

SquareOne Personal Internet Server
SQ201-N(wired) / SQ201-W(wireless)
User's Guide
(Ver 1.2)

Copyright

Copyright © 2007 ITian Corporation All rights reserved.

Square One is trademarks of ITian Corporation. Other trademarks are the property of their owners. Specifications subject to change without notice.

FCC Notice – Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

CE Notice –Class B

Warning!

This is a Class B product. In a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

Achtung !

Square One User's Guide

Dieses ist ein Gerät der Funkstörgrenzwertklasse B. In Wohnbereichen können bei Betrieb dieses Gerätes Rundfunkstörungen auftreten, in welchen Fällen der Benutzer für entsprechende Gegenmaßnahmen verantwortlich ist.

Avertissement!

Cet appareil est un appareil de Classe B. Dans un environnement résidentiel cet appareil peut provoquer des brouillages radioélectriques. Dans ce cas, il peut être demandé à l'utilisateur de prendre les mesures appropriées.

VCCI-B

This equipment is a Class B product (information equipment to be used in commercial and/or industrial areas) and conforms to the standards set by the Voluntary Control Council for Interference by Data Processing Equipment and Electronic Office Machines aimed at preventing radio interference in commercial and/or industrial areas. Consequently, when used in a residential area or in an adjacent area thereto, radio interference may be caused to radios and TV receivers. Read the instructions for correct handling.

この装置は、クラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI- A

Table of Contents

About Your Square One Personal Server	6
<i>Safety Precautions.....</i>	<i>7</i>
<i>Specifications & Package contents</i>	<i>8</i>
<i>Product Exterior</i>	<i>10</i>
Setting Up Your Square One Personal Server	12
<i>Setting up your Personal Server as your router</i>	<i>13</i>
<i>Setting up your Personal Server behind an external router</i>	<i>16</i>
<i>Setting Up Dynamic DNS.....</i>	<i>18</i>
<i>Adding user accounts.....</i>	<i>19</i>
Using Your Square One Personal Server	20
<i>Using network shares.....</i>	<i>21</i>
Accessing a share in Windows.....	22
Accessing a share in Mac OS X or Linux.....	22
Mapping a share to a drive letter (Windows only).....	23
<i>Using external storage devices</i>	<i>24</i>
Using a USB drive	24
Using a USB memory card reader	24
Using an eSATA drive	25
<i>Sharing a USB printer.....</i>	<i>26</i>
Adding a shared printer to your computer	26
Printing to a shared printer.....	29
<i>Managing users, groups, and shared folders.....</i>	<i>30</i>
Why create user accounts, groups, or additional shared folders?.....	30
Creating, modifying, and deleting user accounts.....	30
Creating, modifying, and deleting groups	31
Creating, modifying, and deleting shared folders.....	32
<i>Using the BitTorrent client</i>	<i>34</i>
Working with torrents.....	34
<i>Using Casgle Broadcatcher</i>	<i>35</i>
<i>Using the preinstalled web applications</i>	<i>39</i>
Advanced Topics.....	41
<i>Accessing your Personal Server remotely.....</i>	<i>41</i>

Square One User's Guide

Using network shares remotely	42
Access files remotely with FTP or SFTP	43
Accessing files remotely using a web browser	44
Accessing the server remotely through an external router	46
<i>Setting up a website</i>	<i>48</i>
Uploading website files to the server	48
Managing local write access to web files	49
<i>Forwarding incoming connections</i>	<i>50</i>
Introduction to port forwarding	50
Choosing a port forwarding method	51
Creating and editing port mapping rules	52
Creating and editing port triggering rules	53
<i>Managing storage devices</i>	<i>55</i>
About disk encryption	56
<i>Upgrading your Personal Server</i>	<i>57</i>
Upgrading the server's software	57
Upgrading the internal hard drive	58
<i>Accessing the command line interface</i>	<i>60</i>
Executing commands with elevated privileges	61
Product Registration	62
Product Warranty	63

Part One

About Your Square One Personal Server

Congratulations on acquiring your Square One Personal Server, the most versatile network appliance in the world.

Before you begin using your new Personal Server, please read the following pages to familiarize yourself with important information about the product.

Safety Precautions

Please read these safety instructions and precautions carefully before using your Square One Personal Server.

- Use a grounded electrical outlet.
- Place the server where there is good ventilation. There should be at least three inches of clearance on all four sides.
- Do not place the server where it could be exposed to high temperature or direct sunlight.
- Do not put wet or heavy objects on top of the server.
- Do not install or leave the server, its power cable, or LAN cables in areas of heavy foot traffic.
- Do not install the server in areas of high humidity (bathrooms and areas exposed to rain or splashing water).
- Keep the server out of reach of infants and young children.
- Use only good quality cables.
- Place the server on a level and stable surface.

Specifications

Product name:	Square One Personal Server SQ201N / SQ201W
Hard disk drive:	3.5" SATA Fluid Dynamic Bearing
Processor:	300-MHz ARM9 32-bit RISC CPU w/ 16KB L1 cache
Memory:	128 MB DDR SDRAM / 16 MB Flash ROM
Network interfaces:	1 x Gigabit Ethernet WAN port 4 x Gigabit Ethernet LAN ports 802.11 b/g Wireless (SQ201-W model only)
Expansion ports:	3 x USB 2.0 (support drives, printers, memory card readers) 1 x eSATA
External drive support:	FAT32, NTFS, XFS, ext2, ext3
Internet services:	HTTP, WebDAV, FTP, SFTP, Telnet, SSH, POP, SMTP, Samba, OpenVPN
Dimensions:	62 x 200 x 200 millimeters (2.44 x 7.87 x 7.87 inches) HWD
Weight:	about 1.3 kg (2.87 lbs), depending on installed hard drive
Power:	Adapter input: 90–200V AC, 50/60 Hz Adapter output: 12V DC, 4A Max power consumption: 24W
Certifications:	FCC Class B, CE, MIC Class B, CTick, CSA
Operating temperatures:	0°–40° C (32°–104° F)
Warranty:	1 year

Package contents.

SquareOne package contains the followings. If any of the below contents are missing, please enquire at the place of purchase.



SquareOne Main Body – 1EA



LAN Cable – 1EA



Power Adapter – 1EA



Power Cable – 1EA



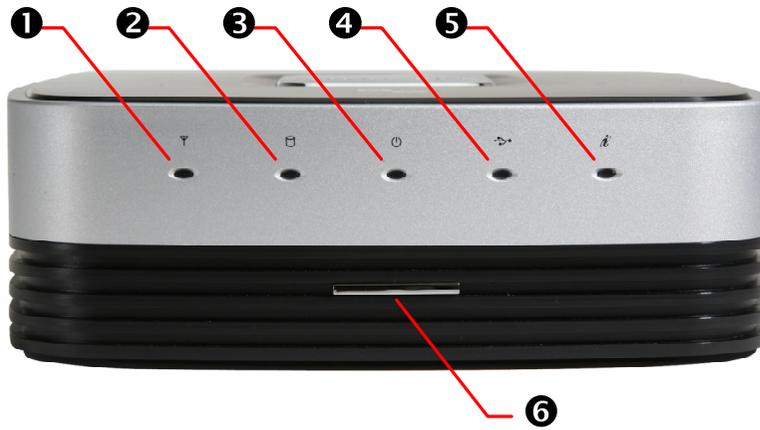
Antenna – 2EA
(Wireless model only)



SquareOne User's Guide - 1EA

Product Exterior

Front



1 Wireless LAN Status Indicator

EXPLANATION NEEDED

2 HDD Activity Indicator

Blinks when the internal hard drive is being accessed.

3 Power Status Indicator

EXPLANATION NEEDED

4 USB Status Indicator

EXPLANATION NEEDED

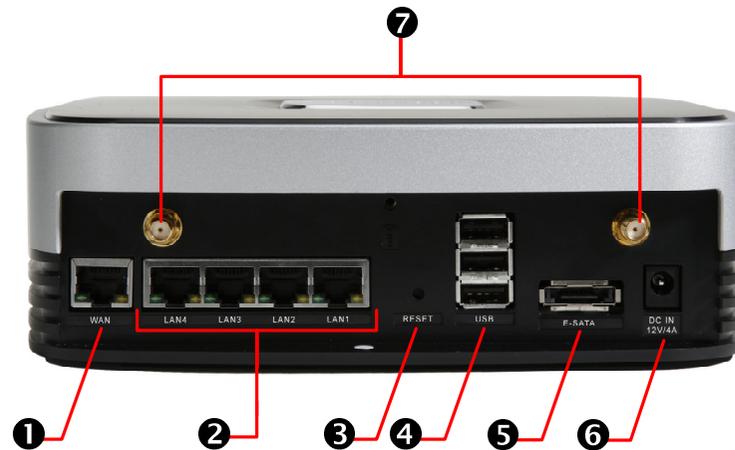
5 WAN Status Indicator

EXPLANATION NEEDED

6 Power Button

Press to turn the Personal Server on. Press and hold for at least one second to turn the Personal Server off.

Rear



1 WAN Port

Connect your broadband modem or primary router here.

2 LAN Ports

Connect wired clients here.

3 Factory Reset Button

Using a thin object such as a straightened paper clip, push this to reset all settings to factory defaults.

4 USB 2.0 Ports

Connect external USB drives, memory card readers, and/or a USB printer here.

5 eSATA Port

Connect an external eSATA drive here.

6 DC Input

Plug the Personal Server's external power supply in here.

7 Antenna Mounts (SQ201-W models only)

If you have a wireless Personal Server, screw its antennas in to these mounts.

Part Two

Setting Up Your Square One Personal Server

The way you set up your Square One Personal Server depends on whether you will use it as both a server and a router, or only as a server in conjunction with another router.

The following sections contain setup instructions for the most common network configurations. Please make sure to follow only the instructions for the configuration you intend to use.

Setting up your Personal Server as your router

Follow these instructions if you intend to use your Personal Server as your (only) router, in addition to using it as a server. In this configuration, the Personal Server connects directly to your broadband modem, and your computers connect directly to the Personal Server (see Figure 1).

Step 1: Prepare Your Computers

Configure each of your computers to obtain an IP address automatically (using DHCP). The instructions below are for computers running Windows XP. If your computer runs another operating system, please refer to your OS's network documentation.

1. On the Start menu, click **Control Panel**, and then double-click **Network Connections**.
2. If the computer will connect wirelessly, right-click the **Wireless Network Connection** icon, and then click **Properties**. Otherwise, right-click the **Local Area Connection** icon, and then click **Properties**.
3. On the **General** tab, find the box labeled **This connection uses the following items** and scroll down the list until you see **Internet Protocol (TCP/IP)**. Double-click **Internet Protocol (TCP/IP)**.
4. Make sure the options **Obtain an IP address automatically** and **Obtain DNS server address automatically** are selected (see Figure 2), and then click **OK**.
5. Click **OK** to close the connection properties window.

Note: If your Internet connection uses Point-to-Point Protocol over Ethernet (PPPoE), you must disable the PPPoE login window, since PPPoE login will be handled by your Personal Server from now on. If your Internet connection does not use PPPoE, you can skip these instructions.

1. On the Start menu, click **Control Panel**, and then double-click **Internet Options**.
2. On the **Connections** tab, select **Never dial a connection**, and then click **OK** (see Figure 3).

Step 2: Connect the Personal Server to Your Broadband Modem

1. Turn your broadband modem off.

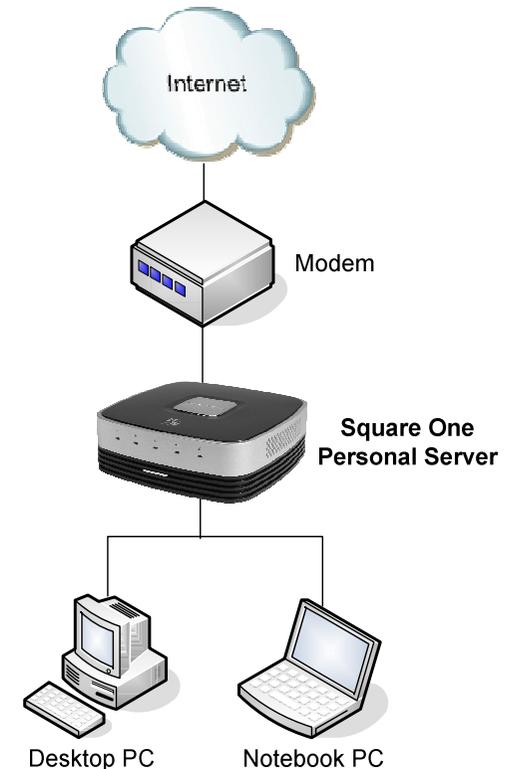


Figure 1

Square One User's Guide

2. Plug one end of the supplied Ethernet cable into your modem's Ethernet port and the other end into the WAN port on the back of the Personal Server (see Figure 4).
3. Connect the Personal Server's AC adaptor to the power port on the Personal Server and plug the adaptor into an electrical outlet.
4. Turn your modem on. Wait until the modem's Internet light is steady before continuing.
5. Turn your Personal Server on by pressing the chrome button on the front.

