BRICKServer 2

Installation, Configuration and Administration

Table of Contents

Chapter 1.

Introduction

Thank you for purchasing the BRICKServer 2 Appliance, and welcome to the world of secure Web servers. The BRICKServer 2 is intended to be a user-friendly and easy-to-operate tool. It is designed for those who want to run Web sites, FTP and mail services in-house — without having to wrestle with giant manuals or learn arcane computer security techniques. It is software using Process-Based Security to keep these services running fast and without crashes — while keeping out hackers.

BRICKServer 2 is easy to manage. Novice systems administrators can set it up in minutes. You may administer it from anywhere, even across the Internet, using the secure remote administration and secure configuration programs that run on a *Windows* desktop.

Our goal…is to provide the capability to take full advantage of a secure Internet presence insuring internal and external hackers cannot compromise your Web site.

Our commitment…is to develop and provide reliable Web security products meeting the security needs of your business.

Our security approach…is designed to provide affordable, bulletproof protection. We offer a resilient Web site security solution addressing the challenges of the ever-expanding online marketplace.

About BRICKServer 2

This manual describes the setup, configuration, and administration of the BRICKServer 2 by using step-by-step instructions.

- **Setup**—Physical and initial setup of the BRICKServer 2.

- **Configuration**—Configure the BRICKServer 2 to meet your needs.

- **Administration**—Administer the BRICKServer 2 remotely using a computer connected either to the Internet or the same network as the BRICKServer 2. This computer is commonly referred to as a "client".

Four categories of people can access the BRICKServer 2:

- **BRICKServer 2 Owner(s)**—Determines the following aspects of the BRICKServer 2.

    ♦ Physical location

    ♦ IP address(es)

    ♦ Domain(s) and who can access

     ◆ Sets up the Administrator(s)

- **Domain Administrator(s)**—Set up other administrators and could also fall into the category of Other Administrators.

- **Other Administrator(s)**—Work with any combination of areas depending on their user rights, including Users, Web, POP3, FTP, Logging, Backup/Restore, and Certificates.

- **Users**—Access web pages and email services on the BRICKServer 2.

Technical Specifications

- **Hardened OS**—With Process-Based Security modifications

- **Webserver**—HTTP 1.1 compliant, thttpd/2.20c 29feb00 with BRICKServer 2 Modifications

- **Server Side Include (SSI)** —1.1 standard

- **Encryption**—When logging into the Appliance, MD5 Digital Signatures are used for initial authentication. AES is used for encryption of data transfers.

- **Perl**—Version 5.8

- **PHP**—Version 4.06

- **Python**—Version 1.5

- **TCL—**Version 8.4

BRICKServer 2 Support

Telephone .... 806-354-8185 or 800-580-0025

Email... support@sage-inc.com

Web site .... www.sage-inc.com

The SAGE Web site features a Frequently Asked Questions section as well as update downloads.

About this Manual

One chapter is devoted to each critical area, and sections within each chapter describe the features to which the chapter is devoted. The manual also contains a glossary of terms and an index for fast lookup of information by topic.

This manual contains chapters to explain the following.

- **Chapter 1-Introduction.** Fundamental information about the BRICKServer 2 and the layout of this guide.

- **Chapter 2-BRICKServer 2 Setup.** Physical and initial setup of the BRICKServer 2.

- **Chapter 3-BRICKServer 2 Secure Config.** Explains how the BRICKServer 2 owner and all administrative users can run the BRICKServer 2 remotely.

- **Chapter 4-BRICKServer 2 Secure Remote Admin.** Describes how to set up administrators and users for the domains on the BRICKServer 2.

- **Chapter 5-BRICKServer 2 Secure Config – Remote Command Line Interface.** A list of the commands available on the BRICKServer 2 along with their definitions.

- **Chapter 6-Advanced Web Topics**

- **Chapter 7-Additional Information**

- **Chapter 8-Glossary**

- **Chapter 9-List of Figures**

- **Chapter 10-Index**

Special Notations

Notes, Warnings, and Cautions in this manual alert you to potential hazards and point out operating hints and tips. Notes appearing after a procedure provide extra information. Warnings and Cautions precede hazardous actions. The use of these special notations is described in the following paragraphs.

<u>Notes</u>

A note brings a particular topic to your attention when further thought is warranted. It often describes what others might do in a given situation. Notes appear in the following format.

> **Note:**
>
> Commands are always executed by first typing the command and then pressing the Enter key on the keyboard (case is irrelevant, with the exception of passwords).

<u>Cautions</u>

A caution brings to your attention a possible problem that might occur, steering you away from action that may cause trouble. Cautions appear in the following format.

