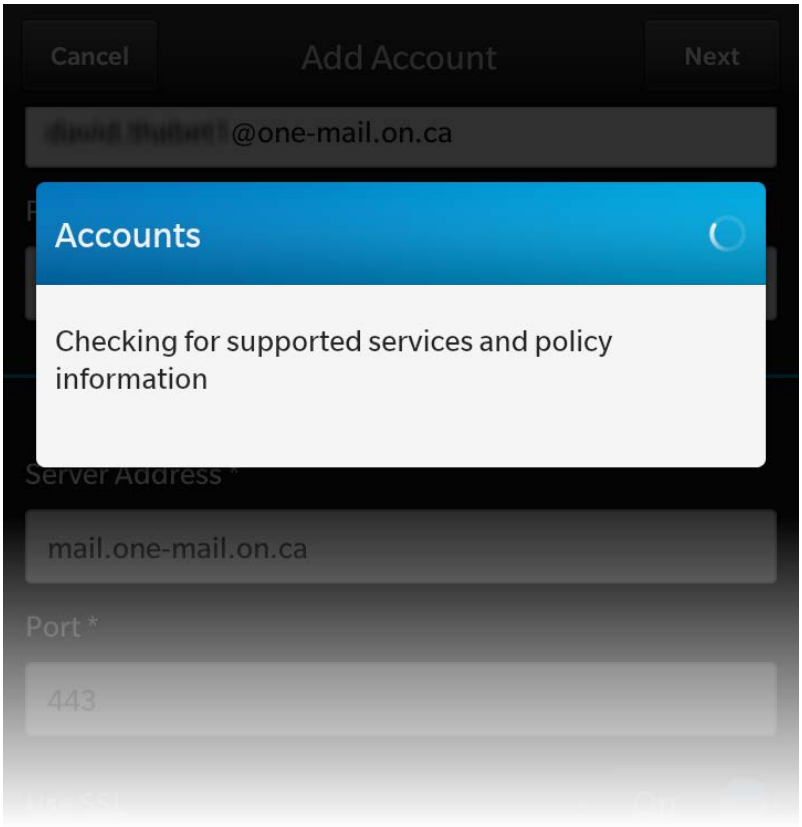
Select **Microsoft Exchange ActiveSync:**



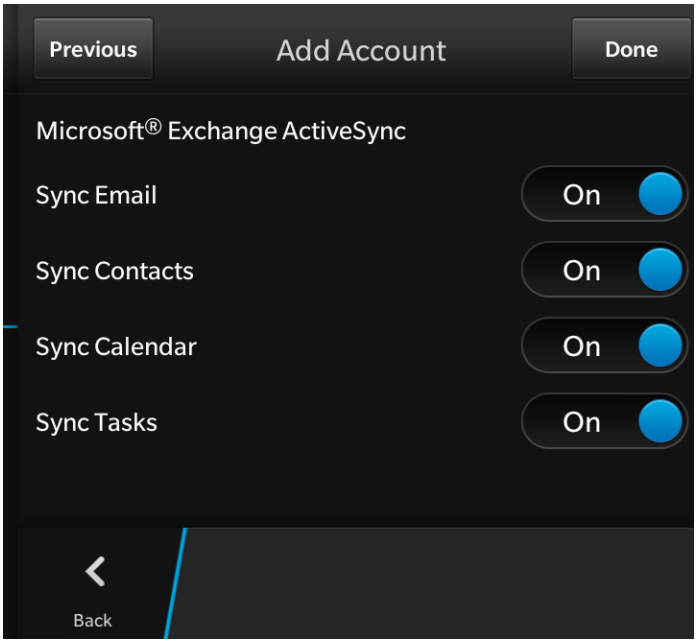
Fill in the fields as shown:



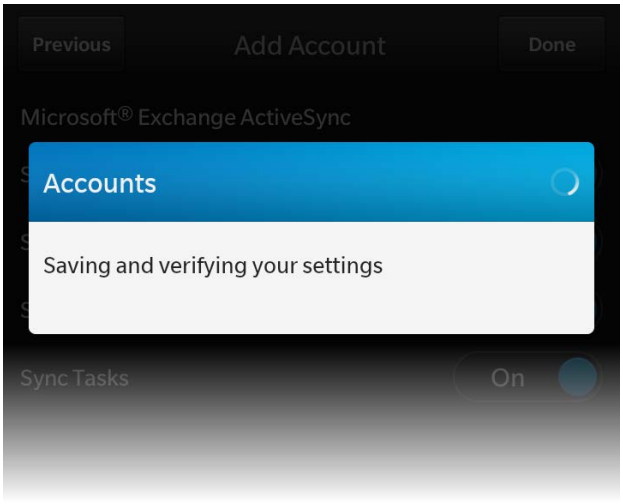
Select **Next**, and the device configures the account:



Select which combination of mail, contacts, calendars, and tasks to synchronize:

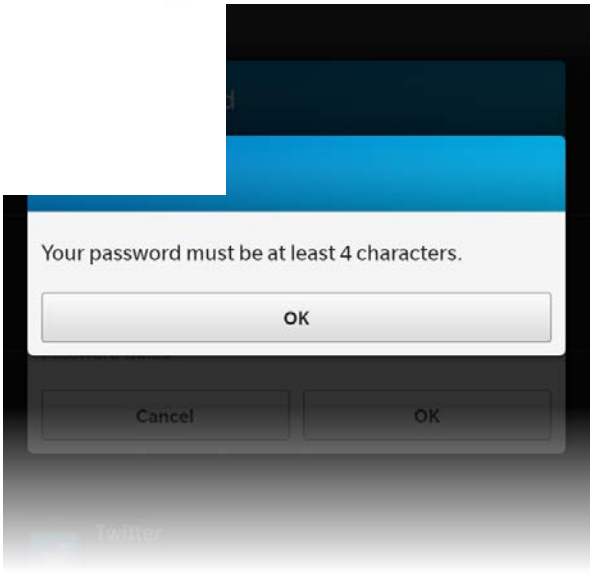


Select **Done,** and the device saves and verifies:



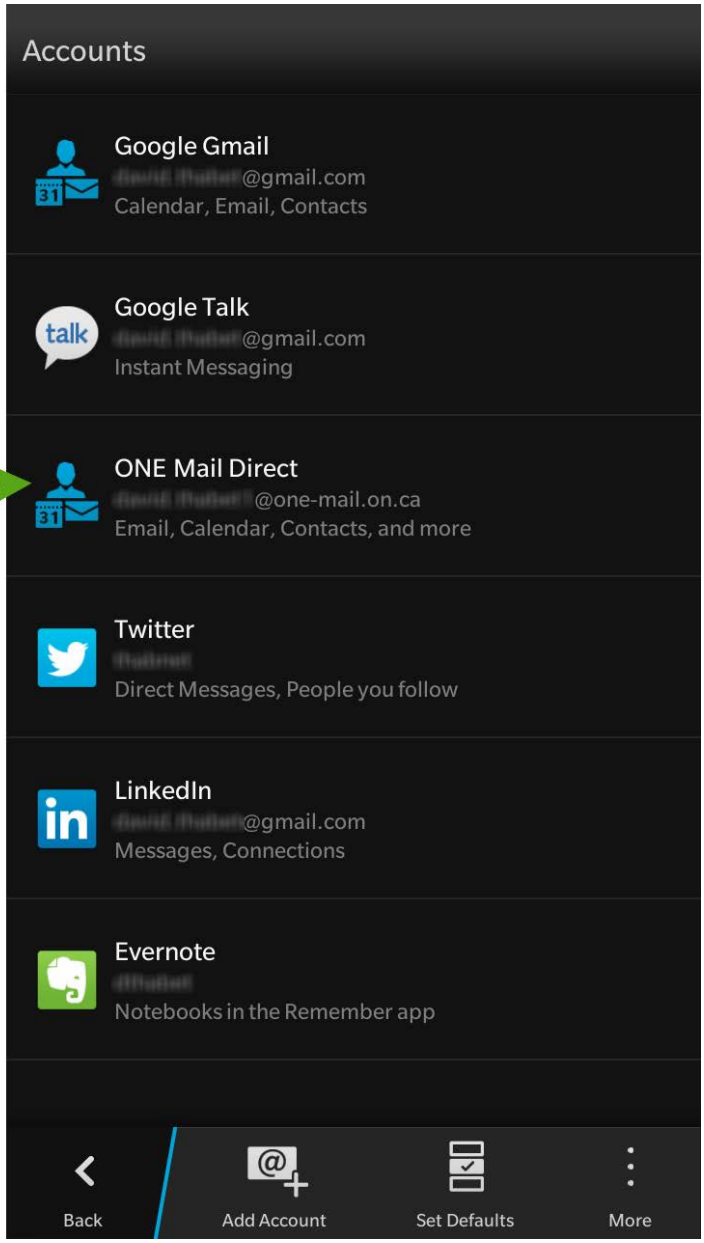
Security policy requires that every device accessing ONE Mail have a device password (which is distinct from a ONE Mail password). If the device currently has no password, it will prompt for one:

If necessary, select **Password Rules** to view the criteria for password format:



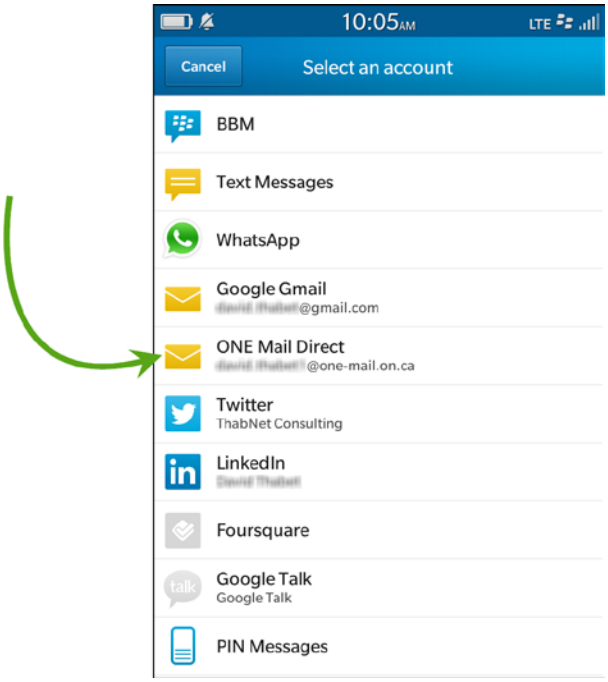
The device is now configured for ONE Mail access.

