Own Web Now Corp

Advanced Mail Server Settings Options for Shared Hosting Clients

The following document describes the more advanced mail server settings that are optional for shared hosting clients. These settings offer more security, reliability and flexibility.

November 14, 2007

Preface: Identifying Mail Problems

The e-mail infrastructure behind POP3 and SMTP has been designed a long time ago and has only had slight modifications over the years. Meanwhile, the way we rely on email changes radically every year from new operating systems, new email clients, new mobile devices and services.

Just over a decade ago e-mail consumption was still a centralized affair. You would send, read and manage e-mail from your "shell account" on the central Unix server. Almost all the connections were local. Fast forward ten years: not only is email consumption decentralized it is quite likely that you check email on multiple computers, multiple operating systems, multiple email clients and perhaps even different Internet Service Providers or even different devices – PC at work, Mobile phone on the road and Media Center at home.

While receiving e-mail has always been trivial, sending e-mail has become overly complex due to the problems we now face from viruses, SPAM, Trojans, malware and other unwanted Internet pests. Because you are sending email from various locations on the Internet, each Internet Service Provider (ISP) tries to validate your identity. Can the ISP be absolutely certain that it is you sending that email or the virus that has infected your computer?

Unfortunately, most ISP's do not have advanced security software to police their networks so they get by using various filtering methods. Some outright block outbound traffic, known as an SMTP connection on port 25. Some filter the outgoing emails and force it to go through their local mail servers first, through a transparent and stateless proxy. Some do it all the time, some do it only occasionally while other ISPs just lock down when they notice suspicious or unusual activity from your computer.

If your mail server is hosted remotely, true for almost everyone with the exception of home based businesses and IT enthusiasts, these new realities pose a huge issue in your ability to effectively send mail. Not to mention the desire to send mail from multiple computers, networks, mobile devices or even while roaming.

This document outlines some strategies you may want to consider and adopt in your settings to be able to more effectively relay messages as Own Web Now's client.

Avoid SMTP connections on port 25

Standard SMTP connections are always initiated over port 25. This is what all the remote mail servers use to receive and send email, from client to server as well as from server to server. It is the standard port that is used by everyone. Naturally, if the ISP blocks port 25 traffic to any destination outside its network you will never be able to access your remotely hosted SMTP service at Own Web Now.

> First trick to become aware of is that Own Web Now mail servers accept mail over ports 25 **as well as** 2525 and 25252.

Always, Always use secure SSL connections

The second basic principle behind secure e-mail communications is to always rely on SSL or secure socket layers. This process uses the same level of encryption that you rely on for online banking and e-commerce transactions. If you would not trust a hacker with your credit card number why let them read all your email along with password reminders that are likely in it?

> All Own Web Now shared hosting servers support SSL so you should always try to encrypt the mail as well as authentication between your computer/phone and our servers.

Client Setup Walkthrough

Following is a brief walkthrough of the configuration examples in Microsoft Windows Mail, Outlook and Entourage.

Setting up Windows Mail

Windows Mail comes with Microsoft Windows Vista by default. It is a program similar to Microsoft Outlook Express that comes with Microsoft Windows XP. The underlying process is quite simple, you will just change the settings you currently use and make them rely on secure connections. Let's get started with Windows Mail.