> **Caution:**
>
> **Federal and State laws must be reviewed before launching an official county Web site.**

Warnings

A warning focuses your attention on a problem or side effect that can occur in a specific situation. It often attempts to steer you away from a course of action that might cause trouble. When you see a warning, read it carefully because it will help you avoid possible problems. Warnings appear in the following format.

> **WARNING:**
>
> **Giving a user Administrative rights to Users is the same as giving that user rights to ALL the Administrative areas!**

Chapter 2.

BRICKServer 2 Setup

The BRICKServer 2 setup involves physically setting up the BRICKServer 2 appliance as well as initializing the settings. The BRICKServer 2 appliance is packaged with the following items.

- Power cord
- Documentation
- Client program CD

Use the following checklist before beginning the physical or initial setup.

☐ **Location**—Identify a location for the BRICKServer 2. The BRICKServer 2 Appliance is designed to fit into a server rack, or it can be placed on a table or desktop. Be careful not to block the air vents on the front, back or sides, and keep it out of direct sunlight and away from sources of heat.

☐ **Owner Password**—The BRICKServer 2 owner decides upon a password with which to secure the BRICKServer 2.

☐ **Power**—An available power outlet. Our suggestion is that the BRICKServer 2 be connected to an Uninterruptible Power Supply (UPS).

☐ **Client workstation**—A *Windows* 95, 98, 2000, NT, or XP computer with the ability to connect to the BRICKServer 2 either via the Internet or on the same network.

☐ **Domain Name Service (DNS) entries**—Records that allow other systems on the Internet to find the BRICKServer 2. The Internet Service Provider (ISP) usually takes care of DNS entries. If BRICKServer 2 will be used to handle email, let the ISP know so the proper entry can be made.

☐ **IP Address**—Each computer and server on the Internet has at least one IP (Internet Protocol) address that uniquely identifies it from all other computers on the Internet. 10.1.1.2 is an example of an IP address. Your ISP or network administrator can provide you with the IP Address of your computer and/or BRICKServer 2.

☐ **Subnet Mask**—The Subnet Mask identifies the portion of the Internet Address that identifies the network and/or subnetwork for routing purposes. Subnetting is a technique used to allow a single IP network address to span multiple physical networks. Your ISP or network

administrator can provide you with the Subnet Mask of your computer and/or BRICKServer 2.

☐ **Gateway**—A network point that acts as an entrance to another network. The Gateway Address is the address of the computer that connects your BRICKServer 2 to the Internet. Your ISP or network administrator can provide you with the Gateway address of your computer and/or BRICKServer 2.

☐ **Ethernet Port**—The Ethernet Port is the interface connecting the BRICKServer 2 to the Internet or network is also referred to as a NIC (Network Interface Card). It uses a cable known as a patch, CAT-5 or Ethernet cable, having a RJ-45 connection. BRICKServer 2 knows the NIC as ETH. The interface naming convention is determined by how many network interface cards (NIC) are in the BRICKServer 2 and how many IP addresses (up to 64 per NIC) will be added to each NIC. The naming convention of ETHN:N is used to name the interface. The first interface, for example, would be named ETH0, the second interface would be named ETH0:1.

Physical Setup

The BRICKServer 2 can be maintained from anywhere on the Internet as long as it is connected to the Internet via a network or other type of network connection such as broadband, DSL, etc.

1. Move the BRICKServer 2 to the predetermined location and connect it to a power source, monitor, and keyboard.

2. Connect the BRICKServer 2 to the Internet connection using a network cable. The network cable connection is on the back of the unit and looks like the following.

Figure 1. Network Cable Connection on the BRICKServer 2

When viewing the back of the Mini BRICKServer 2 (Figure 2), you will notice two network cable connections. The connection located in the middle of the panel is the main interface and is referred to as ETH0. The one next to the mouse connection is the secondary interface, or ETH1. It is important to note which is used.
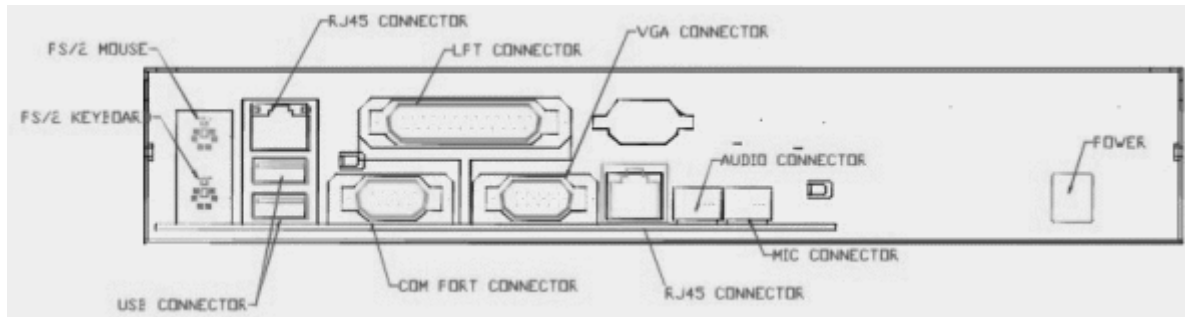
Figure 2. Back View of the Mini BRICKServer 2

When viewing the back of the Rack Mount BRICKServer 2 (Figure 3), you will notice two network cable connections. The connection located in the middle of the panel is the main interface and is referred to as ETH0. The one next to the mouse connection is the secondary interface, or ETH1. As with the Mini BRICKServer 2, it is important to note which is used.