The new ONE Mail ac
the Accounts screen:

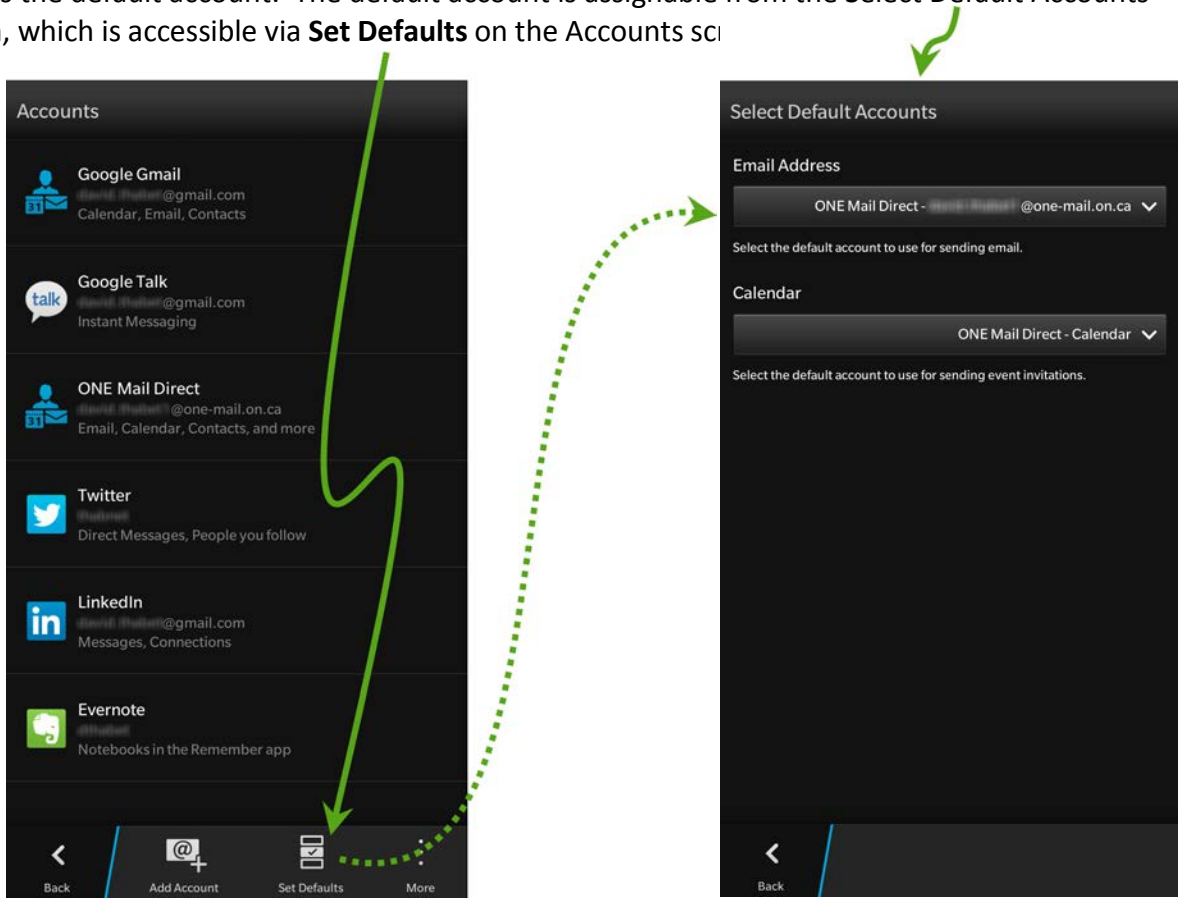


8.3 Account Access

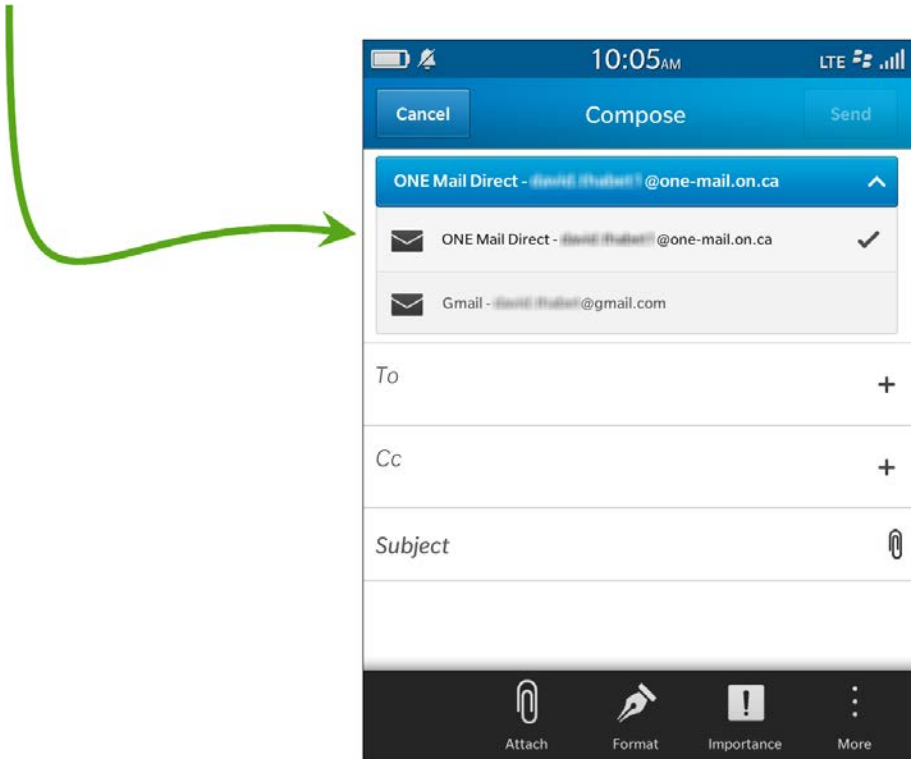
After configuring the device, the ONE Mail account shows up in the hub:



If the device is configured for multiple e-mail accounts (for instance ONE Mail as well as Gmail), one of them is the default account. The default account is assignable from the Select Default Accounts screen, which is accessible via **Set Defaults** on the Accounts sc



When composing a message on a device configured for multiple e-mail accounts, be sure to select the appropriate account from which the message should be sent:



8.4 Wipe Device

It is possible to delete ("wipe") all data from a BlackBerry device by remote control. This feature is useful if the device is lost or stolen.

A wipe permanently deletes data; the data cannot be recovered. Deletion includes e-mail accounts, calendar items, tasks, contacts, text messages, media files, downloaded apps, documents, browser bookmarks, and settings.

For lost or stolen devices, contact the eHealth Ontario service desk to have the device remotely wiped. The service desk is available 24/7:

1-866-250-1554
ServiceDesk@ehealthontario.on.ca

See the Security section of this document for more information.

9 Exchange ActiveSync Setup for Windows Phone

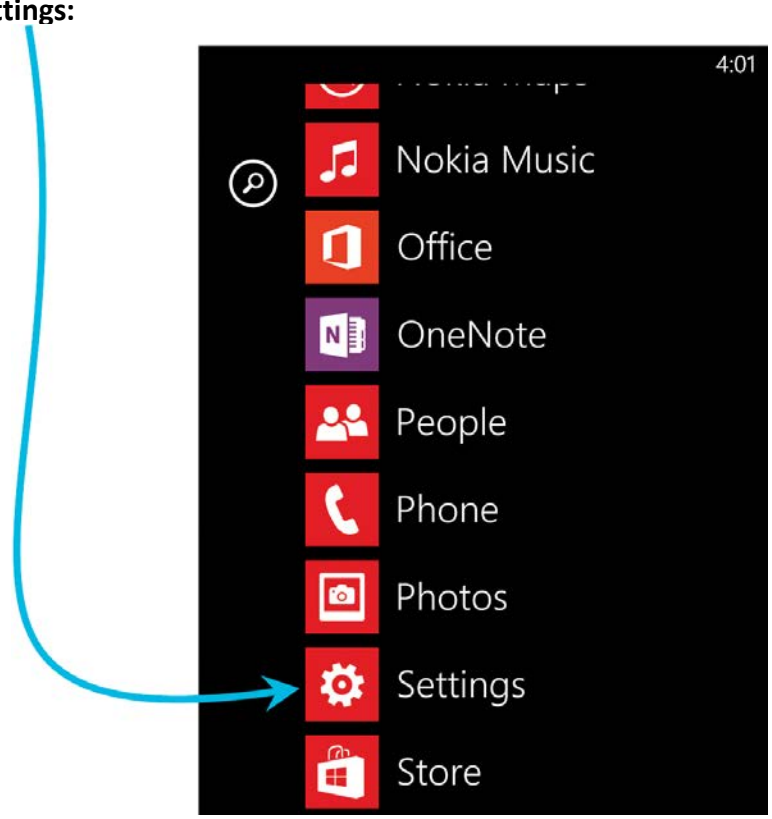
9.1 Preamble

The following procedure applies to mobile devices running the Windows Phone operating system. Screenshots below come from Windows Phone 8, so they may differ from other versions, but the setup procedure for ActiveSync is similar for all varieties of Windows Phone software.