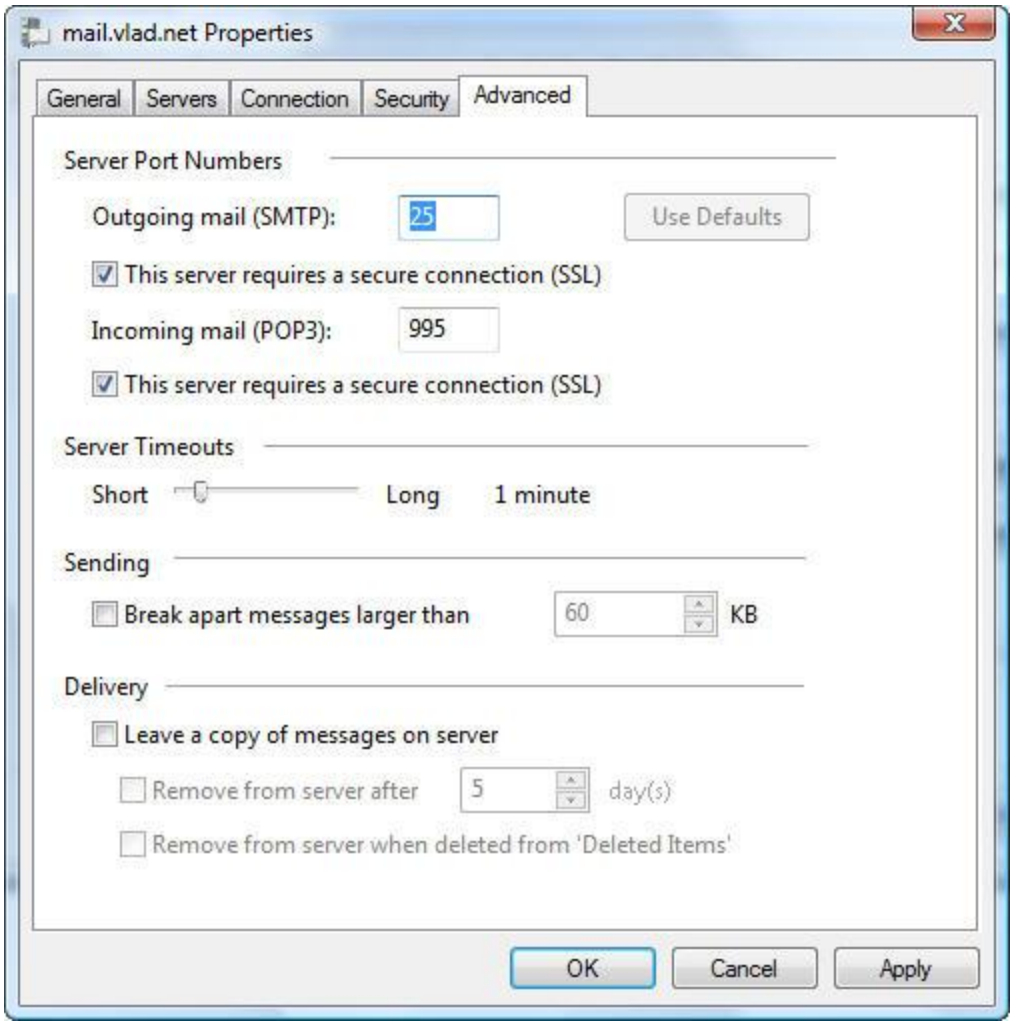
Important Note: While this is a specific walkthrough for a specific client, the theory and suggestion behind it is compliant with the standards. You can apply the same advice to Mozilla, Thunderbird, Eudora and any other modern POP3/IMAP/SMTP client in use as well as many mobile devices.

First, **Start** Windows Mail.

Click on **Tools** and select **Accounts**.

Select your default **Mail account** (possibly mail1.ownwebnow.com) and click on **Properties**.

Go to the **Advanced Tab.**



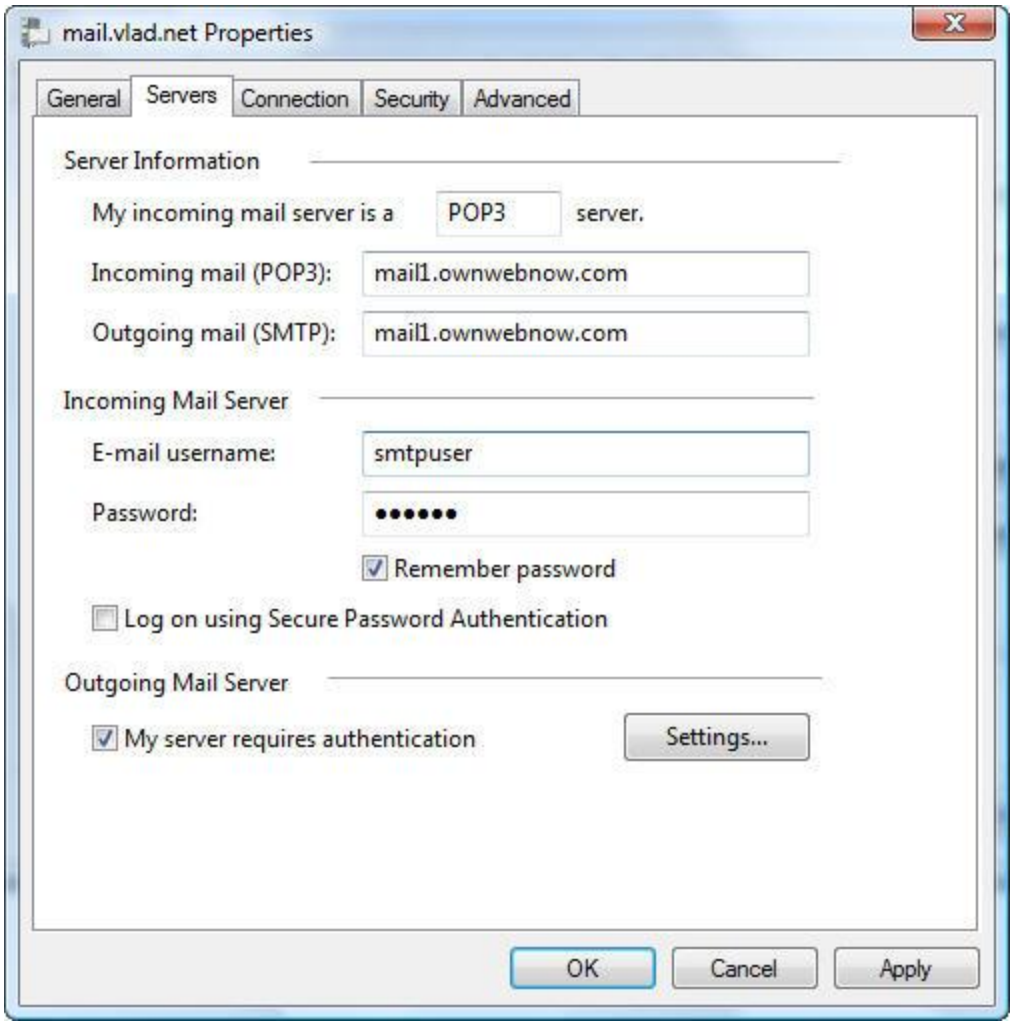
Under Outgoing mail (SMTP), **check the box** next to *This server requires a secure connection (SSL)*

