INTRODUCTION.....2

Setting Up your Internet Service.....2

Basic Requirements.....2

END USER CONTROL PANEL.....3

EUCP - Change Password.....4

EUCP - Add or Remove Basic Services.....5

EUCP - Modify Spam and Virus Settings.....5

EUCP - Advanced Spam Settings and Filtering Options.....8

EUCP - Add / Edit child accounts.....12

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), Content Filtering and Parental Controls. Windy City 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 for examples only. Your actual screens may vary depending upon the controls and services made available to you by Windy City. Contact Windy City Customer Service (611) if you have questions regarding controls and services that are available to you.

Setting Up your Internet Service

Contact Windy City Customer Service (611) 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

Userid's and Passwords

Userid's should be entered in all lower case letters, since many email systems can only accept email addresses in lower case and your userid 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 userid **(bobsmith@domain.com for example)** and password when initiating email sessions in order to be able to send email as detailed below. Please guard your userid and password information carefully. See the Additional Resources section for password attributes, length, legal characters, etc.

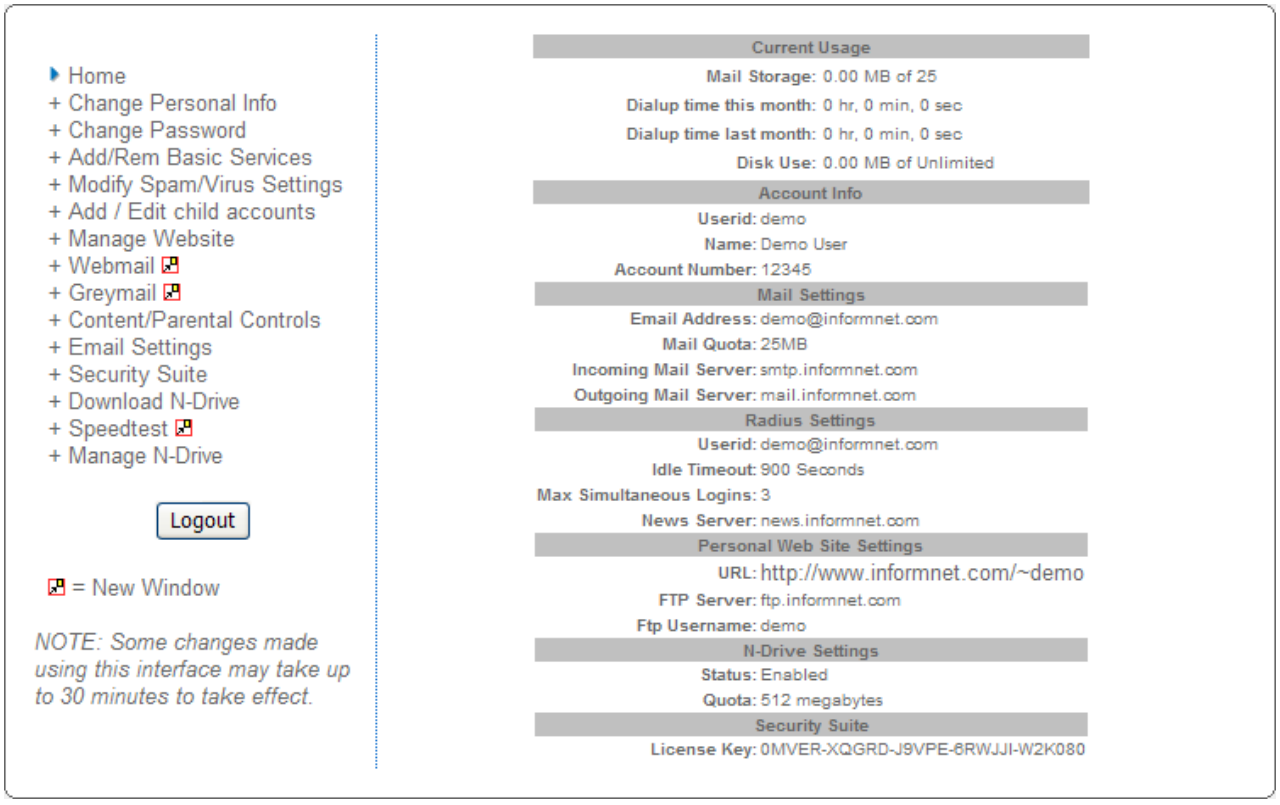
SMTP Authentication

In order to reduce virus and spam proliferation, the outgoing email servers used to support your email account(s) require SMTP Authentication. This will require that minor configuration changes in your email program be updated to support and enable SMTP Authentication, and that you log in with your full userid 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 setup Outlook Express to implement SMTP authentication go to <http://www.microsoft.com/windows/ie/ie6/using/howto/oe/setup.mspx#EEB> and follow the instructions using pop.adaktu.net for the incoming, or pop3 server, and smtp.adaktu.net for the outgoing, or smtp server.

