indoglobal.com
web services

User's Guide

indoglobal.com
total internet presence solution

Published 26 July 2004

Table of Contents

Quick Start Guide

Congratulations for choosing **indoglobal**.com as your web hosting provider. This section will guide you through step by step process to quickly set up and use your account with minimum effort. For more in depth instruction please see other sections of this manual.

In this quick start guide, we will use *example.com* as example domain. You will need to substitute that with your real domain name. This quick start guide will assume that the account is already set and Internet name servers (DNS servers) are already configured to point to the correct name servers.

Logging in to SiteManager

SiteManager is your central point of managing your account. You will use **SiteManager** in order to do almost all aspect of managing your account.

1. Open your preferred web browser and go to our web site [http://intl.indoglobal.com]
2. Type in your account username and password in the login box and click *Go*. You account username must begin with u and followed by one or more numbers.
3. If you entered the correct username and password, you should now see the main page of **SiteManager**

Note

Your web browser may emit warnings about SSL certificate as we might not use CA signed SSL certificate. However any transmission from and to SiteManager should be safe and encrypted. Please click *OK* on warning messages to dismiss them.

Tip

You can also use your domain name as your username if you don't want to remember your account number.

Now you have logged in, we will try to use various functions inside SiteManager to configure your account. So don't close your web browser yet!

Creating Web Site Content

Right now your web site will only have a single placeholder

page. Of course, we will want to remove it and install our own web site. We will now try to do that using file manager feature of **SiteManager**.

1. Click on *File manager* on the navigation bar. File manager menu should appear shortly.

2. You should now see one subdomain name *example.com* . On the right of it you will see *browse* among other choices. For now, just click on *browse* to browse the web site directory of *example.com*.

3. Now you should see a directory listing of your web site directory. Right now it will only list one file index.html. This currently contains the boring placeholder page. So we will remove it. Check the checkbox beside the filename, and then click on the *Delete* button below. You need to confirm your action on the next page. After confirming, the file should now be removed. Click on *Browsing example.com* to go back to previous menu.

4. Now we will create a new file, click on *Create New File*. You will now be presented with a form. On filename please enter `index.html`. In the content text area, you can enter HTML code here. Press *Create File* to finalize creating the file.

Note

While the File Manager in **SiteManager** is convenient to quickly edit a few files, there are numerous other ways of publishing your work on your web site. Please see *Publishing and Uploading Files* [21] for more in depth information about publishing your web site.

Congratulations, you are now able to delete and create files.

Creating an Email Account

Now we will try to create an email mailbox in your account.

1. Click on *Email* on the navigation bar. This will bring you the Email menu.

2. Click on *Add new POP/IMAP account*. We will create a new email account that you can use with your favorite POP or IMAP email client as well as web based email.

3. On the next menu you will be presented with a form. On the email account text field, please fill with your name, for example 'john'. On the right of it is a dropdown list of your domain and subdomain. For this time just leave it as it is.

4. Then please fill the password on the Password and Confirm Password text fields. You need to enter it twice to prevent you from inputting the wrong password. Click on *Add New POP/IMAP account* to create the email account.

Congratulations, you have just created your first email account.

Accessing your email account

We will now try to access the previously created email account using web based email feature.

1. By default your webmail account is installed on http://webmail.example.com. Please substitute example.com with your own domain name. Visit that address by using your web browser.

2. You should now be presented with a login screen. Enter your email address and password. Click on *Login* to continue.

3. If you entered the right username and password, you will now be presented with your email inbox. From here the user interface should be self explanatory. You can use the left pane to navigate inside your mailbox. You can use the *Compose* menu to compose a new message, and so on.

Note

You can also use your favorite email client to check your email. Please see the relevant chapters for more information. For more information about configuring common email clients please refer to Appendix C, *Email Clients Configuration* [99].

Closing Remarks

Congratulations, now you are able to do basic things like publishing your web content, creating an email account and checking your mails. However, your account is capable of much more than that. On the other chapters you will learn how to make use all of the features we are offering.

Thank you for choosing **indoglobal**.com as your hosting provider.

Introduction

Your account in a glance

By hosting your account with **indoglobal**.com you will have access to a unprecedented wealth of features combined with ease of use.

SiteManager lets you configure nearly all of your account's features while still retaining ease of use. **SiteManager**'s interface is web based, you can use it anywhere with Internet access and a web browser.

You can create subdomains on your account. They will let you organize your sites in a more professional way.

You will also get complete control to your DNS zone. You can do everything related to DNS such as changing MX records, adding A record and others.

To publish your web site, you can choose from several options: FTP, WebDAV, SSH, rsync as well as web based file manager.

Your account is equipped with sophisticated, subdomain aware email system. You can have several types of email account like POP/IMAP account, email forwarder or autoresponder. You can access your mail by using a standard POP/IMAP email client as well as web or WAP based email.

The server environment is highly tuned for flexibility in developing web sites. You have access to various programming language or tools like PHP, Perl, Python, Ruby, ASP and others.

You account is also equipped with database servers. You can use both MySQL and PostgreSQL. You can also make more than one database.

Those features above are not meant to be exhaustive, you can see more sales pitch on our homepage :). We are sure just by using your account, you will discover a lot of new features.

Pointing Your Domain to Our DNS Servers

Before your account can be accessed from the Internet, you will need to point your domain to our DNS servers. For more information on how to do this, please refer to the welcome message we sent to you. If you need more assistance please contact our technical support.

While it is highly recommended that you point your domain

to our DNS servers, you also have the option to use our account without pointing your domain to our name servers. However you will need to manually maintain DNS records on your name servers so that they contain the same records as our DNS servers. You can see DNS records for your account by logging in to **SiteManager** go to *Subdomain & DNS* and then *Raw DNS Records*.

Caution

It is strongly recommended to point your domain to our DNS servers. Maintaining your own DNS server requires expertise and extra administration tasks in order to synchronize records on your DNS server.

Note

DNS updates on most top level domains or second level domains are typically propagates within three days, depending on the registrar.

Logging in to SiteManager

When first signing up our service, you will given a username and password. You can use that username and password to log on to **SiteManager**. Please follow the instructions below to log on to **SiteManager**.

Note

Your account username should begin with 'u' followed by one or more numbers.

1. Visit our homepage [http://intl.indoglobal.com] with your favorite web browser. Our website will appear very shortly.
2. Use your username and password on the provided login box and then click *Go*
3. If you entered the correct username and password, you should now see the main page of **SiteManager**

Note

Your web browser may emit warnings about SSL certificate as we might not use CA signed SSL certificate. However any transmission from and to SiteManager should be safe and encrypted. Please click *OK* on warning messages to dismiss them.

Tip

You can also use your domain name as your username if you don't want to remember your account number.

Logging in to UNIX Shell Account

The provided username and password combination is also used to log on to your UNIX shell account. Your account is also equipped with access to shell account. Shell account is an environment where you can manage your account using a text based command prompt like interface.

Note

To properly use shell account you need to know how to properly use it. Information on what and how you can do inside shell account is beyond the scope of this user guide. However most of your account features can be used without using shell account.

There are two ways to log on to your shell account: using Telnet or SSH. You will need an appropriate client software like standard telnet or PuTTY [http://www.chiark.greenend.org.uk/~sgtatham/putty/] when using Microsoft® Windows®. Under UNIX®, Linux or similar system you can use standard telnet or OpenSSH [http://www.openssh.com].

Warning

Using telnet when logging in to your shell account is discouraged. It is highly recommended to use SSH for better security.

Logging in using FTP

You can also use the provided username and password to log on using FTP. FTP is a common way of transferring files. Some operating system provide a way to transfer files using FTP, some will require you to use a third party FTP client software, please consult your operating system documentation for more information. More information about FTP is available on the section called “Transferring Files Using FTP” [21]

.

Warning

Using FTP is a security risk as your username and password is transmitted in plain text. Please use other means of transferring files whenever possible.

Monitoring Resource Usage

Your account comes with a limited amount of resource like disk space and data transfer. The amount of resource allocated to your account depends on the level of your account.

Caution

It is very important to keep your account from using all of the allocated disk space at all time. Many programs will cease working properly when there's not enough disk space.

When logging in to **SiteManager**, you will see the amount of allocated disk space and data transfer. You can also see more details about your resource usage on *Resource Usage* menu.

Directory Structure

When creating your account, several files and directories are created within it. This section will let you know the role and functions of those files and directories. Your account is placed on a directory under `/home`, for example `/home/u321`. This directory is referred as 'home directory'.

Under your home directory there are several files and directories. The following explanation list their role and functions.

- `clipboard`. This directory contains files and directories cut or copied to clipboard using the web based file manager. This directory might not appear when you first access your account.
- `domain`. This directory contains all directories and files related to your domain and subdomains. Directly underneath this directory you can see other directories named with your domain and subdomains.
- `etc`. This symbolic link serves no purpose other than maintaining compatibility with older part of **SiteManager**. etc used to be a directory but for technical reason separated from your home directory.
- `lib`. This directory contains various support files used by programming languages and other programs. It is used by programming languages like Perl, PHP and Python to look for user installed libraries and other files. For example, any user installed PHP module goes into `lib/php/modules/`.
- `lists`. This directory holds information about mailing lists you have created.
- `logs`. This directory contains archived log files of your account. For example, web server access log for your domain is stored here.
- `stats`. This directory contains the result of log file analysis performed daily by our system. By default, its contents can be accessed by visiting http://stats.example.com, replace example.com with your domain name.

- `tmp`. This directory is used by various programs to store temporary files.
- `trash`. This directory holds files and directories when deleted from web based filemanager. This directory might not appear when you first access your account.
- `var`. This directory holds work files used by programming languages and other programs. For example, PHP support files are stored under `var/state/php/`.

Caution

Please do not remove any files you don't know about. Blindly deleting files could result in problems. Please only delete files or directories that created by you in the first place.

Subdomain and DNS

Subdomain is an extension of your main domain. For example if your domain is example.com, you could create subdomains singapore.example.com and tokyo.example.com. These subdomains could be accessed just like your main domain.

Our email system is also subdomain aware. You can create email for subdomains hosted on your account. Based on the example above, you could create john@singapore.example.com and john@tokyo.example.com, both are different users.

As you can see, subdomain is a nice way of organizing your your Internet site in a more professional and structured way.

Creating new Subdomains

It is easy to create a new subdomain:

1. Log on to **SiteManager** if you haven't already logged in.
2. Go to *Subdomain & DNS* menu.
3. Go to *Create New Subdomain or DNS Record*, and follow the instruction on the next screen.

Tip

You are not confined into a single level of subdomain. For example, if you have the domain 'example.com', you can create the subdomain 'research.japan.example.com'. You only have to specify 'research.japan' as the name of the subdomain.

Types of Subdomains

There are several types of subdomain you can create.

- *Regular subdomain*. This type of subdomain is hosted on our server. This subdomain can serve web sites and host email mailboxes.
- *Microsoft® FrontPage® subdomain*. Microsoft® FrontPage® subdomain is similar to regular subdomain with an exception you need to use Microsoft® FrontPage® client to develop its web contents.
- *Webplication*. Weblications are canned web applications that you can install to a subdomain. For example, our web mail feature is implemented as a webplication. It is

installed by default on http://webmail.example.com.

- *DNS record*. You can define a custom DNS record using this type of subdomain. You can add A records, NS records and CNAME records.
- *Dynamic DNS*. This is a special type of DNS record. You can use this type of subdomain to assign a static hostname to a dynamic IP address.
- *Other types*. You can make a subdomain that is an alias to another subdomain. You can also make your web server log file analysis result available as a subdomain.

Regular and Microsoft® FrontPage® subdomains

To create regular or Microsoft® FrontPage® subdomain, you need to do the following:

1. Log on to **SiteManager** if you haven't already logged in.
2. Go to *Subdomain & DNS menu*.
3. Go to *Create New Subdomain or DNS Record*, enter the name of subdomain you want to create, select *Blank web subdomain*, and then click *Next*.
4. On the next screen you can choose whether you want to create a regular subdomain or a Microsoft® FrontPage® subdomain. Choose accordingly and press *Next*.
5. On the next screen you will be confirmed of your choice. Press *Finish* to continue.

To publish your web site on a regular subdomain, you need to place your web contents inside `/home/u777/domain/tokyo.example.com/web`, assuming your username is u777 and your subdomain is tokyo.example.com.

To publish your web site on a Microsoft® FrontPage® subdomain, you need to use Microsoft® FrontPage® client. Please refer to the section called “Publishing using Microsoft FrontPage” [26] for more information about Microsoft® FrontPage®.

Webplication

Webplications are a special kind of subdomain that they will be preinstalled with a web application of your choice. An example of webplication is the web based email. Your account's web based email is installed by default when you first receive access to your account. However you can create another webplication if you wish, and there are more webplication other than web based email to choose from.

To create webplication subdomain, you need to do the following:

1. Log on to **SiteManager** if you haven't already logged in.
2. Go to *Subdomain & DNS menu*.
3. Go to *Create New Subdomain or DNS Record*, enter the name of subdomain you want to create, select *webplication*, and then click *Next*.
4. Next you can choose one webplication to install. Please press *Next* to continue.
5. On the next screen you will be confirmed of your choice. Press *Finish* to continue.

Webplication is special that you need to do almost nothing to make it work. After you create a webplication, you can configure it by visiting *Webplication* menu. From there you can click *manage* beside the webplication subdomain name you want to configure. On the Manage Webplication screen you can do the following things:

- Get information about the installed webplication, its program name, where we get it, its license, description and more.
- Convert it to a regular subdomain. If you want to make a modification to a webplication, you should convert it to a regular subdomain, otherwise your changes could be undone when we upgrade the webplication.
- Reinstall the webplication. If you find out that your webplication doesn't work as intended, you can try to reinstall it.
- Recreate the database used. If the webplication utilizes a backend database, you have the option to recreate the database.
- Modify properties of your webplication. Your webplication could have several options that you can change in order to modify its behavior or appearance. You can also revert all the properties items to their default values.

Warning

If you want to modify files in a webplication, please convert it first to a regular subdomain, otherwise your changes could be lost when we upgrade the webplication.

DNS Record

DNS record subdomains are useful if you need to point a subdomain to another IP or hostname. There are several types of DNS records you can create:

- *'A' record*. 'A' record is used to point your subdomain to an IP address. This IP address can be any IP address, not confined to server IP address. For example your broadband connection at home is assigned a static IP by your ISP, then you can use A record to point a subdomain to this IP address. After that you can call it by using the hostname, for instance: home.example.com.
- *'NS' record*. 'NS' record is used to delegate control of your subdomain to a DNS server. For example, your company have a branch office in France, and they elect to manage their own web site. You can make subdomain france.example.com pointing to their DNS server using NS records. Then they will be able to control france.example.com and configure it on their own without consulting with you first.
- *'CNAME' record*. 'CNAME' is an alias to another existing hostname. For instance, you can make foo.example.org an alias to foo.example.com.

Note

Using DNS records, especially NS records will require deep understanding about DNS in general.

To create DNS records, please do the following:

1. Log on to **SiteManager** if you haven't already logged in.
2. Go to *Subdomain & DNS menu*.
3. Go to *Create New Subdomain or DNS Record*, enter the name of subdomain you want to create, select *DNS record*, and then click *Next*.
4. On the next screen you can choose whether you want to create A record, CNAME record or NS record. Choose accordingly and press *Next* to continue.
5. The next screen will differ according to the choice you made on the previous screen. If you choose A record you will be asked an IP address to point the A record to. If you choose CNAME record you will be asked another hostname to make alias to. If you choose NS record you will be asked up to four DNS servers to delegate to. Answer the question and click *Next* to continue.
6. On the next screen you will be confirmed of your choice. Press *Finish* to continue.

Dynamic DNS

Every host on the Internet must have at least one IP address to be able to communicate with others. However there are only a limited number of IP addresses available to use and that's running out very fast. IPv6 is supposed to solve this problem but it is not widespread yet. Therefore, ISPs today treat IP addresses as very precious resource and must be conserved as much as possible. To make use IP address eficiently, they started to assign dynamic IP address to dial-up clients. This means every time a client get connected, he/she will be assigned a different IP address. Usually this won't be a problem for typical client activies, but all server applications suffers. This is like having your telephone number change every day, people will have a very hard time reaching you.

We offer Dynamic DNS feature to overcome this problem. Dynamic DNS will assign a static hostname (such as: myhome.example.com) even if your IP address changes. The only requirement is that you need to have an email client check a specified fake POP3 account periodically. This is required to inform our Dynamic DNS server your current IP address so that it can be updated on the server whenever it changes.