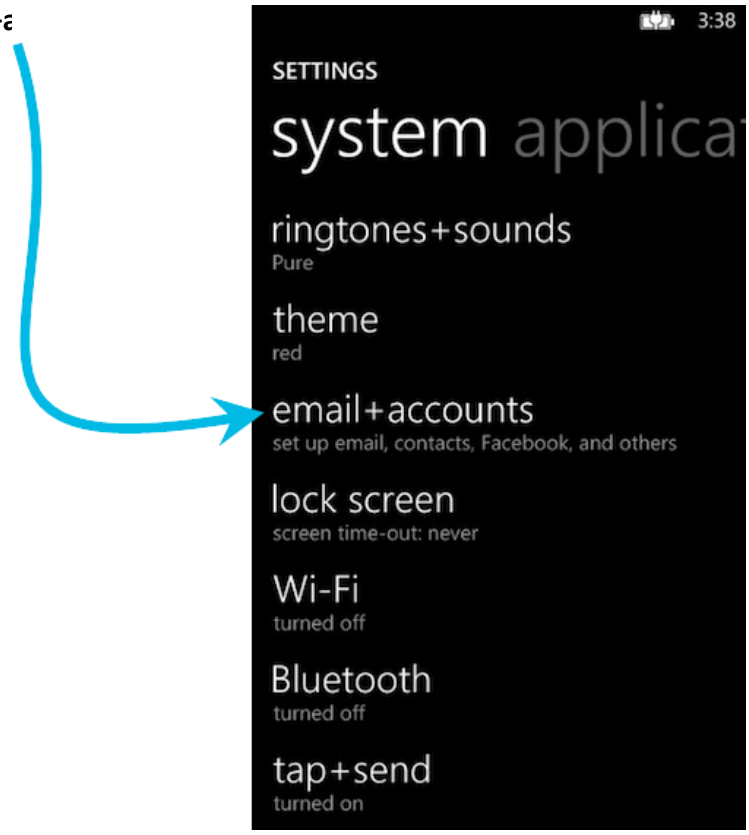
9.2 Procedure

On the Windows Phone 8 device's start screen, swipe left to display the app list.