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 http://myaccount.<domainname.xxx>, Once there, you must enter your full userid 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.



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.

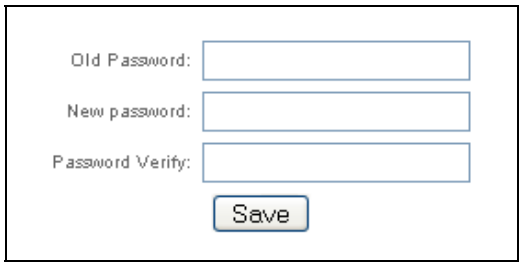
EUCP - Change Personal Info

By clicking on this link, the screen below allows you to update your personal information. Customer Service will be notified of the changes you are making within 24 hours. Remember to click on **Save** after you have entered in your new information!

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 userid and password. If you have a DSL account, it may be necessary to match this password in your DSL modem or router. Contact Technical Support for more information.

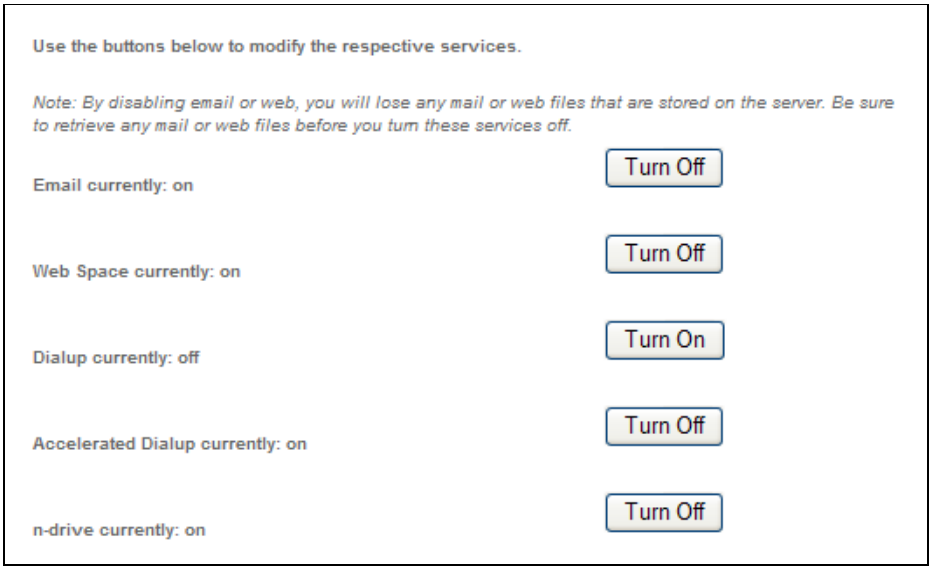
Forgot your password? Contact Technical Support.



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. This can be useful if you add a child account and need to go in and add or remove services to it. You can turn Email, Web Space, Dialup, Accelerated Dialup and N-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.



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 Content Filtering and 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 userid 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.

You have the ability to turn your Spam Filtering service off by selecting the **Off** tab**.** If you choose to employ Content Filtering, then you can select the **Content-Based** tab for Content-Based filtering and then clicking **Change**. Spam Filtering options will be detailed later in this document.

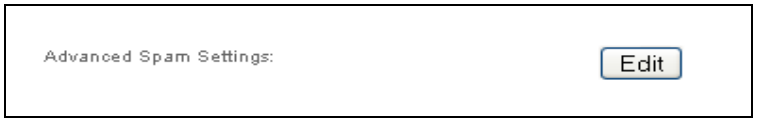
A Greymail Notification consists of an emailed report containing all of the emails you received which were either classified as spam or classified as containing a virus and were sent to your Greymail. You can decide to receive this report on a daily or weekly basis or not to receive it at all by clicking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

The 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. (Windy City may elect to have this function on at all times regardless of the user settings to prevent proliferation of viruses.)

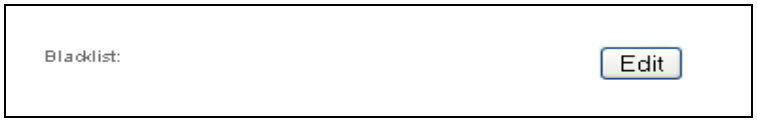
The Virus Notification is an email which is sent to you and the email sender each time an email is flagged as containing a virus. You have the ability to turn this service on or off as shown below.