There are a lot applications that could benefit from having a static hostname.

- *File Transfer*. Transfering files over the Internet is not always a simple matter especially if they are very big. Files over 10 MB in size are almost impossible to transfer by email, most mail servers are rejecting emails too big in size. It is not efficient either, files grow larger when attached to an email. Uploading to hosting account might not be possible due to disk space limitation, not to mention it will cost twice the time. With dynamic DNS you can have the files transferred directly between two regular dial-up accounts without requiring static IP addresses. Have one host named using dynamic DNS and the other host download or upload the files by using FTP.
- *Remote Administration*. Give a dynamic DNS name to your home computer and install a remote administration software. If you leave your home computer running and connected to the Internet, then you will be able to control it while you are at work, Internet cafe, or anywhere with Internet access.
- *Virtual Private Network (VPN)*. If your office is still using a dial-up account, it is normally hard to do VPNs since you don't know the IP address in advance. With dynamic DNS you can easily have any employee connect to company network remotely even if the Internet IP address changes.
- *Internet Voice & Video Communication*. With software like Microsoft® Windows® NetMeeting® or any compatible software you can receive audio and video calls. With dynamic DNS you can have your friends call

you by using an address like myself.example.com

- *Webcam and Home Surveillance*. With a webcam and a web server software you can publish live pictures to the Internet. With dynamic DNS you can easily publish the address to your friends. It is also possible to use webcams as home surveillance system so that you can monitor your house, kids, etc while at work.

Note

We only provide the Dynamic DNS service part of the service, the above examples of applications are only a few example that can utilize Dynamic DNS service we are providing. We don't provide those services, corresponding technical support and the required software. Some of the examples above are advanced topics and might require qualified technician.

To create dynamic DNS record, please do the following:

1. Log on to **SiteManager** if you haven't already logged in.
2. Go to *Subdomain & DNS menu*.
3. Go to *Create New Subdomain or DNS Record*, enter the name of subdomain you want to create, select *Dynamic DNS*, and then click *Next*.
4. On the next screen you will be asked the password that can be used for changing this hostname's IP address. Try not to forget the password now and press *Next* to continue.
5. On the next screen you will be confirmed of your choice. Press *Finish* to continue.

Before your dynamic DNS subdomain is usable, you need to have an email client check a special POP3 mailbox in a regular interval. For example, if you created home.example.com as a dynamic DNS subdomain, you need to have an email client check email with the following configuration:

- Hostname: 'setup.home.example.com' without quotes; i.e. add 'setup' in front of your subdomain name.
- Port: 8110; the default port of POP3 is 110, you need to change it to 8110.
- Protocol: POP3
- Username: 'home.example.com' without quotes; the POP3 username is your full subdomain name.
- Password: the same password you set when creating the

dynamic DNS subdomain.

You need to have the email client check the above mailbox every 10 minutes. You will not actually receive any email from the POP3 account. This POP3 checking is only a way to tell our server the current IP address of your computer. When the POP3 server receives your authentication from your email client, it will note your current IP address and update our dynamic DNS server accordingly.

There are also several options you can set on your dynamic DNS subdomain. On of the actions of a dynamic DNS subdomain should be *settings*. From there you can configure whether to use wildcard address or not; the MX record; and whether the MX record is a backup MX record. When wildcard option is enables, you can also have the current IP address accessed using anything.home.example.com, where 'anything' is, well, anything. MX record is used to deliver emails to another email server other than the current IP address. When backup MX is enabled, the specified MX record will act as a backup email server, if your current host is not reachable, it will accept your subdomain's email and deliver it to your dynamic host once it becomes online.

Other Types of Subdomains

There are other types of subdomains, alias to main domain or access to web site statistics.

Alias will only make the subdomain point to the same IP address as your main domain. Alias is useful for names that won't be used for email address or web sites but used for other purposes. When we first created your account, we also configure several aliases such as smtp.example.com, pop.example.com, imap.example.com and others. smtp.example.com for example is used for sending emails. Why use smtp.example.com instead of just example.com? If you tell your email users from now that they should be using smtp.example.com then it will be easier for you in the future if you need to move your mail server to another IP address. If you had told them to use example.com instead, then you need to tell them again to change their email client configuration.

Access to web statistics will make the result of daily web site analysis accessible to a subdomain. By default we configure stats.example.com for this purpose.

To these types of subdomains, please do the following:

1. Log on to **SiteManager** if you haven't already logged in.
2. Go to *Subdomain & DNS menu*.
3. Go to *Create New Subdomain or DNS Record*, enter the name of subdomain you want to create, select *Miscellaneous*, and then click *Next*.

4. On the next screen you will be asked the type of subdomain you want to create, choose accordingly and press *Next*.

5. On the next screen you will be confirmed of your choice. Press *Finish* to continue.

Deleting Subdomains

To delete subdomains, do the following steps:

1. Log on to **SiteManager** if you haven't already logged in.

2. Go to *Subdomain & DNS menu*.

3. There should be an action columns with several options depending on the type of subdomain. Click *delete* link on the corresponding subdomain name you want to delete.

4. On the next screen, you need to confirm that you want to really delete the subdomain.

Warning

Deleting a subdomain will also delete all its web contents and email mailboxes. Please make sure you are absolutely sure that don't have anything important inside the subdomain you want to delete.

Email and Subdomains

Our email system is subdomain aware, you can create email addresses under a subdomain. However how emails are handled on a subdomain depends on the type of subdomain.

- On normal, Microsoft® FrontPage®, alias and webplication subdomains, you have the option to have our email system handle the email; deliver emails to other server(s) using DNS MX records; or refuse all emails.

- On A record subdomains, you have the option to use MX records to deliver email to IP address other than one the A record pointing to. Without MX record(s), emails will be sent to the IP address pointed by A record.

- Email to a dynamic DNS subdomain cannot be hosted on our server, you have the option to specify an MX records to deliver emails to.

The current email policy of each subdomains you have are listed on the Mail Handler column in Subdomain & DNS menu. You can also see that every normal, Microsoft®

FrontPage®, alias and webplication subdomains each should have their own *edit mail handler* menu, and every A records will also have their own *edit MX records* menu. You can use this menu to configure your email configuration for a particular subdomain.

Inside edit mail handler menu there are several options. You can see the current subdomain policy about emails, and modify them by clicking on the *edit* menu. You can also add and remove DNS MX records here.

Note

DNS MX records are always ignored unless the email policy is set to be handled by MX records.

DNS Zone Transfers

DNS zone transfer is a mechanism to replicate DNS data from one DNS server to another. You can add your own DNS server IP address here and set it as a slave (or secondary) server for your zone. Please consult your DNS server documentation for more information.

Zone transfer could be useful if you want to replicate your DNS data on your local DNS server in order to conserve bandwidth, to speed up requests or to make DNS data available when disconnected from the Internet. Or your domain registrar requires you to allow zone transfers from certain IP address.

Caution

To use zone transfer you need to have a DNS server, expertise to configure it, and good understanding on how DNS works.

To prevent privacy leaks, nobody is allowed to do zone transfers by default. To allow zone transfers, you need to explicitly define which IP address(es) are allowed to do zone transfers. Other IP address than ones allowed by you will not be granted zone transfer access. To add an IP address to your allow list, please do the following:

1. Log on to **SiteManager** if you haven't already logged in.
2. Go to *Subdomain & DNS menu*.
3. Go to *IP Addresses Allowed for Zone Transfers*.
4. Go to *Add New IP Address*.
5. On the next screen please specify the IP address you want to allow doing zone transfers with your DNS zone. Press *Add New IP Address* to add it.

Publishing and Uploading Files

To be able to serve your web site, first you will need to publish your web site contents to our server. We provide several ways for you to do that.

Note

These publishing methods have different security implication, please refer to the section called “Use Secure Protocols When Managing Your Account” [?] for more information.

Transferring Files Using FTP

FTP is a very common way to transfer files on the Internet. To upload files using FTP you need to use an FTP client. Some operating system already ship with an FTP client that you can use, so that you don't have to use an FTP client from a third party.

Important

You need to use ASCII mode when uploading CGI script files such as Perl, Python or Ruby scripts. You also need to chmod +x those files. If your FTP client doesn't provide that function, you can fix the uploaded files by using AutoCorrect function of **SiteManager**. the section called “Using AutoCorrect Feature” [37].

Uploading files to main FTP account

To upload files to your account using FTP you need to connect to hostname primary-ip.example.com using your favorite FTP client (assuming your domain name is example.com) and use your account username and password. Your account username must begin with the letter 'u' and followed by one or more digits.

Tip

You can also use your full domain name (i.e. example.com) instead of your account username (i.e. u777) to log on to your account using FTP.

Important

Please note that our FTP server does a chroot to your home directory, that means you will see your home directory as the root directory. The file `/home/u777/domain/example.com` will be seen as

`/domain/example.com` under FTP.

Subdomain FTP accounts

Our FTP server provides a way for subdomains to have their own FTP accounts. This is useful if you want to delegate development work to others without giving them the main account.

To configure subdomain FTP accounts, log on to **SiteManager** and go to *FTP Accounts* menu. From there you can see your subdomains, their physical directory, and whether FTP access is enabled or not. To enable or disable FTP access to a subdomain, click on *enable* or *disable* respectively. To set FTP password, please use the *set password* function.

Note

Subdomain FTP access can only be enabled for regular subdomains.

Important

Note that our FTP server will do a chroot to the subdomain directory. The directory `/home/u777/paris.example.com/web` will be seen as just `/web` on the FTP server.

To upload to a subdomain account, you need to use the full subdomain name as username. The password is the one that you set from *FTP Accounts* menu.

For more information about configuring various FTP client, please see Appendix A, *FTP Clients Configuration* [91].

Using SiteManager's File Manager

Our **SiteManager** provides a convenient way to upload and manage files on your account. You can upload files, edit text files, manage access control, create archives and a lot more! Like every other part of **SiteManager**, file manager is web based, you need to use a web browser to use it.

Managing Files on File Manager

To use file manager, you need to log on to **SiteManager** and then go to *File Manager* menu. Under that menu there are the list of your subdomains and various action menu on the right of them. To manage your files on a subdomain, you *browse* it.

Note

Only regular subdomains can be browsed from file manager.

Inside there is a tabular list of your files and directory under

your subdomain. From the leftmost column: the file or directory name along with its icon and check box; file's UNIX attributes; size; last modified; and various action such as rename or edit. Directory names are also clickable, allowing you to navigate inside them.

On top of the page there are several menu:

- *Upload Files*, this menu will take you to the upload menu where you can upload up to ten files from your local computer. The uploaded files will be stored on the current directory.
- *Create Directory*, this function will, as the name suggests, create a new directory. The new directory will be created under the current directory.
- *Create File*, this will create a new file on the current directory. You will need to provide a filename and the content for the file you want to create. The content could be anything as long as it is text, such as HTML or Perl scripts.
- *Create Counter*, this function lets you to easily create a graphical counter. See the section called “Creating a Graphical Counter” [39] for more information.
- *Access Control*, this will let you restrict access to this part of your web site to a specified class of users. See the section called “Access Control Configuration” [38] for more information.
- *DAV Access Control*, same as *Access Control*, except that it controls access for WebDAV clients. See the section called “Using WebDAV to Manage Files” [25] for more information.

On the bottom of the screen, there are some button. Those buttons will act for the currently selected files and directories. For example *Cut* will cut the currently selected files and directories to the clipboard.

- *Cut*. This will 'cut' the selected files and directories to the clipboard.
- *Copy*. This will copy the selected files and directories to the clipboard.
- *Paste*. This will paste the selected clipboard objects to the current directory. You will need to select files from the clipboard before using *Paste*.
- *Delete*. This will, as the name suggests, delete selected files and directories. Please be careful with this function, as deleted files and directories are not recoverable.
- *Chmod*. This will change the UNIX permission for the

selected files and directories.

- *Archive*. This will create an archive file with extension tar.gz on the current directory from the selected files and directories.
- *Download*. This will create a tar.gz archive file out from selected files and directories, and prompt the user to download it.

On the right hand side there are various actions for each files and directories. The list of actions will be different for different kind of files.

- *Rename*. This will rename the file or directory name.
- *Edit*. This will only available for text files, allowing you to edit them.
- *Visit*. This will open a new browser window, viewing the file just as viewed by visitors.
- *Extract*. This will extract the contents of archive file to the current directory. The currently supported files are: tar.gz, tar.bz2, tar.Z, gz, bz2, Z, and zip.

Tip

You can upload a lot of files easily by zipping them on your computer, upload the zipped file, and then extract it using file manager.

Clipboard Operation

Clipboard is useful for copying and moving files within your account. It is similar to clipboard operations (cut, copy and paste) used by common operating system software. There are three clipboard functions:

- *Cut*. This will 'cut' the selected files and directories to the clipboard.
- *Copy*. This will copy the selected files and directories to the clipboard.
- *Paste*. This will paste the selected clipboard objects to the current directory. You will need to select files from the clipboard before using *Paste*.

To move files to a different directory, first you use 'cut' on files you want to move, 'cut' will move the files from the original location to the clipboard. Then you browse for desired destination directory, and 'paste' those files there.

Similarly, to copy files to another directory, you use 'copy' instead of 'cut'.

Downloading the Whole Subdomain Contents

You can also download the whole contents of your subdomain, i.e. for creating backups. To do that, go to *File Manager* menu and then click on *download* for the subdomain you want to download. The downloaded file will be in tar.gz format. You will need a decompression tool that understands tar.gz format in order to open in on your local computer.

Using WebDAV to Manage Files

WebDAV is a fairly new way of managing files remotely. It is becoming more and more preferred to other methods because it is standardized, and therefore available on almost all newer operating system. And since it is based on HTTP, it can be more secure than most other protocols when using HTTPS. It also means that it is compatible on more firewall configurations than most other protocols.

Note

On several Microsoft® Windows® version, WebDAV is also known as WebFolders or WebDrive.

Important

Our WebDAV server is listening on port 81 for standard HTTP and port 444 for WebDAV over HTTPS.

Configuring Subdomain for WebDAV Access

Before you can access your account using WebDAV, you first need to enable WebDAV access. WebDAV access is enabled per subdomain basis, so you can have one subdomain enabled for WebDAV while others disabled. To enable WebDAV please follow these instructions:

1. Login to **SiteManager** if you haven't already logged in.
2. Go to *DAV/WebFolders*.
3. Click *enable* to the right of the subdomain name you want to enable DAV access.
4. Confirm your action on the next screen.

Important

You need to wait for at most one hour before any changes in WebDAV configuration is propagated on the server configuration.

Configuring DAV Access Control

After enabling DAV, you need to assign access control from

file manager. You need to tell our system who will be granted read access, who will be granted read-write access, etc.

1. Assuming you are already logged on to **SiteManager**, go to *File Manager* menu.
2. *Browse* for directory that you had enabled its DAV access
3. On the browse screen, you will notice that there will be a *DAV Access Control* menu. This menu will take you to DAV access control screen where you can configure who will be granted DAV access. For more information on how to configure access control, please refer to the section called “Access Control Configuration” [38].

Tip

DAV access control is defined on per subdirectory basis. You can have different access restriction on different directory. An access control defined on a deeper directory will override access control defined on the parent directory.

For more information about WebDAV clients, please refer to Appendix B, *WebDAV Clients Configuration* [95] where you can find instructions on how to configure various WebDAV clients.

Tip

You can use WebDAV as a virtual hard drive residing on the Internet. You use access control accordingly to give access to your users. Then your users will be able to share files with each other. Sharing files this way is a lot more efficient than using email attachment.

Publishing using Microsoft® FrontPage®

Microsoft® FrontPage® is a special software for publishing web sites. To use all its features fully, you need to use it with Microsoft® FrontPage® subdomain. For more information on how to create a Microsoft® FrontPage® subdomain please see the section called “Regular and Microsoft FrontPage subdomains” [12].

Caution

Microsoft® FrontPage® is only suitable for small sites. Medium to heavy sites (more than approximately 100 pages) will consume too much server resources. Please consider splitting your site to multiple subdomains or do not use Microsoft® FrontPage® to build your site.

To publish using Microsoft® FrontPage® client, you will need a username and password pair. This username and password is not the same as your account password or FTP password. To change password used by Microsoft® FrontPage® subdomain do the following steps.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *FrontPage* menu to list all your Microsoft® FrontPage® subdomains.
3. Click *password* to change password for the respective Microsoft® FrontPage® subdomain. On the next screen you will be asked to input the password.

To publish using Microsoft® FrontPage® use the username 'administrator' with the password you already set on the steps above.

