

Mail Servers

Introduction

WinWare, the IT department of Windsor Graphics operates and maintains three mail servers whose sole purpose is to receive, store and deliver electronic mail. Obtaining an account hosted on either of these three Mail Servers is reserved exclusively for Windsor Graphics clients.

The three Mail Servers operate through the same mail exchange software package featuring exactly the same security features and Spam detection plug-ins. The only difference between the three mail servers is the extensive filtering of incoming mail on the Primary Mail Server while there is virtually no filtering on the Client Mail Server. Client accounts are predominantly hosted on the Client Mail Server where there is no filtering, however, client accounts can be hosted on the Primary Mail Server on request.

The third Mail Server is a "Mailbag" Server, a backup of the other two. In the event of an outage or failure of either of the two account hosting Mail Servers, the "Mailbag" Server will accept and retain client emails until such time as service is restored on the two account hosting Mail Servers.

All three Mail Servers employ extensive Spam detection plug-ins which can be too restrictive for some email users. Therefore it is very important for any client contemplating having their email hosted on a WinWare Mail Server to be aware of the restrictive configuration of the servers. The restrictive configuration may result in the occasional legitimate email being refused by the mail server because the email did not satisfy one or more of the configuration settings.

The remainder of this document will outline the configuration and Spam detection plug-ins employed by the Mail Servers, instructions for setting up email on your mail handler as well as a description of WinWare Webmail to allow our clients to retrieve their email even when they're away from the office.

Configuration & Spam Detection

Most of the configuration and Spam Detection on the Mail Servers are standard and no different than any other Mail Server. However, those listed below are unique to the WinWare Mail Servers.

Blank Subject Line - The Winare Mail Servers do not accept any email with a blank subject line.

Attachment Restrictions - The Winware Mail Servers remove the attachment(s) on any email where the attachment(s) file extension is .exe, .dll, .bat, .com, .cpl, .hta, .pif, .rtf, .scr, .tmp, .tpm, .vbs, or .zip.

SMTP Authentication - The Winware Mail Servers require the client to provide username and password to send mail.

POP before SMTP - The Winware Mail Servers retain login credentials for a period of time to augment and by-pass the need for SMTP Authentication.

Sender Policy Framework (SPF) - The Winware Mail Servers employ SPF and refuse any email originating from a mail exchanger that is not in the authorized list for the sender's domain. SPF is a DNS based protocol. The domain DNS administrator identifies the mail exchangers authorized to be sending mail for the domain. SPF reduces email address spoofing.

DNSBL - The Winware Mail Servers check every incoming email for listing in three Spam databases; spamhaus, spamcop and sorbs. If the sender's Mail Exchanger's IP address is listed in any of these Spam databases, the Winware Mail Server will refuse the email.

Sender Address Verification - The WinWare Mail Servers refuse any email sent from an email address that the sender's email account host will not verify as legitimate.

Auto Lockout - The WinWare Mail Servers will refuse connection, for a 24 hour period, from any IP Address which has failed

Mail Servers

Configuration & Spam Detection Cont'd

authentication 3 or more times in a 60 minute time period.

GeoIP - The originating country of every email handled by the WinWare Mail Servers is determined and recorded by the Mail Servers. The WinWare Mail Servers refuse any email originating from a small list of specific countries.

Spam Assassin - The WinWare Mail Servers employ Spam Assassin and will refuse any email scored by Spam Assassin as Spam.

Clam AntiVirus - The WinWare Mail Servers employ Clam AntiVirus which checks every incoming email and refuses those containing a malicious threat.

Symantec AntiVirus - The WinWare Mail Servers employ Symantec Endpoint Protection removing any malicious threat on the servers.

In terms of Mail Server Configuration and Spam Detection, it is important to recognize that 90% or more of the incoming email connections on any Mail Server is Spam. While we make every effort to eliminate the acceptance and delivery of Spam emails, it is impossible to catch and block all of them. There will always be the odd one that gets through.

To emphasize the significance of Spam email on a Mail Server, consider this. Our Mail Servers receive over 30,000 incoming mail connections every day. With over 90% of those being Spam emails, our Mail Servers receive over 27,000 incoming Spam email connections every day. Even if only 0.1% of those get past detection, that's over 27 Spam emails a day being delivered to our clients. Our goal is to eliminate Spam entirely.