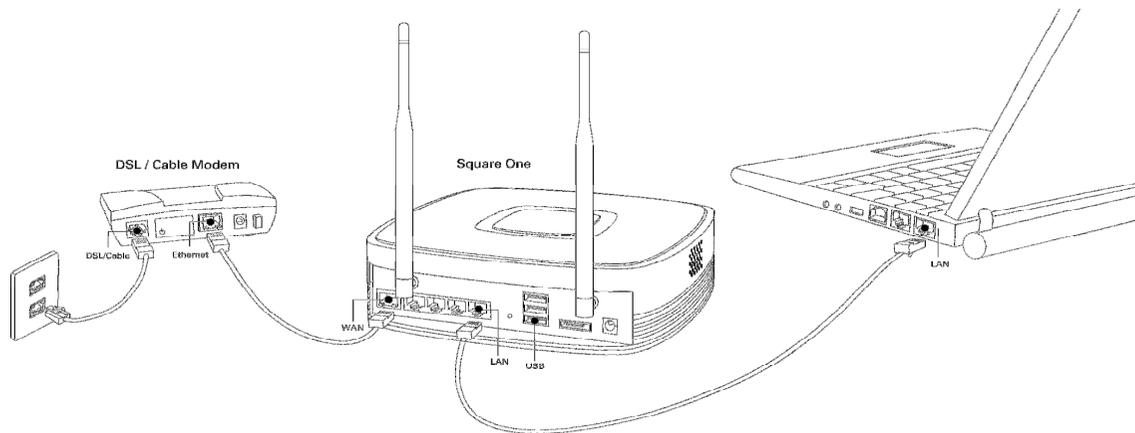


Figure 4

Step 3: Connect Your Computers to the Personal Server

Connecting through an Ethernet cable

1. Plug one end of an Ethernet cable (Cat 5 or higher) into one of the four LAN ports on the back of the Personal Server, and plug the other end into your computer's LAN or Ethernet port (see Figure 4).
2. If the computer is off, turn it on.

Connecting wirelessly (SQ201-W only)

1. If the computer is off, turn it on.
2. Using your wireless network browser, locate and connect to your Personal Server's wireless network at the network name (SSID) **SquareOne**.

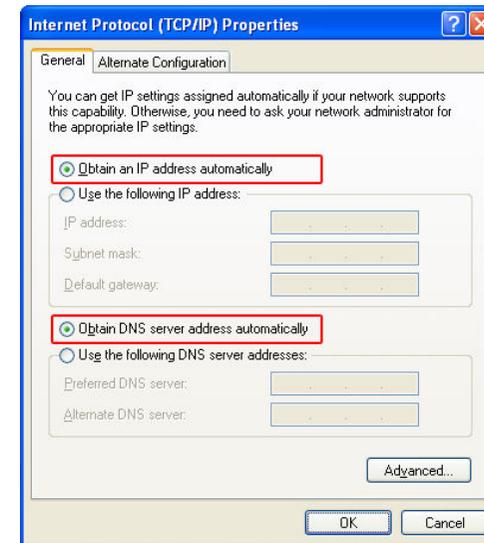


Figure 2

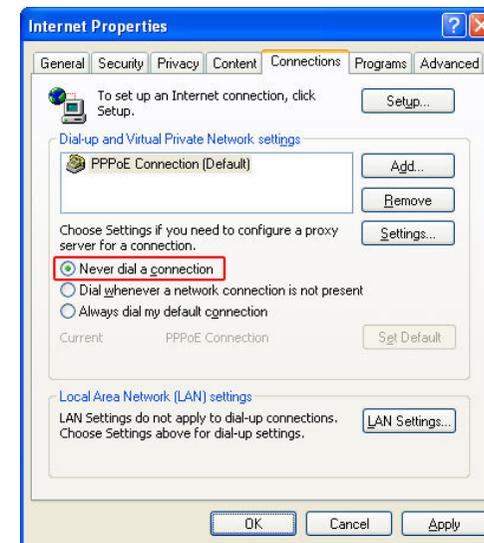


Figure 3

Step 4: Configure Your Personal Server's Network Settings

1. On a computer connected to your Personal Server, open a browser window. In the address bar, type <http://squareone:8090/> and press Enter.
2. Log in to the administrative interface with username "admin" and password "admin".
3. In the navigation menu on the left side of the window, under **Setup Wizard**, click **Basic Settings** (see Figure 5).
4. Complete the setup wizard to configure your Personal Server for Internet connectivity.

Step 5: Check Internet Connectivity

After you finish the setup wizard, make sure your computer can connect to the Internet by trying to visit a Web site. If you cannot access the Web, you may need to change your Personal Server's network settings. To do so, open your web browser, go to <http://squareone:8090/>, log in as "admin", and click **Network** on the main menu.

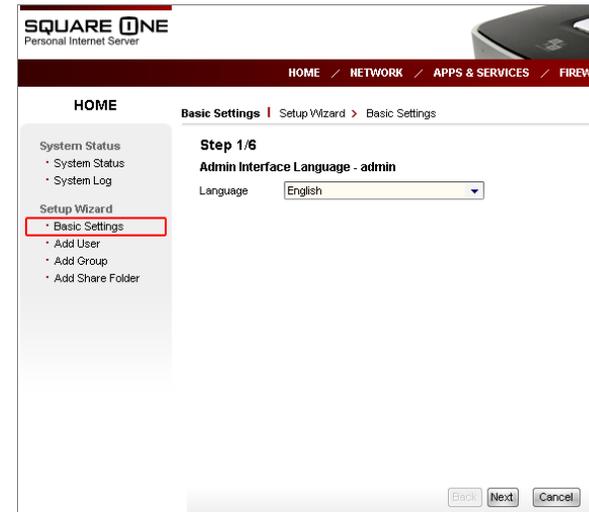


Figure 5

Setting up your Personal Server behind an external router

Follow these instructions if you intend to use your Personal Server as a server only, in conjunction with an external router. In this configuration, both your computers and the Personal Server connect to your router, and your computers access the Personal Server through the external router (see Figure 6).

Note

If you set up your Personal Server behind another router, you will not be able to access the Personal Server from a remote location (over the Internet) unless you configure your router to “forward” certain network ports to the Personal Server, depending on which services you want to make available remotely. Please refer to **Accessing the server remotely through an external router** and your router's documentation for more information.

Step 1: Configure Your Personal Server to Use a Static IP Address

You should configure your Personal Server to use a static IP address on its WAN interface, so that you can always access it at the same IP address. To complete this step, you will need to temporarily connect a PC directly to the Personal Server in order to access its admin interface. Afterwards, you can disconnect the PC from the Personal Server.

1. Connect the Personal Server's AC adaptor to the power port on the Personal Server and plug the adaptor into an electrical outlet.
2. Turn your Personal Server on by pressing the chrome button on the front. Before continuing, wait at least one minute for your Personal Server to finish starting up.
3. Connect a computer to your Personal Server by plugging one end of the supplied Ethernet cable into one of the four LAN ports on the back of the Personal Server and the other end into your computer's LAN or Ethernet port. If the computer is off, turn it on.
4. On the connected computer, open a browser window. In the address bar, type <http://squareone:8090/> and press Enter.
5. Log in to the administrative interface with username “admin” and password “admin”.
6. On the main menu at the top of the page, click **Network**. On the left-side menu, under **WAN**, click **Basic Settings** (see Figure 7).

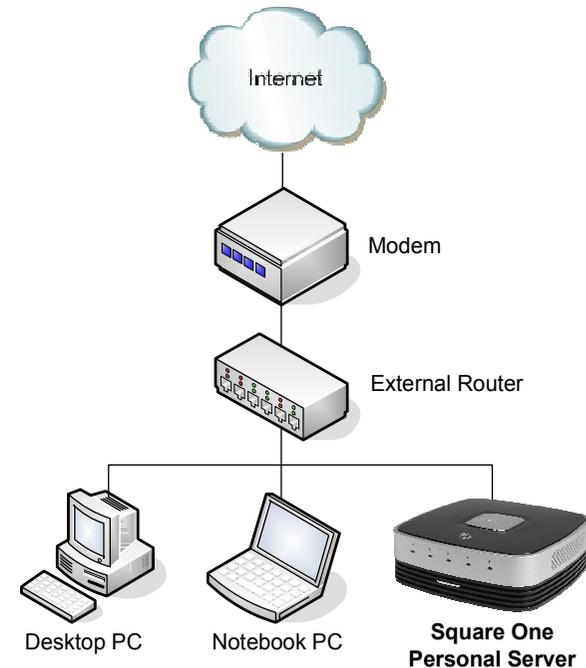


Figure 6



Tip
Instead of configuring the Personal Server to use a static WAN IP address, if you prefer, you can achieve the same result by configuring your router to assign a fixed IP address to the Personal Server, based on its WAN MAC address. (This is often called Static DHCP or Fixed DHCP.) Your Personal Server's WAN MAC address is printed on the bottom of the server. Please refer to your router's documentation for more information.

Square One User's Guide

7. Set **WAN mode** to **Static IP**.
8. In **IP address**, enter the IP address you want your Personal Server to use. For example, if your router's LAN IP address is 192.168.1.1, you might enter 192.168.1.100. Make sure to specify an address that is not already in use by any other device on the router's network. The address should be outside the range of addresses your router assigns to DHCP clients.
9. Enter appropriate values in **Subnet mask** and **Default gateway**. If you are not sure what the subnet mask of your router's network is, try 255.255.255.0. The default gateway address is usually the same as your router's LAN IP address.
10. In the **DNS server 1** fields, enter your router's LAN IP address. Optionally, you may enter backup DNS server addresses in **DNS server 2** and **DNS server 3**.
11. Click **Save**.

You may now physically disconnect the computer from your Personal Server.

Step 2: Connect the Personal Server to Your Router

Plug one end of the supplied Ethernet cable into the WAN port on the back of the Personal Server and the other end into one of the LAN ports on your router.

Step 3: Check Connectivity

Check whether you can access your Personal Server through the router. On a computer that is connected to the router (not directly to the Personal Server), open a browser window and try viewing the Personal Server's default web page at **http://ip_address**, where *ip_address* is the static WAN IP address you assigned to the Personal Server. For example, if you assigned the Personal Server the address 192.168.1.100, enter **http://192.168.1.100** in your browser. You should see the server's default home page.

If you cannot access the default home page, shut down the Personal Server and turn it on again. To shut down the server, press and hold the power button for at least five second. Press the button again to turn the server on. Wait at least two minutes for the web service to become ready, and then try to access the default home page again.

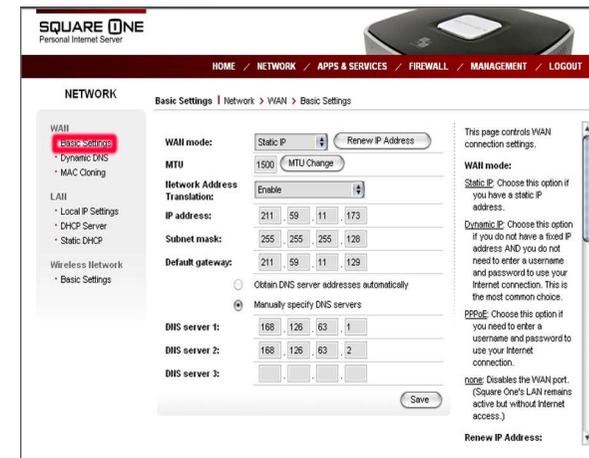


Figure 7

Setting Up Dynamic DNS

If you intend to access (or allow others to access) your Personal Server remotely—across the Internet—and your public IP address is not static, you should configure your Personal Server to send IP address updates to a Dynamic DNS (DDNS) service. Then, you will always be able to access your Personal Server at the specified hostname, even if its public IP address changes.

Note

If your Personal Server is behind another router, do not enable Dynamic DNS updating. Because the Personal Server does not “know” your true public IP address in this network configuration, it will send a publicly-inaccessible private IP address to the DDNS provider. In this case, enable DDNS on the router instead. Please refer to your router’s documentation.

Before you can use the server’s DDNS update feature, you must create an account with a Dynamic DNS service provider. On the Dynamic DNS admin page, check the **DDNS provider** menu to see which service providers are supported.

To set up Dynamic DNS updating

1. Access your Personal Server’s admin interface at <http://squareone:8090/>.
2. On the main menu, click **Network**. On the left-side menu, under **WAN**, click **Dynamic DNS** (see Figure 8).
3. Next to **DDNS updater**, click **Enable**.
4. Select a DDNS provider and enter your username, password, and hostname.
5. Click **Save**.