Warning

Under any circumstances do not attempt to upload or modify web files residing on a Microsoft® FrontPage® subdomain without using Microsoft® FrontPage® client. Doing so could result in a catastrophic loss of data!

If you found problems with your Microsoft® FrontPage® subdomain, you can try to reinstall the Microsoft® FrontPage® extension. To do that perform the same steps above, but click on *reinstall* instead of *password*.

Transferring Files Using scp, sftp and rsync

scp, sftp and rsync are transfer protocol implemented above SSH and therefore should be very secure. You will need to use your account username and password to transfer files using scp, sftp or rsync.

rsync has an advantage that it will only send the differences over the wire. For example, suppose that you have a file `index.html` on both your computer and your account. If you upload `index.html` from your computer to your account using other method, then the whole `index.html` will be transferred, replacing the current `index.html` that is on your account. On the other hand, when you use rsync, only the differences will be transferred, not the whole file, saving you bandwidth and time. The downside of rsync is that it currently lacks graphical client programs and it is not straightforward to install and use rsync on Microsoft® Windows® operating system.

Web Site Development

We provide our customers with tools and utilities for developing web applications.

Naming Filenames and Directory Locations

Each of your regular subdomains has their own web directory. You need to put all of your web contents there. For example, if your subdomain is named madrid.example.com and your username is u777, then its web directory is `/home/u777/domain/madrid.example.com/web`. If a file `test.html` is uploaded to this directory, then it can be visited by a web browser using `http://madrid.example.com/test.html`.

Important

In our server filenames are case sensitive. For example `index.html` is different than `INDEX.HTML` and `Index.HTML`. This is different than for example Microsoft® Windows® environment. Please make sure that you uploaded your files in with the intended case especially when using Microsoft® Windows®.

Our web server will determine the file type from the file extension. The following lists commonly used file extensions for typical web files.

- HTML files: `.html` or `.htm`
- Javascript files: `.js`
- CSS files: `.css`
- JPEG images: `.jpeg`, `.jpg`, or `.jpe`
- PNG images: `.png`
- GIF images: `.gif`
- WML files: `.wml`
- WML scripts: `.wmls`
- WBMP images: `.wbmp`
- Shockwave Flash files: `.swf`

Important

Please make sure the file extension is in lowercase.

Server Side Includes (SSI)

From Apache manual: SSI (Server Side Includes) are directives that are placed in HTML pages, and evaluated on the server while the pages are being served. They let you add dynamically generated content to an existing HTML page, without having to serve the entire page via a CGI program, or other dynamic technology.

SSI is useful when you have a piece of HTML code that is massively duplicated in all your HTML files, like navigation headers. To simplify development, you can move that piece of common HTML code to a separate file, then use SSI on other HTML files to include it.

To use SSI, the only requirement is that you need to name your HTML files with the extension `.shtml`.

Note

SSI is only useful for simple includes, for creating more complex web sites, you need to use full programming languages like PHP or Perl.

For more information about SSI usage, please see the Apache web server SSI documentation [http://httpd.apache.org/docs/howto/ssi.html].

Using PHP Scripts

PHP is the fastest growing language for web development. PHP is a language that is embedded on HTML code, simplifying web development. PHP is suitable for any sites that requires dynamically generated contents.

To use PHP, you need to named your PHP files with `.php`, `.php3`, `.php4` or `.phtml`. You can also define additional extensions to be parsed by PHP if you wish to do so.

Important

Traditionally, our system require every PHP files to be set with their executable bit on (chmod +x). However, as of June 2004, this is no longer the case. It is no longer required to do an AutoCorrect after uploading your PHP files.

Note

Our PHP system is CGI based, not the more common Apache module based. This has the advantage that we don't have to restrict you using safe_mode while still retaining security. That means you don't have to worry about PHP disabling some function calls.

Configuring PHP

Our customers can configure their PHP settings themselves. You don't have to rely on our administrators to install PHP modules or changing configuration parameters. You can even install your own PHP modules by yourself.

To configure PHP, you need to do it from **SiteManager**. Go to *Language Settings* and then *PHP Setttings*. From there you will see the list of regular domains you have. Every regular subdomains can use the main global PHP settings or have their own PHP configuration. The configuration to use is shown in PHP Settings column. 'Use global configuration file' means the subdomain is using the main account's PHP configuration file. 'Use local configuration file' means the subdomain is using its own PHP configuration file. You can change that by using the action menu *use local settings* or *revert to global* respectively.

To edit PHP configuration for subdomains that set to use local settings, you need to use *view settings* action menu. To edit the main global PHP configuration you need to use *View global settings* menu on the bottom of the page.

Inside Configuration Menu

Inside the configuration menu you change the way PHP works. To add modules, use the *Edit Loaded Extensions* menu. From there you can add or remove modules that will be used by the particular configuration. For example, you can enable gd and mysql module if you are going to use image functions and MySQL database.

Caution

Loading more extensions will require more resources on your account and might cause problems with PHP scripts. Please consider splitting multiple PHP functions into multiple subdomains if you need a lot of modules.

You can also change various PHP configuration parameters from this menu. For example, you can change register_globals and magic_quotes_gpc settings here. For more information about PHP configuration parameters, please refer to the official PHP documentation [http://www.php.net/docs.php].

Caution

Do not blindly change PHP settings without knowing their functions. Incorrectly altering PHP configuration might result in problems running PHP scripts.

Note

Since we don't use Apache module version of PHP, please do not attempt to alter configuration parameters using .htaccess file. It will result in

web server errors.

Installing Your Own PHP Module

You have the option to install your own PHP module if the needed module is not already installed on our server. For example if you obtain a commercial module from a third party.

To install a PHP module, go to *Custom PHP extensions* under PHP Settings menu. It will open a new page listing the currently installed custom PHP modules. You can upload a new PHP module by using *Upload new extension* menu here.

Caution

Please make sure that the module you are trying to install is compatible for the version of PHP on our server. Our system will tell you the current version of PHP when you are trying to upload the extension. You will also need to upgrade the PHP extension you uploaded whenever we upgrade PHP on our servers.

After the module get installed, you can enable it just like any other modules using *Edit Loaded Extensions* menu.

Installing PEAR Modules

PEAR is is a framework and distribution system for reusable PHP components. Your application might need to use some PEAR modules, before you can run your application, you will need to install the appropriate PEAR modules.

To manage PEAR modules, you need to go to *Manage PEAR Packages* menu from the main *PHP Settings* page. In that page, there will be a list of PEAR packages, globally installed or locally installed.

You can install PEAR packages by using *Install new PEAR module* on the bottom of the screen. From there you can choose which package to install. The list of packages should be current as listed on PEAR web site [http://pear.php.net].

Manually Editing PHP Configuration File

If you don't want to use **SiteManager** to configure PHP or if the setting you want to change is not editable yet on **SiteManager**, you can manually edit the `php.ini` files by yourself.

Assuming your account username is u777, the global PHP configuration is located on `/home/u777/var/lib/php/php.ini`. And the local configuration for subdomain bangalore.example.com is `/home/u777/domain/bangalore.example.com/php.ini`.

Warning

Using **SiteManager** to configure your PHP settings after manually editing it could result in loss of your manual changes.

Adding Another Extension To Be Used By PHP

By default, our system will treat filenames ending with .php, php3. php4 or .phtml as PHP files. However, sometimes it is necessary to add additional files to be treated as PHP files. For example, if you want files ending with .html to be parsed as PHP files.

To add additional extensions to be parsed as PHP, please do the following:

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *File Manager* and then choose *Properties* for a subdomain you want to add additional extension to. Or you can also choose *Default Subdomain Properties* if you want your additions to be recognized by all of your subdomains.
3. Go to section *MIME Types, Apache Handlers, Charsets, Encoding, Language* and then choose *Map an extension to an Apache handler (AddHandler).*.
4. On *Apache Handler* field, choose *x-httpd-php*. On *File extension* field, specify an extension (e.g. html). Click *Add Extension* to continue.
5. Repeat previous two steps if you need to add additional extensions to be recognized as PHP files.

Differences From Apache Module Version of PHP

There are several differences between Apache modules version of PHP and our unique PHP system. Most of the time you will not notice them, however there are a few differences that might affect your PHP scripts development:

- Our PHP system run as CGI mode. This means PHP scripts run more or less the same way as CGI scripts like Perl, Python or Ruby scripts.
- Apache specific functions are not available, these include but not limited to: apache_child_terminate, apache_get_modules, apache_get_version, apache_getenv, apache_lookup_uri, apache_note, apache_request_headers, apache_response_headers, apache_setenv, ascii2ebcdic, ebcdic2ascii, getallheaders, virtual. Please see http://www.php.net/manual/en/ref.apache.php for more information about these Apache specific functions. While these functions are unavailable, there should be

other ways to accomplish the same task. You will need to use other calls and functions that are not Apache specific.

- PHP running inside Apache will honor php_flag and php_value directives inside .htaccess file. Since our system is not running Apache module version of PHP, these directives will cause error. In order to modify PHP settings on our system, please refer to the section called "Configuring PHP" [30].

- HTTP Authentication works a little differently. The PHP Manual at http://www.php.net/manual/en/features.http-auth.php states that HTTP authentication will not work with CGI version of PHP, however it does work on our system with a little modification. The following is an example of HTTP authentication on our system:

```
<?php
if (!isset($_SERVER['PHP_AUTH_USER'])) {
   header('WWW-Authenticate: Basic realm="My Realm"');
   header('Status: 401 Unauthorized');
   header('HTTP-Status: 401 Unauthorized');
   echo 'Text to send if user hits Cancel button';
   exit;
} else {
   echo "<p>Hello {$_SERVER['PHP_AUTH_USER']}.</p>";
   echo "<p>You entered {$_SERVER['PHP_AUTH_PW']}
      as your password.</p>";
}
?>
```

Note that the only difference than the example from PHP manual is how we send status headers.

- On some PHP providers, you are not allowed to configure PHP yourselves. Any reconfiguration or module additions will require pestering their system administrator. On our system, it is not necessary to get in touch with our system administrator to change PHP configuration (however we will be gladfully help you if you ask us). Please see the previous sections on how to configure PHP on our system.

Using CGI Scripts in General

CGI scripts are basically regular scripts that called by web browser. You can create CGI scripts by using Perl, Python, Ruby or even shell scripts and C/C++.

To use CGI scripts you need to name your scripts with any of these extensions: `.cgi`, `.pl`, `.py`. You will also need to chmod +x or chmod 0755 your CGI scripts. AutoCorrect can do that automatically to all of your CGI scripts, please see the section called "Using AutoCorrect Feature" [37] for more information.

When developing CGI scripts, you might need information about the exact location of interpreters or utilities such as Perl interpreter or UNIX sendmail. These information can be

obtained from *Language Settings* menu.

Caution

CGI scripts must be in UNIX text format. If you create the scripts within Microsoft® Windows® environment you will need to use ASCII mode when uploading using FTP, or fix the uploaded file afterwards by using AutoCorrect. Please see the section called “Using AutoCorrect Feature” [37] for more information about AutoCorrect.

Installing Perl CPAN Modules

CPAN is a repository of Perl modules. Perl is shipped with command line tools to automatically install Perl modules. **indoglobal**.com goes a step further by offering an interface for customers to install CPAN modules from **SiteManager**.

To install CPAN modules, go to *Perl Settings* under *Language Settings* from **SiteManager**. There you will see the currently installed Perl modules under your account.

Click *Perl Module Installation* start installing Perl module. On the next screen you will see detailed instruction on how to install Perl module. First, you should try automatic install first. If it fails then you can try the other methods in order. Automatic installation sometimes won't work if the module in question requires user interaction when installing.

To perform the other methods of installation, you need to log on to your shell account. Please refer to the section called “Logging in to UNIX Shell Account” [7] for more information.

Using Active Server Pages (ASP)

Active Server Pages (ASP) is a web development environment commonly used in legacy Microsoft® Windows® based server environment. While **indoglobal**.com uses Linux servers exclusively, we also offer Sun ONE Active Server Pages for our customers who need to run their legacy ASP based scripts on our servers.

Note

If you starting a new development and not starting from existing legacy ASP based code, consider using programming language other than ASP. While our servers supports ASP, it is not the native environment for running legacy ASP based scripts, especially when the ASP code in question is developed under Microsoft® Windows® environment. Other languages like PHP or Perl are better supported on our servers.

In order to use ASP, as usual you need to name your files

with extension `.asp`. Make sure the extension is in lower case, especially when you are uploading from a Microsoft® Windows® environment. Please also note that filenames on our servers are case sensitive. This is different from Microsoft® Windows® environment where filenames are case insensitive.

For more information about developing ASP applications using Sun ONE Active Server Pages, please see the official documentation [http://aspdoc.indoglobal.com].

Tip

If you find ASP is too limiting for developing your application, you can try converting your ASP scripts to PHP scripts. Please refer to the section called “Converting ASP Scripts to PHP” [48] for more information.

Difference From Microsoft® Windows® Version

ASP's native environment is Microsoft® Windows® and therefore most ASP scripts also developed under Microsoft® Windows®. Since **indoglobal**.com uses Linux based servers exclusively, care must be taken when developing ASP based application. The following listed several differences between original Microsoft® Windows® version of ASP and Sun ONE ASP installed on our servers.

- *Case sensitivity*. Filenames are case insensitive in Microsoft® Windows® environment, while under Linux they are case sensitive. It is advisable that you use lowercase to name files and also when referencing a filename inside your ASP code.

- *Database support*. Most ASP application developed under Microsoft® Windows® system uses Microsoft® SQL Server™ or Microsoft® Access® for its database backend. However, under our servers there are no option to use either product, you will need to use MySQL or PostgreSQL as your application's database backend. If you already have database under Microsoft® SQL Server™ or Microsoft® Access® you will need to migrate your data to one of our supported database products. There are several utilities for converting your data to MySQL at http://www.mysql.com/doc/en/Contrib_converters.html. For PostgreSQL, there are also several useful conversion utilites at http://techdocs.postgresql.org/.

- *Connecting to database*. ASP applications developed under Microsoft® Windows® typically use ODBC system DSN to make connection to database. However, for security reason we don't use system DSNs. Instead you will need to use DSN-less connection string. For more information about connecting to databases, please refer to the section called “Using MySQL Database in Your Application” [58] or the section called “Using PostgreSQL

Database in Your Application" [61].

ASP Components

Other than the standard ASP components, there are also other popular ASP components:

- SMTP sending component. We use the CDONTS.NewMail similar to NewMail component included with Microsoft IIS. However it does not include these properties and methods: AttachURL, ContentBase, ContentLocation, MailFormat, SetLocaleIDs, Version.
- POP component. This component is used to retrieve email messages from a POP3 server.
- File upload component. This component enables users to save files uploaded by site visitors to the server.

For more information on how to use these components, please refer to ASP Online Help at http://aspdoc.indoglobal.com.

Using AutoCorrect Feature

AutoCorrect is a feature of **SiteManager** that will attempt to automatically fix common errors. At the moment, it will attempt to do the following.

- Fix the attributes of home directory. Improper permission of your home directory could result in security hole or problem serving your web files.
- Fix the attributes of web files. AutoCorrect will automatically fix attributes of web files such as HTML, or CGI.
- Convert legacy Microsoft® Windows® text files to standard UNIX text format. Text files include most CGI scripts, HTML and PHP files. Using Microsoft® Windows® format will result in problems serving most CGI scripts.
- Lowercase the extension of web files. File extensions such as `.html`, `.cgi` or `.php` must be in lowercase, AutoCorrect will try to automatically fix those.
- Create support files, directories and symlinks if they are not already exist. Some directories and files under your home directory is required for some applications. Deleting these could result in problems. For example, PHP session support needs to store session files under `var/state/php` under your home directory, if this directory is missing, PHP session will not work correctly.

Note

Please try AutoCorrect first if you encountered errors on your web site.

To use AutoCorrect, please do the following:

1. Log on to **SiteManager** if you haven't already done so.
2. Click on *AutoCorrect* on the navigation bar.
3. On the next screen you will be prompted by a confirmation screen. Click *Yes* and then click *AutoCorrect*.

Access Control Configuration

indoglobal.com provides an easy way to restrict access to part of your web site. You can manage your web users and groups information. You can also modify access control information for part of your web site. All can be done conveniently without leaving **SiteManager**.

Managing Your Web Users and Groups

Our **SiteManager** has a database for storing username and password information. You can use this database for authenticating access to part of your web site. You can manage this database by using *Web User & Group* from inside **SiteManager**

There are several operation that can be done from this menu.