WinWare WebMail

WinWare Webmail is accessible through any Internet browser. The URL (Internet Address) you must go to is the same as the Internet Address of your incoming mail server included in the email account notification provided by Windsor Graphics.

WinWare Webmail Continued

To determine the Internet Address giving you access to WinWare WebMail, substitute everything to the left of the @ sign and the @ sign in your email address with `http://mail.` giving you `http://mail.yourdomain`

For example, the Internet Address to access WebMail for the email `winner@bigbucks.com` is `http://mail.bigbucks.com`

Additional examples may help you better understand the concept. The following examples give an email address and the corresponding Webmail URL.

Email: `joe@andjane.ca`
Webmail: `http://mail.andjane.ca`

Email: `mary@cattle.ca`
Webmail: `http://mail.cattle.ca`

Email: `john@horses.com`
Webmail: `http://mail.horses.com`

Email Accounts

When you are issued an email account on one of the WinWare Mail Servers you will receive notification from Windsor Graphics outlining information you will need to set up your Email Handler so that your Email Handler will connect with the WinWare Mail Server and pick up mail in your email account automatically. The notification from Windsor Graphics will contain:

Your Email Address - all lower case characters

Account Username - your full email address

Account Password - the password associated with your Account Username

Incoming Mail Server (POP3) - the Internet address of the Mail Server hosting your email account.

Outgoing Mail Server (SMTP) - the Internet address of the Mail Server configured to send mail for your email account.

Authentication Required - the authentication required to send mail on your email account. The "Server requires Authentication" must be checked and "Use

Mail Servers

Email Accounts Continued

same settings as Incoming Mail" must be selected.

SSL Authentication - do not check this option, the Mail Servers do not run on SSL (Secure Socket Layer) protocol.

Outgoing Mail Server Port - the port must be changed from 25 to 587

Leave Copy on Server - the option to leave a copy on the server must not be checked except on mobile electronic devices (Blackberry, iPhone, iPad).

Any and all other settings in the configuration of your Email Handler do not impact the ability of your Email Handler to connect to and pick up and send emails on your email account.

We do not support Email Handler setup and configuration. There are far too many Email Handler software packages to be fluent in all of them. However, instructions for setting up your email account in Windows Live Mail are provided at the end of this document.

Email Account Notes

In terms of your email account, there are some things that may assist you in working with your email address and your email account on a WinWare Mail Server.

Sender Policy Framework (SPF) is activated and defined on all email accounts hosted on any of the WinWare Mail Servers. SPF is designed to eliminate email address spoofing. Email address spoofing is when someone sends out emails using someone else's email address as though the email was sent by the email address owner. While email address spoofing is only eliminated on Mail Servers employing SPF protocol and for domain zones where SPF is defined, the number of Mail Servers and domain zones adhering to SPF is steadily growing. Ideally all Mail Servers and domain zones would subscribe to SPF.

The impact SPF has on your email address and email account is that it is more difficult for someone to spoof your email address including yourself. SPF defines the Mail Servers

Email Account Notes Continued

authorized to send mail using your email address as the sender. The only Mail Servers authorized to send mail using your email address as the sender are the WinWare Mail Servers. A SPF record is created for every domain DNS WinWare hosts identifying the WinWare Mail Servers as the only mail exchangers authorized to be sending mail for the hosted domain. As such, if you attempt to send mail through your own ISP Mail Server using your WinWare email account, any server subscribing to SPF will deny delivery of the email. To prevent this from happening, only use the WinWare Mail Server to send emails on your WinWare hosted email account.

WinWare WebMail is provided as a service to allow you to pick up your email even when you're away from your office, on holidays or on a business trip. It is not intended to be used as a routine means by which you access your email account. WebMail places additional, unnecessary load on the Mail Servers impacting the operation of the Mail Servers in receiving, processing and delivering emails for all accounts hosted on the servers. Users who abuse the WebMail service by routinely accessing their email account through WebMail will have their WebMail access terminated.

