# DNS Record Information for the Pushex Exchange server

Changing your DNS records can be daunting if you haven't had much experience doing it before. We'd be pleased to make all the required changes for you if you can give us the logon details for your DNS control panel, which is usually at the website of your domain registrar where you bought your domain name.

## MX Records

If your email domain is hosted on the Pushex Exchange servers it's best if your incoming emails come straight to our servers instead of being collected from a POP3 mailbox on another system or forwarded on from another mail-server. It's quicker, there are fewer steps to go wrong and our
anti-spam system deals directly with the mail-server where an email has originated and is therefore better able to judge if it's genuine or spam.
MX records contain the names of the servers which are responsible for receiving emails for a particular domain.
If we're hosting your domain, your domain's MX records should be:-

| | Priority |
|---|---|
| **mx1.pushex.com** | **30** |
| **mx2.pushex.com** | **30** |
| **mx3.pushex.com** | **30** |
| **mx4.pushex.com** | **30** |

The priority is a number between 0 and 99 and determines which MX record should be used first – a server with a lower number has a higher priority and it is contacted first by the sending mail-server.
We want ***all*** our 4 Internet-facing servers to share the load equally so that's why we ask you to create MX records with equal priority.
Any number between 0 and 99 would do, as long as it was the same for all the MX records, but 30 is conventional, sensible and what we recommend.

**It's important that you delete any other existing MX records.**

Some DNS control panels don't allow you to have more than 2 MX records, so in that case just have this one:

| | |
|---|---|
| **mx.pushex.com** | **30** |

This one MX record will work fine but not quite as good as having the 4 we recommend.

## AutoDiscover CNAME Record

Outlook 2007, Outlook 2010 and Outlook 2013 have the ability to use our Exchange server's AutoDiscover feature which enables Outlook to configure itself to connect to our servers, by a user just supplying their name, email address and password.

Outlook 2016, which includes versions supplied with Office 365, can ***only*** connect to our Exchange server using an AutoDiscover record.

In our experience things works more smoothly with AutoDiscover enabled, and all you have to do to enable AutoDiscover for your domain is to create one DNS CNAME record similar to this one:-

**autodiscover.lockeconsultants.com CNAME autodiscover.pushex.com**

(Of course, substitute ***your*** domain name for lockeconsultants.com**)**

A CNAME is a very common type of DNS record and all DNS control panels should allow you to create one.

We recommend that you create an AutoDiscover record but, unless you are using Outlook 2016, it's not compulsory.

**Some points to note:-**

1 – Without an AutoDiscover record, in Outlook 2007/10/13 you will notice:-

a) You can't set Out-Of-Office from within Outlook (you can still set it from Webmail).
b) You can't download the Offline Address Book (not normally important).

2 – If your company has a Windows Domain that uses the same domain a name as your emails then its DNS server may have an AutoDiscover record that will override the one you set on the Internet for machines located inside your office.

3 – If you choose to have as your main address an email address from some other email system, such as btinternet.com, then the AutoDiscover information that this other email system has published will override any manual settings that you have used to connect your Outlook to the Pushex servers.

4 – If you have some of your users using your in-house Exchange server and some using the Pushex server with email addresses at the same domain, then any AutoDiscover records will force some users to the wrong Exchange server.

Our PDF guides for setting up Outlook give instructions on how to make Outlook ignore AutoDiscover information which will solve problems 2, 3 and 4 above unless users have Outlook 2016.

## SPF Record

Sender Policy Framework (SPF) is an anti-spam initiative supported by many leading Internet companies. You don’t need me to tell you that it hasn’t stopped spam but it can mean that, if there isn’t a valid SPF record for your domain, the emails that you send out are more likely to be classified as spam.
Many spammers have managed to get a valid SPF record so you should too.
One problem is that some DNS Control Panels still don’t support SPF records and, if you find that yours doesn’t, that’s a pretty good reason to change your DNS host – it doesn’t have to be your domain registrar.