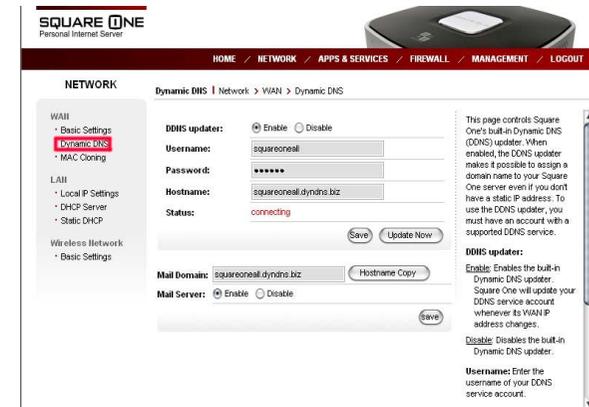


Figure 8

Adding user accounts

If you will be sharing your Personal Server with others, you should create an account for each user. This lets you control how much disk space each user can use and which shared folders each user can access.

1. Access your Personal Server's admin interface at <http://squareone:8090/>.
2. On the main menu, click **Management**. On the left-side menu, under **Users & Groups**, click **Users** (see Figure 9).
3. Enter a username, a password, and (optionally) a description in the provided fields.
4. If you want the user to have his or her own private folder, select **Create private folder**.
5. If you want to limit how much internal disk space the user can occupy, select **Enable disk quota** and enter the limit in MB.
6. Click **Save**.
7. Repeat steps 3–6 for each user you want to create.

Later, if you wish, you can create shared folders (called *shares*) and decide which users can access each one. You can also create *groups* of users, allowing you to grant or deny access to specific shares for several users at once. For more information, see **Managing users, groups, and shares**.

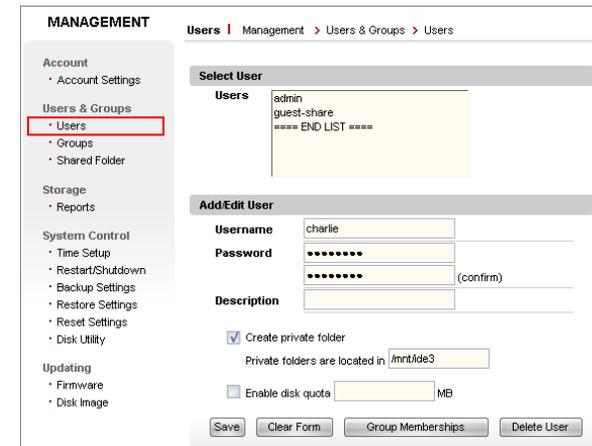


Figure 9

Part Three

Using Your Square One Personal Server

Your Square One Personal Server offers a wealth of functionality. This chapter will help you get the most out of the product.

Using network shares

As a network-attached storage device, your Personal Server can provide both shared and private storage space to all the users on your network.

At the highest level, the user storage space on your Personal Server is organized into two kinds of folders: *private folders* and *shared folders*. Technically, both are called *network shares*, or just *shares* (although private folders are not actually shared). Like folders on your computer's own hard drive, network shares can contain both files and folders.

A private folder is accessible only by its owner (the user whose username is the same as the folder name). By contrast, a shared folder may be accessible by all users, some users, or no users. You can control who has access to a shared folder on the **Shared Folders** page of the admin interface (see *Managing users, groups, and shares*).

From the factory, your Personal Server comes with one private folder, **admin** (owned by the server administrator), and one shared folder, **public**, already created. You can create more shared folders on the **Shared Folders** page of the admin interface. When you create a new user account, you can choose to create a new private folder for that user at the same time.

On a Windows PC, you can view all available shares on your Personal Server by doing the following:

1. On the Start menu, click **Run**. The **Run** dialog box opens.
2. Type **\\squareone** and press Enter (see Figure 10). (If you are accessing your Personal Server through an external router, replace "squareone" with the server's WAN IP address.)

A window will open, showing all shares. Double-click a share to open it. You will be prompted to enter a username and password. You can enter those of any user who is authorized to access the share. If you have not yet created any user accounts on your Personal Server, you can access the share as "admin" with the administrative password (by default, "admin").

Note

If you are accessing your Personal Server through an external router, you cannot address it by its hostname ("squareone"). Instead, you must address the server by its WAN IP address. For example, to view all available shares on the server, if the server's WAN IP address is 192.168.1.100, you would enter \\192.168.1.100.

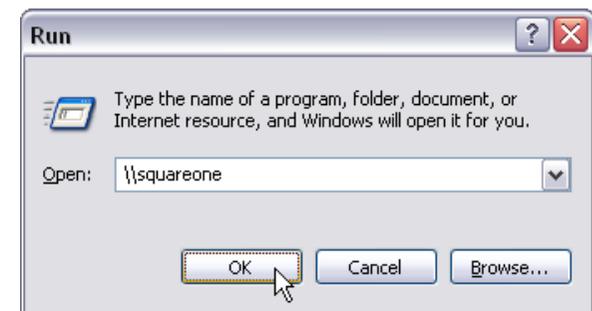


Figure 10

Square One User's Guide

Once you have opened a share, you can use it as you would a folder on your local hard drive. For example, you can copy a file or folder into a share by dragging it from another folder in Windows Explorer or your desktop and dropping it in the share.

Accessing a share in Windows

To access a specific share directly, enter a network address in the form:

`\\hostname\share_name`

where *hostname* is your Personal Server's hostname ("squareone", by default), and *share_name* is the name of the shared or private folder you want to access. For example, to access the **public** shared folder, you would enter **`\\squareone\public`**. You will be prompted to enter a username and password, unless you have previously instructed Windows to remember your password.

If you are accessing the Personal Server through another router, enter a network address in the form:

`\\ip_address\share_name`

where *ip_address* is your Personal Server's WAN IP address.

You can enter a network address in the **Run** dialog box or in Windows Explorer if you want to browse or manage the files and folders in a share. If you want to save or open a file in a share directly within a Windows application, you can enter the network address of the share in the **Open** or **Save As** dialog box of the application.

Accessing a share in Mac OS X or Linux

To access a specific share on a Mac OS X or Linux computer, enter a network address in the form:

`smb://hostname/share_name`

or

`smb://ip_address/share_name`

where *hostname* is your Personal Server's hostname ("squareone", by default), *ip_address* is your Personal Server's WAN IP address (required if accessing the server through an external router), and *share_name* is the name of the shared or private folder you want to access. You will



Tip

If you are unable to access shares on your Personal Server from a Windows PC, you may need to enable the Client for Microsoft Networks service on your PC's network interface. To do so in Windows XP:

- 1. On your desktop, right-click **My Network Places** and select **Properties**. (If you do not have a **My Network Places** icon on your desktop, click **Start > Run**, type "ncpa.cpl", and press Enter.)*
- 2. Right-click your active network connection and select **Properties**.*
- 3. Select the check box labeled **Client for Microsoft Networks**, and then click **OK**.*

Square One User's Guide

be prompted to enter a username and password, unless you have previously instructed the operating system to remember your password.

In Mac OS X, you can enter the network address in the **Connect to Server** dialog box. In the Finder's menu bar, click **Go**, and then click **Connect to Server**.

To enter a network address in Linux, please refer to your Linux distro's network documentation.

Mapping a share to a drive letter (Windows only)

On a Windows PC, you can assign a drive letter to a specific share on your Personal Server, so that you can access the share more conveniently in the future. (This is called *network drive mapping*.) After assigning a drive letter to a share, you can access the share any time by simply clicking the network drive in Windows Explorer, even after restarting your computer.

It is not possible to assign a drive letter to the Personal Server as a whole, only to individual shares.

To map a share to a drive letter in Windows XP, do the following:

1. On your desktop, right-click **My Network Places** and select **Map Network Drive**. (If you do not have a **My Network Places** icon on your desktop, open Windows Explorer and click **Tools > Map Network Drive**.)
2. Select the drive letter you wish to use, enter the network address of the desired share, and click **Finish**. (For an example, see Figure 11.)
3. You will be prompted to enter a username and password. You can enter those of any user who is authorized to access the share. To avoid having to re-enter a username and password every time you log onto or restart the computer, select **Remember my password**. Click **OK**.

Note

*If you change your Personal Server's hostname after mapping a network drive, you will have to disconnect the network drive and map it again using the new hostname. To disconnect a network drive, right-click its icon and select **Disconnect**.*



Figure 11

Using external storage devices

You can connect various kinds of external storage devices to your Personal Server—either temporarily, in order to copy files to the server (from a USB thumb drive, for example); or more permanently, in order to add storage space beyond that of the server's internal hard drive. Supported external storage devices include USB drives, USB memory card readers, and eSATA drives.

Using a USB drive

You can connect up to three USB drives simultaneously, including most thumb drives and external hard drives, to your Personal Server's three USB 2.0 ports. The server supports the following file systems for USB drives: FAT, FAT32, NTFS, ext2, ext3, and XFS.

Each USB drive you connect will appear as a shared folder named **usb1**, **usb2**, or **usb3** (depending on whether other USB storage devices were already connected). If a USB drive has more than one partition, only the first partition will be available as a shared folder.

To access a connected USB drive, use the network address `\\squareone\usb1` (or **usb2** or **usb3**), substituting the actual hostname if you have changed it. Please note that it may take a few seconds after you connect a drive before it is accessible.

You can also map a drive letter to the USB drive, as you would to any other share.

Using a USB memory card reader

You can connect up to three USB memory card readers to your Personal Server's three USB 2.0 ports. The same file systems are supported for memory cards as for USB drives.

To access a memory card, insert the card into the reader *before* you connect the reader to your Personal Server. When you connect the reader, the memory card appears as a shared folder named **usb1**, **usb2**, or **usb3** (depending on whether other USB storage devices were already connected). You can then access the memory card's contents at the network address `\\squareone\usb1` (or **usb2** or **usb3**), substituting the actual hostname if you have changed it. Please note that it may take a few seconds after you connect the card reader before the card is accessible.

Square One User's Guide

If you have a multi-format card reader, please use it with only one memory card at a time. If you connect a card reader to your Personal Server with more than one card inserted, the server will only recognize one of the cards.

Note

When you are finished using a memory card, always disconnect (physically unplug) the card reader from your Personal Server before attempting to access another card. If you replace the card without disconnecting the reader, the new card will not be recognized. The old memory card will still appear to be available at the same network address, even though it is not.

Using an eSATA drive

You can connect one External SATA (eSATA) drive to your Personal Server's eSATA port. The server supports the following file systems for eSATA drives: FAT, FAT32, NTFS, ext2, ext3, and XFS.

When you connect an eSATA drive, it will appear as a shared folder named **esata1**. If the drive has more than one partition, only the first partition will be available as a shared folder.

To access a connected eSATA drive, use the network address `\\squareone\esata1`, substituting the actual hostname if you have changed it. Please note that it may take a few seconds after you connect a drive before it is accessible.

You can also map a drive letter to the eSATA drive, as you would to any other share.

Sharing a USB printer

If you connect a compatible USB printer to one of your Personal Server's three USB 2.0 ports, you can use it from any computer on the server's local network. Most standard USB printers are compatible, although "bidirectional" features such as reporting ink levels are not supported. Some multifunction printers (MFPs) are also compatible, but for printing only—not scanning or faxing. In general, if a printer is compatible with other USB print servers using "raw socket", "port 9100", or HP JetDirect-compatible printing technology, it should work with your Square One Personal Server.

Only one printer can be shared through your Personal Server at a time.

Adding a shared printer to your computer

Before you can use a printer connected to your Personal Server, you must first register or "add" the printer to your computer. Part of this process is installing the correct printer driver on your computer, just as you would for a printer that was directly attached to your computer. You do not need to install a driver on the Personal Server. Before adding a shared printer, please make sure either that its driver has already been installed on your computer, or that you have the driver ready on CD-ROM or other media.

Different ways to add a shared printer to your computer

In Windows XP, there are two ways to add a shared printer to your computer: the *network printer method* and the *TCP/IP port method*. Instructions for both methods are given below.

The network printer method is more intuitive and requires fewer steps, but this method is not recommended because a printer added this way is often slow in use. This is because, whenever you use the Print command, Windows must search for the shared printer and determine its status. The TCP/IP port method, while it takes a little longer to add a printer, does not result in such delays when you use the printer.

If you use a non-Windows operating system, please refer to your operating system's documentation for instructions on adding a network printer.

Adding a shared printer using a TCP/IP port

1. On the Start menu, click **Run**. The **Run** dialog box opens.
2. Type **control printers** and press Enter. The **Printers and Faxes** window opens.



Figure 12

Square One User's Guide

3. Click **Add a printer** or double-click the **Add Printer** icon. The **Add Printer Wizard** dialog box opens. Click **Next**.
4. Select **Local printer attached to this computer**. *Clear* the check box labelled **Automatically detect and install my Plug and Play printer**. (See Figure 12.) Click **Next**.
5. Select **Create a new port**. In the drop-down menu, select **Standard TCP/IP Port** (see Figure 13). Click **Next**. The **Add Standard TCP/IP Printer Port Wizard** opens. Click **Next**.
6. In the **Printer name or IP address** box, enter **squareone** (see Figure 14). (Note: If you are connecting to your Personal Server indirectly through another router, enter the Personal Server's WAN IP address instead.) Click **Next**.
7. Under **Device Type**, select **Custom**, and click **Next**.
8. Click **Finish** to return to the Add Printer Wizard.