Your **Account Username and Password** are authenticated by the Mail Server as a matched pair. This provides security on the Mail Server and your email account. The safe and private keeping of your email Account Username and Password is your responsibility. Store them in a safe, secure location.

Changing the **Outgoing Mail Server Port** from 25 to 587 is extremely important for some users. Some service providers 'hijack' all Internet traffic being transmitted on a specific port and direct it to a specific, predetermined Internet address. For example, Shaw Internet service 'hijacks' all Internet traffic being transmitted on port 25 of their system to their own Mail Servers. If your Internet is provided by Shaw or one of its subsidiaries and you don't change the Outgoing Mail Server Port in your email handler, you will not be able to send

Mail Servers

Email Account Notes Continued

emails using your WinWare hosted email address. While this is especially true for Shaw Internet Service, it is also true for many other ISPs.

While our Mail Servers have massive storage capacity, the Email Handler on your primary desktop or laptop computer should not be configured to **Leave a Copy of Emails on the Server**. Our Mail Servers are not intended to be an archive medium for your email. In the event that we find email accounts containing large volumes of stale dated emails, we will limit the storage capacity for those email accounts on the Mail Servers. We do recognize the need to **Leave a Copy on the Server** when accessing email accounts by mobile electronic devices but expect our clients to access their email accounts from their primary desktop or laptop computer removing all email in their account at least once per week.

Definitions

Mail Exchanger - is a computer connected to a network configured to exchange mail with other mail exchangers and Email Handlers. A mail exchanger may or may not be connected to the Internet.

Mail Server - is a Mail Exchanger connected to the Internet and hosts email accounts. While a Mail Exchanger may do the same thing, a Mail Exchanger doesn't necessarily host email accounts, it may simply exchange emails.

Email Handler - is a software program designed to communicate with Mail Exchangers. Examples of Email Handlers would be MS Outlook, Outlook Express and Windows Live Mail.

DNS Server - is a application specific computer connected to the Internet whose purpose is to resolve domain names to the IP Address of the Internet Server where a service for the domain is hosted. A DNS Zone on a DNS (Domain Name System) Server will contain IP Addresses for domain services like:

- the DNS authority

SPF Continued

- the domain's website
- the domain's mail exchangers
- sub-domains
- SPF (Sender Policy Framework)

While there may be many other records listed in a DNS zone for a given domain, these are the records pertinent to Email accounts and Email handling. The DNS administrator controls the entries for a given domain on the DNS Server.

Sender Policy Framework (SPF)

Sender Policy Framework is a protocol used by DNS administrators to identify the Mail Exchangers that are authorized to be sending mail for a given domain. SPF is a simple text record in the DNS Zone on a DNS Server for a given domain. SPF returns four responses to a DNS inquiry:

- **Pass** - the sending mail exchanger is authorized to be sending mail for the domain in question
- **Fail** - the sending mail exchanger is not authorized to be sending mail for the domain in question
- **Softfail** - it is inconclusive whether the sending mail exchanger is authorized to be sending mail for the domain in question
- **None** - there is no SPF record in the DNS Zone for the domain in question.

If SPF returns a Pass rating for any given email, the sending Mail Exchanger is authorized to be sending mail for the given domain and the mail should be and is delivered. If SPF returns a Fail rating for any given email, the sending Mail Exchanger is not authorized to be sending mail for the given domain and the mail should not and is not delivered. If SPF returns a Soft Fail rating for any given email, the sending Mail Exchanger may or may not be authorized to be sending mail for the domain in question entirely due to incorrect creation of the SPF record in the domain's DNS. What the domain DNS administrator is saying is it is alright for anyone and everyone to send mail for the domain in question from the sending Mail Exchanger. In this case the authority of the sending Mail



Mail Servers

SPF Continued

Exchanger to send mail for the given domain is unknown and the mail should not be and is not delivered. If SPF returns a None rating for any given email, all domains are authorized to send mail from the sending Mail Exchanger because the given domain does not subscribe to SPF. In this case the mail should be and is delivered.