- *Creating new user*. Click on *Create new user* menu and fill the information of the new user on the next screen. The most important part is User ID and password, they are used by your users to authenticate themselves. You can also fill the group membership if you want this user to be a member of a group. A user can be a member of more than one group.
- *Creating new group*. Click on *Create new group* and fill the group information on the next screen. The important field here is Group ID.
- *Deleting a user or group*. You can delete a user or group by using *delete* link on the right side of user or group ID you want to delete.
- *Editing a user or group*. You can edit a user or group by using *edit* link on the right side of user or group ID you want to edit. Please note that you will not be able to change the user or group ID.

Restricting Access to Part of Your Web Site

There are several place where the above user & group database can be useful inside **SiteManager**.

- *Restricting access to part of your web site.*. You can restrict access to part of your web site by using *Access*

Control menu under file manager. Please see the section called “Using SiteManager's File Manager” [22] for more information.

- *Restricting access for WebDAV users*. You can restrict access for your WebDAV users by using *DAV Access Control* menu under filemanager. Please see the section called “Using WebDAV to Manage Files” [25] for more information about WebDAV.
- *Restricting access to your log files analysis result*. You can do that by using *Site analysis access control* under Log Files & Analysis menu. Please see the section called “Access Control Configuration” [38] for information.

Under each of those menus, you can configure who has access to a particular resource. On the configuration page you will see several fields.

- *Authentication String*. This is the string sent to web browser as an identifier. You can leave this to default if you wish.
- *User Allowed to Access*. Specify which class of users you want to allow access to this resource. You can allow any visitors, allow any authenticated user, allow users belong to specific group(s), or only allow specific user(s). To allow specific users or groups, you also need to specify in the selection box which users or groups will be allowed.
- *Host Allowed to Access*. You can specify which host to allow or deny access here. You can allow all hosts except the listed hosts, or you can deny all hosts except the listed hosts.
- *Access Allowance*. This field configures how user and host based authentication above interacts. You can choose if access granted whenever both user authentication and host authentication are successful. You can also choose to grant access if any of user authentication and host authentication is successful. Leave it to default if you don't understand.

Creating a Graphical Counter

You can easily create a graphical counter using file manager.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *File Manager* menu and then click *browse* on the subdomain in which you want to create the counter. You also might want to browse for directory where you want to put the counter into.

3. Click on *Create Counter* when browsing your subdomain contents.

4. On the next screen you need to specify the name of the counter file. The counter will be created under the current directory. You also need to specify the digit style and starting value of the counter. You can choose from our extensive collection of digits consisting more than 500 digit styles!

5. Click on *Create Counter* to create the counter

On the confirmation screen you can see the code you need to paste to your HTML files. For example if you created a counter named 'mainpage.count' then you will need to use the HTML fragment similar to this to call the counter:

```
<img src="mainpage.count" />
```

Log Files and Analysis

Every hit to your web site will be logged to a log file on our server. That log file will then be rotated, archived to your account, and analyzed once every 24 hours.

Active Log Files

Before getting rotated, every log files are not owned by your account. If your account username is u777, your active log files are stored under directory `/home/userdata/u777/logs/`. Every log files under this directory are still active, data is still being written into it. Inside this directory, there are several log files:

- `active_http_access_log`, logs access to HTTP web server.
- `active_https_access_log`, logs access to HTTPS web server.
- `active_httpdav_access_log`, logs access to WebDAV over HTTP server.
- `active_httpsdav_access_log`, logs access to WebDAV over HTTPS server.
- `active_http_error_log`, logs errors for HTTP web server.
- `active_https_error_log`, logs errors for HTTPS web server.
- `active_httpdav_error_log`, logs errors for WebDAV over HTTP server.
- `active_httpsdav_error_log`, logs errors for WebDAV over HTTPS server.
- `active_pop3_log`, logs access to POP3 server.
- `active_smtpauth_log`, logs email deliveries done using our

SMTP server.

- `active_smtp_in_log`, logs incoming email deliveries to your account.
- `active_smtp_out_log`, logs outgoing email deliveries from your account.

Note

Every active log files are not owned by your account. And therefore they won't use your account's disk space allocation.

Archived Log Files

Active log files are archived every 24 hours. Every 24 hours, all the active log files above are compressed and moved to your home directory. If your account's username is u777 then your log archive directory is `/home/u777/logs`.

Important

We don't guarantee the log rotation will always run everyday. If you find one or several days are missing, you will find the data for the particular day(s) in the next archived log file.

Unlike the active logs, the archived log files do take up your account's disk space. You can set the maximum size of archived log files you want to keep in your account. If the amount of archived log files exceeds the specified maximum size, our system will start deleting old log files until they are below the specified maximum size. This maximum size defaults to 5000 KB. To change the maximum archived log files please do the following.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Log Files & Analysis* menu.
3. Inside you will see the current maximum size of archived log files to keep. To change it, go to *Change log files configuration* menu.
4. On the form, change the value of field 'Size of old log files to keep' and click *Update*.

You can also download the archived log files. You can download them using standard means such as FTP, scp or sftp.

Log Files Analysis

Your log files will also get analyzed by our system while rotated. The result of analysis will be stored under `stats`

directory under your home directory. For example if your username is u777 then they are stored under `/home/u777/stats`. By default you can access them from a web browser by visiting http://stats.example.com, assuming your domain name is example.com.

Our system uses third party analysis engines when analyzing. Currently we use Webalizer [http://www.webalizer.org] and AWStats [http://awstats.sf.net]. By default only Webalizer engine is used. You can change which engine to use from *Log Files & Analysis* menu.

Access from web site to the analysis results (i.e. http://stats.example.com) by default is restricted only to group administrator. By default nobody is member of this group, you still need to define user that will be allowed to access them from *Web Users & Groups*.

Tip

You can change the time zone used in your log files and analysis results by changing the time zone setting at the *Preferences* menu.

To change which user or group that will be granted access to your analysis results, you can use *Site analysis access control* menu under *Log Files & Analysis* menu. For more information about access control in general please refer to the section called “Access Control Configuration” [38].

Running Scheduled Tasks

Task scheduler is used if you want to run a task periodically. To add a new task to be scheduled, please do the following steps.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Task Scheduler* menu where you can see the list of your scheduled tasks.
3. Click on *Add New Scheduled Task* to add a task.
4. On the next screen you will see three fields. 'Task Name' is the name of the task, you can put anything to describe the task you want to create, it will be shown on your list of scheduled task. The second field 'Command to Run' is the most important, please specify the complete command line of task you want to execute. The third field 'Comments' is simply a comment box, you can specify any information here. Click on *Add New Task* to proceed.
5. Go back to the main *Task Scheduler* menu. You will see the task in question, but it is not scheduled to run yet. To create a schedule for this task, click *edit* on the right of the task in question.
6. Click *Add New Schedule* to create a schedule for this

task.

7. Follow the instruction on the next screen. You can add yearly, monthly, weekly, daily or hourly schedule. You can also set this task to run everytime our server boots.

Tip

You can add more than one schedule to a single task.

On the edit task menu, you can also edit the task information if you need to change something. For example if you want to change the command line to perform.

Tip

To schedule a PHP script, you can use wget as the command line. For example, you want http://example.com/daily.php to be scheduled, you can use a command line like 'wget http://example.com/daily.php -O- -o /dev/null'.

Creating HTML to Email Forms

Sending email to the owner of the site is fairly common. **indoglobal**.com provides an easy way to do this. You don't have to install your own HTML form to email CGI scripts. Of course you may still install your own CGI scripts if you wish.

Our preinstalled form to email handler resides on `/global/nms-fmail.cgi`. To make use of it, you need to write an HTML form that refers to that script. Here's an example HTML snippet code which will send mail to address feedback@example.com when someone submits the form.

```
<form method="POST" action="/global/nms-fmail.cgi">
  <input type="hidden" name="recipient"
    value="feedback@example.com" />
  <p>
    Please enter your comments<br />
    <input type="text" name="feedback" />
  </p>
  <p>
    <input type="submit" />
  </p>
</form>
```

Form Configuration

The hidden 'recipient' input field in the example above told the HTML form to email script who to send the email to. This is how the script configuration works. Here is the full list of field names that you can set using hidden form inputs.

- *recipient*: the email address to which the form submission should be sent. If you would like it copied to more than one recipient then you can separate multiple email addresses with commas. Please note that you are

not allowed to send emails to outside of your domain, for example you cannot set recipient field to email addresses not ending with example.com, assuming your domain account is example.com.

- *subject*: the subject line for the email.
- *redirect*: if this value is present, it should be a URL and the user will be redirected there after successful form submission. If you don't specify a redirect URL, then instead of redirecting, it will generate a success page telling the user that their submission was successful.
- *bgcolor*: the background color of the success page.
- *background*: the URL of the background image for the success page.
- *text_color*: the text color for the success page.
- *link_color*: the link color for the success page.
- *vlink_color*: the vlink color for the success page.
- *alink_color*: the alink color for the success page.
- *title*: the title for the success page.
- *return_link_url*: the target URL for a link at the end of the success page. This is normally used to provide a link from the success page back to your main page.
- *return_link_title*: the label for the return link.
- *sort*: This sets the order in which the submitted form inputs will appear in the email and on the success page. It can be the string 'alphabetic' for alphabetic order, or the string 'order:' followed by comma separated list of the input names. For example the sort field of 'order:name,email,age,comments' will have the fields ordered as such.
- *required*: this is the list of fields that the user must fill in before they submit the form. If they leave any of these fields blank then they will be sent back to the form to try again.
- *missing_fields_redirect*: if this is is set, it must be a URL, and the user will be redirected there if any of the fields listed in 'required' are left blank. Use this if you want finer control over the error that the user sees if they miss out a field.
- *env_report*: This is a list of the CGI environment variables that should be included in the email. This is useful for recording things like the IP address of the user in the email. For example you could specify env_report value of 'HTTP_USER_AGENT,REMOTE_ADDR,REMOTE_HOST' if you want the form to report back to you the web browser, IP address, and hostname of the submitter.

- *print_blank_fields*: if this is set then fields that the user left blank will be included in the email. Normally, blank fields are supressed to save space.

As well as the above hidden inputs, there are a couple of non hidden inputs which get special treatment.

- *email*: this will be used as the address part of the sender's email address in the email.
- *realname*: this will be used as the name part of the sender email address in the email.

Using SSL/TLS

SSL (Secure Sockets Layer) or TLS (Transport Layer Security) is used to secure traffic between two hosts on the Internet. For example it can be used for securing traffic from and to an e-commerce site.

By default SSL/TLS is enabled on your account but using a self signed certificate. That means users will be asked to trust the certificate before using the service. A self signed certificate is like a fully signed certificate, traffic will be fully encrypted. The only difference is it is not trusted by web browsers, users will need to trust the certificate before using the service.

Getting and Installing a Fully Signed Certificate

You also have the option to use a fully signed certificate with the following condition.

- A fully signed certificate signed for your domain will require a dedicated IP address. By default your account will not have a dedicated IP address. Please refer to our homepage or contact our sales department to get a dedicated IP address.
- You will need to get your certificate signed by a certificate authority by yourself. They will probably ask you to give them some information about your domain and an administrative fee.

Important

Please note that any dedicated IP address request must be justified. We will only grant a dedicated IP address to accounts that absolutely require fully signed SSL/TLS certificate such as e-commerce sites or similar sites.

To install a fully signed certificate to your account please follow the following steps.

1. Log on to **SiteManager** if you haven't already logged

on.

2. Go to *SSL/SSH/OpenPGP* menu and then *SSL/TLS Settings* menu.

3. In this page you will see the current information about your current SSL/TLS certificate. If you haven't installed an SSL/TLS certificate it should tell you that SSL/TLS certificate is not installed. Click on 'Install or Renew SSL/TLS Certificate'.

4. In this page there are a step by step instructions you need to take. The first step is to generate or import web server private key. Choose accordingly from the action field and follow the instructions. Only choose import if you already have a private key with another server.

5. Next, create a certificate signing request (CSR). Click on *Create* on the action field. On the next screen you will be asked information about your organization. A special field is Common Name, you will need to enter your domain name to be used in the certificate here, you can also enter your subdomain name here. Please note that only one domain or subdomain may be specified here, you can't specify all of your subdomains. Please double check the name of your domain before continuing. When done, click on *Create CSR*

6. On the next screen you will be presented with a text box containing a CSR block. You will need to copy this text fully (including the BEGIN CERTIFICATE and END CERTIFICATE line.

7. Make the necessary arrangement with your choice of certificate authority to get your certificate signed. You probably will need to pay them an administrative fee. You will also need to confirm your identity, probably by phone. Usually you will need to send them the necessary paperwork, either by fax or by mail. You will also need to send them your certificate signing request (CSR) at some point, usually by copying and pasting it to a web form or sending it by email. Every certificate authorities differs in the way they verify your information, please contact them if you need more information.

8. If the certificate authority authorizes you, you will receive an SSL/TLS certificate from them. Please save this certificate to a file and don't lose it!

9. Go back to the Install SSL/TLS Certificate menu and upload the certificate to our web server. Click on 'upload' on the right of 'Upload the SSL certificate from certificate authority' step. On the next screen you will be presented with a text box. Paste the SSL/TLS certificate content to this box. Make sure you also include the lines BEGIN CERTIFICATE and END CERTIFICATE.

10. (this step is optional) If the certificate authority requires an intermediate CA certificate or server certificate chain, you will need to upload it here. Your certificate authority will provide you with the intermediate certificate you can upload here if required.

11. Activate the SSL/TLS key pair to install them to our web server. Please wait at most one hour before the certificate gets installed.

Warning

Do not delete your web server private key after you receive your certificate from certificate authority. Doing so will make it completely unusable and you will need to regenerate it again..

Note

An SSL/TLS certificate file has an expiration date. You will need to renew your SSL/TLS certificate when it expires.

Migrating From Another Server

We provide a feature for you to easily migrate your web contents from another server. This is useful if you are migrating from another web hosting company.

To migrate your web contents please do the following.

1. Log on to **SiteManager** if you haven't already logged on.

2. Go to *Migration Tools* menu and then *Migrate web contents from another server* menu.

3. On the first screen you will be asked about the target subdomain where you will download the files. Please note that any web files inside this subdomain will possibly be overwritten.

4. Click on *Next*. On the next screen choose the type of remote host, please choose accordingly.

5. Follow the instructions on the next screens. The amount of information you need to provide depends on the type of host you choose on the previous screen.

Checking Your Web Site from Link Errors

Sometimes when developing a web site you will sooner or later make a mistake when creating a link. Also, an external

URL could no longer be available and thus a link to it will become a dead link. We provide a tool to check your web site for such errors.

To check your web site for linking errors, please do the following.

1. Log on to **SiteManager** if you haven't already done so.
2. Go to *Miscellaneous* menu and then go to *Check your web sites for link errors*.
3. On the next screen, choose your current subdomains you want to check for linking errors. And then click *Check for Errors*.

The analysis might take some time to finish. When it finishes, it will send you an email notification. The result will appear under your web statistic subdomain in the directory `linbot/`. By default the result will be under http://stats.example.com/linbot/ assuming your account's domain is example.com.

Converting ASP Scripts to PHP

Sometimes programming in Active Server Pages (ASP) could be very limiting. PHP on the other hand is a similar language but have a lot more features and flexibility. You have the option to convert your ASP scripts without doing everything from scratch again.

To attempt to convert your ASP scripts to PHP, you need to do the following.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Miscellaneous* menu and then go to *ASP to PHP converter* sub menu.
3. Inside, you will be presented with several fields. Choose your subdomain on the 'subdomain to convert' field to convert every ASP files inside that subdomain. You also have the option to choose more than one subdomain.
4. On the database field, please specify the database used by the ASP script you want to convert. Or you can choose Automatic detection to let it detect the database automatically. If the ASP scripts in question does not use database, please use Automatic detection.
5. If the ASP scripts you want to convert come from a non Y2K compliant Microsoft® Windows® NT Server, please set Y2K Problem Handling to 'yes'.
6. On the variable name case mangling field, you can choose if you want to converter to change the case of variables. Variable names in ASP is case insensitive,

unlike PHP where variable names is case sensitive. You can use this option to force the case of variable names.

7. On the last field, you can choose if you want every created PHP files includes `global.php`.

8. Click on *Convert ASP to PHP* in order to start the conversion.

Important

ASP to PHP conversion is not guaranteed to be 100% perfect. However it is still better than rewriting the scripts from scratch.

File Permission

Important

Don't worry if you don't understand anything in this section, just use AutoCorrect to fix almost all your permission problems automatically.