Figure 3. Back View of the Rack Mount BRICKServer 2

3. Connect the power cord from the BRICKServer 2 to a power outlet or UPS and proceed with the Initial Setup (refer to page 2-3).

Initial Setup

The BRICKServer 2 owner performs the initial setup after completing the physical setup.

1. Turn on the power to the BRICKServer 2.

    ● Rack mount servers have two power switches. Once the switch on the back has been flipped, the front switch can be used to turn the BRICKServer 2 on and off.

    ● Looking at the front of the Mini BRICKServer 2, the power button is located on the right.

2. Type a password of **at least 7 characters** that will be used to secure the BRICKServer 2, and press Enter. This password is considered to be the BRICKServer 2 owner password.

    It is critical for you to create a good, strong password that is impossible to guess and to safeguard your password from others by not writing it down. The strongest passwords will be at the very least eight characters long and include lower and upper case letters of the alphabet, numbers, and other keyboard characters, for example:

Example:

```
4Ppl3+L1Z4Rd
```

3. Type the owner password again, and press Enter to set the password on the BRICKServer 2.

> **Note:**
>
> Going forward, commands discussed in this manual are always executed by first typing the command and then pressing the Enter key on the keyboard (case is irrelevant, with the exception of passwords).

4. Type the owner password to log into the BRICKServer 2.

5. Each computer and server on the Internet has at least one IP (Internet Protocol) address that uniquely identifies it from all other computers on the Internet. 10.1.1.2 is an example of an IP address. Your ISP or network administrator can provide you with the IP address of your computer and/or BRICKServer 2.

   The Subnet Mask identifies the portion of the Internet Address that identifies the network and/or subnetwork for routing purposes. Subnetting is a technique used to allow a single IP network address to span multiple physical networks. Your ISP or network administrator can provide you with the Subnet Mask of your computer and/or BRICKServer 2.

   The Interface is the physical connection to the network and is also referred to as a NIC (Network Interface Card). The BRICKServer 2 knows the NIC as ETH. Depending on the number of NICs in the BRICKServer 2, they are known as ETH0, for the first and ETH1 as the second.

   Add the IP address to the BRICKServer 2 by executing the following ADDIP command, replacing NNN.NNN.NNN.NNN with the IP address, SSS.SSS.SSS.SSS with the subnet mask, and ETHN with the interface.

Command:

```
ADDIP <NNN.NNN.NNN.NNN> <SSS.SSS.SSS.SSS> <ETHN>
```

Example:

```
ADDIP 12.210.115.190 255.255.255.0 ETH0
```

   Review the information presented on the monitor and ensure that the words full-duplex appear. If the words half-duplex appear, use the DELIP command

(5-9) to remove the IP address and then add a different IP address using the ADDIP command.

6. A gateway is a network point that acts as an entrance to another network. The Gateway Address is the address of the computer that connects your BRICKServer 2 to the Internet. Your network administrator or ISP can provide you with the Gateway address of your computer and/or BRICKServer 2.

    Set up the gateway by executing the following ADDGATEWAY command, replacing NNN.NNN.NNN.NNN with the destination, SSS.SSS.SSS.SSS with the subnet mask, GGG.GGG.GGG.GGG with the gateway address, and ETHN with the interface as in the following command example.

    Command:

    `ADDGATEWAY <NNN.NNN.NNN.NNN> <SSS.SSS.SSS.SSS> <GGG.GGG.GGG.GGG> <ETHN>`

    Use the following example to add a gateway for a non-complex network or other type of network connection such as broadband, DSL, etc. The zeros denote there is no other route, other than the gateway.

    Example:

    `ADDGATEWAY 0.0.0.0 0.0.0.0 12.210.115.1 ETH0`

    The following example shows how to route the gateway for a more complex network, for instance, one that uses a firewall. The IP address of 12.210.115.190 is the firewall, 255.255.255.0 is the Subnet Mask of that firewall, and 12.210.115.1 is the Gateway address to the firewall.

    Example:

    `ADDGATEWAY 12.210.115.190 255.255.255.0 12.210.115.1 ETH0`

    Notes:

    Unless a specific Route is designated, add only ONE gateway per interface as adding more than one gateway per interface can cause conflicts when adding or deleting IP addresses.