Under Incoming mail (POP3), **check the box** next to *This server requires a secure connection (SSL)*

That's all, you're all set to transfer email securely from your client to our mail server!

Important Note: If your ISP filters or prohibits traffic on port 25 you can also use ports 2525 or 25252. Just change the default value for Outgoing mail (SMTP) port from 25 to 2525 or 25252.

Furthermore, it is important not to use mail server aliases when relying on SSL. Because SSL validation always checks the name of the server and compares it with the name of the certificate you must use the full name of our server, **mail1.ownwebnow.com**, not an aliased name from your own domain (mail.yourdomain.com for example). To make this adjustment or just make sure that you have the correct server in the settings **Click on the Servers tab.**



Make sure your *Incoming mail (POP3)* and *Outgoing mail (SMTP)* servers are both set to **mail1.ownwebnow.com**

You're now all set!

Setting up Microsoft Office Outlook 2007

Microsoft Outlook is perhaps the most widely used business email client out there. Even though it provides some of the most advanced security tools and plugins, it's default configuration is also the least secure one and least appropriate for business use. Let's set Outlook to securely send and receive email from Own Web Now servers.

First, **Start** Microsoft Outlook.

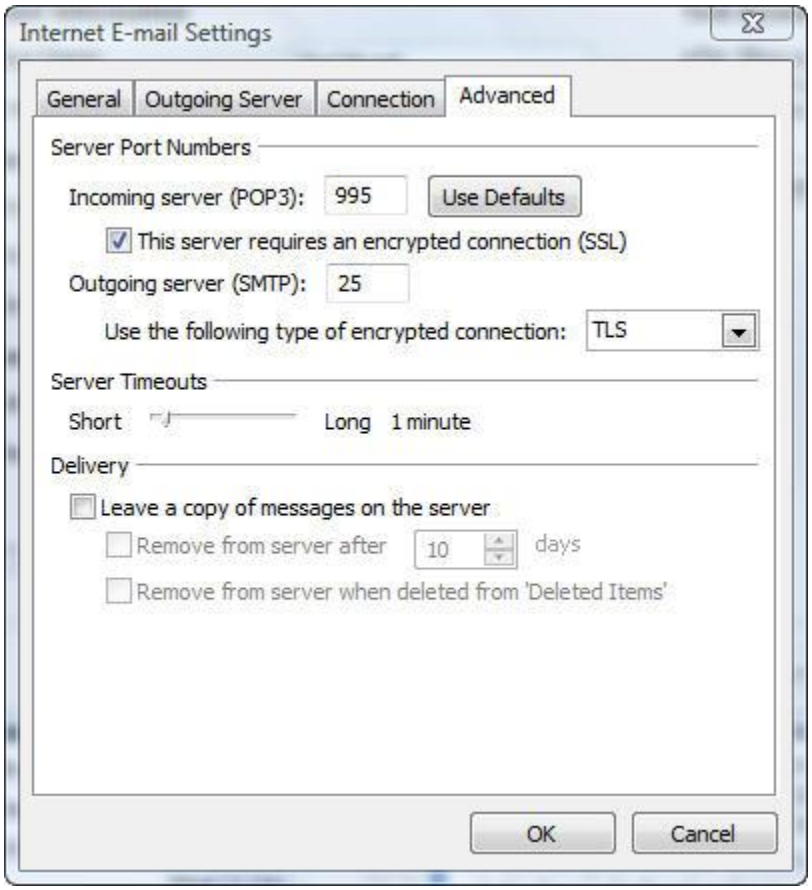
Click on **Tools** > **Accounts** > Select **POP3/SMTP Account** and click on **Change**