Any file in your account needs to be in correct permission before it can function correctly. You can change file permission by using **SiteManager**'s file manager or FTP. AutoCorrect will also fix your files' permission automatically. If you find your scripts do not function correctly, please try AutoCorrect first. For more information about AutoCorrect please refer to the section called “Using AutoCorrect Feature” [37].

Directories on your account need to be in mode 0755. This is the default when creating directories, so you won't need to do chmod after creating them. More permissive mode (like 0755) is not allowed, CGI scripts will refuse to function if placed within too permissive directories.

Dynamic CGI scripts (such as Perl, Python, or Ruby) should be in mode 0755. Static files (such as HTML documents or images) should be at least in mode 0644 (but it won't hurt to have them in 0755). Under no circumstances should files be in mode 0666 or 0777.

Important

Some scripts come with installation manual that tell the user to chmod files or directories to mode 0777 or 0666. This is not required in our system where CGI scripts are running as their own owner privileges. In fact, in some cases, our system will refuse to run scripts when they are in those modes.

Database Server Administration

Types of Database

indoglobal.com offers two types of database servers: MySQL and PostgreSQL. Both are popular databases dan sometimes required by third party software.

MySQL Database

MySQL is the most popular relational database management system (RDBMS) in the Internet today. A lot of web applications, free or commercial depends on MySQL for their database backend. The speed, compactness and simplicity of MySQL makes it suitable for most web sites.

PostgreSQL Database

PostgreSQL is another popular database product. It has a complete set of features found in higher end database systems. While not as popular as MySQL, PostgreSQL still have its place in web sites. Quite some third party applications utilizes PostgreSQL as backend database server.

Support for More Than One Database

indoglobal.com offers these two databases to its clients. You can create more than one database on an account. This has the advantage that it will simplify your development process since you can easily separate database for various functions, and will not clobber a single database with various unrelated tables.

Aside from that, you will also find a lot of third party software that uses the same table name, especially with common table names such as 'user' or 'group'. If you need to install two or more programs that uses a table named 'user' and only allowed to use only a single database, then you are in trouble. The only solution would be to edit those programs so that it would use another table name. In indoglobal.com system you are able to create two databases for two different programs and they won't conflict or require heavy modifications.

You are allowed to create as many databases as you need. The maximum limit of databases you can create is only limited by your disk space quota.

Creating and Managing Databases

To create a database, please follow the following steps.

1. Log on to **SiteManager** if you haven't already logged on.

2. Go to *Database server* menu.

3. Inside database server menu, there are two options for creating database, one for MySQL and one for PostgreSQL. Click on appropriate menu to create a database.

4. Specify the name of database and its password. You can use the *Generate* to generate a random password. For PostgreSQL, please also specify the encoding to be used in the new database.

5. Click on *Create Database* button to create the database.

Note

Database name is always prepended with your account username in order to avoid name conflict with other users.

From the database server menu, you can see the currenly created databases. There are also several actions you can do to your existing databases.

- *manage*, this will manage your database from inside **SiteManager** you can add tables, modify tables, make a dump, execute queries, and others. This is currenly only available for MySQL database.
- *password*, this is used to change your database password.
- *delete*, this is used to delete your database. Please be careful when using this function, since it will delete the database and its contents without means to reverse the action.
- *example*, shows you how to connect to the database, execute a simple query and disconnect in various popular languages.

Managing MySQL Database

Our **SiteManager** includes a complete administration interface for managing your MySQL database. To access it, go to *Database server* menu and click on *manage* for the database you want to manage.

Alternatively you can also manage your MySQL databases using the more familiar command line tools.

Managing MySQL Database Using Command Line

To manually manage your MySQL databases, you need to log on to your shell account. Please see the section called “Logging in to UNIX Shell Account” [7] for more information

about logging on to your shell account.

Inside shell account, you can use the standard MySQL command line client to manage your database. If your database name is u777_database and the password is PASSWORD, you can connect to the database by issuing the following command.

```
mysql -uu777_database -pPASSWORD  u777_database
```

Inside MySQL shell, you can issue any SQL command to the database server. Please consult MySQL documentation for more information.

Note

Due to security concerns, our database servers do not allow LOAD DATA or any SQL commands that accesses filesystem directly.

Managing MySQL Database Using Alternative Software

While we provide a way to easily manage your MySQL Database, you may opt to use third party tools. There are basically two class of MySQL management software: web based application that might need to be installed on the server, and client based application that must be installed on user's computer.

The first class of MySQL management software need to be installed on your account, just like other regular web based application. One popular software of this class is phpMyAdmin. To configure these kinds of management software, follow the instruction in the section called “Using MySQL Database in Your Application” [58].

Important

There are several administration task that can't be done from third party management software. For example, you can't use them to create database.

The second class of management software are basically regular client application that must be installed on your computer. These software do their work by remotely connecting to MySQL database on our server. You need to supply several information to the software before it will be able to work correctly:

- Hostname: primary-ip.example.com, assuming your domain name is example.com
- Database name: specify the name of database you want to connect to. For example: u777_database
- Username: the name of database, the same as your database name above.

- Password: the password of this database that set from **SiteManager**

Creating new Table

Tables can be created by using *Create New Table* menu. To create a table, please follow these steps.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Database Server* menu and then click on *manage* for the database you want to create. From there click on *Create New Table*.
3. On the first screen you need to enter the table name, the table type and an optional comment. Table type can be MyISAM, ISAM or BerkeleyDB. The difference of each table types is described at MySQL manual. Click *Next* to continue.
4. On the next screen you need to specify the name and type of the first field of the table. You can add more fields later in the following menu. Click *Next* to continue.
5. On the next screen you will see your current information about the table you want to create. At this point the table is not created yet. You can add or remove more fields and indexes. The interface should be self explanatory.
6. When done designing table, choose *Finished, create the table*.

Modifying Table Structures

You can also modify table structures after it has been created. You can add and remove fields and indexes. To modify table structure, please do the following steps.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Database Server* menu and then click on *manage* for the database you want to create. From there click on *edit structures* for the table you want to modify.
3. Follow the instruction on the next screen. You can change table type, create new field, modify or drop existing fields, create new index or drop existing index.

Caution

Changing table type might result in lost of certain table attributes. Please see MySQL documentation for more information.

Deleting/Dropping MySQL Table

To delete a MySQL table, please do the following:

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Database Server* menu and then click on *manage* for the database you want to create. From there click on *drop* for the table you want do delete.
3. Confirm your action on the next screen.

Note

Tables that have been dropped cannot be recovered. Please be careful when dropping tables.

Modifying Records inside a MySQL Table

You can also add new records and modify existing records inside a MySQL table from **SiteManager**.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Database Server* menu and then click on *manage* for the database you want to create. From there click on *browse records* for the table you want do edit its records.
3. Inside the menu, you will be able to add new records or modify the existing ones. The interface should be self explanatory. You can change how the records are sorted by modifying the appropriate drop down boxes.

Note

You can't delete or edit records on a table without primary key.

Manually Entering SQL Query

You can also manually enter SQL queries from **SiteManager**. This allows you to perform more complex tasks by entering SQL queries directly into MySQL database. To manually enter SQL queries, you need to do the following.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Database Server* menu and then click on *manage* for the database you want to enter queries into. From there click on *SQL shell*.

3. Inside the menu, you will be able to perform SQL queries by typing SQL commands into the text area and clicking on *Send Query*. If you enter an SQL command that returns a result, the result in question will be displayed at the bottom of the page.

Tip

In this page there are tables and fields drop down boxes containing the currently created tables and fields in the current database. Clicking on the drop down box will input the value into the text area. There are also a history field containing previous SQL commands you performed before.

Note

Due to security concerns, our database servers do not allow LOAD DATA or any SQL commands that accesses filesystem directly.

Repairing and Optimizing MySQL Database

Sometimes database can get corrupted due to various reasons. You can attempt to fix your database by doing the following.

1. Log on to **SiteManager** if you haven't already logged on.

2. Go to *Database Server* menu and then click on *manage* for the database you want to repair. From there click on *Check, repair, analyze and optimize all tables*.

Dumping and Restoring MySQL Database

Dumping and restoring are fairly common task of managing database. Dumping is a process of making a file containing SQL queries that can be used to construct the whole database. Dumping is commonly used to download your database for backup or other purposes. Restoring is the reverse process of dumping.

Dumping MySQL Database Using SiteManager

To dump MySQL database please do the following.

1. Log on to **SiteManager** if you haven't already logged on.

2. Go to *Database Server* menu and then click on *manage* for the database you want to dump. From there click on *Dump database*.

3. Inside the menu, there are several options you can choose to determine how you want the database to be dumped. Choose accordingly and click *Dump Database*.

The available options are described below.

- *What to dump*. You can choose to dump both structure and data, structure only or data only.
- *Add DROP TABLE*. If this option is selected, a DROP TABLE command will be created before creating tables. Useful if you want to replace existing database on the target database.
- *Add LOCKs*. If this option is selected, a LOCK TABLE command will be added before creating tables.
- *Complete INSERTs*. Use complete INSERT command.
- *Include all MySQL specific create options*. This will include MySQL specific create options such as specifying the type of table.
- *Compress result*. You can choose whether to compress the result or not. You can choose gzip or bzip2 compression.

Note

Sometimes the dump result is not compatible with different MySQL version. Please consult MySQL documentation for more information.

Restoring Database Using SiteManager

The dump file created above can be used for restoring database. You can also use dump file created elsewhere, and optionally compressed with gzip or bzip2. To restore database please do the following.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Database Server* menu and then click on *manage* for the database you want to restore into. From there click on *Batch Query*.
3. Inside the menu, you need to choose an MySQL dump file on your system and then click on *Send Query* to continue. Optionally you can choose if you want MySQL to ignore when it encounter an error when restoring database.

Manually Dumping Database

You can also manually dump database using your shell

account. You can also make SQL dump files on other system using this method. To make an SQL dump you need to log on to your shell account. Refer to the section called “Logging in to UNIX Shell Account” [7] for more information. Issue the following command to dump your database. The following assumes your database name is u777_database with the password PASSWORD.

```
mysqldump -uu777_database -pPASSWORD \
     u777_database > u777_database.sql
```

That command should create a file named `u777_database.sql` containing the SQL dump. You can make a gzip compressed SQL dump by issuing the following command instead of the above, useful when your database is large in size.

```
mysqldump -uu777_database -pPASSWORD \
     u777_database | gzip > u777_database.sql.gz
```

Manually Restoring Database

Similarly, to restore a database from a dump file, please do the following command.

```
mysql -uu777_database -pPASSWORD \
     u777_database < u777_database.sql
```

To do the same but with a gzip compressed dump file, do the following instead of the above.

```
gunzip < u777_database.sql.gz | \
     mysql -uu777_database -pPASSWORD \
     u777_database
```

Tip

On the above commands, you can substitute gzip with bzip2 to use bzip2 instead of gzip compression.

Using MySQL Database in Your Application

To connect to MySQL database, you need to specify the following in your application.

- Hostname: localhost or 127.0.0.1. Or if it is possible, use UNIX socket `/var/lib/mysql/mysql.sock`
- Database name: specify the name of database you want to connect to. For example: u777_database.
- Username: the name of database. In other words, this is the same as your database name above.
- Password: the password of this database where can be set inside **SiteManager**.

The following examples illustrates how to use MySQL

database inside your application, assuming the database to be used is u777_database with password 'PASSWORD'.

Tip

You can also see examples inside **SiteManager**. Go to *Database Server* and then click *examples* for the database in question.

Using MySQL Database With PHP

```
<?php
// Code taken from PHP manual

$username = "u777_database";
$password = "PASSWORD";
$hostname = "localhost";

// Connecting, selecting database
$link = mysql_connect($hostname, $username, $password);
mysql_select_db("my_database");

// Performing SQL query
$result = mysql_query($sql);

// Closing connection
mysql_close($link);
?>
```

Using MySQL Database With Perl

```
# code taken from Perl DBI documentation
use DBI;

# connecting to database
my $username = 'u777_database';
my $password = 'PASSWORD';
my $dbh = DBI->connect("DBI:mysql:$username",
    "$username", "$password");

# executing a single query without result
my $rv = $dbh->do($sql);

# retrieving result from a query
my $arrayref = $dbh->selectall_arrayref($sql);

# disconnect from database
my $rc = $dbh->disconnect();
```

Using MySQL Database With Python

```
import MySQLdb

# connecting to database
username = "u777_database"
password = "PASSWORD"
hostname = "localhost"
conn = MySQLdb.Connect(host=hostname,
    user=username, passwd=password, db=username)

# create result/cursor object
cursor = conn.cursor()

# perform a query
cursor.execute(sql)

# get result set
result = cursor.fetchall()
```

```
# close the connection
conn.close()
```

Using MySQL Database With ASP

```
connect_string = "Driver={Mysql}; " & _
   "Server=localhost; Database=u777_database; " & _
   "UID=u777_database; PWD=PASSWORD"

' opening connection to database
set dbConn = server.createObject("ADODB.connection")
dbConn.open connect_string

' perform a query
Set recordset = dbConn.Execute(SQL)

' closing connection
dbConn.Close
```

Managing PostgreSQL Database

At the moment you need to log on to your shell account in order to manage your PostgreSQL database. Please see the section called “Logging in to UNIX Shell Account” [7] for more information about logging on your shell account.

When inside your shell account, you can use the standard `psql` command line utility to administer your PostgreSQL database. Assuming your PostgreSQL database name is u777_database, you can connect to your PostgreSQL database by issuing the following command.

```
psql u777_database u777_database
```

When asked for password, enter your database password.

Inside psql shell, you can issue SQL commands. Please see PostgreSQL documentation for more information.

Dumping and Restoring PostgreSQL Database

Dumping is a process of making a file containing SQL queries that can be used to contruct the whole database. Dumping is commonly used to download your database for backup or other purposes. Restoring is the reverse process of dumping.

Dumping PostgreSQL Database

To dump your PostgreSQL database you need to be logged on to your shell account. Please see the section called “Logging in to UNIX Shell Account” [7] for more information about logging on shell account. Assuming your database name is u777_database, you need to use the following command to dump your PostgreSQL database.

```
pg_dump -U u777_database u777_database \
    > u777_database.sql
```

That command should create a file named `u777_database.sql` in the current directory. You can use FTP or other means to

download the file.

To make a gzip compressed dump file, you can use a few modification to the above command.

```
pg_dump -U u777_database u777_database \
    | gzip > u777_database.sql.gz
```

Restoring PostgreSQL Database

To restore previously dumped database you need to use psql.

```
psql -U u777_database u777_database -f - \
    < u777_database.sql
```

Similarly, you can use the following command to restore PostgreSQL database when the dumped file is gzip compressed.

```
gunzip < u777_database.sql | \
    psql -U u777_database u777_database -f -
```

Tip

In order to use bzip2 instead of gzip compression, you need to substitute gzip with bzip2 and gunzip with bunzip2 respectively.

Using PostgreSQL Database in Your Application

To connect to PostgreSQL database, you need to specify the following in your application.

- Hostname: localhost or 127.0.0.1.
- Database name: specify the name of database you want to connect to. For example: u777_database.
- Username: the name of database. In other words, this is the same as your database name above.
- Password: the password of this database where can be set inside **SiteManager**.

The following examples illustrates how to use PostgreSQL database inside your application, assuming the database to be used is u777_database with password 'PASSWORD'.

Tip

You can also see examples inside **SiteManager**. Go to *Database Server* and then click *examples* for the database in question.

Using PostgreSQL Database With PHP

```
<?php
```

```
// Code taken from PHP manual

$username = "u777_database";
$password = "PASSWORD";
$hostname = "localhost";

// Connecting to database
$link = pg_connect("dbname=u777_database ".
    "user=u777_database password=DATABASE");

// Performing SQL query
$result = pg_exec($sql);

// Closing connection
pg_close($link);
?>
```

Using PostgreSQL Database With Perl

```
# code taken from Perl DBI documentation

use DBI;

# connecting to database
my $username = 'u777_database';
my $password = 'PASSWORD';
my $dbh = DBI->connect("DBI:Pg:$username",
    "$username", "$password");

# executing a single query without result
my $rv = $dbh->do($sql);

# retrieving result from a query
my $arrayref = $dbh->selectall_arrayref($sql);

# disconnect from database
my $rc = $dbh->disconnect();
```

Using PostgreSQL Database With Python

```
import pgdb

# connecting to database
username = "u777_database"
password = "PASSWORD"
hostname = "localhost"
conn = pgdb.Connect(host=hostname, user=username,
    passwd=password, db=username)

# create result/cursor object
cursor = conn.cursor()

# perform a query
cursor.execute(sql)

# get result set
result = cursor.fetchall()

# close the connection
conn.close()
```

Using PostgreSQL Database With ASP

```
connect_string = "Driver={Postgres}; Server=localhost; " & _
    "UID=u777_database; PWD=PASSWORD"

' opening connection to database
set dbConn = server.createObject("ADODB.connection")
dbConn.open connect_string

' perform a query
```

```
Set recordset = dbConn.Execute(SQL)

' closing connection
dbConn.Close
```

Improving Security

By its nature, it is harder to secure a web hosting environment. It is very easy to secure a server whose job is solely serving web pages, just close all ports besides HTTP port and make sure the web server is up to date. However, in shared web hosting environment, it is not possible to do that. What's good a web server, if you, our customers, can not update your web site.