    Always add the IP address first and then the Gateway address. When removing an IP address, always remove the Gateway address first and then the IP address. Use SAVECONFIG and then VIEWCONFIG after executing each command.

7. Save the configuration by executing the following SAVECONFIG command.

   `SAVECONFIG`

   > **Note:**
   >
   > The VIEWCONFIG command can be used to check the configuration.

The BRICKServer 2 is now setup. Additional commands are executed from a remote client using the BRICKServer 2 Secure Config (Chapter 3), the BRICKServer 2 Secure Remote Admin (Chapter 4), and the BRICKServer 2 Secure Config – Remote Command Line Interface (Chapter 5).

Chapter 3.

BRICKServer 2 Secure Config

The **BRICKServer 2 Secure Config** provides the BRICKServer 2 owner and all administrative users with the ability to run the following functions from remote locations.

- Manage IP Addresses, Domains, DNS Entries, and Route Entries
- Shutdown and reboot the BRICKServer 2
- Run Web, Mail, FTP, and SSL services
- Apply software updates
- Save the configuration
- Change the password, date, and time

> **Warning:**
>
> Changes made to IP Addresses, Domains, DNS Entries, Route Entries, and Running Services will only be saved after using the Save Configuration button.

Install the BRICKServer 2 Secure Config

Administrators who use BRICKServer 2 Secure Config will need to install it onto their desktop or laptop computer by following these instructions.

1. Insert the CD into the CD-ROM drive.
2. Follow the on-screen instructions for installing BRICKServer 2 Secure Config.

Connect to the BRICKServer 2

1. Run BRICKServer 2 Secure Config by selecting Start, Programs, BRICKServer 2, Config (or the location specified during installation). The BRICKServer 2 Secure Config window will open (Figure 4).
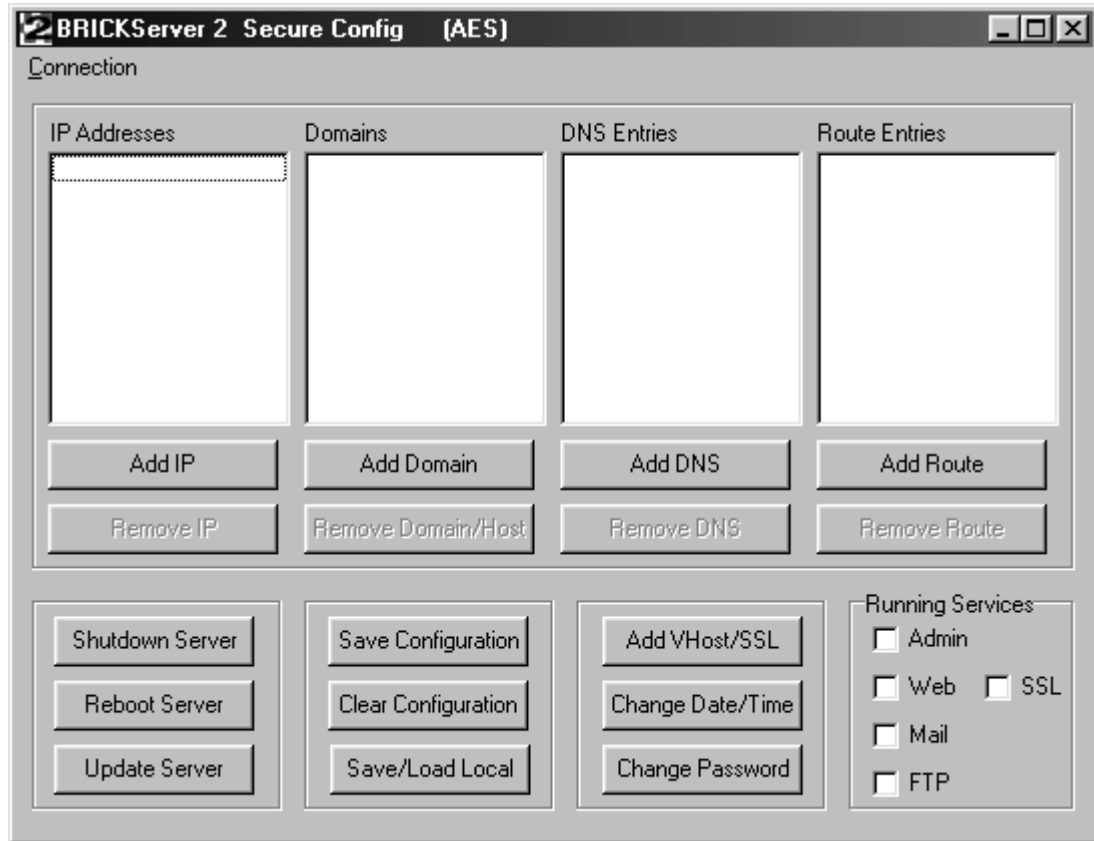
Figure 4. BRICKServer 2 Secure Config Window (pre-connection)