The significance of SPF is enormous. It protects the security and identity of your email address, preventing a spammer or anyone else from spoofing your email address. For example, suppose your email address is joe@johndoe.com and some person in Germany attempts to send out thousands of Spam emails using your email address. Because your domain DNS hosted on a WinWare DNS Server automatically has a SPF record which exclusively identifies only WinWare Mail Exchangers to be authorized to send mail on the johndoe.com domain, all Mail Exchangers that subscribe to SPF receiving the Spam emails from the guy in Germany will refuse delivery of the Spam emails.

Regardless of what Mail Server your email accounts are hosted on or what Mail Exchangers are responsible for sending and receiving emails for your email account, you should insist SPF be implemented on those Mail Exchangers. You should also insist that your domain DNS administrator create an appropriate, concise and explicit SPF record for your domain.

SPF is terribly misunderstood and under utilized. One would think that public enterprises would actively protect the integrity and security of their domain email addresses yet the Town of Carstairs, Town of Didsbury, Town of Bowden and Town of Olds do nothing of the sort. One would also think that huge ISPs like Telus and Shaw who offer Shared Hosting would automatically create SPF records in the DNS of your hosted domain. Such is not the case.

You are responsible for the maintenance and conduct of your domain and your domain email addresses. It is up to you to make sure the integrity and security of your domain and domain email addresses are protected.

Mail Servers

Email Account Setup

Following are step-by-step instructions for properly setting up your email account using Windows Live Mail. If you use an Email Handler other than Windows Live Mail, the settings will be the same but the step-by-step process may be slightly different.

1. Launch Windows Live Mail
2. If you already have an email account set up in Windows Live Mail, click 'Add e-mail account'. If this is the first email account being set up in Windows Live Mail, continue at step 3.
3. Enter your full 'Email Address' (provided in the notification Email from Windsor Graphics)
4. Enter your 'Password' (provided in the notification Email from Windsor Graphics)
5. Check 'Remember Password'
6. Enter your 'Display Name'
7. Check 'Manually configure server settings for email account'
8. Click 'Next'
9. Ensure 'My incoming mail server is a ...' is set to "POP3"
10. Enter your 'Incoming server' (provided in the notification Email from Windsor Graphics)
11. Ensure the 'Incoming server Port' is set to 110
12. Leave 'This server requires a secure connection (SSL)' unchecked
13. Set 'Logon using' to "Clear Text Authentication"
14. Enter your 'Login ID' as your full email address
15. Enter your 'Outgoing server' (provided in the notification Email from Windsor Graphics)
16. Ensure the 'Outgoing server Port' is set to 587
17. Leave 'This server requires a secure connection (SSL)' unchecked
18. Check 'My outgoing server requires authentication'
19. Click 'Next'
20. Click 'Finish'
21. Right-click the email account you just created and select 'Properties'
22. Enter 'Organization' if appropriate
23. Enter your full email address in 'Reply address'
24. Ensure 'Include this account when receiving mail or synchronizing' is checked
25. Click the 'Servers' tab
26. To the right of 'My server requires authentication', click 'Settings'
27. Ensure 'Use same settings as my incoming mail server' is selected
28. Click 'Okay'
29. Click the 'Advanced' tab
30. Uncheck 'Leave a copy of messages on the server'
31. Click 'Apply'
32. Click 'Okay'

Mail Servers

How Email Works

A step-by-step description of how email works may assist you in understanding what is happening when you pick up your email or send an email. Some terms used in this description may be foreign to you. Definitions of some terms are included at the beginning of this document.

Picking up your email

1. Your mail handler sends a inquiry request to a DNS Server to find out the IP Address of the Mail Server hosting your email account.
2. The DNS Server responds with the Mail Server's IP Address.
3. Your mail handler sends a POP3 request to the Mail Server hosting your email account.
4. The Mail Server records the time and date, connection IP Address, and connection Country.
5. The Mail Server checks the Auto Lockout database for the registry of the requested POP3 connection IP Address. If registered, the connection is terminated.
6. The Mail Server responds asking for your username and password.
7. Your mail handler responds with your username and password.
8. The Mail Server verifies the username and password, records your IP Address in the POP before SMTP database, and delivers your mail to your mail handler.
9. Your mail handler receives the mail and confirms receipt.
10. The Mail Server sends an end of mail delivery notice to your mail handler.
11. Your Mail handler responds and requests a termination of the POP3 connection.
12. The Mail Server responds deleting copies of the delivered mail and terminating the POP3 connection.

