



Blog

[Home](#) > [Blog](#)
[Previous Post](#)
[Next Post](#)

Microsoft Exchange 2003 Direct Push and the Apple iPhone 3G

Like any good technophile I picked up a new iPhone 3G on Friday the 11th and the very first thing I did when getting back to the office was to try to get my Exchange Server to do Direct Push. I have had some small frustrations from the wide distribution of documentation on the subject so hopefully this post will save someone some time.

For the sake of simplicity this article will deal with the simple case of:

- Stand alone Exchange, i.e. not a front-end/back-end setup
- No proxy server, e.g. ISA
- Single firewall

Frankly if your setup is more complicated than that you probably already know how to do this and aren't reading this anyway. Moving right along...

This is what you'll need before you get started:

- An iPhone 3G (it doesn't work on the v1 phone)
- Exchange Server 2003 **SP2** or later
- Access to your firewall/router
- A fixed IP address on the internet
- Access to your domain settings
- A valid SSL certificate on your Exchange server – get one, they're not that expensive
 - <http://www.completessl.com> from USD\$49
 - <http://www.instantssl.com> from USD\$65
 - <http://www.trustico.com.au> from AUD\$20

Background

Direct Push works because the internet is slow. That's the headline.

Basically the iPhone will make an HTTPS connection to your Exchange Server's "Microsoft-Server-ActiveSync" virtual folder (most likely on the default web site). It will hold each connection open as long as possible, or until some pre-configured timeouts occur. Should you receive an email during this open connection, Exchange will send notification down to the iPhone which will tell you that you have new mail. Simple as that. The reason it works is because the internet protocols were designed to not receive an instant response from the server when making a request (see "slow" above). Direct Push takes advantage of this extended open connection.

To prevent your battery from draining in 25 minutes flat the chatter on the connection is kept to a minimum. It's very clever.

Before You Start

If you have a Wi-Fi connection active on the phone it won't work. Direct Push only works over the air (the 3G connection). This is because the Wi-Fi radio *will* kill your battery. With Wi-Fi enabled I believe the phone reverts to a pull model, based on observation, but I can't confirm that.

Setup

Is your iPhone's Wi-Fi off?

Step 1. Router/Firewall Setup

- Go to the "Port forwarding" or "Services" setup
- Open port 443 on TCP to enable the HTTPS communication – do not be tempted to do this using HTTP. It's possible, but don't do it. You have been warned.

Archives

- [September 2009](#)
- [May 2009](#)
- [July 2008](#)
- [June 2008](#)
- [April 2008](#)
- [April 2007](#)
- [March 2007](#)
- [February 2007](#)

Tag Cloud

[.NET](#)
[Development](#)
[debugging](#) [Dynamics CRM](#)
[Exchange 2003](#) [Explorer](#) [Flash video](#) [FLV](#) [IIS](#)
[iPhone](#) [Javascript](#) [jQuery](#) [Licensing](#)
[Microsoft](#) [MIME types](#) [MOSS](#)
[2007](#) [remote debugging](#) [SurveyGizmo](#) [Virtual PC](#)
[Vista](#) [Visual Studio](#) [Windows Vista](#) [WSS](#)
[3.0](#)

- Make sure the endpoint is your Exchange server's internal IP address
- Restart the router/firewall

Step 2. Domain Name Setup

- Add a new host to your internet domain called "exchange" and point it to your router's fixed internet IP address – not absolutely necessary but it makes everything a bit clearer if you ask me.

Step 3. Exchange 2003 SP2 Setup

- Open Exchange System Manager
- Expand "Global Settings"
- Right-click "Mobile Services" and select "Properties"
- There are several options required to support older technologies but the ones you want right at the moment are as follows:
 - Enable user initiated synchronisation – get the whole thing started
 - Enable Direct Push over HTTP(S) – the bit we want
- Optionally configure Device Security – I recommend it cause then if you lose the thing you can do a "remote wipe". These are the settings I like:
 - Enforce password on device – makes you enter a PIN to get into the iPhone which is a bit of a pain but worth it for the security. Do you want anyone who finds your phone to have access to all your email and contacts? Cause that's what will happen.
 - Wipe device after failed attempts – this means if you get the password wrong enough times the phone will wipe itself. Set this number as low as you dare.
 - Refresh settings on the device – set this to 24 to ensure the security policy is checked for updates daily