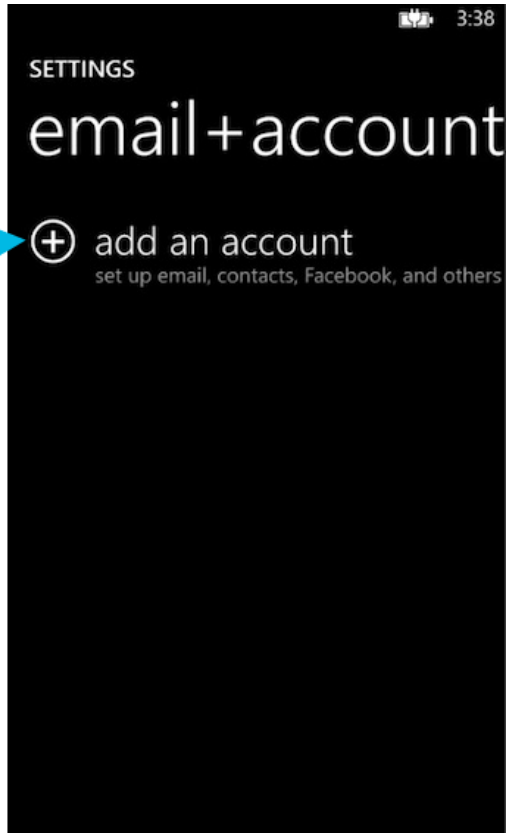
Select **Settings:**



Select **email+a**

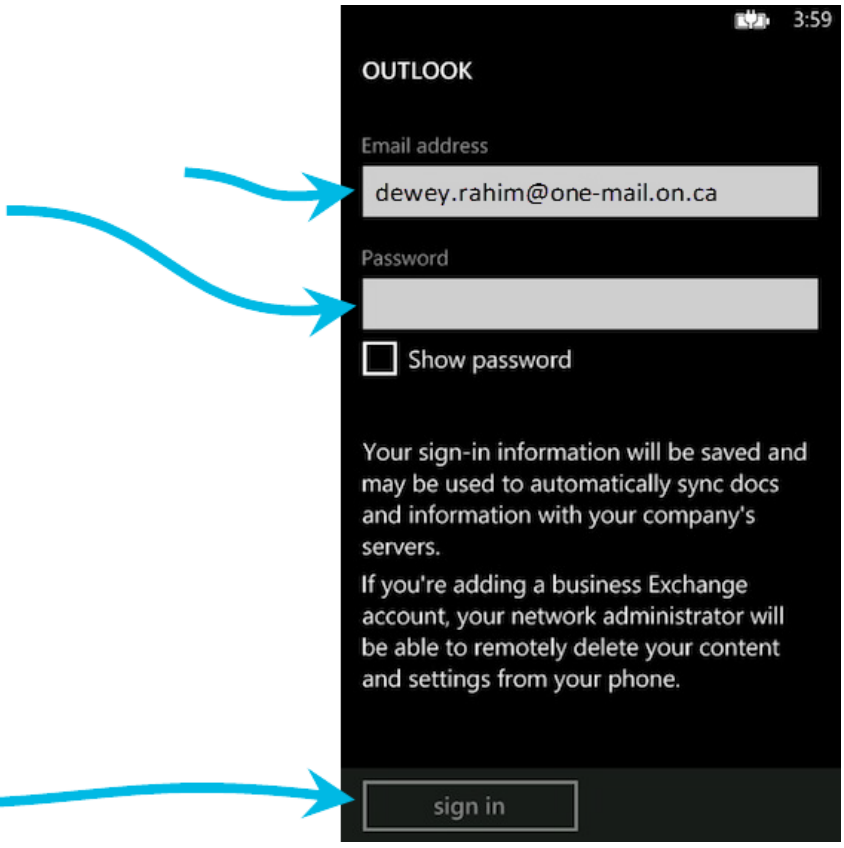


Select **add an**



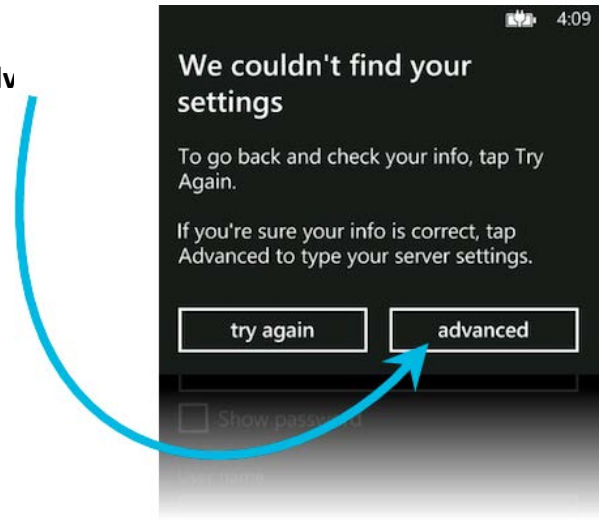
Select **Ou**

Enter ONE Ma
(probably endi
and its associa



Select **sign in:**

Select **adv**



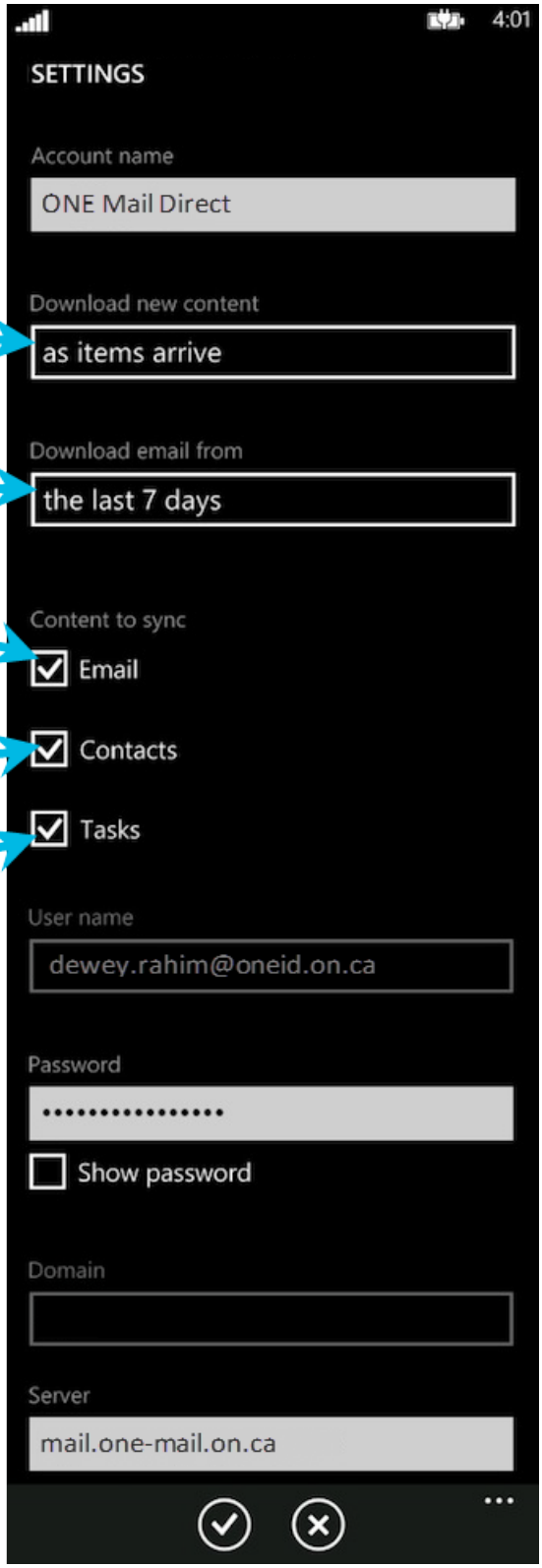
Fill in the fields as shown:

Select **sign in:**

Select download timing:

Select time period for which to download mail:

Select the type(s) of content to synchronize:



All mobile devices accessing ONE Mail must have passwords. If there is no password in place during configuration as described in this document, the device will ask the user to create one. If the device remains without a password, the ONE Mail service will be disabled.

9.3 Wipe Device

It is possible to erase ("wipe") all data from a Windows Phone device by remote control. This feature is useful if the device is lost or stolen.

A wipe returns a Windows Phone device to its initial state. All personal content is erased, and the device is restored to its factory settings.

For lost or stolen devices, contact the eHealth Ontario service desk to have the device remotely wiped. The service desk is available 24/7:

1-866-250-1554
ServiceDesk@ehealthontario.on.ca

See the Security section of this document for more information.

10 Controlling Mailbox Size

The standard maximum size for a ONE Mail Direct mailbox is 3GB. This limit includes inbox, sent items, deleted items, drafts, and calendar. When a mailbox gets close to its capacity, the system sends automated messages warning the mailbox owner of the situation. If a mailbox reaches its capacity, it is no longer possible to send or receive messages, and any attempt to do so triggers an automated response informing the user of the issue.

The largest allowable size for a single message, including attachments, is 50MB. Messages larger than that are not sent, and they trigger an automated note informing the user of the problem.

To free up space in a mailbox, delete e-mail messages and/or other items such as calendar entries.

11 Dormant Account Handling

Dormant accounts may be removed from the ONE Mail system per criteria set out in the "ONE Mail Direct Dormant Account Policy & Procedure."

There are two types of dormant accounts: non-activated and inactive.

A non-activated account is one that has never been used, meaning that no user has ever logged in to it. Non-activated accounts may be deleted from the network after six months.

An inactive account is one that no user has logged in to for over 13 months. Inactive accounts will be disabled.