From this point forward, follow the same steps you would use to add a printer that is attached directly to your computer.

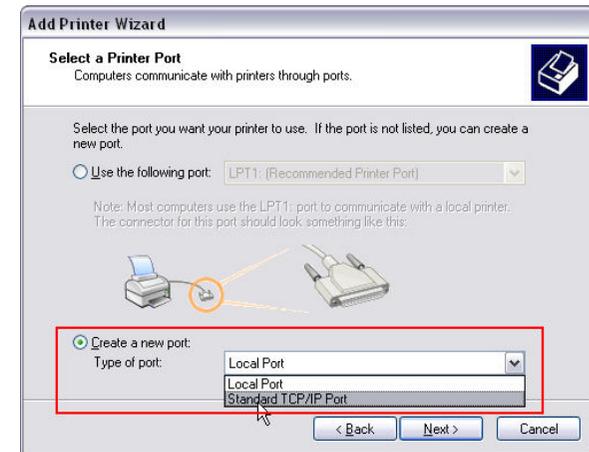


Figure 13

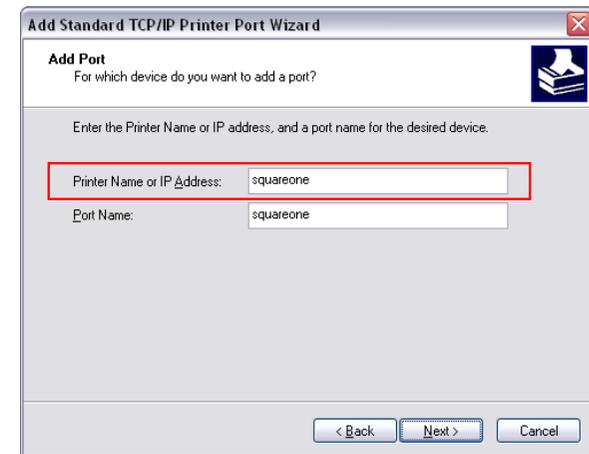


Figure 14

Adding a shared printer as a network printer

1. On the Start menu, click **Run**. The **Run** dialog box opens.
2. Type **control printers** and press Enter. The **Printers and Faxes** window opens.
3. Click **Add a printer** or double-click the **Add Printer** icon. The **Add Printer Wizard** dialog box opens. Click **Next**.
4. Select **A network printer, or a printer attached to another computer** (see Figure 15). Click **Next**.
5. Select **Connect to this printer** and then, in the provided field, type **\\squareone\printer** (see Figure 16). (Note: If you are connecting to your Personal Server through another router, substitute the server's WAN IP address for "squareone".) Click **Next**. The **Connect to Printer** dialog box opens.
6. Click **Yes**. The **Connect to Printer** dialog box opens again. Click **OK**. A second **Add Printer Wizard** dialog box opens.
7. If the correct printer driver is already installed on the computer, select the printer manufacturer and model, click **OK**, and skip to Step 10.
8. Click **Have Disk**. The **Install From Disk** dialog box opens.
9. Click **Browse**. Locate the folder containing the appropriate printer driver and click **Open**. Click **OK**. A third **Add Printer Wizard** dialog box opens.
10. Select the correct printer, and then click **OK**.
11. If a **Software License Agreement** dialog box appears, click **Yes**.
12. Click **Finish** to close the Add Printer Wizard.

When you finish the Add Printer Wizard, the shared printer will appear in the **Printers and Faxes** window as **printer on squareone**.



Figure 15

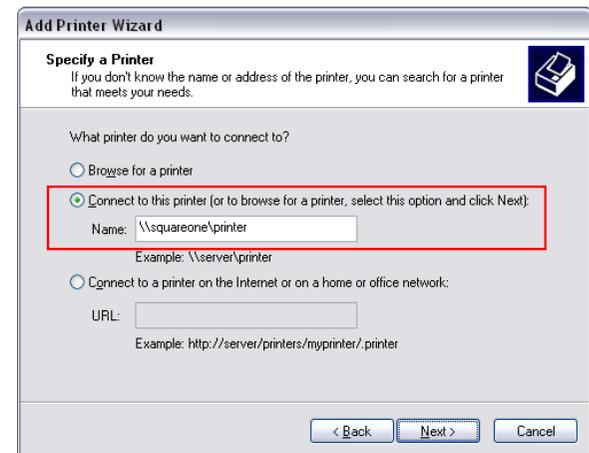


Figure 16

Printing to a shared printer

Before using a printer that is shared through your Personal Server, make sure the printer is connected and turned on, and that the Personal Server is turned on. Then, simply print as if the printer were directly connected to your computer. For example, in a Windows application, select the shared printer in the **Print** dialog box and click **Print**.

Managing users, groups, and shared folders

Why create user accounts, groups, or additional shared folders?

Benefits of multiple user accounts

There are two reasons to create different user accounts on your Personal Server: security and privacy.

Multiple user accounts enhance *security* because they allow non-administrators to access shares on the Personal Server without being able to access the admin interface. This prevents users from making undesirable changes to the server configuration.

Multiple user accounts enhance *privacy* because each user can have their own private folder that no other user can open (unless they know the user's password). Also, having different user accounts allows you to make a shared folder accessible by some users and not by others.

Benefits of groups

Groups are a convenient way to grant or deny access to a specific shared folder to several users at the same time. For example, your Personal Server has ten users—five adults and five children. You want adults, but not children, to be able to access a shared folder. If you did not create groups, you would have to add each adult to the access list for that share, taking care not to add any of the children. By creating two groups in advance—**Adults** and **Children**—and placing all the users in the appropriate group, you can simply grant access to the Adults group.

Benefits of additional shared folders

Flexibility is the main reason you might want to have more than one shared folder. Each shared folder has its own list of users who can access it. So, for example, you could have one share that everyone in the family can access, and another share that only adult users can access. You can also control whether a particular user or group has read-only access or full access. With read-only access, users can open and copy files from the shared folder, but they cannot add, change, or delete files in it.

Creating, modifying, and deleting user accounts

To create, modify, or delete a user account, open the Personal Server's admin interface (<http://squareone:8090>) and click **Management > Users & Groups > Users** (see Figure 17).

Square One User's Guide

To create a user account

1. Enter a username and password for the user.
2. To give the user a private folder, select **Create private folder**.
3. To limit the amount of internal drive space the user can use, select **Enable disk quota** and enter the maximum space in MB.
4. Click **Save**.

To specify a user's group memberships

1. Select the user in the **Users** list box, and then click **Group Memberships**.
2. To add the user to a group or groups, select the group(s) in the **< Not a member of >** list box, and click **<< Add**.
3. To remove the user from a group or groups, select the group(s) in the **< Member of >** list box, and click **Remove >>**.
4. When you are finished, click **Save**.

To edit or delete a user account

1. Select the user in the **Users** list box.
2. Edit the account settings as needed, and then click **Save**. Or, to delete the account, click **Delete User**.

Note

When you delete a user account, the user's private folder (if any) is not automatically deleted. You can access or delete such "orphan" folders using the Personal Server's command line interface. For more information, see **Accessing the command line interface**.

Creating, modifying, and deleting groups

To create, modify, or delete a group, open the Personal Server's admin interface (<http://squareone:8090>) and click **Management > Users & Groups > Groups** (see Figure 18).

To create a group

Enter a name for the new group and click **Save**.

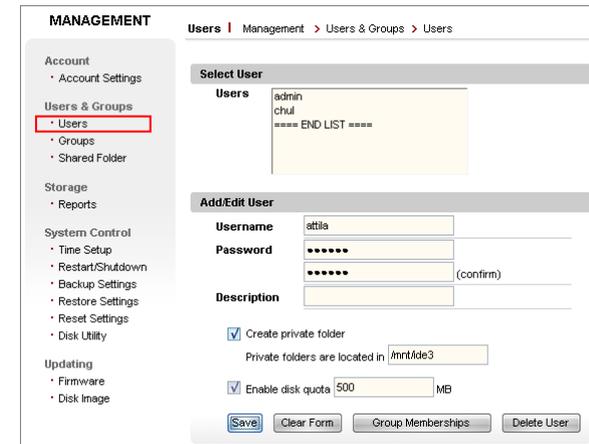


Figure 17

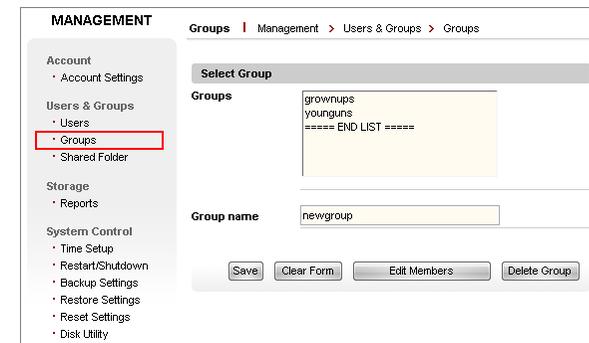


Figure 18

To edit a group's member list

1. Select the group in the **Groups** list box, and then click **Edit Members**.
2. To add a user or users to the group, select the user(s) in the **< Non-Members >** list box, and click **<< Add**.
3. To remove a user or users from the group, select the user(s) in the **< Members >** list box, and click **Remove >>**.
4. When you are finished, click **Save**.

To delete a group

Select the group in the **Groups** list box and click **Delete Group**.

Creating, modifying, and deleting shared folders

To create, modify, or delete a shared folder, open the Personal Server's admin interface (<http://squareone:8090>) and click **Management > Users & Groups > Shared Folders** (see Figure 19).

To create a shared folder

Enter a name for the new share and click **Save**.

To control who can access a shared folder

1. Select the desired share in the **Shared folders** list box, and then click **Manage Access**.
2. To grant read-only access for a user or a group (or several of them), select the user(s) or group(s) in the **< No Access >** list box, and click **<< Add R/O**.
3. To grant full access for a user or a group (or several of them), select the user(s) or group(s) in the **< No Access >** list box, and click **<< Add Full**.
4. To deny access for a user or a group (or several of them), select the user(s) or group(s) in the **< Allowed >** list box, and click **Remove >>**.
5. When you are finished, click **Save**.

To grant full access to everyone

1. Select the share in the **Shared folders** list box, and then click **Manage Access**.

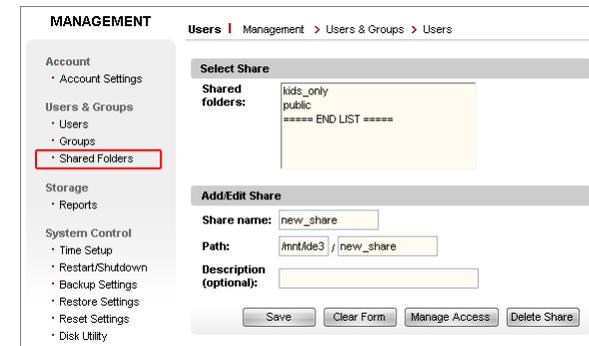


Figure 19

Square One User's Guide

2. Select **Allow everyone full access** and click **Save**.

To delete a shared folder

Select the share in the **Shared folders** list box and click **Delete Share**.

Note

*When you “delete” a shared folder using the admin interface, the folder is not actually deleted on the hard disk. You can access or delete such “orphan” folders using the Personal Server’s command line interface. For more information, see **Accessing the command line interface**.*

Using the BitTorrent client

Your Personal Server has a built-in BitTorrent client, a program that can download files from the popular BitTorrent peer-to-peer (P2P) file sharing network. The BitTorrent client's user interface is part of the Personal Server's admin interface. To access it, on a computer connected to the Personal Server, open a browser window and go to <http://squareone:8090>. On the main menu, click **Apps & Services**, and then on the left-side menu, under **Applications**, click **BitTorrent Client** (see Figure 20).

On the **BitTorrent Client** page, you can add a torrent to download, view the progress of torrents you are downloading, and pause or delete a torrent. You can also specify the maximum download and upload speeds, thus controlling the amount of bandwidth the BitTorrent client can use. (Since BitTorrent is a file *sharing* network, clients contribute to the availability of files by uploading to other clients parts of files that have been downloaded.)

The BitTorrent client downloads the files contained in torrents to the **btdownload** folder at network address <\\squareone\public\btdownload>. Please note that as soon as you start downloading a torrent, the client program creates all the files contained in the torrent at their final sizes; thus, you cannot tell by looking at the size of a file in the **btdownload** folder whether it has finished downloading.

Note

The BitTorrent client stores **.torrent** files (files that contain information about a torrent, required by the BitTorrent client) in <\\squareone\public>, along with **.runtime** files (files generated by the BitTorrent client for tracking purposes). Please do not delete these files until you are finished downloading the torrent from the BitTorrent network.

Working with torrents

Before downloading a torrent, you must first download a **.torrent** file to your computer from a download website or other source of torrents. Then, you upload the **.torrent** file to the Personal Server using the BitTorrent Client interface and start the download.