2.   Connect to the BRICKServer 2 by selecting Connection, Connect (Figure 5).
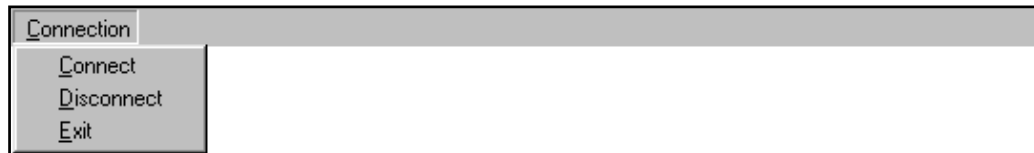
Figure 5. Connection Menu

3.   Type the IP address or domain of the BRICKServer 2 into the Address field of the Login window (Figure 6).
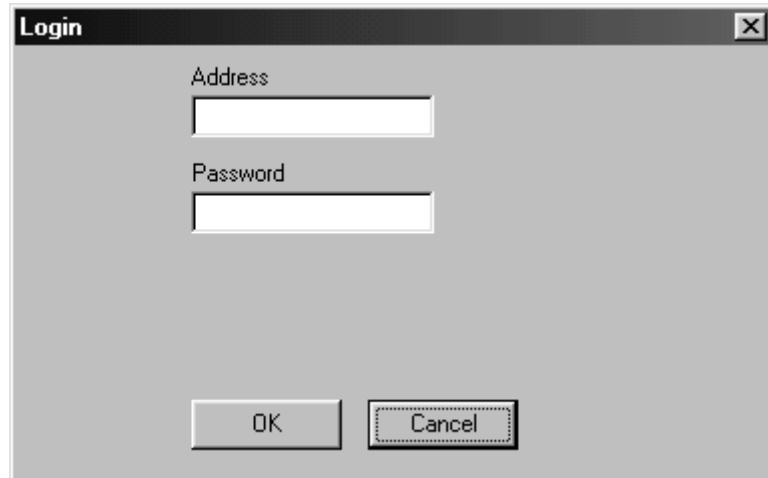
Figure 6. Login Window

4.   Type the BRICKServer 2 owner's password into the Password field.

5.   If the incorrect IP address / domain or password is typed during Login, a Connection Error window will appear (Figure 7).

Figure 7. Connection Error Window

6.   Click OK, and select Connection, Connect to begin again.

7.   When the correct IP address / domain or password is typed during Login, The Host Machine Available window will appear (Figure 8).

Figure 8. Host Machine Available Window

8.   Select OK and the BRICKServer 2 Secure Config window will reappear with data from the BRICKServer 2 populating the IP Addresses, Domains, DNS Entries, and Route Entries list boxes (Figure 9).
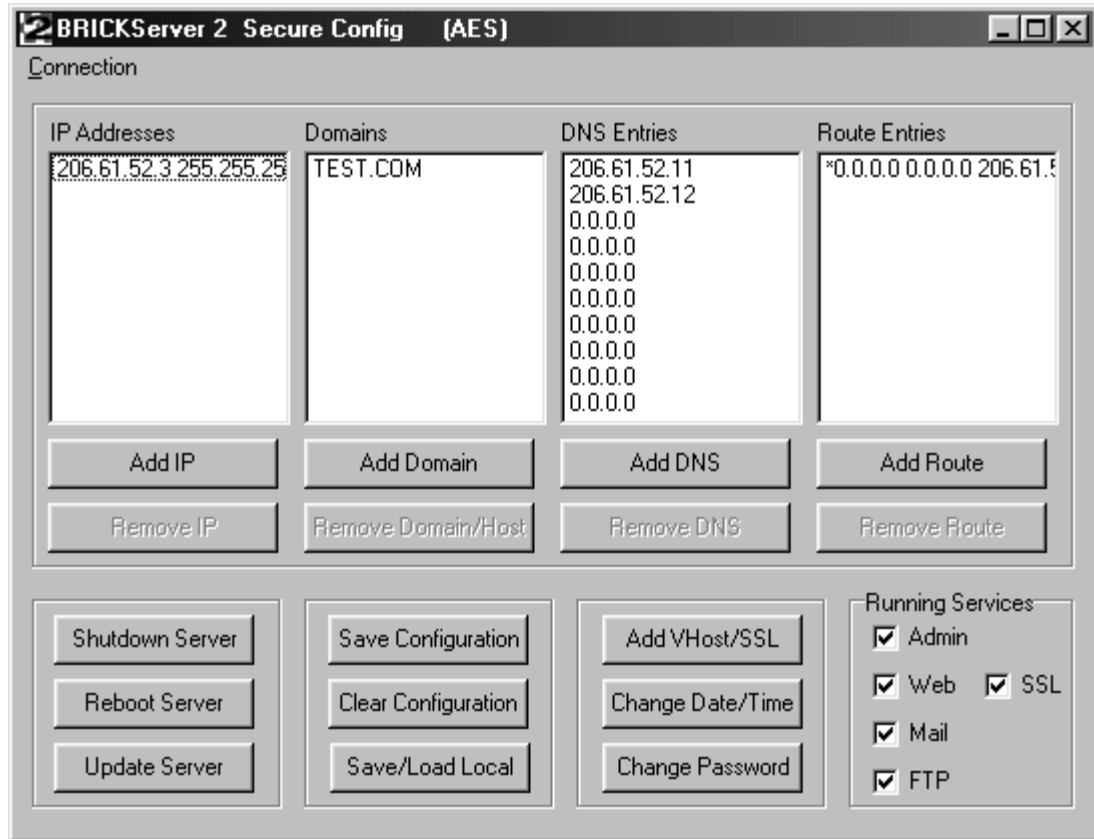
Figure 9. BRICKServer 2 Secure Config Window