Note that it is possible to flag an account so that it is temporarily exempt from entering dormant status. This feature is useful for, for instance, covering maternity leaves.

For full text of the "ONE Mail Direct Dormant Account Policy & Procedure," see the ONE Mail resources web site.

12 Security

12.1 Policies

In this context, "policies" refers to rules that are set up on eHealth Ontario's ONE Mail servers in order to enforce certain ways that mobile devices function in conjunction with ONE Mail.

Some elements of mobile device security are pushed (that is, sent automatically) to all mobile devices that have access to ONE Mail Direct. If there are changes to these policies in the future, mobile devices may, for instance, ask users to change their passwords.

All mobile devices accessing ONE Mail must adhere to security policies pushed by eHealth Ontario. If the device remains without accepted policies, the ONE Mail service will be disabled.

12.2 Passwords

Each mobile device accessing the ONE Mail Direct service must have a local password. This requirement is enforced through Exchange ActiveSync policies configured by eHealth Ontario.

The minimum length for a password is four (4) characters.

12.3 Timeout (lock) for Inactivity

The timeout for devices occurs after 15 minutes of inactivity. After that, the device's regular password must be entered to continue using it. This requirement is enforced through Exchange ActiveSync policies configured by eHealth Ontario.

12.4 Device Wipe

"Device wipe" refers to the process of automatically deleting data from a mobile device. This security feature is intended to protect sensitive contents such as personal health information (PHI) if the device is lost, stolen, or subject to unauthorized access attempts. This requirement is enforced through Exchange ActiveSync policies configured by eHealth Ontario.

If the local password is entered incorrectly ten (10) times in a row, contents of the device are automatically deleted (wiped).

If the device is lost or stolen, contact eHealth Ontario's help desk to request a remote wipe. The service desk is available 24/7:

1-866-250-1554
ServiceDesk@ehealthontario.on.ca

For some devices, users can initiate a remote wipe command through Outlook Web App (OWA). See the user manual for the particular device for more information.

Different devices may interpret the remote-wipe command in different ways, but, in general, a wipe deletes e-mail messages, calendar items, contacts, photos, music, text messages, documents, browser bookmarks, and settings.

12.5 Lost or Stolen Device

If the device is lost or stolen, contact eHealth Ontario's help desk to request a remote wipe. The service desk is available 24/7:

1-866-250-1554
ServiceDesk@ehealthontario.on.ca

12.6 Policy Refresh Interval

All security configuration restrictions (that is, policies as discussed above) are re-sent to all connected mobile devices every 24 hours.

12.7 Security Tips

The tips below are an introductory look at protecting mobile devices and the sensitive information they contain. For further information, consult organization policies, privacy regulations, and the device's user manual.

The Office of the Privacy Commissioner of Canada provides these tips:

- Become educated about the mobile device and how to enable or add privacy and security tools.
- Limit the personal information stored on mobile devices to that which is absolutely necessary.
- Ensure that mobile devices are protected with hard-to-guess passwords. Never rely on factory setting passwords.
- Use an automatic lock feature so that a password is required to access the device.
- Consider using an up-to-date encryption technology to provide added protection for personal information on mobile devices. Without encryption, personal information is vulnerable to unauthorized access. Encryption involves using an algorithm to transform information into text that is unreadable without a key to read the code.

- Install and run anti-virus, anti-spyware, and firewall programs on your mobile device, and keep those programs up to date. Attacks against mobile devices from spam, viruses, spyware, and theft are on the rise. For example, downloading an infected program could infect a mobile device.
- Do not send personal data over public wireless networks (at cafés, for example) unless you have added security such as a Virtual Private Network (VPN). Public wireless networks may or may not be secure, and there is a risk that others may be able to capture data sent over these networks.
- Never leave a mobile device unattended in a public place or a vehicle. Across North America, hundreds of thousands of mobile devices are lost or stolen every year. One survey by an information security and privacy research centre suggests that a laptop has a 5 to 10 per cent chance of going missing over a three-year period.
- Ensure that data stored on mobile devices that are no longer needed is purged prior to disposal.

Additional tips*:

- Put a password on the device and a PIN on its SIM card. Do not rely on the default factory settings. Using a password and PIN will stop thieves getting access to the device or using the SIM in another device to make calls. All phones have security settings, so become familiar with them and turn them on.
- Set up the device to automatically lock. If the device has not been used for a few minutes, it should automatically lock and require a password or PIN to reactivate.
- Stay with reputable websites and apps.
- Be careful when allowing third party unsigned applications to access personal information. This includes access to the device's location. Always read permission requests before installing new apps or app upgrades, looking for unusual requests or pleas for money.
- Do not click on unsolicited or unexpected links, even when they appear to be from friends.
- Check the bill for unusual data charges or premium rate calls, and contact the service provider immediately if there are any unusual calls or data usage on the bill.
- Check for updates to the device's operating system regularly. Install them as soon as they are available.
- Be careful with Wi-Fi and Bluetooth. When connecting to the Internet using Wi-Fi, try to use an encrypted network that requires a password. Avoid online banking or financial transactions in busy public areas and over unsecured Wi-Fi networks. Turn Bluetooth off when not in use.
- Back up the device regularly. Set up the device so that it backs up data as part of its synchronization process, or back it up to a separate memory card.
- Before discarding a mobile device, delete all personal information. Most devices have an option to reset to factory settings. Remember to remove or wipe any inserted memory cards.

