



**End User Control Panel  
(EUCP)**

**User Manual**

**Version: 1.3**

<b>INTRODUCTION .....</b>	<b>3</b>
Setting Up your Internet Service .....	3
Basic Requirements .....	3
<b>END USER CONTROL PANEL .....</b>	<b>4</b>
EUCP - Change Password.....	5
EUCP - Add or Remove Basic Services .....	5
EUCP - Modify Spam and Virus Settings.....	6
EUCP - Advanced Spam Settings and Filtering Options .....	8
EUCP - Manage Website .....	11
EUCP - Webmail .....	13
EUCP - Greymail.....	14
EUCP - Parental Controls/Tattlemail .....	15
EUCP - Email Settings .....	16
EUCP - S-Drive Remote Network Storage .....	17
EUCP - Trend Micro AV .....	22
<b>BANDWIDTH SPEED TEST .....</b>	<b>25</b>
<b>ADDITIONAL RESOURCES.....</b>	<b>27</b>
User ID and Password Attributes .....	27

## Introduction

This document is a user manual for your email and Internet services. It provides instructions for managing your email account(s) with the End User Control Panel, including personal information and password changes, spam and virus settings, Webmail (email access from the World Wide Web), Greymail (spam and virus repository), and Parental Controls, Video email, and other services. Sandhill reserves the right to make these controls available to you or manage these controls on your behalf. Therefore, you may or may not have access to the controls mentioned in this manual. Screen shots used in this manual are *examples* only. Your actual screens may vary depending upon the controls and services made available to you by Sandhill Telephone. Contact Customer Service at 843-658-3434 if you have questions regarding controls and services that are available to you.

## Setting Up your Internet Service

Contact Sandhill Tech support if you have questions related to the initial setup of your account. This manual is intended to cover managing your account and services after your account(s) are established.

## Basic Requirements

### User ID's and Passwords

User ID's should be entered in all lower case letters, since many email systems can only accept email addresses in lower case and your User ID is an email address in this system. However, passwords are case sensitive, meaning upper or lower case letters used to establish your password will be checked for matching case each time you log in. This provides an increased level of security with less likelihood of your account(s) being accessed by password generation technology employed by hackers and identity thieves. Users must log in with their full User ID (**bobsmith@shtc.net for example**) and password when initiating email sessions in order to be able to send email as detailed below. Please guard your User ID and password information carefully. See the Additional Resources section for password attributes, length, legal characters, etc.

### SMTP Authentication

In order to reduce virus and spam proliferation, the outgoing email servers used to support your email account(s) require SMTP Authentication. This may require that minor configuration changes in your email program be updated to support and enable SMTP Authentication. Log in with your full User ID and password when initiating an email session. Otherwise, you will not be authorized to send email and will receive error notifications upon attempting to send email. This is an important step in preventing unauthorized individuals from distributing attacks and junk email, and in uniquely identifying those users who launch such attacks. This support only has to be enabled once for each account. For information on how to update most email applications to implement SMTP authentication go to SMTP Instructions and follow the instructions.

# End User Control Panel

The End User Control Panel (EUCP) is a quick and easy way for you to manage your Internet account and account settings via the web.

To access the EUCP, you must browse to our website [www.shtc.net](http://www.shtc.net) and click or click the [MY Account](#) link on the homepage of our website [www.shtc.net](http://www.shtc.net). Once there, you must enter your full User ID and password to log in. You will then see the home page below which shows your current usage for the month (metered Dialup), your account information, as well as your mail, radius, and personal website settings. This is a good location to check your email and personal web storage info. This screen is known as: Home in the drop down menu on the left.

Help

- ▶ Home
- + Change Password
- + Add/Rem Basic Services
- + Modify Spam/Virus Settings
- + Manage Website
- + Webmail
- + Greymail
- + Email Settings
- + Trend Micro AV
- + Download S-Drive
- + Speedtest
- + Manage S-Drive

**Logout**

= New Window

*NOTE: Some changes made using this interface may take up to 30 minutes to take effect.*

Current Usage
Mail Storage: 22.04 MB of 100 MB
Dialup time this month: 0 hr, 0 min, 0 sec
Dialup time last month: 0 hr, 0 min, 0 sec
Disk Use: 0.00 MB of 10 MB
S-Drive Use: Unknown
Video Mail Use: 0 Mins

Account Info
Userid: demo
Name: Demo User
Account Number: 521-1234

Mail Settings
Email Address: demo@shtc.net
Mail Quota: 100MB
Incoming Mail Server: mail.shtc.net
Outgoing Mail Server: smtp.shtc.net

Radius Settings
Userid: demo@shtc.net
Idle Timeout: 900 Seconds
Max Simultaneous Logins: 2
News Server: news.shtc.net

Personal Web Site Settings
URL: <a href="http://www.shtc.net-demo">http://www.shtc.net-demo</a>
FTP Server: ftp.shtc.net
Ftp Username: demo

S-Drive Settings
Status: Enabled
Quota: 10 megabytes

Please take a look at the menu on the left side of the main page above. This menu gives you the ability to make changes to the services you receive, as well as to add or cancel individual services. You can make changes to the services listed in the menu above and below you will find instructions on each one. As noted, some changes made using this interface may take up to 30 minutes to take effect.

As mentioned earlier, you may not have the ability to change all of these services shown. The parameters shown in the account info on the right are for example only and may not reflect the settings of your actual account. Some screens in this manual may not appear like actual screens.

## ***EUCP - Change Password***

The screen shown below allows you to change your password. Remember that passwords are case sensitive. You must input your existing password and then a new password; you will then need to verify your new password. This will ensure that you do not mistype the new password. Remember to click on **Save** after you have entered in your new information! It is important to remember that it could take up to 30 minutes after you click **Save** for this change to take effect, and it will affect all services that require you to login with User ID and password. If you have a DSL account, it may be necessary to match this password in your DSL modem or router. Contact 843-498-6600 for more information.

Forgot your password? Contact 843-658-3434.