Make sure Incoming mail server is: **mail1.ownwebnow.com**

Make sure Outgoing mail server (SMTP) is: **mail1.ownwebnow.com**

Click on **More Settings.**

Click on **Advanced tab**.



Check the box next to: **This server requires an encrypted connection (SSL)**

Select TLS under the dropdown for: *Use the following type of encrypted connection*.

Click on **OK**, **Next**, and you're done.

Important Note: Same caveat as for Windows Mail, if your ISP prohibits traffic on port 25 change the **Outgoing server (SMTP):** to 2525 or 25252.

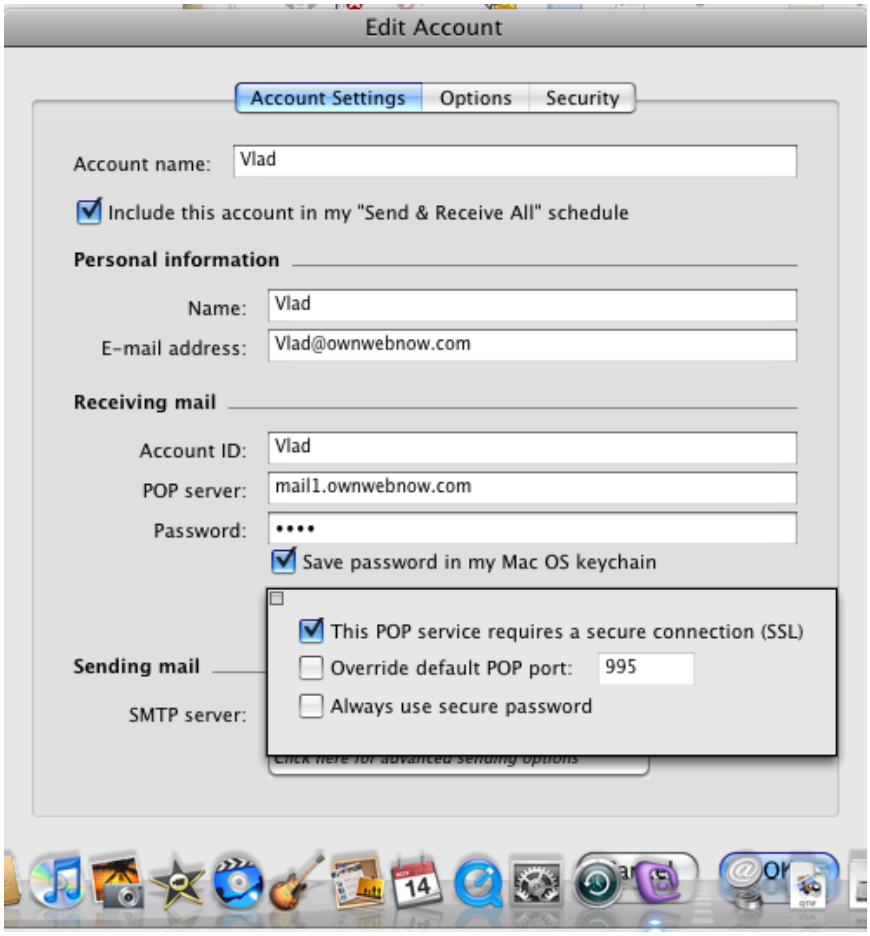
Setting up Microsoft Entourage

Even Apple Macintosh can communicate with our servers in a secure manner. Let's set your Entourage up to use SSL/TLS.

First, **Start** Microsoft Entourage.

From the top menu, **Click** on **Tools** then **Accounts**.