To add a torrent:

1. On a computer connected to your Personal Server, download a **.torrent** file and save it on your local hard disk.

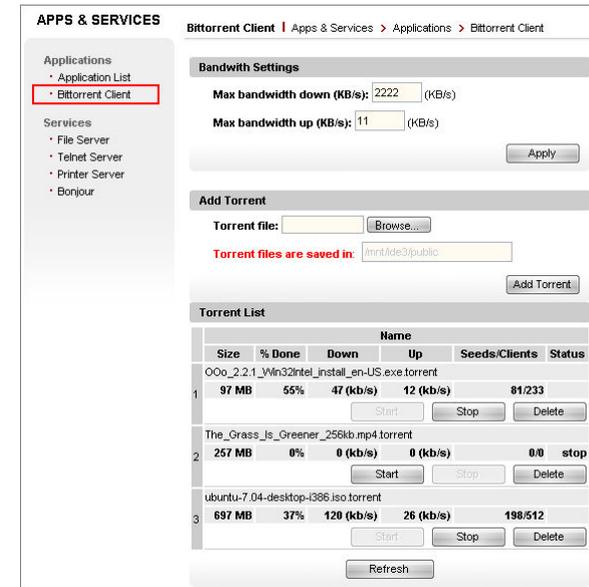


Figure 20

Using Casgle BroadCatcher

Casgle BroadCatcher is a preinstalled third-party application that downloads free video and audio clips from selected media providers to your Personal Server, which you can then play on any computer on the network. Using the application, you subscribe to various media *feeds* that have been selected by Casgle, the application's developer. When a new clip is available on a subscribed feed, the BroadCatcher client running on your Personal Server automatically downloads it to the internal hard drive. You can then view the clip, either by opening the downloaded file directly, or by selecting it in BroadCatcher's browser-based user interface.

Starting BroadCatcher

BroadCatcher is *disabled* by default. To enable it and start downloading media clips, do the following:

1. Access your Personal Server's admin interface at <http://squareone:8090/> and navigate to **Apps & Services > Applications > Casgle BroadCatcher**.
2. Select **Start** and click **Save**.

Once enabled, the BroadCatcher application will always be running on your Personal Server and will run automatically every time you start the server. To stop running BroadCatcher, disable it in the server's admin interface.

The first time you start BroadCatcher, will connect to Casgle's feed server, update itself with the latest program files, and start downloading available clips in the default feeds.

Before accessing to Casgle_player.

Must set the following : Open web browser - Select Tools - Internet options – Security – Trusted sites and then add “ <file://192.168.10.1>” to Add this website to the zone and click “Add”

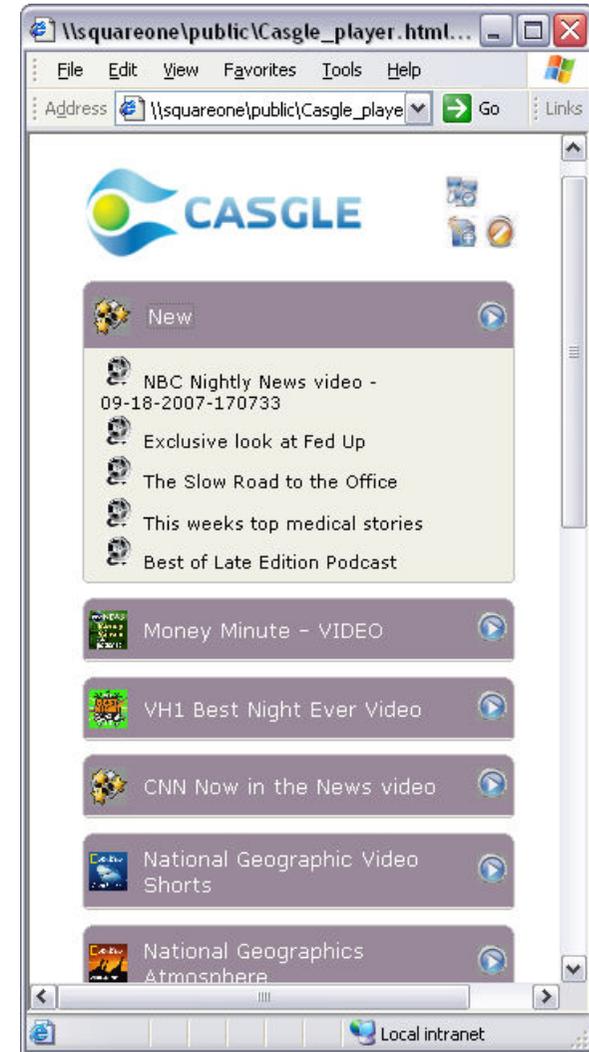
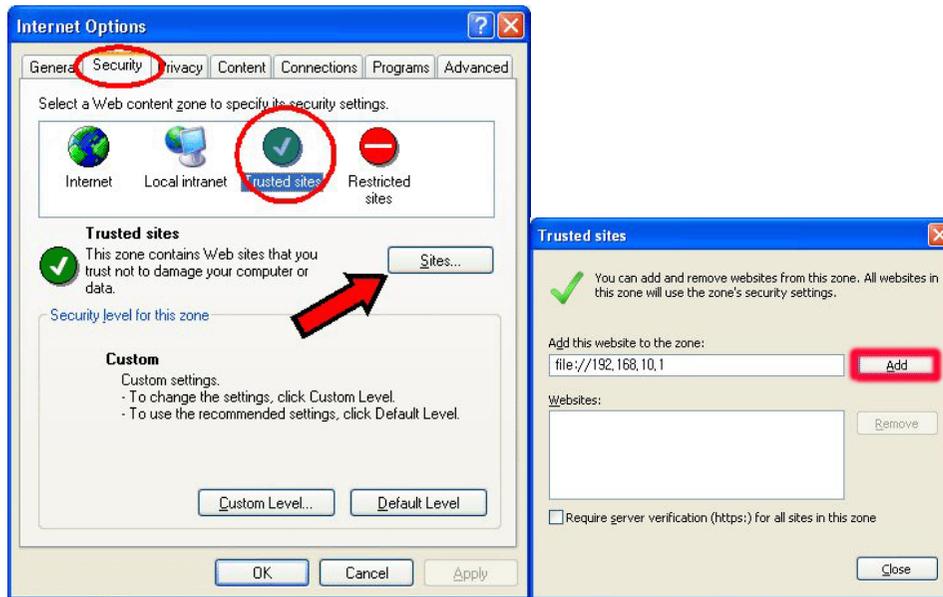


Figure 21



Viewing feeds and clips

To access the BroadCatcher user interface, open the file **Casgle_player.html** in the **public** share of your Personal Server. In Windows, do the following:

1. On the Start menu, click **Run**. The **Run** dialog box opens.
2. Type **\\squareone\public\Casgle_player.html** and press Enter.
3. If you are prompted to enter a username and password, enter those of any user that has read access to the **public** share.

Note: If Windows displays an error message stating that the resource cannot be opened, try opening the **public** share (**\\squareone\public**) first and then double-clicking the file **Casgle_player.html**.

After opening the BroadCatcher user interface for the first time, it's a good idea to save the page as a favorite or bookmark in your browser, so you can open it more conveniently in the future.



Figure 22

Square One User's Guide

A typical BroadCatcher user interface view is shown in Figure 21. The interface shows a list of feeds you have subscribed to; and for each feed, a list of available media clips. Clicking a feed title shows or hides its clip list. If a clip is currently being downloaded or is queued for download, its title is shown in italics; the titles of clips that have finished downloading are shown in plain type. At the top of the feed list is the **New** category, which lists clips that have recently finished downloading.

Viewing a clip

To view a clip, click its title. If the clip format is one your web browser supports, the clip will play immediately in a popup window of the browser. If not, the browser will prompt you either to save the media file or to open it with an external application.

Most video clips that BroadCatcher downloads come in MPEG4 format with a file extension of **.m4v**, **.mp4**, or **.mov**. To play these video clips, your computer needs to have appropriate media playback software installed. Recommended players include *VLC Media Player* for Windows and Mac OS X (<http://www.videolan.org/vlc/>), *mplayer* for Linux clients (<http://www.mplayerhq.hu/>), and *mplayer* in conjunction with the *rulesPlayer* front-end for Windows (<http://rulesplayer.altervista.org/>).

Managing feed subscriptions

Out of the box, BroadCatcher comes configured with subscriptions to several default feeds that have been selected by Casgle. You can change feed subscriptions at any time by clicking the **Change Program Subscriptions** icon in the BroadCatcher user interface (see Figure 22). Casgle's feed selection interface will open in a new window.

Feeds are arranged in categories such as *News & Politics*, *Entertainment*, and *Sports*. Click a category title to reveal the list of feeds in that category. Select the check box next to a feed title

to subscribe to it; clear the check box to unsubscribe. (See Figure 23.) Changes are saved automatically.



Figure 23

More information and technical support

For more information about Casgle BroadCatcher,
For technical support with Casgle BroadCatcher, please send email to support@casgle.com.
Please do not contact ITian Corporation for BroadCatcher issues.

Using the preinstalled web applications

Your Square One Personal Server comes with several free, open-source web applications already installed, so you can run a useful web site right out of the box. The preinstalled web applications are listed in the table below.

Application	Path	Software Home Page	Description
PHPfileNavigator [*]	/pfn	http://pfn.sourceforge.net/	Web-based remote file access.
Gallery	/gallery	http://gallery.menalto.com/	Web photo album creator.
phpBB	/phpbb	http://www.phpbb.com/	Web forum application.
PHPMYAdmin [†]	/phpmyadmin	http://www.phpmyadmin.net/	Browser-based MySQL database manager.
WordPress	/wordpress	http://wordpress.org/	Bloggng platform.
MediaWiki	/wiki	http://www.mediawiki.org/	Wiki (collaborative website) platform.
Aapache/PHP/MySQL info	/phpinfo		Controls many aspects of PHP's behavior.
Web Mail	/mail	http://www.squirrelmail.org/	Sandards-based webmail package written in PHP
eGroupWare	/egroupware	http://www.egroupware.org/	enables you to manage contacts, appointments, todos and many more for your whole business.

The “paths” in the above table indicate each application’s location relative to your Personal Server’s *base web URL*. Your base web URL is simply your Personal Server’s public IP address or

^{*} For more information about using PHPfileNavigator, see **Accessing files remotely using a web browser**.

[†] PHPMYAdmin is not so much an application as it is a utility to manage the MySQL databases of other applications on your Personal Server. These databases provide data storage for most of the preinstalled web applications and for other web apps you might install yourself. When adding your own database-driven web application, PHPMYAdmin provides an easy way to create the application’s database, among other tasks.

Square One User's Guide

domain name preceded by the characters “http://”—that is, the web address of your Personal Server. For example, if your public IP address is 208.67.219.137, your base URL would be **http://208.67.219.137**. Then, to access WordPress, for example, the correct URL would be **http://208.67.219.137/wordpress**.

Most of these applications require you to log in to add or edit content. Others require you to log in only to perform administrative tasks, such as adding and managing user accounts. All of the applications have been initially set up with one user, named “admin”, whose password is “squareone”. For those apps that require it, “admin” is also the administrator.

Note: Website Baker may not show an admin login link on its main page. If this is the case, to access the admin page, add **/admin** to Website Baker's URL.

Instructions for working with these applications are beyond the scope of this user's guide. You are encouraged to explore the apps on your own and to visit their respective home pages on the Internet for more information about them.

Part Four

Advanced Topics

Part intro.

Accessing your Personal Server remotely

Using network shares remotely

When you need to access files on your Square One Personal Server from a remote location over the Internet, you can access the same network shares that you use locally. However, you *cannot* use the same network addresses (such as `\\squareone\public`) that you use when you access these shares locally. This is because the Personal Server's hostname, "squareone", can only be used on the server's own local network, not on the Internet.

For remote access, you must use the Personal Server's WAN IP address in place of the hostname in the network address. For example, if the server's WAN IP is 74.211.157.83, you can access the **public** share at network address `\\74.211.157.83\public` from a Windows computer, or at `smb://74.211.157.83/public` from a Mac OS X or Linux machine.

Using Dynamic DNS

If your Internet service provides a dynamic IP address instead of a static one—that is, if your Personal Server's WAN IP address changes from time to time—then it is not practical to use the WAN IP to access the server remotely. (Most residential Internet accounts, and even some business ones, use dynamic IP addresses.)

In this case, it is helpful to use Dynamic DNS to associate an *Internet hostname* with your Personal Server. Once you set up Dynamic DNS, you can access your Personal Server from anywhere on the Internet using an unchanging hostname such as "itian.dyndns.org", regardless of the server's current WAN IP address. For instructions, see ***Setting Up Dynamic DNS***.