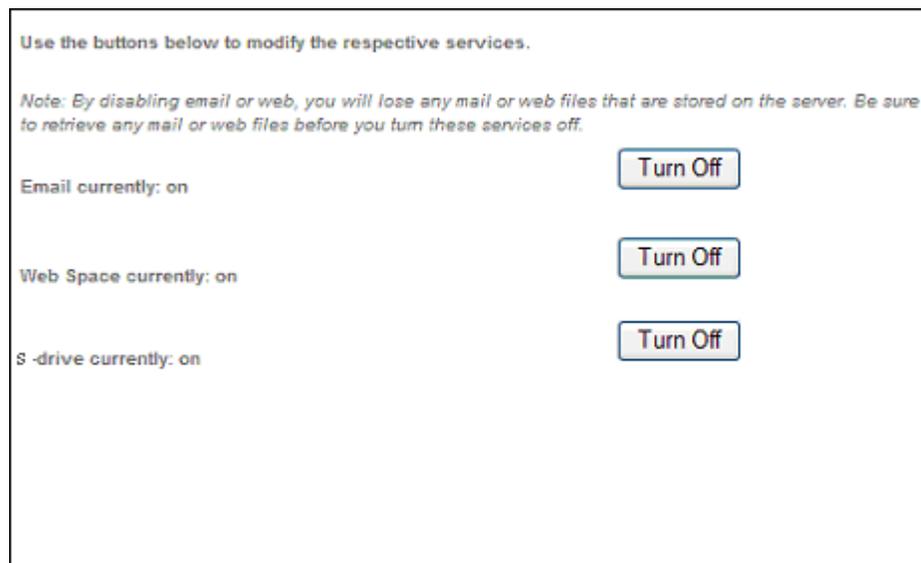


A screenshot of a web form for changing a password. It contains three text input fields labeled "Old Password:", "New password:", and "Password Verify:". Below the fields is a "Save" button.

See the Additional Resources section for password attributes, length, legal characters, etc.

## ***EUCP - Add or Remove Basic Services***

This screen allows you to enable or disable your basic services. You can turn Email, Web Space, Dialup, and S-Drive either on or off by clicking the buttons that are labeled **Turn On**, or **Turn Off**. As the screen below mentions, by disabling Email or Web Space, you will lose any mail or web files that are stored on the server. Be sure to retrieve any mail or web files before you turn these services off.



A screenshot of a web page for managing basic services. At the top, it says "Use the buttons below to modify the respective services." Below this is a note: "Note: By disabling email or web, you will lose any mail or web files that are stored on the server. Be sure to retrieve any mail or web files before you turn these services off." There are three rows of controls: "Email currently: on" with a "Turn Off" button, "Web Space currently: on" with a "Turn Off" button, and "S -drive currently: on" with a "Turn Off" button.

## **EUCP - Modify Spam and Virus Settings**

With anti-spam and anti-virus services your time spent using the Internet is now much more enjoyable! Your emails that are classified as spam and those containing viruses are quarantined in one location for you which is called "Greymail", so your inbox isn't cluttered with spam and your computer and valuable data aren't at risk of being corrupted by dangerous viruses. If you have a Tattlemail password in place, this link will not appear on your EUCP. With a Tattlemail password in place, only the Greymail OPTIONS link can be used to access these changes. See the section on Parental Controls for a description of the Tattlemail feature.

If your anti-spam and anti-virus services are not automatically set up for you, you may set them up by visiting the End User Control Panel, and logging in to enable your service and manage your settings. There is also a link to Greymail from the End User Control Panel for your convenience, and the **OPTIONS** tab in Greymail can also be used to adjust your spam and virus filtering options.

Once you have logged in to the EUCP with your User ID and password, click on **Modify Spam/Virus Settings** on the left-hand menu. You will then see the following items which you are allowed to modify. A brief explanation of each item is provided below:

Email messages categorized as spam are left in your Greymail for 14 days as the default setting. You are allowed to change this period of time. You can leave a message in Greymail for any amount of time between 1 and 14 days. It is recommended to not set this time period too low so that you will have enough time to retrieve any email from Greymail that you would actually like to receive. Log in to Greymail, check the box beside the message(s) you would like to receive and click forward. Selected messages are then forwarded to your inbox. Set the amount of days you want messages to remain in your Greymail and then select **Change**. You cannot forward emails that contain viruses to your inbox.



The screenshot shows a control panel for "Spam Life". On the left, the text "Spam Life:" is followed by a text input field containing the number "14" and the word "days" to its right. To the right of the input field is a rectangular button with rounded corners labeled "Change".

You have the ability to turn your Spam Filtering service off by selecting the **Off** tab. Spam Filtering options will be detailed later in this document.



The screenshot shows a control panel for "Spam Filtering". On the left, the text "Spam Filtering:" is followed by two radio button options: "Off" and "Content-Based". The "Content-Based" option is selected, indicated by a green dot in the center of the radio button. To the right of the radio buttons is a rectangular button with rounded corners labeled "Change".

A Greymail Notification consists of an emailed report containing all of the emails you received which were either classified as spam or classified as containing a virus and were sent to your Greymail. You can decide to receive this report on a daily or weekly basis or not to receive it at all by clicking on one of the options below and then clicking on **Change**.



The screenshot shows a control panel for "Greymail Notification". On the left, the text "Greymail Notification:" is followed by three radio button options: "Off", "Daily", and "Weekly". The "Off" option is selected, indicated by a green dot in the center of the radio button. To the right of the radio buttons is a rectangular button with rounded corners labeled "Change".

The Virus Filtering Section simply allows you to turn on or off your Virus Filtering service. This action may be recommended when you use additional software to provide virus protection. (Sandhill Telephone may elect to have this function on at all times regardless of the user settings to prevent proliferation of viruses.)

Virus Filtering:	On	<a href="#">Turn Off</a>
------------------	----	--------------------------

The Virus Notification is an email which is sent to you and the email sender each time an email is flagged as containing a virus. You have the ability to turn this service on or off as shown below.

Virus Notification:	Off	<a href="#">Turn On</a>
---------------------	-----	-------------------------

By selecting **Content-Based Spam Filtering** option, you then have the ability to enter Advanced Spam Settings, create a Blacklist, a Whitelist, and direct mail from blacklisted senders to Discard or Greymail. (See details below). Otherwise, these options do not appear on the EUCP.

Advanced Spam Settings is the section you would use to edit your spam sensitivity settings and specify types of spam to quarantine to Greymail. By selecting **Edit** here you will then be able to modify your settings. The Advanced Spam Settings will be detailed later in this document.

Advanced Spam Settings:	<a href="#">Edit</a>
-------------------------	----------------------

The Blacklist is a mechanism for blocking emails from specific email addresses. If you do not want to receive emails from certain senders you may add their addresses in this section.

Blacklist:	<a href="#">Edit</a>
------------	----------------------

The Whitelist allows you to make sure that you always receive emails from specific senders. To ensure that a certain someone's emails are not sent to Greymail, add them to this list.