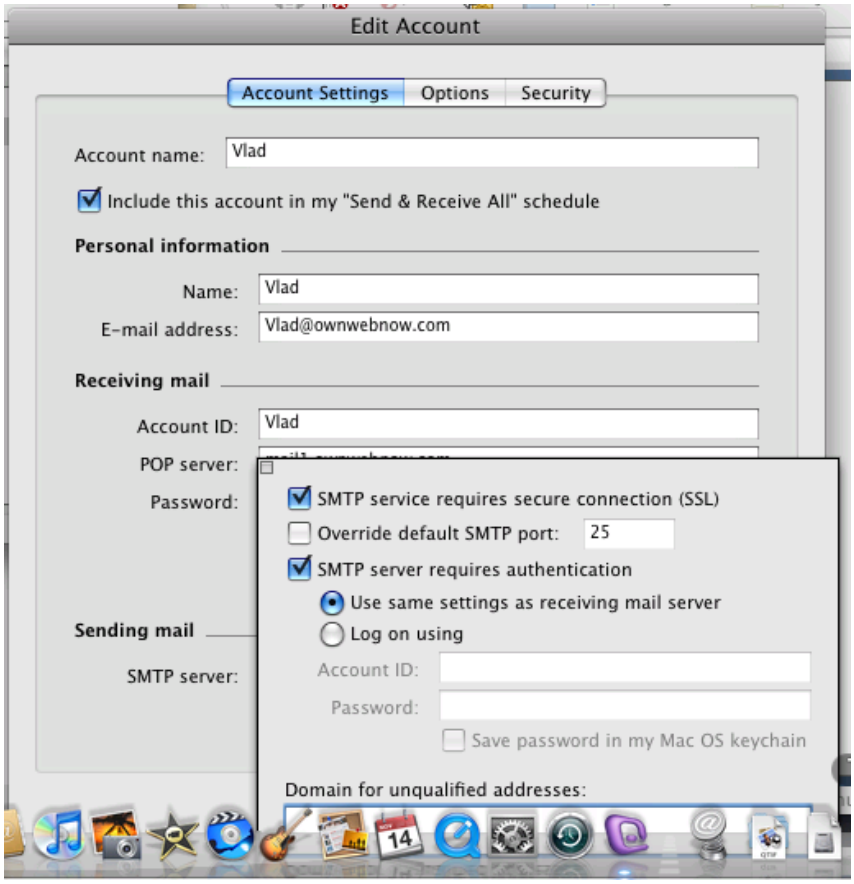
Under accounts, **select** the default (POP) account and click **Edit**.



On the **Account Settings** tab, **click** on **Advanced Receiving Options** button.

C**heck the box** next to **This POP service requires a secure connection (SSL)**

Back on the **Account Settings** tab, click on **Advanced Sending Options** button.



Check the box next to **SMTP service requires secure connection (SSL).**

Check the box next to **SMTP server requires authentication.**

You can select either radio button, default will work.

Important Note: To bypass port 25 restrictions your ISP may be imposing **Check the box** next to **Override default SMTP port** and change the value to 2525 or 25252.

What to do when on the road

Final part of the puzzle is mobility, how do you send email when you are not on the traditional broadband or dialup connection? These are two distinct challenges.

When on mobile device…

If you have a mobile device such as Blackberry or Windows Mobile 5 or 6, you can setup your device with the secure settings outlined so far. Mobile data networks allow access to nearly all the unprivileged ports, just make sure you use SSL/TLS for everything.

When roaming…

If you are on the road and find yourself behind a lot of firewalls or heavily guarded WI-FI connection you may not have access to ports other than 80 or 443 used for basic web browsing. In that scenario you simply have no way to use your Outlook or Windows Mail client software and will unfortunately have to use webmail. However, you should still do so securely:

https://mail1.ownwebnow.com/webmail2

Final Points

Remember that you do have options, you are not limited to just the plain POP3 and SMTP access. Own Web Now supports and further encourages you to use SSL/TLS connections whenever possible. We also encourage you to access our servers on ports other than 25, it might be a little more complex to configure but will save you a lot of time troubleshooting issues in the long term.

Finally, remember that all our shared mail hosting servers support both POP3 as well as IMAP.

As always, at Own Web Now we stand behind our products and gladly support them. If you encounter any issues or would like us to offer assistance please open a support request at https://support.ownwebnow.com

If you like this document and would like to find more please keep an eye on our blog at http://www.ownwebnow.com/blog and our documentation center at http://www.ownwebnow.com/help