Step 4. Configure Your Users

- Open Active Directory Users and Computers on the Exchange server
- Right-click the user to configure and select "Exchange Tasks"
- Select "Configure Exchange Features" from the task list
- Under "Mobile Services" ensure that "User Initiated Synchronisation" and "Up-to-date Notifications" are set to Enabled – the Enable and Disable buttons are cleverly hidden at the bottom of the Features grid

Step 5. Configure IIS

- On the Exchange server open up Internet Information Services Manager
- Locate the web site containing the virtual folder named "Microsoft-Server-ActiveSync"
- Right-click the web site in the left pane tree and select "Properties"
- On the "Web Site" tab enter 443 in the "SSL port" – note this may cause a problem if you already have an SSL site on the server
- On the "Directory Security" tab setup your SSL certificate – setting this up is beyond the scope of this article but very straight forward. Google it. **Remember:** if you have been following along the server will be named **exchange.mydomain.com** and not **www.mydomain.com**. Make sure your SSL certificate has the correct name.

Step 6. Test Your Server Setup

- Open a web browser and point it to <https://exchange/OMA> where "exchange" is the name of your Exchange server (mine is called exchange)
- You might get a certificate error, that will be because the server name on the certificate does not match the server name – that's OK when connecting to the server from the inside – just continue
- Enter your network credentials (i.e. login) in the form **DOMAIN\username** for the "User name" field
- You will probably get a warning page saying the device type is not supported, just click OK
- If you've got it right you will see a text version of your mailbox – if not see **Troubleshooting** below

Step 7. Setup your iPhone

- **Turn Off Wi-Fi**
- Tap "Settings", "Mail, Contacts, Calendars"
- Under "Accounts" tap "Add Account..."
- Tap "Exchange"
- Enter your email address, username (in the form **DOMAIN\username**) and password
- Ensure SSL is on
- Set the "Server" field to **exchange.mydomain.com** (substitute mydomain for whatever your domain name is, obviously)

That's it – should be up and running now. Send yourself an email and see.

Troubleshooting

In my brief time setting this up here are the places where you might come unstuck:

- Router/firewall – make sure the you have 443 pointed at your exchange server
- Exchange test failed? It did for me! – I got a bunch of errors the first time I ran the Exchange test. To resolve them check the following:
 - The ASP.Net version on the OMA virtual folder is set to 1.1.4322 (the Microsoft-Server-ActiveSync can stay at 2.0.50727)
 - The App Pool account (normally Network Service) has read/execute privilege on the appropriate Exchange folders (e.g. “C:\Program Files\Exchsrvr\OMA\Browse”)
 - The App Pool account has read/write privilege on BOTH ASP.Net framework versions temp folders (i.e. “C:\WINDOWS\Microsoft.NET\Framework\v1.1.4322\Temporary ASP.NET Files” and “C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files”)
- DNS name – make sure you have allowed sufficient time for the new name “exchange” to have fully delegated. This can take 24 hrs.
- Firewall problems – Some firewalls have an idle connection timeout that will need to be increased to at least 15 minutes (by Microsoft's recommendations). This means that your firewall is disconnecting you – check your documentation or, as always, Google

Helpful Links

Some of the pages that helped me:

[Microsoft – Enterprise firewall configuration for Exchange ActiveSync Direct Push Technology](#)

[Exchange Team Blog – Direct Push is just a heartbeat away](#)

[Brian M Posey \(Exchange MVP\) – Microsoft Exchange Direct Push Technology](#) (seems to be broken)


[Apple's less than complete instructions](#) (don't worry, it's Apple, it just works! Right?)

This entry was posted on Wednesday, July 16th, 2008 at 1:59 pm and is filed under [General](#). You can follow any responses to this entry through the [RSS 2.0](#) feed. You can [leave a response](#), or [trackback](#) from your own site.


[View Comments \(34\)](#)

[ShareThis](#)


34 Responses to “Microsoft Exchange 2003 Direct Push and the Apple iPhone 3G”

1.  [Tom](#) - July 17th, 2008 at 1:43 am


In the Exchange 2003 settings, does the “Enable Outlook Mobile Access” option need to be selected? This is in the “Mobile Services Properties” pane, just beneath the ActiveSync settings you mention.

2.  [Yalag](#) - July 17th, 2008 at 2:02 am

This is great and all except if push doesnt work over WIFI, it is completely useless. The iPhone will stay on the WIFI whenever it can, and push still stop working....imagine you walk into a coffee shop, WIFI is detected. Push will not work for the time of your stay.....