Problems with using network shares remotely

Some Internet Service Providers (ISPs) block the network ports that are used by computers to access network shares across the Internet. These ports include ports 137-139 (the NetBT ports) and port 445 (Microsoft-DS). If these ports are blocked by any router between the remote computer and your Personal Server, you will not be able to access your network shares remotely. Conversely, if you are unable to access the network shares on your Personal Server remotely, it is probably because the required ports are being blocked by your ISP.

In this case, you should still be able to use one of the other remote file access methods described below, since these use ports that are less often blocked by ISPs.

Access files remotely with FTP or SFTP

In addition to its network shares, your Personal Server provides other ways to access files remotely. The server has built-in FTP and SFTP services, either of which you can use to transfer files between the server and a remote computer. Taking advantage of either of these services requires special software—called an *FTP (or SFTP) client*—on the remote computer.

The steps are similar whether you access the server through FTP or SFTP. In the client, specify your Personal Server's WAN IP address as the host address, and enter the username and password of a user account that exists on the server. If you are connecting through SFTP for the first time, you may be prompted to save the server's *host key* (or "fingerprint" or "signature") on your computer; if so prompted, answer **yes**.

The shared folders a user can access through FTP or SFTP are the same as those he or she can access as network shares. (At a minimum, each user can access his or her private folder, if the account includes one.) Shared folders the user has no access to will be invisible in the FTP or SFTP client (unlike in Windows Explorer, where inaccessible shares are visible but cannot be opened).

Directory structure for FTP and SFTP

Below is a representation of the default directory structure that is visible in an FTP or SFTP client to user "admin", before you have added any private or shared folders, and when no external storage devices are connected.

	[Folder Description]
/	[ftp root]
+--ide3	[parent folder of all shares]
+--admin	[admin's private folder]
+--gallery2data	[data storage for Gallery web application]
+--[various subfolders]	
+--htdocs	[web document root]
+--[various subfolders]	
+--lost+found	[recovered files from disk repair operations]
+--public	[the "public" shared folder]
+--btdownload	[BitTorrent downloads]
+--media	[Casgle BroadCatcher downloads]



Tip

*If you sometimes need to allow people without a user account to remotely upload or download files on your Personal Server, you can tell them to log in through FTP or SFTP anonymously (without entering a username or password). The server will log them in using the "guest" user account. This account has write access to the **guest** share, but no access to other shares. If you have files you want guest users to be able to download, copy them into the **guest** share.*

*If you want to disable guest access, you can do so in the admin interface: Go to **Apps & Services > Services > File Server** and clear the "Enable" check box under **Guest Access**.*

Square One User's Guide

When you log in to your Personal Server's FTP or SFTP service, the *active directory*—the directory you are “in”—is initially the private folder belonging to the user you logged in as. (In the admin user's case, this is the **admin** folder.) From this folder, you can go “up” to its parent directory, **ide3**, which contains all the private and shared folders on the Personal Server's internal hard drive. If you go up one more level, to the *ftp root*, you will see, in addition to **ide3**, folders representing any external storage devices that are connected to the server, such as **usb1**. (When no external devices are connected, only **ide3** will be visible.)

If you log in with a user account that has no private folder, your initial active directory will be the ftp root (/).

Technical note: The ftp root corresponds to the directory **/mnt** on the internal hard drive, which contains the mount points of all connected storage devices. You cannot access the true system root or any of its subdirectories, except for **/mnt**, using FTP or SFTP, although you can access these directories using the server's command line interface through telnet or SSH—see **Accessing the command line interface**.

Accessing external storage devices through FTP or SFTP

To access a connected external storage device through FTP or SFTP, log in as any user, and from your private folder, go “up” twice to the ftp root. Then double-click the folder representing the desired external drive.

Accessing files remotely using a web browser

One of the web applications preinstalled on your Personal Server is a web-based file storage application called PHPfileNavigator. You can use this application to work with files in the Personal Server's **public** shared folder (**\\squareone\public**) from any computer with an Internet connection.

To use PHPfileNavigator, go to **http://ip_address/pfn/** (where *ip_address* is your Personal Server's WAN IP address) and log in with username “admin”, password “squareone”. An example directory listing in PHPfileNavigator is shown in Figure 24.

Using PHPfileNavigator, you can:

- Download files from, and upload them to, your Personal Server.
- Copy or move files between folders on the server.
- Delete files on the server.

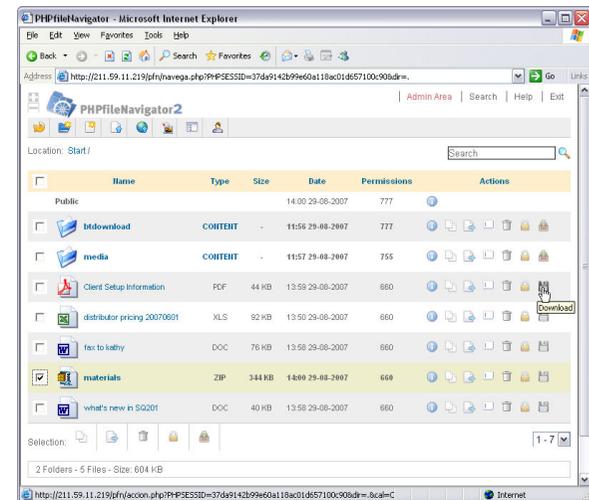


Figure 24

Square One User's Guide

- Download files from other servers directly to your server.
- Create new text files on the server.

Adding other shares to PHPfileNavigator

You can add access through PHPfileNavigator to other shared folders besides **public** by doing the following:

1. Log in to PHPfileNavigator and click the **Admin Area** link at the top of the page.
2. Click the **Create Root** button at the left end of the toolbar (see Figure 25).
3. Fill out the form as follows (see Figure 26 for an example):
 - a. In the **Name** field, enter a name for the shared folder to be accessed. (This name will only be used in PHPfileNavigator.)
 - b. In the **Path** field, enter the absolute path of the shared folder to be accessed. For example, if you are adding access to a share named **marketing**, enter **/mnt/ide3/marketing/**.
 - c. In the **Web Root** field, enter the share name surrounded by forward slashes; for example, **/marketing/**.
 - d. In the **Host** field, enter the WAN IP address or domain name of your Personal Server.
 - e. Set the **Status** drop-down menu to ON.
 - f. Select at least one PHPfileNavigator user to grant access to the share. (Note: Users shown here are specific to PHPfileNavigator and are *not* the same as the user accounts on your Personal Server.)
4. Click **Accept**.

To access the shared folder, click the **Start** link at the top of the page. When the directory listing appears, click the **Choose a Root** link at the top of the page. Then click the name of the desired shared folder.

Note

In PHPfileNavigator, you can only access the contents of shared folders on your Personal Server. You cannot access the contents of private folders. If you add access to a private folder in



Figure 25

The image shows the 'Administration » Modify Root' form. It contains several input fields and dropdown menus:

- Name*: Marketing
- Path*: /mnt/ide3/marketing/
- Web Root*: /marketing/
- Host*: 211.59.11.219
- Maximum Weight: 0 (with a unit dropdown set to MBytes)
- Current Weight: Max size is disabled.
- Status: ON (dropdown menu)

Below these fields, there are two sections for user permissions. The first section is for 'Administrators' with a 'default' config and a 'Check/Uncheck All' checkbox. The 'Administrator' user is checked. The second section is for 'Guests' with a 'default' config and a 'Check/Uncheck All' checkbox. The 'Toby' user is unchecked. At the bottom right, there are 'Back' and 'Accept' buttons.

Figure 26

Square One User's Guide

PHPfileNavigator, its directory listing will be shown as empty, and you will not be able to upload files into it.

Adding users in PHPfileNavigator

As with all of the web applications, user management in PHPfileNavigator is separate from that of your Personal Server. This means that PHPfileNavigator user accounts are not the same as user accounts on the server itself, and adding or removing an account in one will not automatically add or remove a corresponding account in the other. Even the “admin” account in PHPfileNavigator is not the same as the server’s “admin” account, although they share the same name.

You may want to add and use other user accounts in PHPfileNavigator, instead of always using the “admin” account. For example, you may want to give distant people who do not have accounts on your Personal Server restricted access to one particular shared folder, but not to **public**. In this case, you can create a “guest” user account in PHPfileNavigator and give the account access to a guest folder while withholding access to **public** or other shared folders.

Technical note: As with all of the web applications, the actual user account used by PHPfileNavigator when working with files on the Personal Server is the “apache” account. Thus, only folders that are accessible by “apache”, such as **/mnt/ide3/htdocs** and other shared folders, are accessible in PHPfileNavigator.

Learning more about PHPfileNavigator

For more information about using and managing PHPfileNavigator, please visit the software’s home page at <http://pfn.sourceforge.net/>. A forum is available where you can post questions that may be answered by other members of the PHPfileNavigator user community.

Accessing the server remotely through an external router

If you are running your Personal Server behind another router (as described in ***Setting up your Personal Server behind an external router***), and you want to be able to access (or let others access) the server remotely across the Internet, then you must configure your other router to forward certain network ports to the Personal Server. The ports that need forwarding depend on which services you want to expose. The table below lists the ports required for each service on your Personal Server.

Square One User's Guide

Service	Port(s)	Description
FTP	TCP 21	File Transfer Protocol
SSH/SFTP	TCP 22	Secure Shell / Secure FTP
Telnet	TCP 23	Telnet
SMTP	TCP 25	Simple Mail Transport Protocol
HTTP	TCP 80	Hypertext Transfer Protocol (web server)
POP3	TCP 110	Post Office Protocol v3
NetBT	UDP 137, 138; TCP 139	NetBIOS over TCP/IP (Windows File Sharing)
SSL	TCP 443	Secure Sockets Layer (for secure web sites, or HTTPS)
OpenVPN	UDP 1194	OpenVPN Virtual Private Network
MySQL	TCP 3306	MySQL database server

Setting up a website

Your Square One Personal Server is a fully-functional Web server, with Apache HTTP Server, PHP, and MySQL software all preinstalled.

There are two basic ways to create or set up a website on your Personal Server.

The first option is to create a site using one of the preinstalled web applications: Website Baker, WordPress, phpBB, Gallery, or WikiMedia. Each of these applications provides a ready-made structure on which you add content directly in your browser, using a set of special web pages designed to simplify content creation. Each application is best suited for a particular kind of website. WordPress is best for blogs; phpBB, for forums; WikiMedia, for collaborative websites; Gallery, for online photo albums and image galleries; and Website Baker, for general-purpose websites. For more information on using these applications, see *Using the preinstalled web applications*.

Uploading website files to the server

The other option is to upload HTML or PHP files that you have created on your computer (or downloaded from an existing website) to your Personal Server. Store these website files in the **htdocs** folder, which can be accessed at network address `\\squareone\htdocs`, or through FTP or SFTP at `/mnt/ide3/htdocs`. When using FTP or SFTP locally, you can access the Personal Server using the hostname **squareone**.

By default, the **htdocs** folder on the Personal Server contains the following files and folders, although the contents may vary slightly, depending on what version of the Square One hard disk image is installed on your server.

```
/mnt/ide3/htdocs
+--egroupware
+--gallery
+--mediawiki
+--pfn
+--phpmyadmin
+--phpbb
+--wb
+--wordpress
+--index.php
```



Tip

To see what versions of Apache HTTP Server, PHP, and MySQL are installed on your Personal Server, open your web browser and go to <http://squareone/phpinfo/>.

Square One User's Guide

The folders, indicated in boldface in the box above, contain the web applications that your Personal Server came preinstalled with. For example, **wb** contains the application files of Website Baker. The file **index.php** is the factory default index page, which displays information about the server's installed web server software.

Whatever website files you place directly in **htdocs** will be viewable on the Internet at a URL in the form **http://public_ip_address/filename**. For example, if your public IP address is 74.211.157.83, and you have a file named **hello.htm** in **htdocs**, then the Internet URL for that file will be **http://74.211.157.83/hello.htm**.

If you plan to host your own website on your Personal Server, you will most likely delete the default **index.php** and replace it with your own index page file, named **index.php**, **index.htm**, or **index.html**. That way, when a visitor goes to **http:// public_ip_address/**, they will see your own home page, not the default one. Alternatively, you can leave the default index file in place and store your website files in a subfolder of **htdocs**, such as **mysite**. In this case, the home page URL of your website would be **http:// public_ip_address/mysite/**.

Managing local write access to web files

By default, only the admin account can access **htdocs**. However, you can grant access to this folder to other user accounts by adding the desired users to the **web_mgmt** group, which has write access to **htdocs** by default. For information about adding users to groups, see *Creating, modifying, and deleting groups*.

Forwarding incoming connections

Introduction to port forwarding

Like most other routers, your Square One Personal Server by default blocks all *incoming* communication attempts from outside computers to computers and devices on the server's local network, unless the incoming communications are in response to an *outgoing* request from the same computer. (Outgoing connections are not blocked at all.) For example, when you request a web page on the Internet by entering a URL in your browser, your Personal Server's built-in router "remembers" which computer made the outgoing request and to what web server the request was made. Then, when the web server sends the requested page, the router passes the incoming data on to the requesting computer. If a computer on the Internet attempts to connect to a local computer *without* the local computer having initiated communications with it, the router normally blocks the attempt. This is to protect your network against unwanted intrusion.