SPF information is recorded in a TXT record which is a standard DNS record type that is also used for other purposes

A new type of DNS record was defined, specifically for the SPF system, however this didn't catch on plus caused other problems and so is no longer supported.

This makes it easier as you now only have to create one record.
Here’s the SPF record you need to create to authorise Pushex to send out emails for your domain:-

**lockeconsultants.com TXT "v=spf1 include:pushex.com -all"**

We ***strongly*** recommend that you create an SPF record, but it’s not compulsory.

**Some Points to Note:-**

1 - Some DNS control panels need you to enter the quotation marks while others automatically put them in for you. Try putting them in first and if you get an error or the SPF record you create appears with double quotation marks then leave them out.

2 - The **-all** at the end of the SPF record means:-
*"the servers listed in this SPF record are the only ones that can send emails from this domain"*
While **~all** means:-
*"as well as the servers listed here, other servers may send emails from this domain*"
We strongly recommend that you use **-all** otherwise you don't have protection against spammers forging emails so that they appear to come from your domain.

3 - It's possible that you have a website or a 3rd party that sends out newsletter for you and these emails use your domain as the From address.
In these cases you should include the servers that send these emails in your SPF record.

4 - If you already have an SPF record then just modify it by adding **include:pushex.com** before the **-all**

5 - Only one SPF record is allowed. All entries must be included in a single record.

6 - The full syntax of SPF records can be found here:-
http://www.openspf.org/SPF_Record_Syntax

7 - If you have more than one domain name that you send emails from, or you also send emails from sub-domains, you should create a separate SPF record for each domain and sub-domain.

## How to check that the correct DNS records have been created

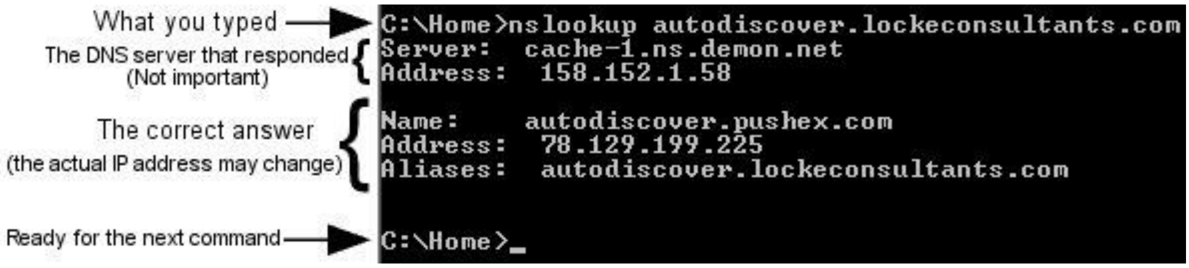
It can take up to 24 hours for changes to your DNS records to take effect and it’s not always clear, in DNS control panels, the exact format required for a particular type of record.
It’s useful, therefore, to be able to check the current values of your DNS records.

Most of the DNS records, mentioned in this document, can be checked using the built-in Windows tool called NSLOOKUP.
To use NSLOOKUP you first need to open a Command Prompt window by clicking:-
**Start – Run – cmd - OK**
or by typing **cmd** into the **Start Menu** search box.

The Command Prompt is a “Terminal Window” which means any new command you type appears at the bottom of the window and then you press ***Enter*** to process a command. Any output from a command also appears, one line at a time, at the bottom of the window and each new line shuffles the current contents up one line. The flashing cursor is where you are ***now*** and everything above it is what’s just happened. It’s a bit like using a real typewriter.