3.  [David](#) - July 29th, 2008 at 2:16 am

You state that push only works with the 3G iPhone. That is not the case. I'm running the 1st gen iPhone with the 2.0 firmware and I can say this for fact: Push email works with Exchange 2007. Not only does email push work, but calendar and contacts as well.

4.  [Ehsan](#) - July 31st, 2008 at 12:04 am

This was by far the best explanation I have found on the web of Exchange Direct Push working with the iPhone (and I've been searching through dozens of sites). Thank you so much for an insightful article.

5.  [Richard](#) - August 3rd, 2008 at 9:46 am

>>> David

Hi David, I have heard of first gen iPhones being set up to work over IMAP, and you can set up the

second gen this way too I believe. The 2nd gen's "push" uses Exchange ActiveSync and this is an event-driven model, rather than the pull model for IMAP (and WiFi).

If you have push setup properly, you can sit in front of your PC/Mac and send yourself an email and the email will show up on the phone as fast or faster than when it hits your Outlook/Entourage client. That's "push". With WiFi on and the same settings it takes many minutes and the phone has to be on (i.e. not in standby), that's the timer.

>>Yalag

Hi Yalag, I agree its stupid. Actually the longer I use the thing the more stupid "features" I discover. I would definately not class this as a business-ready device yet. On the other hand, my plan carries 500MB per month and with WiFi off (note you can't download tunes or software over the air, only on WiFi or in the cradle) I am still barely using 100MB so I just have WiFi off now. 3G is more than enough for email.

>> Tom

Hi Tom, I can't remeber – I'll check and get back to you.

6.  [Richard](#) - August 3rd, 2008 at 9:50 am

Update: Sorry but the excellent article I've linked written by Brian Posey seems to have moved or perhaps requires a password – at any rate I can't seem to find it just now.

7.  [Richard](#) - August 3rd, 2008 at 10:10 am

>>Tom

Hi Tom, the Outlook Mobile Access feature has two components, neither of which is required for the Push to work, 1) Outlook Mobile Client which is MS Outlook for a mobile device – obviously a Win Mobile device; and 2) Web access for mobile devices i.e. HTML, XHTML, or cHTML.

On my phone I can access my email via the iPhone's email client or the web browser using the full web client at "https://mail.mydomain.com/exchange" or the mobile client at "https://mail.mydomain.com/oma".

The short answer is no, you don't need that checked.

8.  [Richard](#) - August 3rd, 2008 at 10:13 am

>>Tom Update:

OK – while technically you don't need the "Enable Outlook Mobile Access" setting on for push to work you will need it to follow my instructions, because the test in Step 6 hits the OMA (Outlook Mobile Access) site.

9.  [ISS_Jon](#) - August 9th, 2008 at 6:24 am

Ok.. GREAT article... but can I get some more info..

I think I am having an IIS issue, but unsure....

We use Webmail while on the road and SSL port 443 was already open in the firewall.

When I browse to our exchange/OMA I get the following: After logging in:

"Item no longer exists. The item you are attempting to access may have been deleted or moved."

Is this a permissions thing? Where do I check?

10.  [dil okulu](#) - August 10th, 2008 at 10:20 pm

is there any information about this in other languages, maybe german or other else?

11.  [Richard](#) - August 13th, 2008 at 7:14 pm

>>IIS_Jon

Hi Jon,

If it's an IIS thing it may help to look at the site logs and make sure you're accessing the URL you think you are – it should have info about HTTP response codes, URLs and security info.


If it's a permissions problem I'd guess Exchange and not IIS so maybe make sure the user account is allowed to access OMA. From AD Users and Computers on the Exchange box right-click the user and check the "Exchange Features".

dil okulu>>

I'm sure other people have written about this stuff in other languages but I only speak English. Can I suggest Google translate or Babelfish?

12.  **Raul Haynes - August 14th, 2008 at 12:09 am**

Hi , I have a 3G Iphone and my issues seem to be very different from all others. I connected to my exchange server over WIFI when I first set up the phone. My account verified and was working as expected. I left for work this morning and turned off WIFI and the 3G/ Edge cell network took over. I continued to receive email for some time over the cell network. However I have noticed that if I use Safari or AIM on the phone it will server my connect to exchange and will not reconnect until I get another WIFI connection. Is there anyone out there having this issue? Also I am able to setup a Moto Q for push without any problems.