There may be times when you want specific kinds of incoming connections to be permitted through to your network—to *not* be blocked by the router—even if they are not in response to an outgoing request. One example involves the popular peer-to-peer file-sharing application, eMule. For eMule to work best, other computers (peers) on the eMule network must be able to connect to your computer running eMule, although your computer does not initiate communications with them. Blocking these incoming connections causes both download and upload speeds in eMule to be reduced.

Port forwarding is provided by the router as a way to accommodate exceptions to the general policy of blocking all unsolicited incoming connections. Port forwarding takes advantage of the fact that, for any given Internet application, incoming connections are almost always addressed to certain specific *ports* on the destination computer. For example, requests for web pages are almost always addressed to the web server's port 80, and the web server is said to "listen" for incoming connections on that port. (It may be useful to think of ports as being like individual mailboxes in an apartment building, and think of the building as being like a computer. For a letter to reach its destination, you must specify both the building's address and the apartment number.)

If you want to allow incoming connections to a program running on your computer—eMule, for example—configure the router to forward connections on the port (or ports) on which eMule

listens for incoming connections. This is much safer than forwarding *all* connections to your computer. (By the way, for eMule, the incoming ports are often 4662 and 4672, but the program allows you to choose the ports on which it will listen for connections. If you want to set up port forwarding for eMule, you will need to check your eMule preferences to see which ports to forward.)

Choosing a port forwarding method

There are two kinds of port forwarding commonly provided by consumer routers: port mapping and port triggering. Both are supported by your Personal Server.

In *port mapping*, incoming connections addressed to a designated port or ports are forwarded to one specific local IP address—and thus to one particular computer. Port mapping is best suited for applications that you run on a single computer only.

Additionally, in port mapping it is possible (although normally not necessary) to forward incoming connections to a *different port* on the destination computer than the port to which the connection was addressed. For example, if an incoming connection is addressed to port 5900, it can be forwarded to the designated computer's port 5901 instead. The port to which the connection was addressed (called the “public port”) is said to be *mapped* to the port on which the designated computer is actually listening (the “private port”)—this is the origin of the term *port mapping*.

In *port triggering*, incoming connections addressed to a designated port or ports are forwarded not to one fixed IP address, but to any local computer that makes an outgoing connection through a designated *trigger port* or ports. When the router detects an outgoing connection through a trigger port, it temporarily forwards connections on the designated incoming ports to the computer that made the outgoing connection. Since there is no need to specify which IP address will receive the incoming connections, port triggering is best suited for applications that might run on any of several computers on the LAN. (However, only one computer can run such an application at any given time.) Port triggering does not support mapping public to private ports.

From a security standpoint, port triggering is somewhat safer than port mapping, because incoming connections are only forwarded while the related outgoing trigger connections exist. If no trigger connections are going out, the incoming ports remain closed. In port mapping, by contrast, specified incoming ports remain open at all times. However, port mapping is the only



Tip

You do not need to set up port forwarding for the Internet services that run on your Personal Server—such as the HTTP, FTP, and SSH services. The ports necessary for the server to accept incoming connections to these services are open by default.

If you want to run an Internet service on your computer that the Personal Server already runs, then you should configure the service on your computer to listen on a different port than the default for that service, and then set up the Personal Server to map that port to your computer. For example, to run a secondary FTP service on your computer, you could make it listen on port 2121 and then set up the Personal Server to map port 2121 to your computer.

viable option for applications that need to be able to receive incoming connections anytime, and do not make trigger connections.

With either port forwarding method, your Personal Server allows you to create any number of “rules”. Each rule specifies the port forwarding details for one port (or set of related ports), and thus for one service or application. You can create as many rules as you need.

Creating and editing port mapping rules

To create a new port mapping rule

1. On the main menu of the Personal Server admin interface, click **Firewall**. On the left-side menu, click **Port Mapping** (see Figure 27).
2. Enter a name for the rule in the **Rule name** field. (Choose a name that will help you remember what the rule is for. Note: After you add a rule, you cannot change its name.)
3. In the **IP address** field, enter the IP address of the local computer to which you want to forward the incoming connections. The IP address must be within the Personal Server's LAN subnet.
4. Select the communications protocol(s) to which the rule applies: TCP and/or UDP. If you are not sure which protocol to choose, select both.
5. In the **Private port(s)** field, enter the port(s) on which the designated computer will listen for incoming connections.
6. In the **Public port(s)** field, enter the port(s) to which the outside computers will address incoming connections. In most cases, the private port(s) and the public port(s) can be the same.
7. Click **Add Rule**.

To edit a port mapping rule

1. In the **Existing Rules** table, click the **Edit** button on the row listing the rule you want to edit.
2. Edit the form as necessary, and then click **Save Changes**.

Note: You cannot change the name of an existing rule.

The screenshot shows the 'FIREWALL' configuration page for 'Port Mapping'. The 'Edit Rule' form includes the following fields and options:

- Enabled:**
- Rule name:** [Text input field]
- IP address:** 0.0.0.0
- Protocol:** TCP UDP
- Private port(s):** (ex. 80-150,832)
- Public port(s):** (ex. 80-150,832)
- Presets:** A dropdown menu with options: Tablet, HTTP, HTTPS, FTP, DNS, SMTP, POP3, WebMeeting.
- Buttons:** Add Rule, Clear Form, Apply Changes.

The 'Existing Rules' table at the bottom is as follows:

Enabled	Rule Name	IP address	Protocol	Private	Public Port	
<input checked="" type="checkbox"/>	elMac UDP	192.168.10.10	UDP	4672	4672	Edit Delete

Figure 27



*If you are creating a port mapping rule for one of the applications listed in the **Presets** box, simply select the desired application, and the form will be automatically filled with the appropriate values (except for IP address, which must be specified manually).*

To disable a port mapping rule

1. In the **Existing Rules** table, click the **Edit** button for the rule you want to edit.
2. Clear the **Enabled** check box and click **Save Changes**.

To delete a port mapping rule

In the **Existing Rules** table, click the **Delete** button for the rule you want to delete.

Creating and editing port triggering rules

To create a new port triggering rule

1. On the main menu of the Personal Server admin interface, click **Firewall**. On the left-side menu, click **Port Triggering** (see Figure 28).
2. In the **Rule name** field, enter a name for the rule. (Choose a name that will help you remember what the rule is for. Note: After you add a rule, you cannot change its name.)
3. Next to **Trigger protocol**, select the communications protocol(s) that will be used by outgoing trigger connections for this rule. If you are not sure which protocol will be used, select both.
4. In the **Trigger port(s)** field, enter the port(s) to which the outgoing trigger connections will be addressed.
5. Next to **Inbound protocol**, select the communications protocol(s) that will be used by inbound connections for this rule. If you are not sure which protocol will be used, select both.
6. In the **Inbound port(s)** field, enter the port(s) to which the incoming connections will be addressed.
7. Click **Add Rule**.

To edit a port triggering rule

1. In the **Existing Rules** table, click the **Edit** button on the row listing the rule you want to edit.
2. Edit the form as necessary, and then click **Save Changes**.

Note: You cannot change the name of an existing rule.

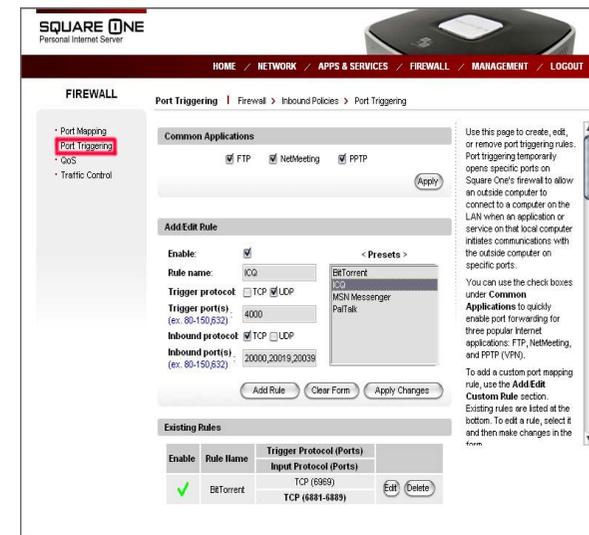


Figure 28



Tip

If you are creating a port triggering rule for one of the applications listed in the **Presets** box, simply select the desired application, and the form will be automatically filled with the appropriate values.

To disable a port triggering rule

1. In the **Existing Rules** table, click the **Edit** button for the rule you want to edit.
2. Clear the **Enabled** check box and click **Save Changes**.

To delete a port triggering rule

In the **Existing Rules** table, click the **Delete** button for the rule you want to delete.

Managing storage devices

Your Personal Server's admin interface includes a Disk Utility that you can use to format or error-check both the internal hard drive and any external storage device. To access the utility, do the following:

1. On a computer connected to your Personal Server, open a browser window and go to <http://squareone:8090> and log in as "admin".
2. On the main menu, click **Management**. On the left-side menu, under **System Control**, click **Disk Utility** (see Figure 29).

Each connected storage device is listed in the Disk Utility, along with some basic information about the device and buttons for available actions. In Figure 29, two storage devices are listed: the internal hard drive (at the bottom) and one USB drive (at the top).

For the internal hard drive, you can:

- Format the drive to various file systems—FAT32, ext2, ext3, and XFS—with optional encryption
- Scan the drive for errors (and fix them if found)
- Display SMART (Self-Monitoring Analysis and Reporting Technology) information about the drive

Note

*If you format the internal hard drive, ALL content on the drive will be ERASED. If the drive contains files you want to keep, please make sure to back them up to another drive or to your computer before you format. Also, please note that you will need to reinstall the Personal Server's hard disk image after formatting. (For instructions on installing a hard disk image, see **Upgrading your Personal Server.**)*

For external storage devices, the available actions include formatting and error-scanning, but not displaying SMART information. In addition, you can *unmount* an external drive. Unmounting removes the shared folder corresponding to the drive, making the drive unavailable for use. You must unmount an external drive before formatting it.

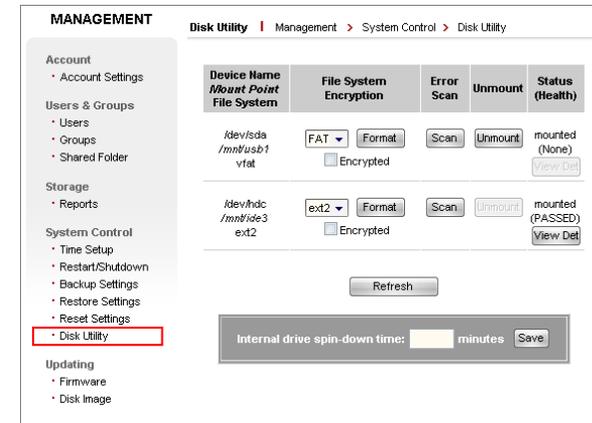


Figure 29

Tip

When formatting an external drive, if you plan to connect the drive to a Windows PC at some point, you should select FAT32 as the file system, since Windows does not support ext2, ext3, or XFS. If you plan to use the drive only with your Personal Server, or with Linux computers but not Windows, then you can choose any file system.

About disk encryption

Using the Disk Utility, you can optionally enable *encryption* on a drive when you format it. When encryption is enabled, the contents of the drive can only be read when the drive is connected to your Personal Server. Once you enable encryption, for example on an external USB drive, it will become effectively unusable except when connected to your particular Personal Server. When connected to any other host (even another Square One Personal Server), the drive will appear to be unformatted, and it will be impossible to read any file on the drive. Formatting the drive again will enable it to be used with another host, but its former contents will remain encrypted and unreadable.

Encrypting an external drive is useful if you want to secure its contents. For example, if someone takes the drive (without taking your Personal Server) they will not be able to access its contents. Encrypting is not useful when it is likely that the Personal Server will be taken with the drive, because then the drive can be read using the server. For this reason, it is not useful to encrypt the Personal Server's internal hard drive, since it is unlikely the drive would be taken without the server.

When you use an encrypted drive with your Personal Server, no special action is necessary to access its contents. The server itself stores the decryption key needed to "unlock" the drive in flash memory, and applies this key whenever the server is powered up or restarted. The decryption key remains in flash memory even if you reset the server to factory default settings.

The only way to remove encryption from a drive is to format it again using the Disk Utility with encryption disabled. Please note that the encrypted contents will be irretrievably lost if you do this.

Upgrading your Personal Server

Upgrading the server's software

From time to time, ITian Corporation may release software upgrades for your Square One Personal Server to add features or correct bugs in the server's operating system or applications. Software upgrades may come in the form of either *firmware upgrades*, which replace system software in the server's flash memory; or *hard disk images*, which replace or supplement the software stored on the server's internal hard drive. Both types of upgrades can be installed through the server's browser-based administrative interface.

You can download the latest firmware or hard disk image (if any has been made available) from the **Downloads** section of the **Support** area of www.myitian.com.