Whitelist:	<a href="#">Edit</a>
------------	----------------------

Both the Blacklist and Whitelist functions will accept "wildcards" using an asterisk "\*" as the wildcard. Using wildcards in front of a portion of an email address means every address that matches the rest of the address will be affected. For instance, if you were to put the following address in your Blacklist file: "\*@bobdomain.net", then all mail from anyone in the "bobdomain.net" domain would be sent to Greymail. Similarly, if you were to put the following address in your Whitelist file: "\*@joedomain.net", then all mail from anyone in the "joedomain.net" domain would be sent to your inbox, provided no viruses were detected.

Finally, you also have the option of having email sent from a Blacklisted sender either discarded immediately, in which case you will never know it was sent to you, or you can choose to have it sent to your Greymail. The default setting is Greymail, and is recommended.

Mail from Blacklisted Senders: Greymail	<a href="#">Change to Discard</a>
---	-----------------------------------

## EUCP - Advanced Spam Settings and Filtering Options

By selecting **Edit** on the Advanced Spam Settings section under Modify Spam/Virus settings, you will then be able to modify your settings. Advanced Spam Settings and Filtering adjustments allow you to customize your spam filters based upon the content within specific emails. Use these screens to edit your spam sensitivity settings and adjust filters for specific types of spam.

Spam Sensitivity:  points

*Lower numbers mean higher sensitivity. You may use fractional numbers. i.e  
4.5*

FILTERS		Off	Low			High	
	General Spam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Make Money Fast / Work From Home scams	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Adult-oriented content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Supplements and drugs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Weight Loss	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Money Laundering	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	HTML/Content tests	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Spam-sending tools and e-mail lists	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Holiday Spam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

You have the ability to set an overall Spam Filtering sensitivity above. You can set sensitivity anywhere between 0 and 999, where the lowest number indicates the strongest of filtering settings. The default setting is 5. You can also choose the level for each individual filter. Experiment with the filters until you are satisfied with your exact filtering specifications. After making your changes, select **Update** in order for your settings to take effect. Below this panel you will see the Real Time Block list panel described on the next page.

Real Time Blocks are a method of blocking emails from specific countries that originate spam. Once you make changes, you must click **Update** so that your new selections go into effect. It is recommended to leave **RBL** and **Dialup List** checked, as these are lists of addresses known to generate spam. You can also **Edit** and **Save** your Blacklist and Whitelist settings as shown below.

REALTIME BLOCKS	
<input type="checkbox"/>	Block mail from Argentina
<input type="checkbox"/>	Block mail from Belgium
<input type="checkbox"/>	Block mail from Brazil
<input type="checkbox"/>	Block mail from China
<input type="checkbox"/>	Block mail from Colombia
<input type="checkbox"/>	Block mail from Germany
<input type="checkbox"/>	Block mail from Greece
<input type="checkbox"/>	Block mail from Hong Kong
<input type="checkbox"/>	Block mail from India
<input type="checkbox"/>	Block mail from Italy
<input type="checkbox"/>	Block mail from Japan
<input type="checkbox"/>	Block mail from Korea
<input type="checkbox"/>	Block mail from Kuwait
<input type="checkbox"/>	Block mail from Malaysia
<input type="checkbox"/>	Block mail from Mexico
<input type="checkbox"/>	Block mail from Nigeria
<input type="checkbox"/>	Block mail from Peru
<input type="checkbox"/>	Block mail from Philippines
<input type="checkbox"/>	Block mail from Russia
<input type="checkbox"/>	Block mail from Singapore
<input type="checkbox"/>	Block mail from Spain
<input type="checkbox"/>	Block mail from Taiwan
<input type="checkbox"/>	Block mail from Thailand
<input type="checkbox"/>	Block mail from Turkey
<input type="checkbox"/>	Block mail from United Kingdom
<input checked="" type="checkbox"/>	Dial Up List
<input checked="" type="checkbox"/>	RBL
<input type="button" value="Update"/>	
<b>Blacklist</b>	<b>Whitelist</b>
Add or edit names in the list, then hit save. All mail coming from these senders will be blocked.	Add or edit names in the list, then hit save. Spam Mail coming from these senders will not be blocked. Viruses coming from these senders will always be blocked.
<input type="text"/>	<input type="text"/>
<input type="button" value="Save"/>	<input type="button" value="Save"/>

The screens below are used to select your Blacklist actions, Spam Life, Virus Notification, and GreyMail Notification settings as described earlier in this document.

### Blacklist Preferences

Messages from blacklisted senders can be sidelined (placed in Greymail) or discarded.

These messages are currently **sent to greymail**.

[Discard messages](#)

**Discarded:** any message from a sender that has been blacklisted will be removed.  
**NOTE:** Messages are unrecoverable.

**Greymail:** any message from a sender that has been blacklisted will be viewable in greymail.

### Spam Life

Spam and Virus messages are automatically purged from greymail.  
You can select the number of days a message stays in the mailbox.

This can be between 1 and 14 days.  
Automatically delete messages after

days.

[Change](#)

### Virus Notification

Greymail can automatically send you an email when you receive a message containing a virus.

This feature is presently **Off**.

[Turn notification on](#)

### Greymail Notification

The system can e-mail reports on the contents of your Greymail.

Daily:

Weekly:

Off:

[Change](#)

## EUCP - Manage Website

The **Manage Website** link will take you to the control panel shown below. Personal web space is a repository for you to store a website, documents, images, files or photos. This space is “write” accessible by you, the site owner, by using your Internet browser, Web Page Editor, or ftp (File Transfer Protocol) Application. It is also “read” accessible to the rest of the world by typing the web space URL (Uniform Resource Locator, also known as your web address) into their Internet browser. Your web space administration is password protected so your files will stay safe and secure and will only be available for others to view or copy by surfing to your URL.

[Upload a file](#) || [Create a directory](#) || [Advanced mode](#)

Current directory: /			
File/Dir	Actions	Size (bytes)	Date
 <a href="#">ftp</a>	<a href="#">Del</a>    <a href="#">Rename</a>	(directory)	Jun 27 10:46
 <a href="#">public_html</a>	<a href="#">Del</a>    <a href="#">Rename</a>	(directory)	Jul 6 09:50

[Upload a file](#) || [Create a directory](#) || [Advanced mode](#)

### How do I put files into my web space?

In order for files to become available from your personal web space, you must first put them there. The method of doing this is called “File Transfer Protocol” (ftp). FTP is the method of delivery, but you must have a way to use this method known as an ftp client. An ftp client is a software application that allows you to put files on the server (upload), and get files from the server (download). There are several types of clients that can be used, as mentioned below. When you select **Manage Website**, you see the one above.