13.  **rgclements - August 19th, 2008 at 11:36 am**

Fantastic article. Just what I was looking for... Thanks for the help.

14.  **shannon - August 22nd, 2008 at 1:52 am**

Great article, thanks for the info, which finally got my push to work. However I'm confused about the security of this.

I've got 3 different places to enable or disable SSL.

2 of which I've had to disable otherwise push won't work because I have a single exchange server.

The first is my IIS Virtual directory. Under secure communications tab I've had to uncheck the "require secure channel (SSL)"

Second is my mobile phone. I've had to uncheck the "server requires an encrypted SSL connection".

If either of these are checked then I get various errors and push doesn't work.

However, in Exchange manager under mobile services I have "Enable Direct Push over HTTP(S)" turned on.

So based on this configuration I'm pretty sure that I'm running without SSL, leaving usernames and password in the clear. Does anyone know how to secure this without building a front-end exchange server?

Thanks.

15.  **[Richard](#) - September 6th, 2008 at 10:02 am**

>> Raul

Hi Raul, haven't come across that myself – maybe check in with the Genius bar at your local Apple store??

>> Shannon

Hi Shannon, I wouldn't run Push without SSL cause your email content is being transmitted in the clear, I will check about passwords cause I have a feeling they are still encrypted. At any rate you are definitely not using SSL in your setup and you should be. You will need to get a commercially signed certificate to get it to work properly in my experience.

16.  **[dil okullari](#) - September 8th, 2008 at 11:25 am**

it would be better with other languages support, but thanks..

17.  **Grant Philipps - September 9th, 2008 at 4:12 pm**

Great Article – Thankyou very much. Been trying to get this working for hours, noticed you mention that if Wifi is turned on it wont work – my problem fixed!!! Just tested it then when the phone is locked and it took less time to to showup on the iphone as it did in outlook. Thanks again!

18.  **marty - September 14th, 2008 at 2:56 pm**

for those that are still having issues even with firewall settings properly set, SSL cert installed, etc.

Send this to your IT guys and ask if this applies to your org. I have a single exchange server at home and SSL enabled so fell into this category.

Once I did the steps here (method 2) I was all good.

<http://support.microsoft.com/kb/817379>

Good luck!

19.  [Daniel Craig](#) - October 4th, 2008 at 9:59 am

Hi there, I was looking around for a while searching for firewall microsoft and I happened upon this site and your post regarding ft Exchange 2003 Direct Push and the Apple iPhone 3G | 5 Limes Blog, I will definitely this to my firewall microsoft bookmarks!

20.  [Buy iphone](#) - October 11th, 2008 at 4:53 am

Very interesting post, i bookmarked your blog, thanks for share
i will visit your blog later

21.  [Derek](#) - January 14th, 2009 at 11:18 am

AWESOME article! Thank you so much for taking the time to write it. As soon as I found this article it took me about 10 minutes to fix my problem!

22.  [Stu](#) - February 13th, 2009 at 9:58 pm

Useful article thanks, one thing I'm not too sure on though, does the subdomain URL absolutely have to begin with "exchange"? As in exchange.xxxx.com.

I currently already have an email subdomain that is called mail.xxxx.com for which I already have a certificate and everything like OWA/Blackberry works fine as it is.

23.  [Morten](#) - February 26th, 2009 at 10:19 pm

Nice article!
but got in to a problem, i need to have outlook open on my computer else I cant recieve new incomming mail.
is there a way to fix this?

24.  [Jojo](#) - March 17th, 2009 at 12:15 pm

Is there a way to set up microsoft exchange mail using the "Other" option? I don't want to use the EXCHANGE because I am going to use that option to sync my calendars and contacts with Google but I still want a way to access/send mail thru our corporate network over wifi.

25.  [Richard](#) - March 25th, 2009 at 10:39 pm


>>>Stu
Hi Stu, I don't see any reason why your exchange server need any name in particular. Actually mine is called "mail" too.

>>>Morton
Thanks Morton, I suspect that your Outlook client is connecting to your mail service as POP3, then delivering new messages into your corporate Exchange folders, which is then being pushed to your phone. Can you confirm that your mail is being delivered to your Exchange server via an SMTP connection? Email me at info@[same domain as the web site] if you get stuck.