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 Graymail. (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.



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.



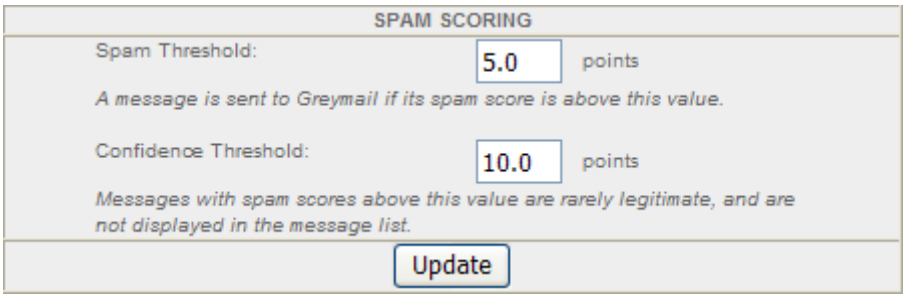
The Whitelist allows you to make sure that you always receive emails from specific senders. To ensure that a certain someone's emails are not sent to Greymail, add them to this list.

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.

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.



Spam Scoring

Every email you receive passes through the Spam filtering system, which analyzes the message, looking for certain traits normally found in Spam. There are hundreds and hundreds of traits the filtering system scans for; all capital letters in the body of the message, an Unsubscribe link, no name in the From: line are just a few. If only one of these traits is found in a message it will be assigned a low Spam score but if a message has many of these traits it will be assigned a higher score. This is how it is decided whether a message should be sent to your Inbox or to Greymail. The Spam Threshold point scale that you can adjust sets the bar for the delivery to your Inbox or Greymail (Spam repository). We recommend most users leave this at 5.0.

When in Greymail, click the View Message Header icon. The line that reads X-X5: Spam: True; 6.4 / 5.0 means that this message scored a 6.4 because of the Spam traits that were found and your Spam Threshold is set to 5.0, so this message was sent to Greymail rather than your Inbox. If you find that legitimate email is being quarantined in Greymail check this X-X5: Spam: True line and tweak your Spam Threshold setting until the messages clear filtering.