13 Troubleshooting: If Device Cannot Connect to ONE Mail

If the device cannot access ONE Mail, try the three steps below.

Step 1

Attempt to access ONE Mail using a non-mobile device (e.g. a desktop computer hard-wired to a network).

If access succeeds, proceed to step 2.

If access fails, call the device's first line of support (probably an organization's help desk), and ask them to contact eHealth Ontario's service desk if they cannot solve the problem locally.

Step 2

Check Internet connectivity on the mobile device. Try accessing any website (other than eHealth Ontario's) or contacting the Internet service provider and asking them to verify Internet access.

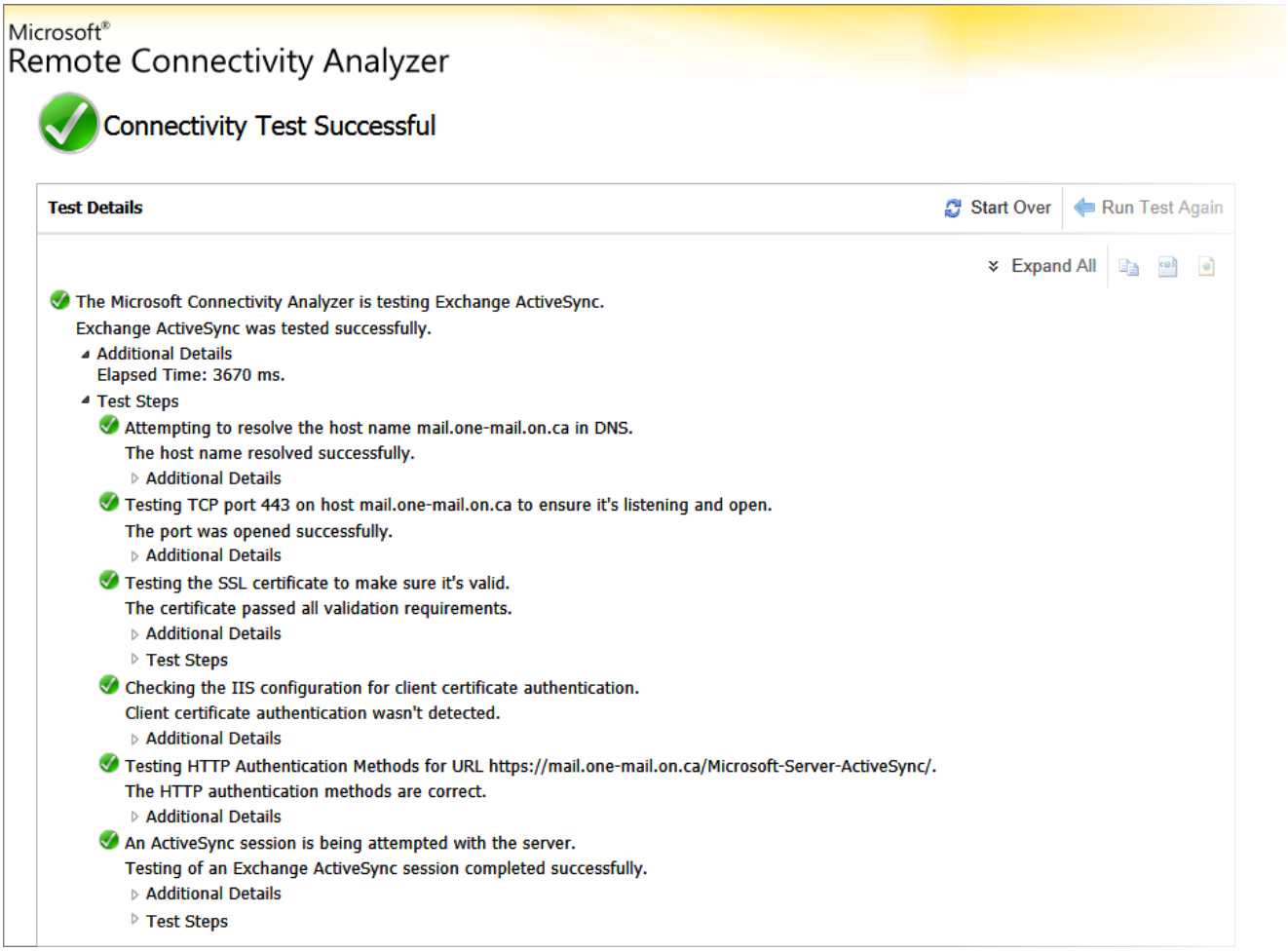
If Internet connectivity succeeds, proceed to step 3.

If Internet connectivity fails, contact the Internet service provider for support.

Step 3

Check if the Exchange ActiveSync service is available: perform the on-line Microsoft Exchange ActiveSync Connectivity Tests.

Below is a screenshot of a successful connectivity test:



If the connectivity tests fail, review the device configuration to ensure that it is set up as per instructions in this guide. After verifying device configuration, repeat step 3 to confirm connectivity.

If, after performing the three steps above, the device still cannot access ONE Mail, call the device's first line of support (probably an organization's help desk), and ask them to contact eHealth Ontario's service desk.

//end af2015