Note:

Double-click to view IP Addresses, Domains, DNS Entries, and Route Entries that are too long to display on the screen.

Warning:

Again, changes made to IP Addresses, Domains, DNS Entries, Route Entries, and Running Services will only be saved after using the Save Configuration button.

Disconnect from the BRICKServer 2

When finished using BRICKServer 2 Secure Config, disconnect to ensure security by using the following steps.

1. Select Connection, Disconnect (Figure 5) to disconnect from the BRICKServer 2.

2. Close the BRICKServer 2 Secure Config by selecting Connection, Exit.

IP Addresses

IP addresses can be added and removed using the BRICKServer 2 Secure Config.

Add an IP Address

Add a new IP Address to the domain by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2. When viewing the BRICKServer 2 Secure Config window (Figure 9), select Add IP and the Add IP window will open (Figure 10).

Figure 10. Add IP Window

3. Type a unique IP Address into the IP Address field. Each computer and server on the Internet has at least one IP (Internet Protocol) address that uniquely identifies it from all other computers on the Internet. 10.1.1.2 is an example of an IP address. Your ISP or network administrator can provide you with the IP address of your computer and/or BRICKServer 2.

> **Example:**
>
> `12.210.145.205`

4.   Type the Subnet Mask into the Network Mask field. The Subnet Mask identifies the portion of the Internet Address that identifies the network and/or subnetwork for routing purposes. Subnetting is a technique used to allow a single IP network address to span multiple physical networks. Your ISP or network administrator can provide you with the Subnet Mask of your computer and/or BRICKServer 2.
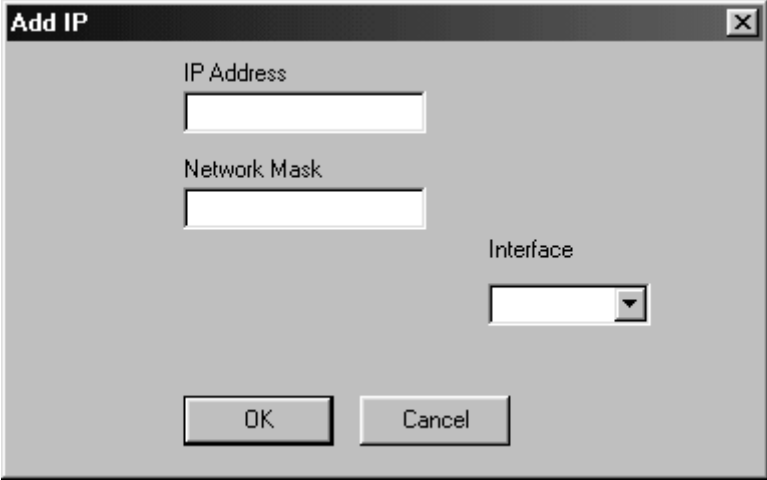
> **Example:**

`255.255.255.0`

5.   Type the interface into the Interface field. The interface is the physical connection to the network and is also referred to as a NIC (Network Interface Card). The BRICKServer 2 knows the NICs as ETH. Depending on the number of NICs in the BRICKServer 2, they are known as ETH0, for the first, and ETH1 as the second.

> **Example:**

`ETH0`

6.   Select OK, the BRICKServer 2 Secure Config window will appear (Figure 9). If all information was entered correctly, the new IP Address will be listed in the IP Addresses list box.

7.   Select Save Configuration.

8.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Remove an IP Address

Delete an IP Address from the domain by following these steps.