To install a firmware upgrade:

1. Access your Personal Server's admin interface at <http://squareone:8090/> and navigate to **Management > Updating > Firmware** (see Figure 30).
2. Click **Browse**. In the **Choose file** dialog box, navigate to the folder to which you downloaded the firmware package, and double-click the file. (The filename should start with "SQ201FW" and end with ".bin".)
3. Click **Start Firmware Upgrade**. A confirmation dialog box appears. Click **OK** to proceed.

When you click **OK**, your browser will upload the firmware package to the Personal Server, and then the server will install the firmware upgrade. Uploading takes several seconds, during which time there will be no feedback except for the page-loading indicator of your browser. Please do not navigate away from the current page, or the file upload will be interrupted and you will have to start over.

Once the firmware package has been completely uploaded, the page will change and display a message indicating that the firmware is being installed. Installation takes up to 20 minutes. During this time, you will not be able to access files or services on the server, and you will not be able to access the Internet (if you are using the Personal Server as your broadband router). When installation is complete, the server will automatically restart, and then you can use the server as normal.

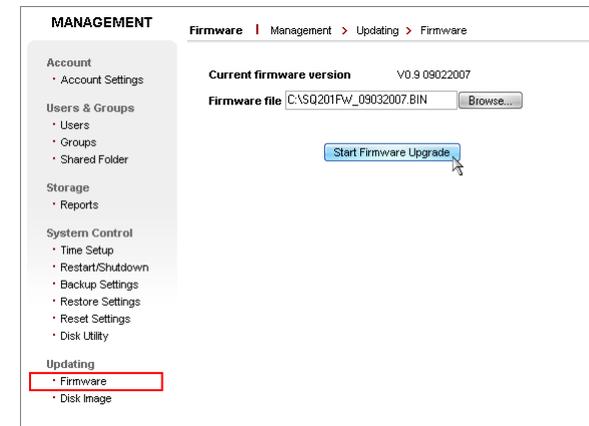


Figure 30

Square One User's Guide

After firmware installation, you can confirm that the new firmware was correctly applied by checking the firmware version number displayed on the **Home** page of the admin interface.

i Caution

While firmware installation is in progress, do not navigate away from the firmware upgrade page or shut down the Personal Server until at least 20 minutes have passed. Interrupting the firmware installation process will render the server inoperable.

To install a hard disk image:

1. Access your Personal Server's admin interface at <http://squareone:8090/> and navigate to **Management > Updating > Disk Image** (see Figure 31).
2. Click **Browse**. In the **Choose file** dialog box, navigate to the folder to which you downloaded the hard disk image, and double-click the file. (The filename should start with "SQ201HI" and end with ".bin".)
3. Click **Start Disk Image Upgrade**. A confirmation dialog box appears. Click **OK** to proceed.

When you click **OK**, your browser will upload the hard disk image to the Personal Server, and then the server will install the disk image. Uploading takes several minutes, during which time there will be no feedback except for the page-loading indicator of your browser. Please do not navigate away from the current page, or the file upload will be interrupted and you will have to start over.

Once the hard disk image has been completely uploaded, the page will change and display a message indicating that the disk image is being installed. Installation takes up to 20 minutes. During this time, you will not be able to access files or services on the server, and you will not be able to access the Internet (if you are using the Personal Server as your broadband router). When installation is complete, the server will automatically restart, and then you can use the server as normal.

Upgrading the internal hard drive

You can upgrade the internal hard drive of your Personal Server, replacing it with one of greater capacity. Only 3.5-inch Serial ATA (SATA) hard drives are supported. Please refer to the printed *HDD Installation Guide* included in your Square One Personal Server package for hard drive installation instructions. (You can also view the *HDD Installation Guide* on your computer by

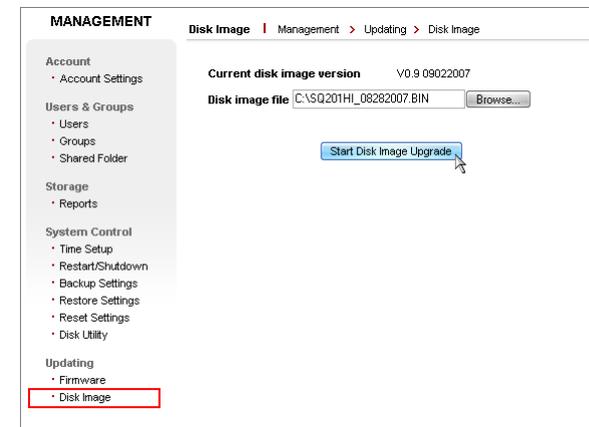


Figure 31

Square One User's Guide

inserting your Square One Personal Server setup disc and clicking the appropriate item in the menu window that appears.)

To remove the existing internal hard drive:

After removing the server's cover as described in the *HDD Installation Guide*, simply unscrew the drive mounting bracket and gently slide the drive away from the SATA connector on the circuit board.

Caution

The hard drive mounting bracket may have sharp edges. Please handle it with care.

After you install a new hard drive, it must be formatted, and a hard disk image must be installed. Again, please refer to the *HDD Installation Guide*.

Accessing the command line interface

Although the browser-based administrative interface at <http://squareone:8090> is your primary means of managing your Square One Personal Server, the server also features a command line interface that you can use to perform tasks that cannot be done through the admin interface, such as deleting orphan folders left over when you remove user accounts or shares. The command line interface (also called the *CLI* or the *shell*) is accessible through Telnet and SSH.

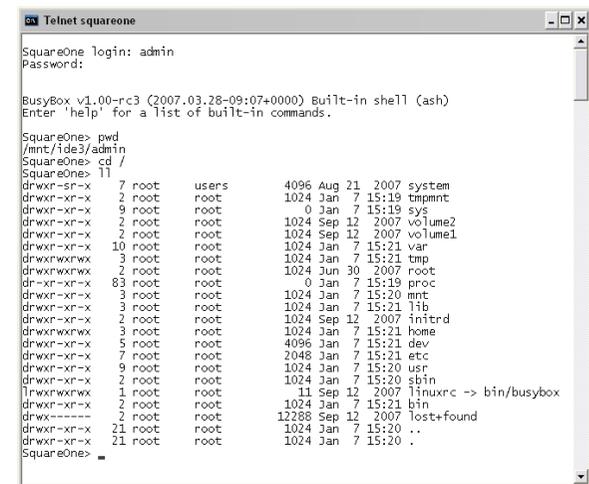
To access the CLI, you use either a Telnet client or an SSH client. Most operating systems include a Telnet client; Windows, for example, provides the command-line client **telnet.exe**. A good, free Windows client that supports both Telnet and SSH is *PuTTY*, available at <http://www.puttyssh.org/>.

In terms of accessing your Personal Server's CLI, Telnet and SSH both provide the same functionality. However, SSH is more secure, because it encrypts the communications between the server and the client, including the username and password you use to log in to the CLI. (Telnet sends all data in clear text.) The enhanced security makes SSH a better choice when you must access the CLI remotely across the Internet, or whenever security is a top concern.

To access the CLI using Windows's built-in telnet client:

1. On the Start menu, click **Run**. The **Run** dialog box opens.
2. Type **cmd** and press Enter. A Windows command prompt window opens.
3. Type **telnet squareone** and press Enter. (If accessing the CLI remotely or through another router, substitute the server's WAN IP address for "squareone".)
4. At the **SquareOne login:** prompt, enter the username of a user on your Personal Server, such as "admin". At the **Password:** prompt, enter the user's password. (The password will not be shown.)
5. At the **SquareOne>** prompt, enter commands as needed.
6. When you are finished, enter **exit** to close the CLI.

Figure 32 shows a typical CLI session in which **admin** has logged in, determined the current directory (**pwd**), changed to the root directory (**cd /**), and listed its contents in long format (**ll**).



```
Telnet squareone
SquareOne login: admin
Password:
BusyBox v1.00-rc3 (2007.03.28-09:07+0000) Built-in shell (ash)
Enter 'help' for a list of built-in commands.

SquareOne> pwd
/mnt/ide3/admin
SquareOne> cd /
SquareOne> ll
drwxr-sr-x  7 root  users      4096 Aug 21  2007 system
drwxr-xr-x  2 root  root       1024 Jan  7 15:19 tmpmnt
drwxr-xr-x  9 root  root         0 Jan  7 15:19 sys
drwxr-xr-x  2 root  root      1024 Sep 12  2007 volume2
drwxr-xr-x  2 root  root      1024 Sep 12  2007 volume1
drwxr-xr-x 10 root  root      1024 Jan  7 15:21 var
drwxrwxrwx  3 root  root      1024 Jan  7 15:21 tmp
drwxrwxrwx  2 root  root      1024 Jun 30  2007 root
dr-xr-xr-x 83 root  root         0 Jan  7 15:19 proc
drwxr-xr-x  3 root  root      1024 Jan  7 15:20 mnt
drwxr-xr-x  3 root  root      1024 Jan  7 15:21 lib
drwxr-xr-x  2 root  root      1024 Sep 12  2007 initrd
drwxrwxrwx  3 root  root      1024 Jan  7 15:21 home
drwxr-xr-x  5 root  root      4096 Jan  7 15:21 dev
drwxr-xr-x  7 root  root      2048 Jan  7 15:21 etc
drwxr-xr-x  9 root  root      1024 Jan  7 15:20 usr
drwxr-xr-x  2 root  root      1024 Jan  7 15:20 sbin
lrwxrwxrwx  1 root  root         11 Sep 12  2007 linuxrc -> bin/busybox
drwxr-xr-x  2 root  root      1024 Jan  7 15:21 bin
drwx----- 2 root  root     12288 Sep 12  2007 lost+found
drwxr-xr-x 21 root  root      1024 Jan  7 15:20 ..
drwxr-xr-x 21 root  root      1024 Jan  7 15:20 .
SquareOne>
```

Figure 32

Executing commands with elevated privileges

Certain kinds of operations you might want to execute in the CLI, such as deleting orphan folders, cannot be executed with ordinary user privileges. For such operations, you need to use the **su** command to temporarily elevate your privileges to that of the built-in **root** user, who has unlimited privileges. (For security reasons, your Personal Server does not permit anyone to log in to the CLI as **root**.)

To execute commands as root:

7. At the **SquareOne>** prompt, enter **su**.
8. When prompted for the root password, enter **squareone**.
9. Enter commands as needed.
10. When you are finished, enter **exit** to return to user mode.

To delete an orphan folder:

1. Use the **cd** command to change to the parent directory of the folder you want to delete (for example, **cd /mnt/ide3/**).
2. Execute the **su** command and enter the root password, **squareone**.
3. Use **rm -r *dirname***, where *dirname* is the name of a folder, to delete the desired folder and all its contents (for example, **rm -r gerald**).
4. Enter **exit** to return to user mode.

Product Registration

Thank you for using SquareOne.

We are receiving customer registration through our online customer registration page. We are looking for product improvements and a more complete technical support and A/S by listening to our customers' opinions.

- ◆ How to Register : Connect to squareone homepage (<http://www.myitian.com>) and click on customer registration on the upper right hand corner of the main page. Fill out the customer registration form online and you will be registered as our member. Customers who are already registered can use the existing user ID and password to submit customer suggestions.

Our registered members will receive regular updates on our new product and events with easier access to technical support and A/S.

HQ Customer Support Center

Itian Corporation

4F YoungHo Building. 1605-1 Seocho-dong, Seocho-gu Seoul, 137-070, Korea.

Tel : 02-6677-6730 / Fax : 02-6677-6704

E-Mail: squareone@myitian.com / <http://www.myitian.com>

Product Warranty

Model Name		Serial Number	
Customer Name		Customer Phone No	
Customer Address			
Place of Purchase		Place of Purchase	
Place of Purchase Address			
Date of Purchase	Year	Month	Date

◆ **Warranty Period - 1 Year**

Warranty period without compensation is calculated from the date of purchase, so please be sure to keep a statement indicating the date of purchase. If purchase date cannot be confirmed, product warranty period is calculated from 3 months after the product manufacturing date.

◆ **Free of Charge Service**

Service is provided free of charge for any performance or functional related faults occurring within 1 year of purchase (within product warranty period) under normal usage conditions.

Major faults in product quality within 30 days of product purchase will be compensated through an exchange to a new product or cash refund.

◆ **Charged Services**

1. Faults caused by customer negligence.

Faults caused by customer negligence or repair and modification.

Faults caused by repairs performed by persons other than the sales person or service center technician.

Faults and damages caused by dropping after installation.

Faults caused by use of incorrect power or by connecting to malfunctioning devices.

2. Faults caused by other reasons such as natural disaster. (i.e. fire damage, salt damage, flood damage).

3. Service requests for products with no fault will incur service charges, so please make sure you read the user manual before requesting for service. (A separate guideline will be applied for cases that cannot be repaired)

◆ Make sure to back up important data from Hard Disk Drive as Itian will not be responsible for any damages or loss caused by data loss.

Please contact customer support center or the place of purchase for any product failure.