Sending email

1. Your mail handler sends a inquiry request to a DNS Server to find out the IP Address of the Mail Server hosting your email account.
2. The DNS Server responds with the Mail Server's IP Address.
3. Your mail handler sends an SMTP request to the Mail Server hosting your email account.
4. The Mail Server records the time and date, connection IP Address, and connection Country.
5. The Mail Server checks its GeoIP settings to see if connections from that Country are allowed, if they are not allowed, the connection is terminated.
6. The Mail Server checks the Auto Lockout database for the registry of the sender's IP Address. If registered, the connection is terminated.
7. The Mail Server checks the POP before SMTP database to see if the sender's IP Address is registered, if not the Mail Server requests Username and Password credentials. Your mail handler sends the credentials and the Mail Server authenticates them. If the credentials cannot be authenticated, the Mail Server terminates the connection.
8. The Mail Server requests the sender's email address and the recipient's email address.
9. Your mail handler responds with the sender's email address and the recipient's email address.
10. The Mail Server checks 3 Spam internet databases for the sender's domain. If the sender's domain is found in any one of the 3 Spam databases, the SMTP connection is terminated.
11. The Mail Server checks with the sender's DNS Server to see if the IP Address of the connection is authorized to be sending emails on that domain (SPF), if not the SMTP connection is terminated.
12. The Mail Server sends a request to the sender's Mail Server to verify (Address Verification) that the sender's email address is legitimate and active, if not the SMTP connection is terminated.
13. The Mail Server responds informing your mail handler it is ready to receive the mail.
14. Your mail handler sends the mail to the Mail Server.

Mail Servers

Sending email Cont'd

15. The Mail Server confirms receipt and checks the Subject Line of the email, if blank the connection is terminated.
16. The Mail Server begins delivery.
17. The Mail Server sends an inquiry request to a DNS Server to find out the IP Address of the Mail Server hosting the recipient's mail.
18. The DNS Server responds with the IP Address of the Mail Server hosting the recipient's email address.
19. The Mail Server sends an SMTP request to the recipient's Mail Server.
20. The recipient's Mail Server correspondingly goes through steps 4 through 12.
21. The Mail Server delivers the mail to the recipient's Mail Server and requests an end of the SMTP connection.
22. The recipient's Mail Server confirms receipt and terminates the SMTP connection.

Mail Sent to you

1. The sender's Mail Server requests an SMTP connection with your Mail Server.
2. The Mail Server records the time and date, connection IP Address, and connection Country.
3. The Mail Server checks its GeoIP settings to see if connections from that Country are allowed. If they are not allowed, the connection is terminated.
4. The Mail Server checks the Auto Lockout database for the registry of the sender's IP Address, if registered the connection is terminated.
5. The Mail Server requests the sender's email address and the recipient's email address.
6. The sender's Mail Server responds with the sender's email address and the recipient's email address.
7. The Mail Server checks 3 Spam internet databases for the sender's IP Address. If the sender's IP Address is found in any one of the 3 Spam databases, the SMTP connection is terminated.
8. The Mail Server checks with the DNS for the sender's domain to see if the IP Address of the connection is authorized to be sending emails on that domain (SPF), if not the SMTP connection is terminated.
9. The Mail Server sends a request to the sender's Mail Server to verify (Address Verification) that the sender's email address is legitimate and active, if not the SMTP connection is terminated.
10. The Mail Server responds informing the sender's Mail Server it is ready to receive the mail.
11. The sender's Mail Server sends the mail to the Mail Server.
12. The Mail Server confirms receipt and checks the Subject Line of the email, if blank the connection is terminated.
13. The Mail Server begins delivery.
14. The Mail Server checks the accounts list to find the recipient's email address. If not found, the Mail Server terminates the connection and adds the sender's IP Address to the Auto Lockout database.
15. The Mail Server sends a terminate SMTP connection to the sender's Mail Server.
16. The sender's Mail Server responds terminating the SMTP connection.
17. The Mail Server delivers the mail to your account.