### What clients can I use to put files in my web space?

As mentioned before, there are several types of ftp clients. Programs such as “WsFTP” and “SmartFTP” are 100% ftp clients. This means that their only function is to put files on a server and get files from a server. These are great for people who are only storing files in their web space or are using a text editor (like Notepad or WordPad) to create web pages and then uploading them when they are done. Programs like “Dream Weaver” and “FrontPage” are webpage editors (also known as HTML editors) that, in addition to creating and editing web pages, also have a built-in ftp client. This is handy for creating many web pages and then uploading them quickly. When uploading with any of these programs ensure the upload is made to the **public\_html** folder in order for uploaded information to be seen by the world. And lastly, there is the web based software that you access from the **Manage Website** link. Our ftp tool allows you to upload files from your Internet browser without the need for these third-party programs. Simply go to our ftp site, log in with your User ID and password, choose the directory that you would like to put your files in and then upload. See details below:

### What steps do I take to use the web-based ftp tool?

1. Surf to <http://webftp.shtc.net>
2. Enter your User ID and password.
3. Click the link of the folder you want to upload your files

[Upload a file](#) || [Create a directory](#) || [Advanced mode](#)

Current directory: /			
File/Dir	Actions	Size (bytes)	Date
 <a href="#">ftp</a>	<a href="#">Del</a>    <a href="#">Rename</a>	(directory)	Jun 27 10:46
 <a href="#">public_html</a>	<a href="#">Del</a>    <a href="#">Rename</a>	(directory)	Jul 6 09:50

[Upload a file](#) || [Create a directory](#) || [Advanced mode](#)

The "public\_html" folder is where you would place all of your webpage related files and images. "Username" is the portion of your email address in front of the @symbol, for instance bob@shtc.net would have a username of "bob".

This public\_html folder is accessible to the rest of the world by surfing to <http://web.shtc.net/~username> (be sure to put a "~" in front of your username.)

The ftp folder is accessible by anonymous ftp, which means a user can surf to <ftp://ftp.shtc.net/username>. (No Tilde ~ needed)

Once you are inside your desired folder, you are presented with three options:

- **Upload A File:** Allows you to put a file from your computer to your web space.
- **Create A Directory:** Organize your web space by creating additional folders.
- **Advanced Mode:** View important information about your files and change permissions.

### What are the addresses that I give to friends and family?

All addresses are composed of two things, the domain of your ISP and your User ID.

Listed below is the format you would use to access these "sites".

- I want to access my files directly from an Internet Browser using ftp:
  - <ftp://ftp.shtc.net/username> (no Tilde ~)
- I want my friends/family to see my webpage:
  - <http://web.shtc.net/~username>
- I made a folder called "images" in my public\_html directory, how do I access it:
  - <http://web.shtc.net/~username/images>

## EUCP - Webmail

The **Webmail** link on the EUCP takes you to your Webmail account. You can also access your Webmail account by browsing to <http://webmail.shtc.net> and logging in with your full User ID (email address) and password.

Webmail allows users to access their email from the Web. They can create and send new messages, import or create contact lists, reply to or forward email, or set up folders to file and store email on the server. They can use the personal calendar, create notes and reminders, or access Greymail to check quarantined spam emails or emails containing viruses from the Greymail link. For more information on using Webmail, see the built in Help files.

**Folders**  
Last Refresh:  
Mon, 10:15 am  
(refresh folder list)

**INBOX (36)**  
Drafts  
Sent  
Trash (purge)  
Work Emails  
GreyMail (2)

<< August 2005 >>  
S M T W T F S  
1 2 3 4 5 6  
7 8 9 10 11 12 13  
14 15 16 17 18 19 20  
21 22 23 24 25 26 27  
28 29 30 31

**Sandhill Telephone Cooperative**

Current Folder: **Work Emails** E-mail Quota: 0.11M of 20M | [Sign Out](#)

[Compose](#) [Addresses](#) [Folders](#) [Options](#) [Search](#) [Help](#) [Calendar](#) [Notes](#) [GreyMail](#)

Toggle All Viewing Messages: 1 to 8 (8 total)

Move Selected To: Transform Selected Messages:

INBOX

<input type="checkbox"/>	From	Date	<input type="checkbox"/>	Subject
<input type="checkbox"/>	Demo User	9:57 am	<input checked="" type="checkbox"/>	<u>Welcome! We are happy to serve you!</u>
<input type="checkbox"/>	Demo User	9:54 am	<input checked="" type="checkbox"/>	<u>MyAccount Change Notification</u>
<input type="checkbox"/>	Demo User	9:57 am	<input checked="" type="checkbox"/>	<u>MyAccount Change Notification</u>
<input type="checkbox"/>	Demo User	9:54 am	<input checked="" type="checkbox"/>	<u>MyAccount Change Notification</u>
<input type="checkbox"/>	Demo User	9:57 am	<input checked="" type="checkbox"/>	<u>MyAccount Change Notification</u>
<input type="checkbox"/>	Demo User	9:54 am	<input checked="" type="checkbox"/>	<u>MyAccount Change Notification</u>
<input type="checkbox"/>	Demo User	9:57 am	<input checked="" type="checkbox"/>	<u>Requesting additional information</u>
<input type="checkbox"/>	Demo User	9:54 am	<input checked="" type="checkbox"/>	<u>TPS Report Reminder</u>

Move Selected To: Transform Selected Messages:

INBOX

Toggle All Viewing Messages: 1 to 8 (8 total)

## EUCP - Greymail

This link on the EUCP takes you to your Greymail account, where you will find emails determined to be spam and emails containing viruses. You may also access Greymail by browsing to <http://greymail.shtc.net>. The Greymail home page is shown below.



Please note the **OPTIONS** link at the top right of the Greymail home page above. When you click on this link, you will see the advanced spam settings detailed in the Advanced Spam Settings section shown earlier in this manual.

Please note the icons at the top right of the Greymail home page which are shown below. :



Tag messages by selecting the **tag box** to the left of the message. You can tag **All** or **None** using these boxes in the header. Selecting the icons above will then take actions as described below.