To check your AutoDiscover record, open a Command Prompt window and type:-

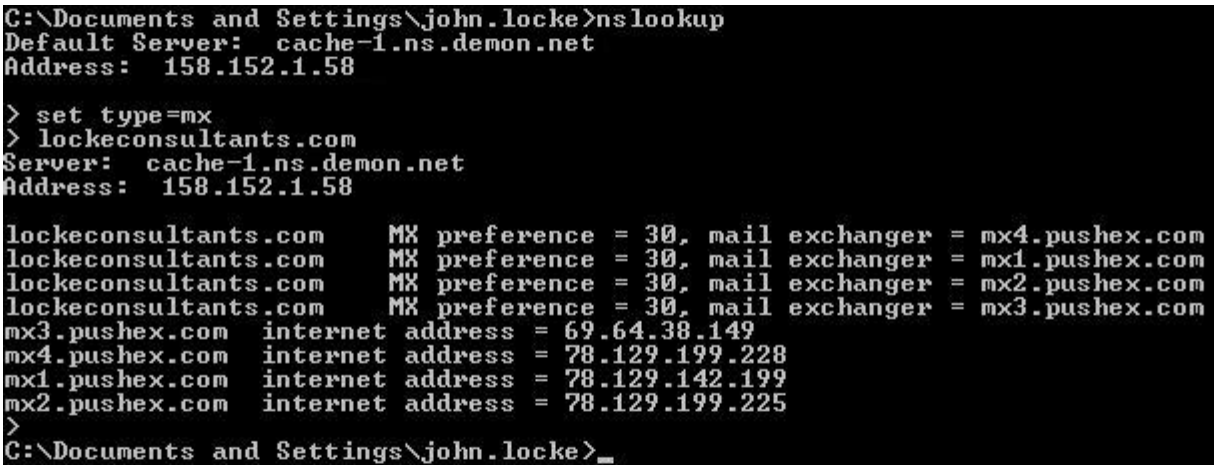
**nslookup autodiscover.lockeconsultants.com** (*Enter*)


What you typed
The DNS server that responded (Not important)
The correct answer (the actual IP address may change)
Ready for the next command

```
C:\Home>nslookup autodiscover.lockeconsultants.com
Server:  cache-1.ns.demon.net
Address:  158.152.1.58

Name:    autodiscover.pushex.com
Address:  78.129.199.225
Aliases:  autodiscover.lockeconsultants.com

C:\Home>_
```

To check your MX records, open a Command Prompt window and type:-

**nslookup** (*Enter*)
**set type=mx** (*Enter*)
**lockeconsultants.com** (*Enter*)



```
C:\Documents and Settings\john.locke>nslookup
Default Server:  cache-1.ns.demon.net
Address:  158.152.1.58

> set type=mx
> lockeconsultants.com
Server:  cache-1.ns.demon.net
Address:  158.152.1.58

lockeconsultants.com    MX preference = 30, mail exchanger = mx4.pushex.com
lockeconsultants.com    MX preference = 30, mail exchanger = mx1.pushex.com
lockeconsultants.com    MX preference = 30, mail exchanger = mx2.pushex.com
lockeconsultants.com    MX preference = 30, mail exchanger = mx3.pushex.com
mx3.pushex.com  internet address = 69.64.38.149
mx4.pushex.com  internet address = 78.129.199.228
mx1.pushex.com  internet address = 78.129.142.199
mx2.pushex.com  internet address = 78.129.199.225
>
C:\Documents and Settings\john.locke>_
```

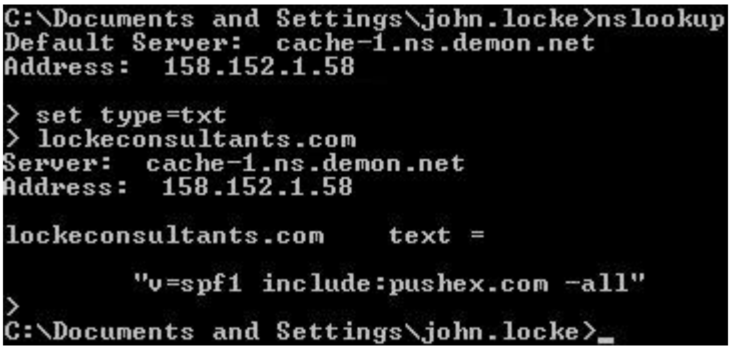
Then **Ctrl+C** to exit the NSLOOKUP command.