>>>Jojo
Hi Jojo, I think that the "Other" option sets up a POP3 or IMAP connection, and not a "push" connection. That means that mail will be periodically downloaded rather than appearing immediately. This may well suit your needs but I just can't wait the extra 3 minutes to get my spam these days 😊
Short answer is yes, you can set it up using either the IMAP or POP3 configuration options, but setup will be quite different from the instructions here.

26.  [Jessicaeroky](#) - May 11th, 2009 at 1:40 am

beautiiful blog merci!!!!


27.  [Troy](#) - May 29th, 2009 at 4:05 am

Nice article. So far the iPhone users are receiving their mail via Exchange 2003 / mobile device implementation. The exchange server seems to have an issue "pushing" policy to the iPhone. Specifically extending the Inactivity time or "passcode-lock" time amount to the iPhone device.

The iPhone has the “auto-lock” and the “pass code-lock”. In our environment the pass code lock can’t be set to anything higher than 5 minutes. However, on the server the setting says 10 minutes. Recently we raised this to 30 minutes. Waited 24 hours for policy to refresh on the devices and nothing changed. Passcode-lock for inactivity remains at 5 minutes maximum.

The blackberry server has the option to force/push policy to the device however a tool that would force policy doesn’t exist for Exchange 2003 and mobile services.


The iPhones that are connected receive everything else, like min password length, wipe device after failed password attempt etc. but changes to inactivity time out does not update.

28.  [Scott](#) - June 6th, 2009 at 5:26 am


Great article. Can you comment further on the mobile device security settings? Exactly when will you need to enter your pin on your iPhone?

Because it’s a global setting in Exchange 2003, we can’t create a test group to determine the user experience. Some members of management foresee a user revolt if we enforce the password policy.

On the other hand, until you provision a policy to a device, the “true” remote wipe functionality isn’t available, correct?

29.  [Clyde Radcliffe](#) - June 8th, 2009 at 4:42 am

I have been trying for days now to get push mail working with my Iphone 3G. I’ve read many how-to’s, forums and documentations and NONE worked for me. The description in this blog worked PERFECTLY for me!!!
THANKS A LOT GUYS!

30.  [smary](#) - July 23rd, 2009 at 12:25 am

Hello,

This is an excellent post. But I’m still having problems with configuring it. Can you go one step further and please help me with this ?

I dont have SSL certificate. I’m trying to make it work without SSL.

On my iPhone it asks me for the password, when I enter my domain password, it says password incorrect and then it says cannot connect to the server.

I would greatly appreciate if someone can give me some suggestions/feedback.

Thank you

31.  [Rose](#) - August 31st, 2009 at 10:04 am

How long have you been blogging...your good at it.

32.  [meb](#) - September 5th, 2009 at 7:27 am

nice blog, congratulations!

33.  [Richard](#) - September 17th, 2009 at 12:24 am

>> Troy

Not sure if you’ve already solved this problem but for what it’s worth I think you are facing a limitation built into the iPhone itself – it seemsto me you simply can’t do what you are trying to do with the kit you have. Maybe in a future version though...


>> Scott

All of the users I have dealt with have had no issue with the PIN when the security risks and advantages are laid out to them, particularly “that if someone got your phone and it wasn’t locked they could send emails as you, or log into your internet banking” (okay we might be stretching a bit on the banking thing but as I said, everyone has fallen into line so far. To make the process as smooth as possible I get users to set their PIN before trying to setup the connection (this is a phone PIN and not a SIM PIN).

>> smary

While it should all work without SSL can I recommend in the strongest possible terms that you don’t

set it up this way. Worst case you can self-generate your SSL certificate for no money and simply accept the warning when the phone prompts you that the certificate couldn't be validated. That said, presuming you are typing your password correctly (d'oh) it is theoretically possible to not use SSL with the exact same setup as I've described minus the certificate stuff.

34.  **zamri - October 13th, 2009 at 11:12 am**

I have iPhone 3GS & exchange 2003 SP2 behind sit behind the firewall and I have front-end server. Follow the steps and it works!

Leave a Reply

Name (required)

Email (optional)

Website (optional)

Comments (required)

Level 7, 491 Kent Street, Sydney, Australia +61 2 9321 1555 info@5limes.com.au
Copyright ©2009 5 Limes Pty Ltd. ABN 87 119 340 680 All Rights Reserved
[Terms of use](#) | [Privacy policy](#) | [Sitemap](#)

u