- **Mark as Read** - You have the ability to tag an email (click on the box to the left of the email and you will see a checkmark appear) and then click the **Mark as Read** icon and that email will now show that it has been read.
- **Mark as Unread** - You have the ability to tag an email and then click the **Mark as Unread** icon and that email will now show that it has never been opened.
- **Delete Selected** - This icon allows you to delete emails you have tagged.
- **Forward Selected** - Check the box to the left of any email you would like forwarded to your inbox then click this icon. The email will be forwarded to your inbox.
- **Forward and Allow** - This icon forwards the selected email(s) to your inbox and places the sender's email address on your Whitelist. You will be taken to the Greymail options page and must select the **Save** button under your Whitelist to save your changes.
- **Allow Sender** - If you tag an email in your Greymail and then click on the **Allow Sender** icon, this email address will be placed on your Whitelist. You will be taken to the Greymail options page and must select the **Save** button under your Whitelist to save your changes.
- **View Stats** - By clicking on the **View Stats** icon, you will be able to view your spam and virus statistics for the months you have had service.

## EUCP - Parental Controls/Tattlemail

This section of the EUCP allows you to manage your Parental Controls and TattleMail. See below for descriptions of the options available on this screen.

(Note: Parental Controls may not be available to all users. These features require specific authentication methods in order to perform their function. (Contact Sandhill Telephone for further information.)

Parental Control	
<p>Add the time blocks for which you would like this account to be able to log in below. You may add multiple blocks of time in any denomination of 30 mins. Select the day(s) of the week, the start time and the end time, then hit add. <b>After you add or delete a time block, you will need to hit save at the bottom of this page for your changes to take effect.</b></p>	
Day(s) of week:	Monday thru Sunday ▾
Start Time:	12:00am ▾
End Time:	12:00am ▾
<input type="button" value="add"/>	
Current Time Blocks: (to remove a time block, click on it, then hit delete)	
<div style="border: 1px solid black; padding: 5px; display: inline-block;">Monday thru Sunday 12:00am - 01:00am</div>	
<input type="button" value="Delete"/>	
<input type="text"/>	TattleMail Password
<i>Access to Greymail will require this additional password</i>	
<input type="text"/>	TattleMail Address
<i>Email address for TattleMail login and attempt notification</i>	
<input type="button" value="Save"/>	

## EUCP - Email Settings

In the Email Settings section you may have the ability to change your email quota, set-up email aliases, and to set-up email forwards. Sandhill Telephone reserves the right to make these controls available to you or manage these controls on your behalf.

Upon clicking on the **Email Settings** link, you will see a screen like the one below:

Email Quota:	<input type="radio"/> Default (20MB)
	<input checked="" type="radio"/> Custom: <input type="text" value="10"/> MB
Email alias(es):	
<input type="text" value="demotwo"/>	@shtc.net
<input type="text" value="demothree"/>	@shtc.net
<input type="text" value="demofour"/>	@shtc.net
<input type="text"/>	@shtc.net
Forward all mail to: <i>Note: this will remove your mail account and all associated mail, and send all new mail to the address listed below.</i>	
<input type="text"/>	
<input type="button" value="Save"/>	

The Email Quota section above determines the amount of space you may use on the mail server in megabytes. Once you have reached this amount of storage, you will not be able to receive email until you delete old mail from the mail server. Please be aware that increasing your mail storage may result in an increase in your monthly invoice. You may need to contact Customer Service to increase these limits (this option may not be shown in this panel).

The Email Alias section above allows you to add up to 100 different addresses for which email arrives at your one main account. For example, if your User ID is "Bob" and you make an alias called "Jim", any mail sent to "Jim@shtc.net" will be delivered to your "Bob@shtc.net" account. You must click on **Save** to save your changes to this panel.

In the section labeled "Forward all mail to:" above, you can insert a new address for which you would like all email addressed to your old address to be forwarded to. Your existing mail will be removed from the mail server, and all new mail will be redirected to the email address that you enter. It is very important to retrieve any existing mail from the server before you enable this feature or it will be lost permanently. To remove a forwarder, simply delete it, then click on **Save**.



## EUCP - S-Drive Remote Network Storage

Storing critical files on the network reduces the risk or impact of malicious attacks, viruses, hardware problems, accidental deletion and lost or damaged equipment. S-Drive Remote Network Storage provides a safe and secure storage facility on a network server for storing text documents, photos, web pages, spreadsheets and other files. S-Drive combines the security of network storage with the convenience of a local drive. Once S-Drive is enabled, the network drive is accessible from within applications just like a local drive on your computer.

You can drag and drop or copy files to or from the network drive server using Windows Explorer or using DOS commands or Save/Save-as commands within many applications. Searches can also be extended to network drives. Backups can be scheduled and run automatically using the File Transfer Manager, and full or incremental backups are supported. S-Drive makes using remote storage quick, easy, and reliable.

S-Drive allows users with Windows NT 4.0/2000 & XP Operating Systems to securely transfer, store and access files, without having to learn a new application. FTPS using Secure Sockets Layer (SSL) is supported by S-Drive by creating an encrypted "tunnel" through which FTP transfers data. Secure FTP or SFTP is also supported by S-Drive and provides 128-bit encryption of all transmitted data. Server side support is required for both of these secure protocols.



Help

- + Home
- + Change Password
- + Add/Rem Basic Services
- + Modify Spam/Virus Settings
- + Manage Website
- + Webmail 
- + Greymail 
- + Email Settings
- ▶ Download S-Drive
- + Speedtest 
- + Manage S-Drive

**Logout**

 = New Window

*NOTE: Some changes made using this interface may take up to 30 minutes to take effect.*



S-Drive integrates the safety, and security of remote file storage with the convenience of a local drive. S-Drive creates a link directly to a remote storage server which looks and responds just like a local drive. Access this drive from within any application just like you would access your hard disk. This remote server keeps your files safe and secure protecting you from accidental deletion or malicious privacy thieves. Please note that in order for this service to work, you must first be connected to the Internet.

**System Requirements:**

- Windows NT 4.0/2000/XP
- Pentium II or higher
- 50 MB of available hard disk space
- Internet access
- Minimum system RAM: 64MB

---

**Download S-Drive client application:**

• **Download** Windows NT 4.0/2000/XP users

© 2007 Sandhill Telephone Cooperative Inc. All Rights Reserved.