To check your SPF TXT record, open a Command Prompt window and type:-

**nslookup** (*Enter*)

**set type=txt** (*Enter*)

**lockeconsultants.com** (*Enter*)

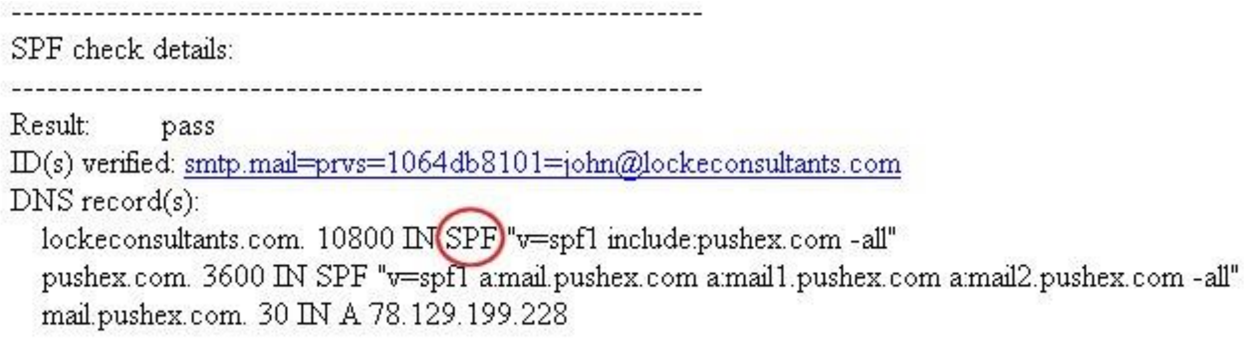


```
C:\Documents and Settings\john.locke>nslookup
Default Server:  cache-1.ns.demon.net
Address:  158.152.1.58

> set type=txt
> lockeconsultants.com
Server:  cache-1.ns.demon.net
Address:  158.152.1.58

lockeconsultants.com    text =

        "v=spf1 include:pushex.com -all"
>
C:\Documents and Settings\john.locke>_
```

Then **Ctrl+C** to exit the NSLOOKUP command.

NSLOOKUP doesn't understand **set type=spf** so, to check your SPF-type record (if you managed to create one), send a blank email from your Pushex email account to:-
check-auth@verifier.port25.com

You should get a reply, almost immediately, and near the top of the reply should be something like:-



```
----------------------------------------------------------
SPF check details:
----------------------------------------------------------
Result:       pass
ID(s) verified: smtp.mail=prvs=1064db8101=john@lockeconsultants.com
DNS record(s):
   lockeconsultants.com. 10800 IN SPF "v=spf1 include:pushex.com -all"
   pushex.com. 3600 IN SPF "v=spf1 a:mail.pushex.com a:mail1.pushex.com a:mail2.pushex.com -all"
   mail.pushex.com. 30 IN A 78.129.199.228
```

If it shows SPF (ringed in red) and "Result: pass" then your SPF-type record has been created successfully.
If instead of SPF it shows TXT then only the text version of an SPF record has been created.
(At present a TXT-type record works equally as well as an SPF-type record.)

If "Result:" is "fail" then there's an error with the SPF record you've created.

## Host your DNS on the Pushex DNS servers for free

If the DNS servers responsible for your domain are causing you problems then we'll host your DNS on our servers. Changing your DNS servers doesn't mean changing your Domain Registrar and shouldn't affect your website, VPN, Remote Access etc. You just have to logon to the Control Panel at your Domain Registrar and change the Nameservers responsible for your domain to ***our*** servers.
This offer is open to all users of the Pushex Hosted Exchange Servers.