> **Note:**
>
> When deleting an IP address, delete the gateway first by using Remove Route. Use Save Configuration after using each feature.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   When viewing the BRICKServer 2 Secure Config window (Figure 9), select the IP address from the IP Addresses list.

3.   Select Remove IP to simultaneously remove the IP Address from the BRICKServer 2 and the IP Addresses list box.

4.   Select Save Configuration.

5.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Domains

The limitation to the number of domains (i.e. virtual hosts) that can be added is dictated by the amount of available disk space on the BRICKServer 2.

Add a Domain

Add a new domain to the BRICKServer 2 by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2. When viewing the BRICKServer 2 Secure Config window (Figure 9), select Add Domain and the Add Domain window will open (Figure 11).

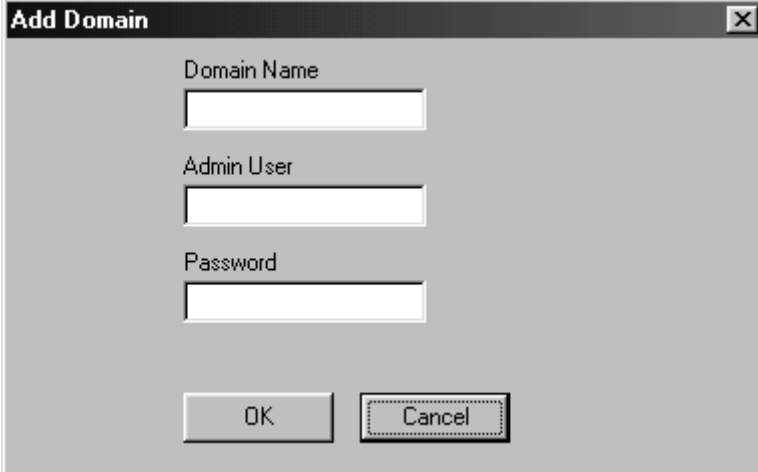*Figure 11. Add Domain Window*

3. Type a new domain name into the Domain Name field, excluding www.

   Example:

   `MYWEBSITE.COM`

4. When working with domains, it is necessary to assign an administrator and administrator password. Type a name for the domain administrator into the Admin User field.

   Example:

   `MYDOMAINADMIN`

   Note:

   All users much be unique to each domain.

5.   Type a password **at least 7 characters** for the administrator in the Password field using any combination of alphabetical characters, numbers, spaces, and symbols. As a security precaution, the password will be displayed as asterisks ("*").

> **Example:**

`DOMAINADMINPASSWORD$123`

6.   Select OK.

7.   At this point, add the virtual host of www.<domain name>.com by selecting Add VHost/SSL and the Add VHost/SSL window will appear (Figure 12).
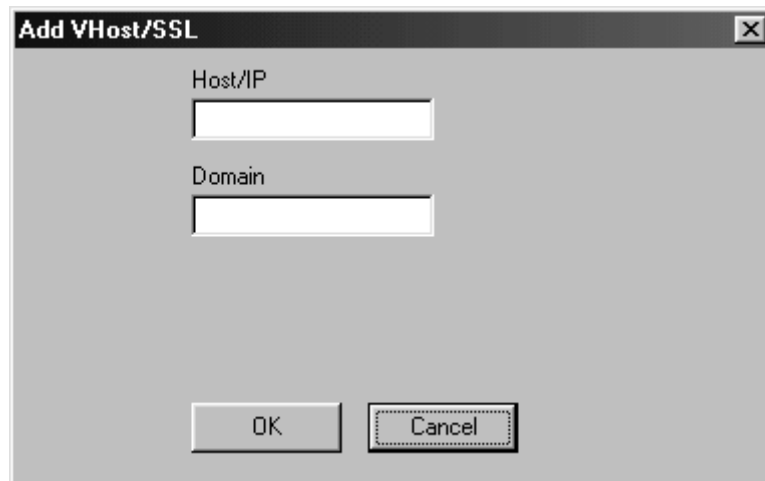
Figure 12. Add VHost/SSL Window

8.   Type host name or the IP address into the Host/IP field.

9.   Type the domain name into the Domain field.

10. Select OK, the BRICKServer 2 Secure Config window will appear (Figure 9). If all information was entered correctly, the new Domain will be listed in the Domains list box.

11. Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Remove a Domain

Delete a domain by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   When viewing the BRICKServer 2 Secure Config window (Figure 9), select the domain from the IP Domains list.

3. Select Remove Domain to simultaneously remove the domain from the BRICKServer 2 and the Domains list box.

4. Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

DNS Entries

The DNS (Domain Name Service) entries translates domain names into IP addresses, allowing others on the Internet to find your BRICKServer 2. A maximum of 10 DNS entries can be set on the BRICKServer 2.