## Downloading the S-Drive Client

Selecting the **S-Drive** link on the End User Control Panel will display the System Requirements/Download page shown below. Selecting the **Download** link will begin the download process. Versions of Windows Operating systems not shown on the System Requirements page will not work with S-Drive. It is recommended that you upgrade to a supported Operating System in order to use this product. ***It is necessary to contact Customer Service to activate this product.*** Be sure and ask about a number of storage capacities that are available. [This product may incur additional billing when used.](#)





## Installing the S-Drive Client

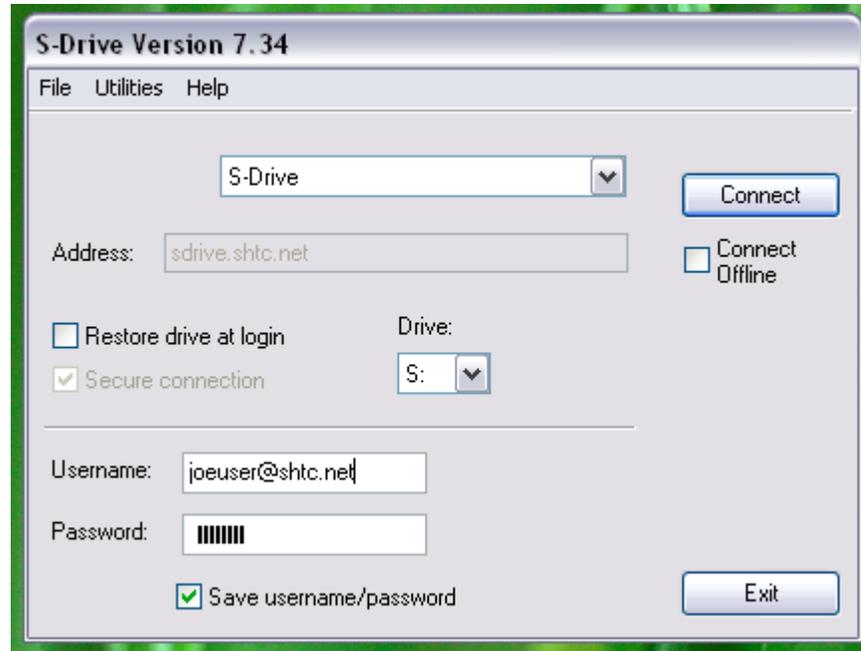
After selecting the **download** box, you will be asked if you want to run or save the installer application. Select **Run** or **Save**. If **Run** is selected, the installer will begin and open the Install Wizard. If **Save** is selected, the installer file will be downloaded to the location specified in the **Save As** dialog box. Once saved, locate the installer application and double click on it to begin the install process. The installer application is typically named setupXYZ.exe, where XYZ refers to the version of the Windows Operating system supported by the installer.

The Install Wizard will prompt you for the folder destination to install the S-Drive program files. You can browse to select the folder for the installation and then click on **Next** to install or click on **Cancel** to exit the Install Wizard. The Install Wizard will copy the program files to the destination folder and then install the program. A restart is required to activate the S-Drive application.

The Install Wizard will also create shortcuts in the Start Menu\All Programs\S-Drive folder for S-Drive and Uninstall S-Drive. Select the shortcut to run the program. The Uninstall shortcut is used to uninstall the program, should this be required.

## Starting S-Drive

When the S-Drive program is initiated for the first time by selecting the program icon in the Start Menu Programs list, system tray, or double clicking the shortcut, the following screen is shown: (Your User ID will be displayed in the Username field.)



This screen serves several functions including as detailed below:

- Allow access to network storage functionality through your full email username and password. (This functionality must be activated by Customer Service.)
- Selecting the Drive letter associated with the network drive from the drop down menu (Typically, letters D thru Z can be assigned as the drive designator.)
- Selecting whether you want the drive to connect at system startup by clicking on this checkbox. This will connect the drive each time your system starts or restarts.
- Select whether you want SSL (Secure Sockets Layer) protocol used in file transfers by clicking on this checkbox (SSL availability requires Windows NT 4.0/2000/XP)
- Access to General settings for the network storage application by clicking on the **Settings** tab (It is recommended to leave these settings at their default values.)
- Access to Advanced settings for the network storage application by clicking on the **Advanced** tab (It is recommended to leave these settings at their default values.)
- When the username, password, and drive letter selections are complete, and choices are made for Connection at startup, SSL encryption, General, and Advanced Settings, click on **Connect** to connect the network drive and finish the initiation of the program.

## Using S-Drive

Once the program is initiated, a screen will be displayed showing the network drive with its designator is connected and available for use just like any other drive on the computer.

If users elect not to have the network drive connect on system start-up, they can connect the drive by selecting the **Start Menu, All Programs**, and the S-Drive program icon from the program list to connect the drive. The same starting network storage connection screen above will appear. The username and password will already be populated and should not be re-input unless a change is required (Your User ID will be displayed in the Username field.) The same selections are available for Connection at startup, SSL encryption, General, and Advanced settings. Click on **Connect** to connect the drive.

The network drive will appear in most Windows applications when users select a **Save As** function and can be chosen as the target drive for saving files or creating folders. The network drive is available for file and directory manipulation using DOS commands. The network drive is also available for most search applications and will display folders or files matching the search criteria.

The network drive will appear when the user selects **My Computer** to display other hard disk drives and devices with removable storage (Hard Drive/CD/DVD/Floppy drives\*\*). Files and folders can be "dragged and dropped" onto the drive icon to create copies of these files and folders on the network drive.



**\*\* Note:** 100GB free space for network storage is shown incorrectly in these screens and is a function of how the Windows Operating System interacts with network drives. Actual capacity will be determined by the network storage package/offering.

We hope you find this to be a safe, secure and convenient method of using network storage to reduce the risk of lost, deleted or damaged information.

Contact Customer Service if you have additional questions.

## EUCP – Trend Micro AV

Trend Micro Internet Security is an industry leader in protecting hundreds of thousands of computers' world-wide.

Trend Micro PC-cillin Internet Security is an easy-to-use, comprehensive security solution that keeps out hackers, viruses, worms, Trojan Horses, phishing attackers, spyware slow downs, and unwanted changes to operating systems and critical software. It uses award-winning firewall technology from Trend Micro, and includes antivirus, phishing and spam protection. You also get home network control, Wi-Fi intrusion detection, URL filtering (parental control), security check, and identity protection.

Trend Micro PC-cillin Internet Security also stops spam that in the past has gotten past security disguised as an image. Plus, coming in a near future release, Trend Micro Internet Security will protect PCs from suspect and risky websites that are included in emails or during surfing.

**\*\*\*NOTE: Uninstall any existing Trend Micro, ISK or other security software before downloading the security suite. \*\*\***

Click on the **Trend Micro AV** link to begin downloading the software.