While **indoglobal**.com tries very hard to improve server security, our clients are also responsible for securing their own accounts. In this chapter, we will discuss many ways to improve your account's security.

Classes of Security

There are several classes of security in web hosting environment, each with its own owner of responsibility. Each responsible party will need to secure their own 'perimeter' before total security can be achieved.

Network Security

Basically, the server hosting your account is connected to a network, which in turn connected to a much larger network called the Internet. Successful attack to the network will make servers inside the network unreachable or at least not easy to reach from the Internet. These are some examples of attacks that target the network:

- Denial of service (DoS) attack. This attack sends a lot of data to a target server or network so that the server or network will not have enough bandwidth in order to serve legitimate requests. The data sent are usually junk random data, but sometimes they are specially crafted packets in order to confuse certain services.
- Distributed Denial of Service (DDoS). This kind of attack are similar to DoS above, however DDoS attacks are launched from several hosts on the Internet simultaneously, usually from trojaned, zombie or cracked hosts. DDoS are several magnitude more catastrophic than a simple DoS. Even big networks such as Yahoo!, Amazon, CNN, and EBay had been taken down by DDoS attacks.
- Attack to network router. A network is connected to the Internet through one or several routers. A successful attack to a strategic router can bring down the whole network.

These classes of attacks are the responsibility of

indoglobal.com's upstream providers.

Server Security

These classes of security involves the server itself. Illegitimate gain to a server usually achieved by exploiting a known vulnerability of a service running on the server. Sometimes it is also possible for an attacker to bring down the server instead of gaining an illegal access.

These classes of security are the responsibility of indoglobal.com. We try to make sure any software running on the server contain no known vulnerabilities. If a vulnerability on a service were found, we always try to update the software in question as soon as possible. We also implement server firewall in order to make it harder for irresponsible parties to gain illegal access to our server.

Since every user on our system doesn't trust each other, we also try very hard to implement a clear separation between our users while still allowing them to do administration tasks without hassle. A user on our system should not be able to access other user's files or data.

User Account Security

The rest of this chapter will mostly discuss this class of attacks. These attacks involves illegitimate gain to your account, for example:

- Shell vulnerability. Crackers can exploit these vulnerability to get them shell access to your account.
- Cross site scripting (XSS). XSS occurs when a web application gathers malicious data from a user, and then present the data to another user verbatim without escaping. This could allow a malicious user to hijack another user's account.
- SQL injection attacks. In this class of attacks, an attacker inserts a carefully crafted query string to a vulnerable script in order to confuse the script in question into executing any arbitrary SQL commands.

User account security are the responsibility of our user. It is impossible to expect us to be able to audit every code in every user's account line by line and make sure all of them do not contain any vulnerability. So it is important for our clients to update third party software when a vulnerability is found. It is also important to reduce mistakes when developing your web application. This chapter will discuss these topics in greater detail.

Keeping Third Party Software Up to Date

We can't stress enough that security is a process, not a one time job. No software is perfect, you shouldn't assume the

software you installed is without security problem. There might be security problem that hasn't been discovered yet.

Once you installed a third party software, you will need to monitor its development progress. If a security related problem is found, you will need to update the installed software. If you continue to let the software running without updating it, malicious party will be able to take advantage of the security problem. The longer it runs unpatched, the greater the risk.

To monitor the software's development, usually you just need to visit the software' web site regularly. If a security problem is found, often they will put an announcement on their web site.

Some software suffers from security problem more often than the others. Below we list several software that traditionally has serious security problem.

- PHP-Nuke. PHP-Nuke is a very popular portal system. However it suffers from several security problem in the past. You should visit their web site at http://www.phpnuke.org from time to time just to know if an update is released to fix a security hole. PHP-Nuke has a modular plugin architecture, if you use a module from outside PHP-Nuke distribution, you will also need to monitor the module's web site.
- PostNuke. Postnuke is a similar system to PHPNuke. While it is considerably more secure than PHP-Nuke, it did have several security problem in the past. It is a good idea to monitor their web site at http://www.postnuke.org.

Writing Secure Scripts

This users' guide doesn't aim to be a complete guide on how to write secure scripts. Instead, we will point you to several web site that specialized on the topic.

Securing PHP Scripts

- http://www.onlamp.com/pub/a/php/2003/07/31/php_foundati
- http://www.developer.com/lang/article.php/918141
- http://www.devshed.com/c/a/PHP/PHP-Security-Mistakes/
- http://www.sklar.com/page/article/owasp-top-ten
- http://www.dwheeler.com/secure-programs/Secure-Programs-H
- http://www.linuxjournal.com/article.php?thold=0&mode=neste

Securing CGI Scripts in General

Securing against cross site scripting (XSS) attacks:

- http://www.cgisecurity.com/articles/xss-faq.shtml
- http://www.cert.org/advisories/CA-2000-02.html
- http://httpd.apache.org/info/css-security/
- http://www.perl.com/pub/a/2002/02/20/css.html

Securing against SQL or command injection attack.

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- http://www.4guysfromrolla.com/webtech/061902-1.shtml
- http://www.aspectsecurity.com/topten/injection.html

Use Secure Protocols When Managing Your Account

Some communication protocols send data in clear text. This is not desirable because a malicious third party could inspect your data on the way to our server. Fortunately, there are safer alternatives that doesn't expose your data so easily.

To provide access to your shell account, we provide two means: telnet and SSH. To improve security, you should consider avoiding telnet. Telnet sends your username and password in clear text. On the other hand, SSH encrypts communication between you and our server. An eavesdropper will have hard time if you are using SSH instead of telnet.

We provide several ways for you to upload your web site contents. Each way has different security implications.

- *FTP*. FTP doesn't encrypt your data, an eavesdropper could see your username and password in plain text.
- *WebDAV*. WebDAV over HTTP (port 81) will not encrypt your data. WebDAV over HTTPS (port 444) will encrypt your data.
- *SiteManager file manager* . Uploading your data using SiteManager should be safe as long as you enable secure mode when logging in.
- *Microsoft® FrontPage®*. You can use Microsoft® FrontPage® over HTTP or HTTPS. Use Microsoft® FrontPage® HTTPS mode to increase security.
- *scp, sftp, rsync*. These protocols use SSH transport, and therefore should be secure.

What To Do When a Security Incident Happens

Even if we did our best, sometimes we get unlucky. Maybe the attacker found the vulnerability by himself before the software author get noticed. Or maybe the attacker was simply lucky to find your web site before you had a chance to make an update. Once an incident happens, you need to do the following things.

1. Firstly, don't panic. Contact us if you require assistance.
2. You will need to erase all of your contents and then reupload from your local backup. There is a chance that the malicious party inserted a backdoor in your scripts.
3. Update any program or scripts to the latest version. Contact the software maker of simply visit their web site for more information.
4. If you happen to know the identity of the irresponsible party, do not under any circumstances get in touch with them. A lot of these people are people with serious mental problems. Talking with them will not make you better, and certainly will not restore your web site. Any contact to these people should be in the form of legal action.

Email Management

indoglobal.com offers a complete email system. You will be able to add accounts and configure them to tailor to your own requirement.

Types of Email Accounts

There are several types of email accounts you can create.

- *POP/IMAP account*. Email sent to this type of account will be stored on the server. Users then will be able to download their email by using an email client software or check their mails by using webmail. A POP/IMAP account also functions as a Jabber® account, please see *Jabber Instant Messaging* [85] for more information about Jabber®
- *Email forwarder*. This type of email accounts will forward any incoming mail to another email address. For example, you can forward your emails to your account with a local ISP, but you can use the address associated with your domain, not your ISP.
- *Mailing list*. Mailing list consists of its members' email addresses. Any email sent to a mailing list account will be distributed to its members. Our mailing list system is fully automatic, for example a user can become a member by themselves, email bounces are handled automatically, etc.
- *Auto responder*. Autoresponder will immediate reply any incoming email with a given message. Beside that, the incoming message can be forwarded to another email address as well.
- *Email bouncer*. This type of email account will simply reject any incoming email, just like when this account has not been made. For a reason why this email type is sometimes necessary, please refer to the section called “Default Mail Handler” [73] for more information.
- *Email blackhole*. This type of email account will simple discards any incoming emails.
- *Custom mail handler*. An advanced user can use dynamic email processing by using custom mail handler. To use this feature, you need a working knowledge on how our email server (qmail-1.03) works.

Tip

POP/IMAP email accounts are also user

configurable to forward email to another address and also as an autoresponder (vacation).

Creating a New Email Account

To create an email account please do the following steps.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Email* menu.
3. Inside the email menu, there are links where you can add the types of email accounts described above. Click on the link and follow the instructions on the next screen.

Depending on which type of account you want to create, you will be presented with different options:

- *POP/IMAP account*. You can limit the maximum size of the mail account. If a new email arrives when the mailbox is full, then it will be bounced back. You can specify 0 (zero) if you don't want to limit the size.
- *Email forwarder*. On the add new mail forwarder menu, you need to specify the forwarding destination. You can also specify more than one email address by separating them with space.
- *Mailing list*. On the add new mailing list menu, you will need to specify the owner of the mailing list. You also need to specify the type and membership restriction of mailing list. You can alter mailing list configuration later after the mailing list has been created.
- *Auto responder*. On the add new autoresponder menu, you need to specify forwarding destination where you want any incoming email be forwarded to and the contents of autoresponder email, including from, subject and the body of autoresponder mail.
- *Email bouncer*. You need to specify the message that will be returned to the sender when an email sent to this address.
- *Email blackhole*. You don't have to specify anything when adding a blackhole email address.
- *Custom mail handler*. You need to specify the custom action to take whenever an email message arrives. Specify the action in dot-qmail format.

Caution

Custom mail handler feature is for advanced users

only, you need to know about qmail server in order to use this feature.

Default Mail Handler

If your email users are located in one single location, for instance in the office or school, you can use the default mail handler feature of our email system. Using default mail handler together with a local mail server will make your email system more efficient.

Note

Default mail handler is also known as DomainPOP or catchall email address.

The default mail handler is given to each created subdomain that can receive email. With default mail handler, any email that get sent to an undefined address in the respective domain (or subdomain) will be saved in the default mailbox that is located on our server. Then your own email server in turn can download the whole mailbox and distribute the email to a local mailbox on your email server* This way, your users don't need to connect directly to our mail server, thus saving your time and bandwidth.

This will explained better in example.

1. You create a mail server using MDaemon on your facility.
2. You add three users to your mail server: joe@uk.example.com, john@uk.example.com and jane@uk.example.com. You configure your mail server to deliver email to these users locally and assign them password for your users to access their mailbox on your mail server.
3. You create subdomain uk.example.com on our server and configure it to use default mail handler. You don't create the individual mailbox on our server, otherwise their email won't get sent to the default mail handler.
4. You configure your own mail server to download email from the default mail account default@uk.example.com periodically. Your mail server then will sort the incoming emails and distribute them to your users, while bouncing any emails with unknown destinations.
5. Your users in turn will be able to download their own email from your mail server inside your facility.

The default mail handler will handle all emails that the address has not been defined by you. In example above, if your add john@uk.example.com on our mail server, the email will get sent to a mailbox on our server, not the default mail handler. Additionally, this is where the email

bouncer accounts come in handy. For example, whenever john@uk.example.com resigns from your company, you can assign a mail bouncer on our server, so any email that get sent to john will bounced at our mail server, and you don't need to download john's email again, saving you some bandwidth.

Warning

Lots of spammers employ spamming technique known as 'dictionary attack'. They don't harvest email addresses, but they simply guess email addresses of a known domain. If you are using default mail handler and a spammer tries to 'dictionary' your domain, then you will get a lot of mails to nonexistant users.

Editing Default Mail Handler

To edit the default mail handler, please do the following.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Email* menu. On the default mail handler section, click *edit* on the right of subdomain you want to edit its default mail handler.
3. On the next screen you can change the default action. You can change it to return to sender as undeliverable (default), deliver to POP/IMAP account, or forward to another email address.
4. If you choose to forward to another email address, you need to specify mail forwarding destination.
5. If you choose to deliver to POP/IMAP account, you need to specify the password that can be used to download incoming email using POP or IMAP.
6. Click *Update Default Mail Handler* to finalize your changes.

To download email messages and distribute them to your local user, you will need to use an email client software that understand how to manage multiple email accounts in a single POP/IMAP mailbox. This software probably must also act as a POP/IMAP server itself to be able to distribute mail to your local users. Examples of such clients are MDaemon or Fetchmail.

Important

You must tell your default mail handler client to filter incoming email messages using 'X-Rcpt-To' or 'X-POP3-Rcpt' headers. Please refer to the client software's manual for more information on how to do this.

Mandatory Email Accounts

There are some email addresses that are required by Internet standards or common practice.

- *postmaster@example.com*, required by Internet standards to contact the email administrator of the domain example.com.
- *hostmaster@example.com*, this address is used to contact the DNS adminstrator of example.com.
- *abuse@example.com*, this address is a common practice within Internet community to report abuses involving the domain example.com.

By default emails to those addresses are forwarded to your contact email address. You can change where they are forwarded by following these steps.

1. Log on to **SiteManager** if you haven't already logged on.
2. Go to *Email* menu and then click on *Mandatory Mail Accounts Configuration* menu.
3. Specify where you want to forward email coming to mandatory email accounts and click *Update Mandatory Accounts* to save the changes.

In addition of the mandatory email accounts, you can also set the bounce email address. This is the default address that will receive any bouncing email from your scripts.

Checking Emails

Every POP/IMAP accounts can be downloaded to users' computers by using an email client software.

Note

This section only applicable to POP/IMAP email accounts. Other type of email account cannot be downloaded to user's computer.

Receiving Emails

To receive emails, you need to set your email clients with the following configuration.

- Protocol: POP3 or IMAP4. POP3 is more suitable for offline operation where you download all emails at once, empty the server mailbox, and read them offline. IMAP4 is more suitable for online operation, it supports more features but some implementation of client software will require emails to be stored on the server.
- Port: use standard port number, 110 for POP3, and 143

for IMAP4

- Hostname: pop.example.com or imap.example.com assuming your account's domain is example.com. Both will work by default for both protocols (POP3 or IMAP) assuming you haven't altered the corresponding aliases from subdomain menu. It is recommended to use imap.example.com for accessing using IMAP and pop.example.com for POP3.
- Username: the complete email address, for example: 'john@example.com' without quotes. Or if your client software doesn't support @ sign, you can use % (percent) instead, for example: 'john%example.com' without quotes.
- Password: the password you set for the POP/IMAP email account in question.

For more information about configuring popular email client software, please refer to Appendix C, *Email Clients Configuration* [99].

Sending Emails

To send emails, it is recommended to use **indoglobal**.com's SMTP server where possible. Alternatively, you may also use your ISP's SMTP server if possible. However, if you choose to use your ISP's SMTP server, please see the section called "Protecting Your Email With SPF" [82].

However, some ISPs doesn't provide an SMTP server you can use to send emails using email address hosted by our server. If this is the case, you can use our SMTP server as follows.

- Protocol: SMTP
- Port: 8025 or 587, please note this is not the standard SMTP port number
- Hostname: smtp.example.com assuming your account's domain is example.com. This will work assuming you haven't altered the corresponding aliases from subdomain menu.
- Username: the complete email address, for example: 'john@example.com' without quotes. Or if your client software doesn't support @ sign, you can use % (percent) instead, for example: 'john%example.com' without quotes.
- Password: the password you set for the POP/IMAP email account in question.

Important

Due to the fact that our SMTP server is always farther than your ISP's SMTP server, sending email using our server will always be slower than using

your ISP's SMTP server. To avoid abuses we are also forced to make the necessary changes to our SMTP server that could make it slower.

Note

Any email sent through our SMTP server will have its From address rewritten.

For more information about configuring popular email client software, please refer to Appendix C, *Email Clients Configuration* [99].