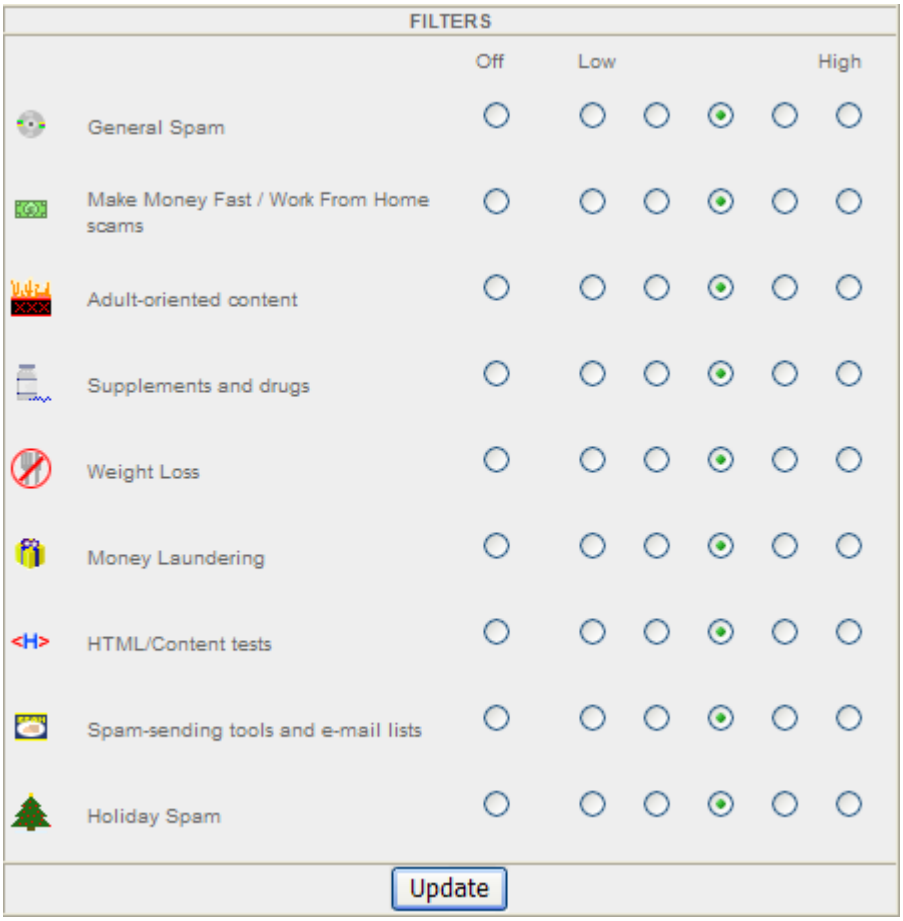
Spam Confidence

The Confidence Threshold lets you decide at what score a message should not appear in the "Normal" confidence tab of the message list. Any message that scores above what you have set in the Confidence Threshold should rarely need review, and will be listed under the "High" confidence tab. All messages, regardless of score, will be shown together under the "Both" confidence tab.

Setting Specific Spam Filters

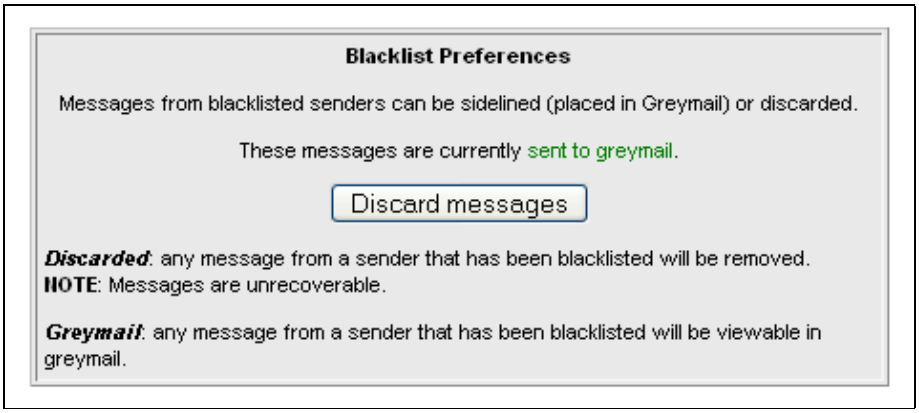
You have the ability to set the individual Spam filters to optimize receiving wanted messages and capturing Spam. Individual filters that recognize specific types of Spam can be set from Low to High or can be turned off by selecting the associated radius buttons. Experiment with the filters

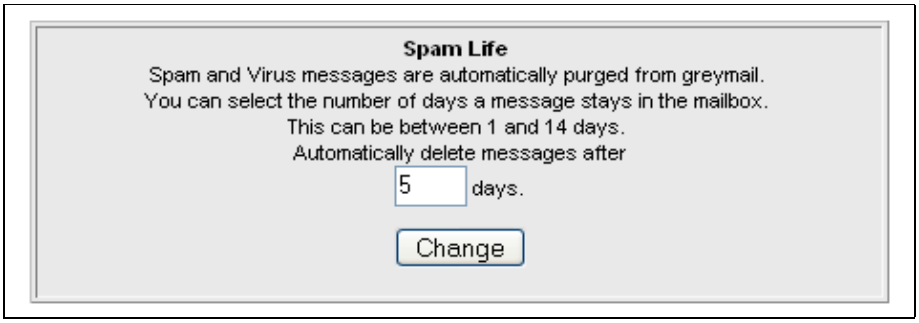
until you are satisfied with your exact filtering specifications. Remember to select **Update** to save your settings.

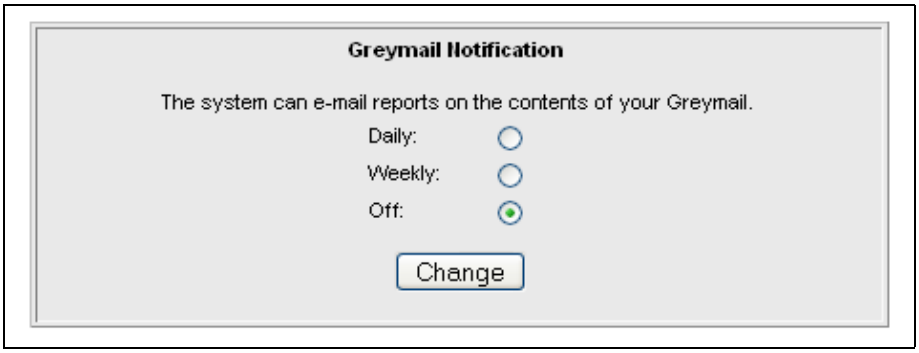


Real Time Blocks are a method of blocking emails from specific countries that originate spam. Once you make changes, you must click **Update** so that your new selections go into effect. It is recommended to leave **RBL** and **Dialup List** checked, as these are lists of addresses known to generate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