The screenshot displays the 'MyAccount Page EUCP' interface. On the left is a navigation menu with the following items: Home, Change Password, Add/Rem Basic Services, Modify Spam/Virus Settings, Manage Website, Webmail, Greymail, Email Settings, Trend Micro AV (highlighted with a red box and a callout), Download S-Drive, Speedtest, and Manage S-Drive. A 'Logout' button is located below the menu. A legend indicates that a small square icon represents a 'New Window'. A note states: 'NOTE: Some changes made using this interface may take up to 30 minutes to take effect.' On the right side, there is a 'Current Usage' section with the following data: Mail Storage: 22.04 MB of 100 MB, Dialup time this month: 0 hr, 0 min, 0 sec, Dialup time last month: 0 hr, 0 min, 0 sec, Disk Use: 0.00 MB of 10 MB, S-Drive Use: Unknown, and Video Mail Use: 0 Mins. Below this is an 'Account Info' section: Userid: demo, Name: Demo User, Account Number: 521-1234. The 'Mail Settings' section includes: Email Address: demo@shtc.net, Mail Quota: 100MB, Incoming Mail Server: mail.shtc.net, and Outgoing Mail Server: smtp.shtc.net. The 'Radius Settings' section shows: Userid: demo@shtc.net, Idle Timeout: 900 Seconds, and Max. Simultaneous Logins: 2. The 'Personal Web Site Settings' section lists: URL: http://www.shtc.net-demo, FTP Server: ftp.shtc.net, and Ftp Username: demo. The 'S-Drive Settings' section shows: Status: Enabled and Quota: 10 megabytes. A 'Help' link is visible in the top right corner.

Click on the **Download** button for Software Download.

- + Home
- + Change Password
- + Add/Rem Basic Services
- + Modify Spam/Virus Settings
- + Manage Website
- + Webmail 
- + Greymail 
- + Content/Parental Controls
- + Email Settings
- + Trend Micro AV
- + Download S-Drive
- + Speedtest 
- + Manage S-Drive

[Logout](#)

 = New Window

NOTE: Some changes made using this interface may take up to 30 minutes to take effect.

Trend Micro® Security Suite is an easy-to-use, comprehensive security solution that keeps out hackers, viruses, worms, fraudulent emails and other threats. It uses award-winning firewall technology from Trend Micro, and includes antivirus, phishing & spam protection, Web site filtering, privacy protection, instant messaging security, and more.

**Key Features Include:**

- Easy-to-use firewall blocks hackers and other unknown threats.
- Stops viruses and worms, and protects against emerging viruses before they attack.
- Protects against identity theft and online profiling.
- Quarantines suspicious email attachments and blocks outbound messages containing potential viruses.
- Protects users of the most popular IM services and shields you from IM spammers, thieves, and online predators. Blocks access to offensive Web site content.
- Anti-Phishing & Spam Blocker automatically stop dangerous phishing emails and spam from getting into your inbox. Plus, they constantly adapt to the ever-changing techniques of professional spammers—protecting you against the latest "phishing" schemes.
- Automatically secures PCs connected to wireless networks—at home or on the road.

**System Requirements:**

- Windows 2000/XP:
  - Pentium III 450 MHz or higher
  - Minimum system RAM: 128 MB
- Windows Vista (32-bit):
  - Pentium III 800 MHz or higher
  - Minimum system RAM: 512 MB
- 50 MB of available hard disk space.
- Internet access.
- Supported protocols for email scanning: POP3 and IMAP4 for incoming; SMTP for outgoing.



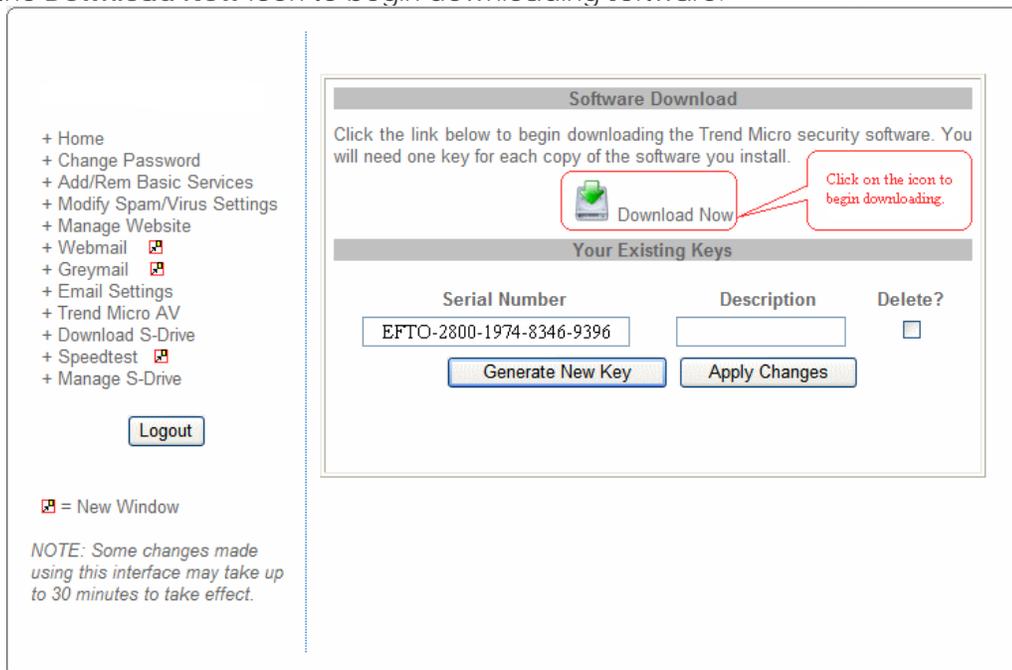
Click the download button to the left to begin your download of the software. You will be taken to a page that displays your user registration number. Please make a note of it for future reference.

[Download](#)

Click button for Software Download

Be sure to **record the Product Registration/Serial Number** for use in installing the software once it is downloaded to your PC. PC-cillin Reg/Serial Number: \_\_\_\_\_-\_\_\_\_\_-\_\_\_\_\_-\_\_\_\_\_-\_\_\_\_\_

Click on the **Download Now** icon to begin downloading software.



Click on the **Run** button at the *Internet Explorer – Security Warning*, then click on the **Run** Button again at the *File Downloading – Security Warning* to start downloading.

Download will take up to 10 minutes with SHTC DSL to Run and complete the installation of the software on to your PC; with SHTC Dial-Up it may take a few hours. If you are using dial-up make sure that the connection does not drop during the download. Once download is complete, restart your computer and follow the **Trend Micro PC-cillin Internet Security – Install Wizard** which will guide you through the installation process.