Checking Email Using Webmail

Webmail is a convenient way to check your email. With webmail you can check your email anywhere with Internet access and a standard web browser. You don't even need to configure an email client software when using webmail.

Note

Webmail can be used only for your POP/IMAP email accounts.

When first creating your account, your webmail is configured at http://webmail.example.com by default, assuming your domain is example.com. Please see *Subdomain and DNS* [11] for more information about subdomain and DNS in general.

To log on to webmail, you need to visit your webmail address using a web browser such as Mozilla or Microsoft® Internet Explorer®. On the login screen, specify your POP/IMAP account email address and password to log in. Inside the webmail, everything should be self explanatory.

Caution

On a shared or public computer, please make sure to log out from webmail when leaving your computer.

Checking Email From WAP Devices

You can also check your email using a WAP device such as cell phone or PDA. The address of WAPmail is the same as webmail, by default it is http://webmail.example.com assuming your domain is example.com.

Our webmail system will automatically detect your device. If you are using a standard web browser you will be redirected to standard web mail. If you are connecting using a cell phone, you will be redirected to a simplified WAP version.

Tip

Some mobile devices are also capable as a standard web browser. To force it to use WAP (i.e. to conserve bandwidth), you can use URL like http://webmail.example.com/wap instead.

Configuring Spam Filter

According to some studies, spam or junk email messages are the worst thing happening in the Internet. We provide several ways to reduce the volume of spam you need to deal with every day.

To configure spam filter, you need to log on to your webmail. Please see the section called “Checking Email Using Webmail” [77] for more information about webmail. Inside webmail, then go to *Options* and then *Spam Filter*.

Inside you can choose how would you like to combat spam. There are several level of spam protection you can use, each with its own weakness and strength. The levels of spam protection are described below.

- *Level 0: Spam protection disabled*. When using this level, spam protection is disabled. You will receive spam along with your legitimate email messages.
- *Level 1: Common keyword analysis*. Our system will analyze incoming email for certain keywords. If the number of keywords found reaches a certain threshold, our system will treat the email as spam and deliver it to Junk Mail folder.
- *Level 2: Spam learning system*. You tell our system which email messages are spam and which ones are not. Our system will then attempt to identify spam based on your input.
- *Level 3: Challenge and response system.*. Our system will keep record of all legitimate senders. Any unknown senders will need to confirm themselves in order to send you email messages.

More information about each level is described on the following sections.

Spam Protection Level 1

With this level active, you don't need to anything else. Any identified junk email messages will be delivered to your Junk Mail folder. This method however is not as effective as the other levels of spam protection. When using this level, it is better if you check your Junk Mail folder for legitimate email messages that get misclassified.

Spam Protection Level 2

When using this level, you will need to get a bit involved

with spam filter. This level of protection requires your feedback, you need to tell our spam filter which messages are junk email messages and which ones are not. There are several ways to accomplish this.

Note

Flagging messages as spam or not spam will still work if this level of spam filter is not active. However our system will not use this information to classify incoming email messages.

- From mailbox view (the view that comes up when you click INBOX or other folders) where you can select using the checkboxes on the left of each of message. Check all email messages that are spam/not spam and then click *Spam* or *Not Spam*, respectively.
- From email view (the view that comes up when you click on an email message). Click *spam* or *not spam* depending on the legitimacy of the message.

Note

Any email messages that marked as spam will be automatically moved to your Junk Mail folder

You will need a sizable amount (1000+) of learned email messages before the filter becomes effective. But when it becomes effective, it is very effective when filtering spam.

Important

You need to identify both spam and non spam email messages you receive. Identifying only spam messages is not enough.

Spam Protection Level 3

This level of spam protection requires active participation from both you and the other party of email communication. This level of spam filter combines several countermeasures such as whitelists, blacklists and challenge and response. Spam protection level 3 should be very effective, however it requires your active participation and a bit knowledge on how the system works. On some cases it will also require your peers to answer challenge sent to them.

Important

You need to understand how the system works before using spam filter level 3. Failing to understand could result in loss of email messages.

When this level is active, every email destined for you will

subject to whitelists and blacklists. If the sender's email address is in your whitelist, the message will be delivered to you. On the other hand, if the sender's email address is in your blacklist, the message will be bounced back. If the sender's email address is not listed on either your whitelist or blacklist, then our email system will send a challenge to the sender, if he/she replies the challenge then the message in question will be delivered to you and he/she will be added to your whitelist, so that he/she won't have to get challenged again when sending you another email in the future.

Important

When subscribing to a Yahoogroups! or an ezmlm based mailing list, you need to whitelist its extension address. For example, if you want to subscribe an ezmlm mailing list list@example.com, you will need to whitelist list-*@example.com.

You can also edit your whitelist and blacklist manually. From inside webmail, go to *Options* and then *Whitelist and Blacklist Management*. Inside, you will be able to add email address to or remove existing ones from your whitelists and blacklists. You can also use wildcards to specify multiple address, here are some common examples.

- *@example.com will match anyone@example.com but not anyone@sub.example.com
- *@*.example.com will match anyone@sub.example.com but not anyone@example.com
- *@=example.com will match both anyone@example.com and anyone@sub.example.com

By using spam filter level 3, in addition of the main email address (i.e. user@example.com) you can also use extension addresses. There are several types of extension addresses.

- *Dated Addresses*. Our system can automatically tag your message with a temporary email address which only works for a defined time internal (e.g. one week). During this period, even those not on your whitelist will be able to contact you using the dated address. An example of a dated address is user-dated-1063892913.a4d8d3@example.com, this particular address can only be used to send you email unchallenged before 18 September 2003.
- *Sender Addresses*. Sender address is an email address that only a certain sender can use to send you email. An example of a sender address is user-sender-a29ecf@example.com. This address will only accept messages from test@example.com unchallenged. Other messages must go through the confirmation

process.

- *Keyword Addresses*. Keyword address is a special address which will work for any sender and indefinitely unless specifically revoked. Any string can be used as the keyword. An example of a keyword address is user-keyword-amazon.8w06e8@example.com, the keyword of this address is 'amazon'. Keyword address are useful when you need to give your address to another party but can't predict beforehand the sendier address that will be used to send you email. For example, you can use keyword address for signing up to Amazon or eBay. If you later find out that Amazon misuse your address, you can revoke this address by blacklisting the keyword address.

When composing email and spam filter level 3 is enabled, you have the option to use extension address. This way, the 'from' field of your email message is replaced by your extension address.

Note

By default, if you send an email to an address that hasn't whitelisted yet, that address will be whitelisted automatically to prevent deadlock when communicating with users that using similar system.

You can also generate extension address manually, useful if you need to hand out an email address without sending an email message (e.g. when dealing with a HTML form that asks for your email address). To generate extension address manually, go to *Options*, then *Spam Filter*, and then *generate extension address*.

Using Global Email Password to Access Your User's Account

Sometimes it is necessary to be able to access your user's email account. Global email password can be used to access your user's email account without changing their regular password. You only need to use global email password in place of your user's regular password. For example, you can log on to your user's webmail account by using their username and the global email password. This will also work with your users' POP and IMAP accounts.

Important

Although email accounts and Jabber® instant messaging accounts share the same username and password, you cannot use global email password to log on to your user's Jabber® account.

To change your global email password, please do the following:

1. Log on to **SiteManager** if you haven't already logged on.

2. Go to *Email* menu and then proceed to *Edit Global Email Password*.

3. On the next screen, specify a password in both fields. Choose *Update Global Password*

4. Now you will be able to use the password you specified in place of your user's password.

Protecting Your Email With SPF

Email has a weakness: it allows anyone to forge anyone else's email address. This means any person could send a message claiming to be from you, and only an email expert would be able to tell the differences. Spammers, viruses and worms exploit this weakness all the time. Viruses and worms often send emails with forged from address to trick the recipients into opening it. Spammers almost always impersonate innocent email address when sending their spam.

SPF protects you from this. It specifies which hosts on the Internet can send mail as a specific user. SPF aware mail servers will then reject emails that don't come from the specified hosts.

indoglobal.com supports SPF. By default any host on the Internet may send email from your domain. This is the most expected setting today, however you should change it to something more restricting in order to be able to protect your domain from impersonation.

To configure your domain's SPF records, please follow these instructions.

1. Log on to **SiteManager** if you haven't already logged on.

2. Go to *Subdomain & DNS*.

3. Choose *edit mail handler* for the domain you wish to configure its SPF records.

4. You can review the current SPF configuration for the domain in question in this page. To configure SPF, choose *Configure approved outgoing mail servers*.

5. Follow the instructions and then choose *Configure SPF Record* to save your settings. Please note that the server hosting your account is automatically added to SPF record, you don't need to add our server's hostname or IP address.

Note

Please allow 24 hours before the new SPF record can take effect.

Important

We recommend that you use our SMTP server when sending emails. If you choose to send using your own or the ISP's SMTP server, please make sure it is whitelisted in SPF.

Jabber Instant Messaging

About Jabber®

Jabber® is an open instant messaging platform that uses an open, XML-based protocols to create the standard functionality people expect of an IM system: one-to-one chat, multi-user chat, the ability to subscribe to someone else's presence, and so on. Jabber has been approved as proposed Internet standard by Internet Engineering Task Force.

The way Jabber® works is similar to legacy instant messaging platform such as ICQ®, MSN® Messenger, Yahoo!® Messenger or AIM®. A user will be able to contact his/her 'buddies' using a client program.

Why use Jabber® instead of other instant messaging services?

- Jabber® is an Internet standard just like HTTP or SMTP. There are several implementations of servers and clients from a lot companies. Just like web and email.
- Jabber® protocol is decentralized unlike proprietary instant messaging system. Every domain owner could have their own Jabber® server, just like email.
- There are fewer privacy concern with Jabber®, because communications between Jabber® users don't involve a centralized server controlled by a third party.
- As such, Jabber® is more suitable for business users. Also, client software offered by proprietary instant messaging system are often targeted to casual users rather than business users.
- Jabber® provides a way for its user to communicate with users from legacy instant messaging platforms like Yahoo!® Instant Messenger, AIM®, MSN® Messenger or ICQ®
- Jabber® is more personalized. Unlike with some of proprietary instant messaging services, it identifies its users with a notation similar to email addresses (user@domain).
- Jabber® supports multiple login. It means you can remain connected at the office, while you connect with the same username from your home.
- Jabber® client software is available on almost all operating system.
- There are several free Jabber® account providers to

register from if the ISP doesn't provide it already.

Creating Jabber® Account

In **indoglobal**.com, your email account doubles as your Jabber® account with an exception: your subdomain email account cannot be used as a Jabber® account. For example: if you create an email account joe@example.com, then the respective Jabber® account is also joe@example.com. However, an email account nick@london.example.com doesn't have a Jabber® account because london.example.com is a subdomain.

Note

We made the Jabber® account the same as email account in order to simplify administration and to reduce confusion. However, there are Jabber® servers that don't follow this rule. You shouldn't assume a Jabber® account is also a working email address, or vice versa.

Tip

The same password is used for both email service and Jabber® service. You can change password from a Jabber® client and the email password will be changed too, and vice versa.

To create an email account (and thus a Jabber® account), please refer to the section called “Creating a New Email Account” [72].

Using Jabber® Client Psi

Unlike proprietary instant messaging platform, there are several client implementations of Jabber®. We provide official support for Psi [http://psi.affinix.com] on Microsoft® Windows® or Linux platform. However there are several other clients [http://www.jabber.org/software/clients.php] if you wish to use them.

In this section we will discuss Psi exclusively. They might of might not apply to other clients. However the basic concept is the same.

Starting With Psi

To download Psi, you need to visit their homepage [http://psi.affinix.com]. Psi is available for Linux, Microsoft® Windows® and MacOSX. Make sure you download Psi for the right platform. To install Psi please follow the instruction that goes with the download.

After running Psi for the first time, you will be greeted by the profile menu. To run Psi for the first time, please follow the next steps:

1. You need to create a profile if you want to use Psi. Click on *Profiles* and then click *New*. On the *Profile Name* field, please add a descriptive name and then click *OK*.

2. You will be taken back to the previous menu and your just created profile should be pre-selected. Click *Open* to start Psi with the profile.

3. Now you will be greeted by *Add Account* menu. Please add a descriptive name for your Jabber® account and then click *Add*. Make sure you don't have the *Register new account* checkbox unchecked.

4. The *Account Properties* menu will appear. On the *Account* tab, please specify your Jabber® ID, for example: 'joe@example.com'. There is also the *Resource* field. Resource is an additional string that identifies your session. Jabber® supports multiple open session, i.e. you can open a new session without shutting down the previous connection. To identify multiple session, you need to change the *Resource* field to something more descriptive. For example, use 'Work' for the session you left at work, and 'Home' for the session you use from home. Priority is the priority of the session. The client with highest priority will receive be the one who receive all incoming events.

5. On the *Connection* tab, please check the *Allow Plaintext Login* checkbox.

6. Click *Save* to continue.

If everything is fine, Psi should now be connected to the server, congratulations!

Using Gateways to Legacy Networks

Ideally, everybody should be using the same instant messaging protocol, just like email. However, we don't live in a perfect world. There are no less than four different popular instant messaging protocol in use today, and that's not counting Jabber®. This makes it hard for average users to communicate with all their friends. They usually end up with several instant messaging accounts and several clients running simultanously.

Jabber® tries to alleviate this problem by introducing a feature called gateway. Gateway is a program on the server that translates events coming from and into other instant messaging networks transparently, so that a Jabber® user can see the events as if it is a normal Jabber® events.

In order to use this feature. A Jabber® user will need to register first. For Psi, please follow the next steps.

1. Click the menu button (the lower left one), and then choose *Service Discovery*. The *Service Discovery* dialog will appear. Please give the program a little time to

download the list of available services from the server.

2. There should be at least four services that can be used as a gateway: AIM Gateway, ICQ Gateway, MSN Gateway and Yahoo! Gateway. Each can be used to connect to the respective instant messaging network. To connect to one, right click on a gateway service, and then click register. Now carry on with the instruction on the next dialog. At least you will be asked your username and password to connect to the other network, but sometimes you will be asked more questions.

3. After successfully registrating with a gateway. The gateway in question will appear in your roster window. You might need to authorize it before it can function properly. Watch your roster window for this.

4. For most network, the gateway will then gather your existing contact list from the legacy servers. They should appear shortly after you successfully register with the gateway.

Note

You can instruct Jabber® to connect or disconnect to a specific instant messaging network by right clicking the gateway name on your roster and then click *Log on* or *Log off* respectively.

Adding Jabber® Contacts

Instant messaging is not useful if you have no contact on your roster. To add new contact, please do the following steps:

1. Click on the menu button (by default it is on the bottom left corner). Then click *Add a contact*.

2. The *Add User* dialog should appear. Specify the Jabber® ID of your contact and then click *Add*.

Note

You will need to wait for his/her authorization before you will see his/her status on your Jabber® roster

Adding Contacts from Legacy Networks

Adding contacts from a legacy network (AIM, ICQ, Yahoo!, or MSN) is very similar to adding Jabber® contacts. The difference is that you need to translate nickname/handle convention used in legacy networks into Jabber® convention. Conversion examples below:

- For ICQ, the format is 'UIN@icq.gateway'. For example, if your UIN of your friend is '1277851', then his translated

Jabber® ID is: '1277851@icq.gateway'

- For AIM, the format is 'screenname@aim.gateway'. For example, if your friend's AIM screen name is 'johndoe', then his translated Jabber® ID is 'johndoe@aim.gateway'
- For Yahoo!, the format is 'yahoousername@yahoo.gateway'. For example, if your friend's Yahoo! username is 'johndoe', then his translated Jabber® ID is johndoe@yahoo.gateway.
- For MSN, the format is 'MSNusername@msn.gateway' but substitute the '@' sign on every MSN username with '%'. For example, if your friend's MSN username is 'john@hotmail.com', then his translated Jabber ID is 'john%hotmail.com@msn.gateway'.

Important

You need to register with gateway before you can add user from the respective gateway, please see the section called “Using Gateways to Legacy Networks” [87] for more information.

After figuring out your friend's translated Jabber ID, then you will be able to add him/her as if he/she is a normal Jabber® user.

Note

Jabber® doesn't support all features offered by legacy clients.

Tips for Using Jabber®

There are free Jabber® servers from all over the world. The list is available from Jabber® web site [http://www.jabber.org/user/publicservers.php]. If your (non indoglobal.com customer) friends want to get into Jabber® bandwagon, you can give them the server list, so they can register themselves.