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



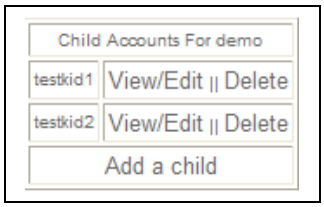
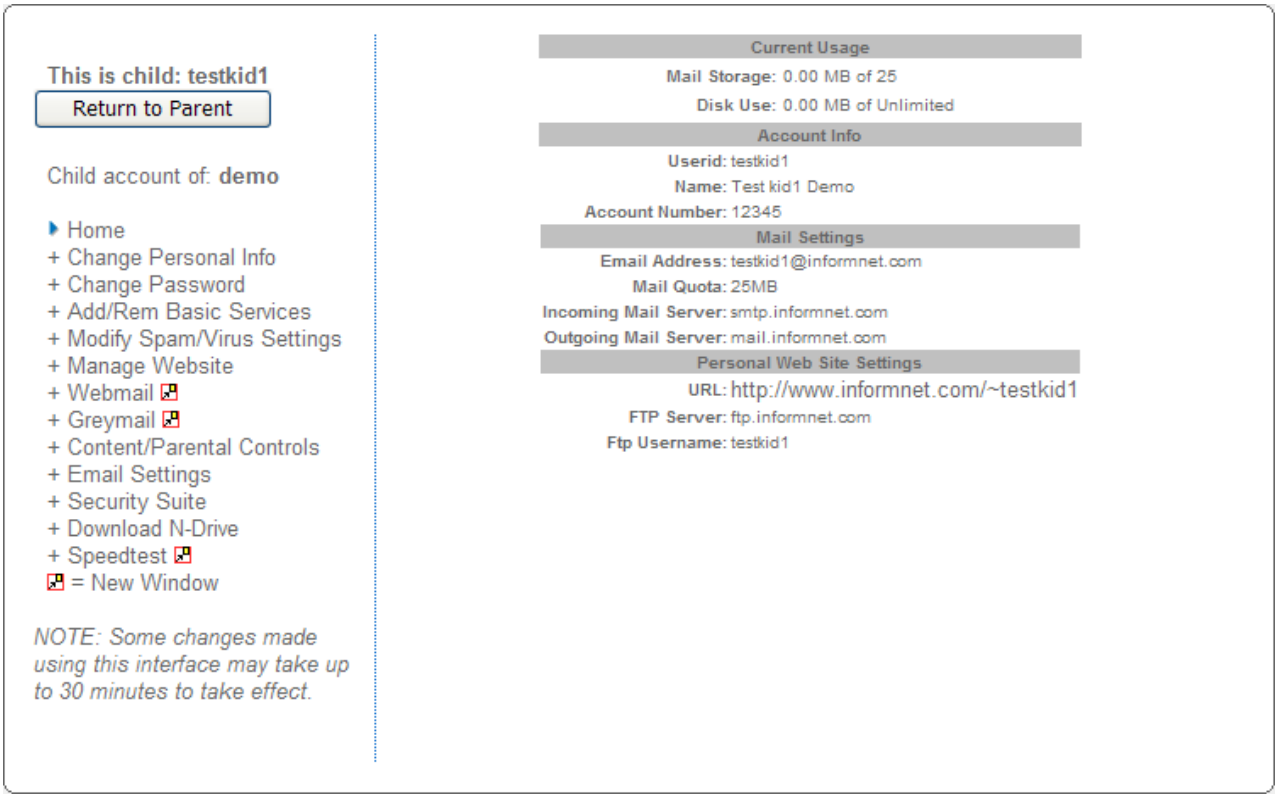




EUCP - Add / Edit child accounts

A child account is an additional email account associated with the main (parent) account. After a parent account is established, child accounts can be opened under that parent account via the EUCP link called **Add / Edit child accounts**. Child accounts typically have features available similar to parent accounts, but this may vary from one product offering (package) to another.

Contact Windy City Customer Service if you have questions or concerns about how to create child accounts and how many you can create at no additional charge. (Exceeding the number of child accounts allowed by your service provider may result in incremental charges.)



Child accounts are identified in the upper left hand corner of their EUCP Home page as a child account and as being associated with their parent account. Select **Return to Parent** tab to return to the parent account's EUCP home page. Child account features may vary or be limited from what is shown below, but typically have many attributes similar to the parent account.