Please read and click on **I accept the terms in the license agreement**, click on the **Next** button.

Enter your **PC-cillin** Reg/Serial Number: \_\_\_\_\_-\_\_\_\_\_-\_\_\_\_\_-\_\_\_\_\_-\_\_\_\_\_, click on the **Next** button.

Select which features you want to install, **Full installation is recommended** and select the folder in which install it, click on the **Next** button.

Change any default Optional Online Services or simply click on the **Install** button. Please wait a few minutes while the setup program installs Trend Micro PC-cillin Internet Security Suite. Once installation is complete you must restart your computer for settings to take affect.

Click on the **Finish** button. Save any open files and close all programs and restart your computer.

After computer has been restarted you will see the Trend Micro PC-cillin Internet Icon. . To configure the protection status, register your subscription, update and scan your computer.

Once your subscription has been registered you will receive a confirmation e-mail from [TMOS\\_reg@trendmicro.com](mailto:TMOS_reg@trendmicro.com). Please do not reply to this e-mail, but keep this information in a secure place for further reference. This information helps our Technical Support Team provide you with assistance, which you can access 24 hours a day, 7 days a week at 498-6600.

## Bandwidth Speed Test

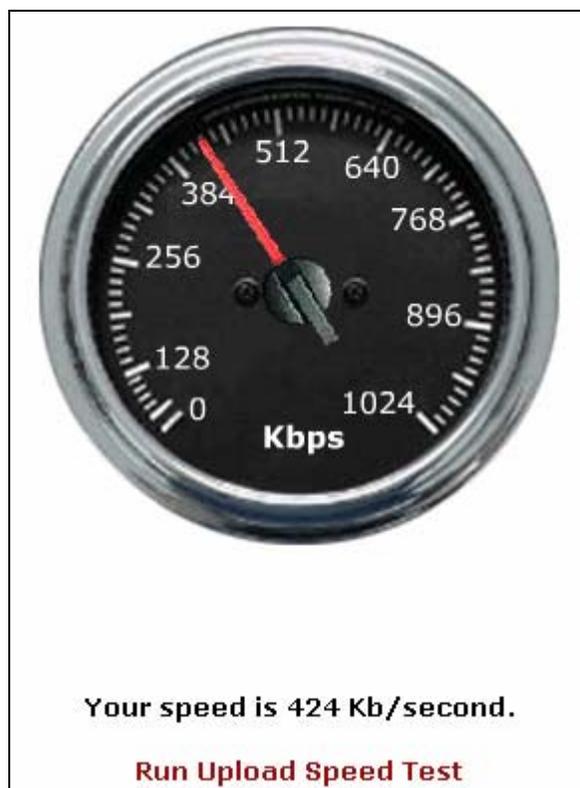
Ever wonder what kind of speed you are really getting? With Speed Test you can find out easily and quickly by running a test on your upload and download connection speeds. Here's how....

To access the speed test, you must visit the following website: <http://speedtest.shtc.net>. First enable JavaScript if this function is not already enabled.

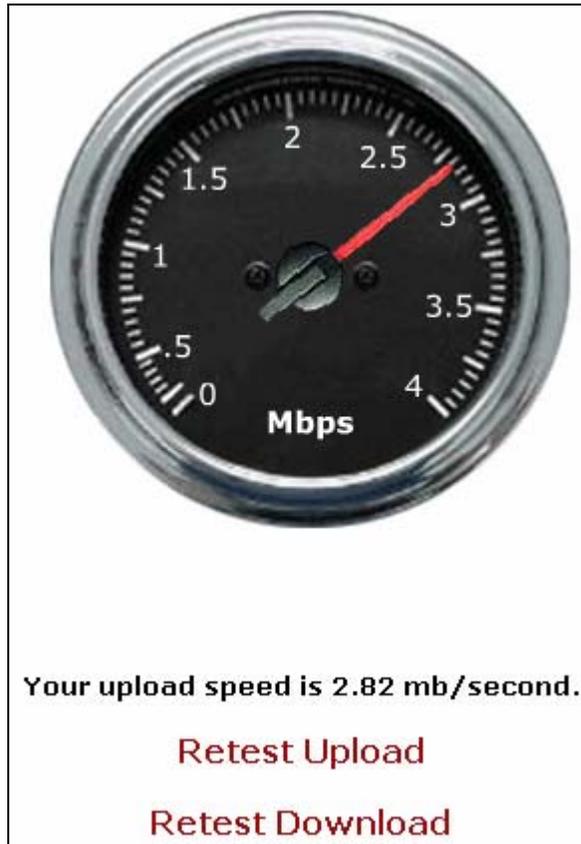
Please enter your email address.

Please remember to enable JavaScript for this test!

You must enter in your email address and click on **Go!** You will then be told that your connection is being tested and to please wait while the revving speedometer is displayed. Once the test is complete you will see the following screen where your speed is displayed...



If you'd like to see your upload speed, click on **Run Upload Speed Test** at the bottom of the previous page. Your speed will then be tested and displayed to you and you will also have the option of running the tests again by clicking on either **Retest Upload** or **Retest Download**.



## Additional Resources

Log in to [www.shtc.net](http://www.shtc.net) for further information regarding your email and Internet services.

You can contact our Customer Service department at 843-658-3434.

For technical support questions regarding your email or Internet services, contact 843-498-6600.

### ***User ID and Password Attributes***

The following attributes represent the acceptable parameters for User ID's and passwords.

#### **User ID's**

User ID's must be **at least 2, but not more than 12 characters in length. (No spaces)**

User ID's may only contain the following characters:

Letters A thru Z,

Digits 0-9

Underscore (\_)

Dash (-)

Period or Dot (.),

User ID's may not begin or end with dot, dash or underscore.

**Upper and lower case User ID's will be accepted, but any uppercase characters will converted to lowercase automatically.** Many email systems only accept lower case email addresses or convert them to lower case. (Since our systems use the email address as the User ID, this convention ensures that Bob@shtc.net and bob@shtc.net do not get each others email.)

#### **Passwords**

**Passwords must be at least 2 but no more than 12 charters in length. (No spaces)**

**Passwords are case sensitive. Case matching will be enforced for passwords.**

Passwords may only contain the following characters:

Letters A thru Z,

Digits 0-9

Underscore (\_)

Dash (-)

Period or Dot (.),

Passwords may not begin or end with dot, dash or underscore.