Jabber® is an open protocol and therefore easy to program. There are Jabber® libraries for all popular programming languages, the list is available from http://www.jabber.org/software/libraries.php. The possibility is endless, for example you could build a notification system to notify you when someone submits a form on your web site. For more example on how these can be done please see http://www.pipetree.com/jabber/fwj.html. There are also numerous Jabber® resources on the Internet.

Appendix A. FTP Clients Configuration

To log on to FTP account, you will need your username and your password. For more information about FTP and logging on to FTP please see the section called “Transferring Files Using FTP” [21]. The examples below will assume your domain name is example.com, your account username is u777 and you are connecting to your main FTP account (not subdomain FTP account).

Microsoft® Windows® My Network Places

The following is how to connect to FTP server using the built in My Network Places feature of Microsoft® Windows® XP Professional. Other versions of Microsoft® Windows® may support My Network Places but the steps involved could be slightly different.

Before you can use My Network Places to connect to FTP server, you will need to add a network place first.

1. Click *Start* and choose *My Network Places*. My Network Places window should appear.
2. Click *Add a network place*. This should present you with Add Network Place Wizard. Click *Next* when done with the introduction.
3. Windows will try to fetch information from the Internet. After a while a menu will appear, choose *Choose another network location* and then click *Next*.
4. On the next screen you need to specify the location of the FTP server. Assuming your account username is u777 and your domain is example.com, specify ftp://u777@primary-ip.example.com. Click *Next* to contine.
5. On the next screen, you can specify a descriptive name of the network place you've just created. Click *Next* and then click *Finish*.

After the FTP server has been added to My Network Place, it is easy to connect to the FTP server.

1. Click *Start* and choose *My Network Places*. My Network Places windows should appear.
2. Double click on the network place you want to connect. You may be asked for a password.

3. When successful, a window showing your FTP network place should appear. Now you can use standard file operation (drag and drop, or cut/copy and paste) on this window.

FileZilla

FileZilla is a free FTP client for windows. It is a free software under GPL and can be downloaded for free from FileZilla's homepage [http://filezilla.sf.net].

To connect to our FTP server using FileZilla, please do the following steps, assuming your account username is u777 and your domain name is example.com.

- Launch FileZilla using Start menu. The FileZilla window should now appear.
- On the quick launch bar, specify 'primary-ip.example.com' in the Address field, 'u777' in the User field, and your account password in the Password field. Click *QuickConnect* to continue.
- After logged in, you are now able to perform file transfer within the Local site and Remote site panel.

Tip

On the subsequent connection attempt, you no longer have to type in your host, user and password every time you log on. FileZilla will remember your settings automatically. Click the arrow beside *QuickConnect* button to show the connections made previously.

KDE Konqueror

Konqueror is a file manager used under KDE. KDE is a desktop environment for Linux, UNIX and similar operating systems. To connect to FTP server using Konqueror please do the following steps.

- Open a Konqueror file manager window by clicking on the home icon on the taskbar.
- On the Location bar, specify ftp://u777@primary-ip.example.com. You may be asked for a password, specify it as necessary.
- After the window shows the contents of your account, you will be able to do file transfer by performing standard file operation like drag and drop or copying and pasting.

Tip

To save the location so you don't have to do the above steps everytime you want to make a connection, click *Bookmarks* and then *Add bookmark*. If you want to make the connection, you only have to choose the site in question from the bookmark.

GNOME Nautilus

Nautilus is a file manager for GNOME desktop environment for Linux, UNIX and similar operating systems. To connect to FTP server using Nautilus please do the following steps.

- Open a Nautilus file manager window by clicking on *Application* menu and then *Home Folder*. A Nautilus window should then appear.
- On the Location bar, specify ftp://u777:PASSWORD@primary-ip.example.com. Replace PASSWORD with your real password.
- After the window shows the contents of your account, you will be able to do file transfer by performing standard file operation like drag and drop or copying and pasting.

Tip

To save the location so you don't have to do the above steps everytime you want to make a connection, click *Bookmarks* and then *Add bookmark*. If you want to make the connection later, you only have to choose the site in question from the bookmark.

Appendix B. WebDAV Clients Configuration

Our WebDAV server is located on port 81. Port 444 is also open for HTTPS based WebDAV connections. For more information about WebDAV please see the section called "Using WebDAV to Manage Files" [25].

Microsoft® Windows® My Network Places

The following is how to connect to WebDAV server using the built in My Network Places feature of Microsoft® Windows® XP Professional. Other versions of Microsoft® Windows® may support My Network Places but the steps involved could be slightly different.

Before you can use My Network Places to connect to WebDAV server, you will need to add a network place first.

1. Click *Start* and choose *My Network Places*. My Network Places window should appear.
2. Click *Add a network place*. This should present you with Add Network Place Wizard. Click *Next* when done with the introduction.
3. Windows will try to fetch information from the Internet. After a while a menu will appear, choose *Choose another network location* and then click *Next*.
4. On the next screen you need to specify the location of the WebDAV server. If your WebDAV enabled subdomain is 'example.com', then specify the location as http://example.com:81/. Alternatively you can also specify https://example.com:444/ if you want to use secure version of WebDAV server. You will be asked for your username and password, specify the username and password set from Web User & Group menu from **SiteManager**. Press *Next* to continue.
5. On the next screen, you can specify a descriptive name of the network place you've just created. Click *Next* and then click *Finish*.

After the FTP server has been added to My Network Place, it is easy to connect to the FTP server.

1. Click *Start* and choose *My Network Places*. My Network Places windows should appear.
2. Double click on the network place you want to connect. You may be asked for a password.

3. When successful, a window showing your FTP network place should appear. Now you can use standard file operation (drag and drop, or cut/copy and paste) on this window.

KDE Konqueror

Konqueror is a file manager used under KDE. KDE is a desktop environment for Linux, UNIX and similar operating systems. To connect to FTP server using Konqueror please do the following steps.

Note

You need at least version 3.0 of KDE to use WebDAV feature.

- Open a Konqueror file manager window by clicking on the home icon on the taskbar.
- On the Location bar, specify webdav://username@example.com:81. Alternatively you can also use webdavs://username@example.com:444 if you want to use the secure version of WebDAV server. Replace username with your username set from *Web User & Group* menu from **SiteManager**. You will be asked for a password, specify it as necessary.
- After the window shows the contents of your account, you will be able to do file transfer by performing standard file operation like drag and drop or copying and pasting.

Tip

To save the location so you don't have to do the above steps everytime you want to make a connection, click *Bookmarks* and then *Add bookmark*. If you want to make the connection, you only have to choose the site in question from the bookmark.

GNOME Nautilus

Nautilus is a file manager for GNOME desktop environment for Linux, UNIX and similar operating systems. To connect to WebDAV server using Nautilus please do the following steps.

Note

You need to use GNOME at least version 2.0 to use WebDAV feature.

- Open a Nautilus file manager window by clicking on *Application* menu and then *Home Folder*. A Nautilus

window should then appear.

- On the Location bar, specify http://username:password@example.com:81. Replace username and password with the username and password from *Web User & Group* menu from **SiteManager**. Also replace example.com with your own WebDAV enabled subdomain. Alternatively, you can also use https://username:password@example.com:444 to use secure version of WebDAV server.

- After the window shows the contents of your account, you will be able to do file transfer by performing standard file operation like drag and drop or copying and pasting.

Tip

To save the location so you don't have to do the above steps everytime you want to make a connection, click *Bookmarks* and then *Add bookmark*. If you want to make the connection later, you only have to choose the site in question from the bookmark.

Appendix C. Email Clients Configuration

For more information about email please see *Email Management* [71]. In this appendix, it is assumed that your domain name is example.com, your email address is 'username@example.com' and your email password is 'password'. Please note that the email username & password is set from the *Email* menu from **SiteManager**, not your account's username & password. It is also assumed that you haven't changed the default subdomain configuration of subdomains pop.example.com, imap.example.com and smtp.example.com.

Microsoft® Outlook Express®

Microsoft® Outlook Express® is the default email client shipped by most versions of Microsoft® Windows®. The examples below is done with Microsoft® Outlook Express® version 6 shipped with Microsoft® Windows® XP Professional.

Warning

Microsoft® Outlook Express® is often used as carrier of viruses and worms. Always make sure you have installed the latest security patch from Microsoft before running Microsoft® Outlook Express®. Alternatively you can use a better email client.

To configure Microsoft® Outlook Express® to download email from our server, please do the following steps.

1. Run Microsoft® Outlook Express® from the Start menu.
2. After Microsoft® Outlook Express® window appears, click *Tools* and then *Accounts*.
3. *Internet Accounts* window will appear, click *Add* and then *Mail*.
4. On the *Display name* field, enter a descriptive text for this email account, for example "My email account". Click *Next* to continue.
5. On the *Email address* field, enter your email address, as in 'username@example.com'. Click *Next* to continue.
6. On the next screen you need to specify email server names. If you want to use POP3, specify 'My incoming mail server is a POP3 server', you also need to specify 'pop.example.com' on your incoming mail server field, substituting 'example.com' with your real domain name.

If you want to use IMAP, specify 'My incoming mail server is a IMAP server', you also need to specify 'imap.example.com' on your incoming mail server field, substituting 'example.com' with your real domain name.

7. On the outgoing mail server field, specify 'smtp.example.com' (substituting example.com with your real domain name) Click *Next* to continue.

8. On the next screen, specify your complete email address (as in username@example.com) in the *Account name* field. Also specify your password in the *Password* field. You need to clear the *Log on using Secure Password Authentication* checkbox if it isn't already cleared. Click *Next* and then *Finish* to continue.

9. Select the account name you have just created, and then click *Properties*. Click on the *Servers* tab and on the *Outgoing Mail Server* section check the *My server requires authentication*. Click on *Settings* and then select *Use same settings as my incoming mail server*. Click *OK*. Click on the *Advanced* tab. Specify '8025' or '587' in the *Outgoing mail (SMTP)* fields. Click *OK* and then *Close* to finalize the configuration.

Qualcomm Eudora

Eudora is a popular email client available for download from its web site [http://www.eudora.com]. To configure Eudora for use with your account, please do the following steps. On the steps below we are using Eudora version 6 under Microsoft® Windows®.

1. Click *Tools* and then *Personalities*.

2. Right click on the personalities area and then click *New*. The New Account Wizard will appear.

3. Choose *Create a brand new email account* and click *Next*.

4. Enter a text describing the account you want to create in the *Personality name* field, for example 'My Email Account'. Click *Next* to continue.

5. Enter your name in *Your Name* field. Click *Next* to continue.

6. Enter your complete email address as in 'username@example.com' in the *Email Address* field. Click *Next* to continue.

7. Enter your complete email address as in 'username@example.com' in the *Login Name* field. Click *Next* to continue.

8. In the Incoming email server, specify 'pop.example.com' if you want to use POP3 or 'imap.example.com' if you want to use IMAP (substituting example.com with your real domain name). Also choose whether if you want to

use POP or IMAP on the selection on the bottom. Click *Next* to continue.

9. Specify 'smtp.example.com' (substituting example.com with your real domain name) as your *Outgoing Server* and check the *Allow authentication* checkbox. Click *Next* and then *Finish*.

10. Right click on the account you have just created and then choose *Properties*.

11. On the *Secure Sockets when Sending* section, choose 'Never'. Click on the *Incoming Mail* tab. On the *Secure Sockets when Receiving* section, choose 'Never'. Click *OK* to finalize the settings.

Unfortunately Eudora doesn't provide an easy way to change the SMTP port number which is required if you decide to use **indoglobal**.com's SMTP server. Please do the additional steps below if you wish to use our server's SMTP server for sending emails.

1. Close Eudora if it is running.

2. Look for a file inside your `C:\WINDOWS` directory (or where you installed Windows) named 'services' and open it with a text editor such as notepad. The exact location of this file could be different with different version of Microsoft® Windows®, use the search/find function of the operating system to locate the file.

3. Change the line that says 'smtp 25/tcp' to 'smtp 8025/tcp' or 'smtp 587/tcp'. Save the file.

4. Open the directory where you installed Eudora (i.e. `C:\Program Files\Qualcomm\Eudora`). Enter the directory `extrastuff`. Inside this directory is a file `esoteric.epi`. Move this file to the main Eudora directory.

5. Start Eudora. Go to *Tools* and then *Options*. Locate the *Ports* menu on the left pane and click it. Specify '8025' or '587' in the *SMTP Port* field. Click *OK* to continue.

Warning

Please note that changing the SMTP port number will affect ALL your personalities including those not hosted on our server.

KDE KMail

KMail is the email client shipped with KDE, a desktop environment for Linux, UNIX and similar systems. The following steps describes the steps required to configure email on KMail under KDE 3.

1. Click *Settings* and then *Configure KMail*. The Configure

KMail window will then appear.

2. Click on *Identities* menu on the left pane. Click *New* to create a new identity.

3. Enter a descriptive name on the *New identity* field as in 'My Email Account'. Select *With empty fields* and then click *OK*.

4. Enter your name, organization and email address in the *Your Name*, *Organization*, and *Email address* fields respectively. Click *OK* to continue.

5. Click on *Network* menu on the left pane. Click the *Sending* tab and click *Add*.

6. Choose *SMTP* as the transport. Click *OK* to continue. Enter a descriptive name on the *Name* field such as 'SMTP server'. Specify 'smtp.example.com' (replacing example.com with your own domain name) in the *Host* field. You also need to specify '8025' or '587' in the *Port* field, check *Server requires authentication* and then specify your complete email address in the *Login* field and its password.

7. Click the *Receiving* tab and then click *Add*.

8. You can choose *POP3* or *IMAP* depending if you want to use POP3 or IMAP for downloading your email. Click *OK* to continue.

9. Specify your complete email address in the *Login* field. Specify 'pop.example.com' or 'imap.example.com' in the *Host* field substituting example.com with your own domain name. Click *OK* to continue.

10. Click *OK* to finalize the configuration.

Novell Evolution (formerly Ximian Evolution)

Novell Evolution is the default email client in the GNOME desktop environment. In the steps below, it is assumed that Novell Evolution version 1.2 is used.

1. Click on *Tools* menu and then *Settings*.

2. Click *Mail Accounts* on the left pane, and then click *Add*. The Evolution Account Assistant Wizard will then appear. Click *Next* to continue.

3. Specify your full name in the *Full name* field and your email address in the *Email address* field, respectively. Click *Next* to continue.

4. Choose POP or IMAP on the *Server Type* drop down box depending on whether you want to use POP or IMAP. Specify 'pop.example.com' or 'imap.example.com' (substituting example.com with your real domain name)

on the *Host* field depending whether you want to use POP or IMAP. Specify your complete email address (as in 'username@example.com) in the *Username* field. Click *Next* to continue.

5. On the next screen, choose the options accordingly depending on your own preferences. Click *Next* to continue.

6. Choose SMTP in the *Server Type*. Specify 'smtp.example.com:8025' or 'smtp.example.com:587' (substituting example.com with your own domain name) in the *Host* field. You also need to check the *Server requires authentication* checkbox, and specify your complete email address (as in 'username@example.com') in the *Username* field. Click *Next* to continue.

7. On the next screen, you can specify a descriptive name for this account in the *Name* fields. Click *Next* to continue. Click *Finish* to finalize the settings.

Mozilla Mail

Mozilla Mail is a part of Mozilla web browser available for download from Mozilla.org [http://www.mozilla.org]. The following steps describe email configuration for Mozilla Mail version 1.4.

1. Open Mozilla Mail window, either by clicking on its icon from menu or by clicking the *Mail & Newgroups* icon on the lower left part of Mozilla web browser window.

2. Click on *Edit* and then *Mail & Newgroups Account Settings*.

3. Click *Add Account*. On the first screen select *Email account* and then click *Next*.

4. Specify your name in the *Your Name* field and your email address in the *Email Address* field. Click *Next* to continue.

5. On the next screen you can choose POP or IMAP depending on whether you want to use POP or IMAP. You also need to specify 'pop.example.com' or 'imap.example.com' (replace example.com with your own domain name) in the *Incoming Server* field. Click *Next* to continue.

6. Specify your full email address in the *User Name* field. Click *Next* to continue.

7. Specify a descriptive name for this account, for example 'My Email Account'. Click *Next* and then *Finish* to continue.

8. Now you should be taken back to the *Mail & Newsgroups Account Settings* menu. Click on *Outgoing*

Server (SMTP).

9. Specify 'smtp.example.com' in the *Server Name* field. You also need to specify '8025' or '587' in the *Port* field and specify your email address in the *User Name* field.

10. Click *OK* to finalize the settings.

Index

Symbols

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

W

X

Z