Add a DNS Entry

Add a new DNS Entry to the BRICKServer 2 by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2. When viewing the BRICKServer 2 Secure Config window (Figure 9), select Add DNS and the Add DNS window will open (Figure 13).
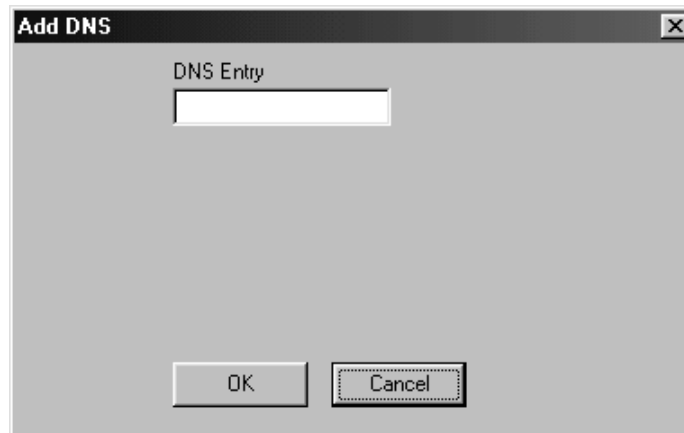
Figure 13. Add DNS Window

3. Type the DNS entry into the DNS Entry field.

> **Example:**
>
> `12.210.115.50`

4. Select OK, the BRICKServer 2 Secure Config window will appear (Figure 9). If all information was entered correctly, the new DNS entry will be listed in the DNS Entries list box.

5. Select Save Configuration.

6. Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Remove a DNS Entry

Delete a DNS entry by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   When viewing the BRICKServer 2 Secure Config window (Figure 9); select the DNS entry from the DNS Entries list.

3.   Select Remove DNS to simultaneously remove the DNS entry from the BRICKServer 2 and the DNS Entries list box.

4.   Select Save Configuration.

5.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Route Entries

The Route Entries feature of the BRICKServer 2 Secure Config is designed to add routes and gateways to the network interface.

Add a Gateway

> **Note:**
>
> Unless a specific route is designated, add only ONE gateway per interface as adding more than one gateway per interface can cause conflicts when adding or deleting IP addresses.

Add a gateway to the BRICKServer 2 by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   When viewing the BRICKServer 2 Secure Config window (Figure 9), select Add Route and the Add Route window will open (Figure 15).
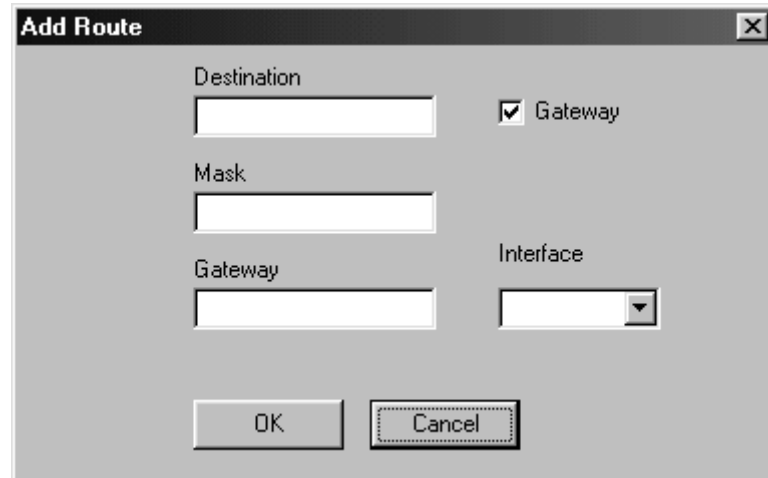
Figure 14. Add Route Window

3.   Click to insert a check mark in the Gateway checkbox.

4.   Type 0.0.0.0 into the Destination field.

5.   Type 0.0.0.0 into the Mask field.

6.   Type the Gateway Address into the Gateway field. The Gateway Address is the address of the computer that connects your BRICKServer 2 to the Internet. Your network administrator or ISP can provide you with the Gateway address of your computer and/or BRICKServer 2.

> **Example:**
>
> `255.255.255.0`

7.   Type the interface into the Interface field. BRICKServer 2 knows the network interface card (NIC) as ETH. The interface naming convention is determined by how many network interface cards (NIC) are in the BRICKServer 2 and how many IP addresses (up to 64 per NIC) will be added to each NIC. The naming convention of ETHN:N is used to name the interface. The first interface, for example, would be named ETH0 and the second interface would be named ETH0:1.

8.   Select OK, the BRICKServer 2 Secure Config window will appear (Figure 9). If all information was entered correctly, the gateway will be listed in the Route Entries list box.

9.   Select Save Configuration.

10.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.
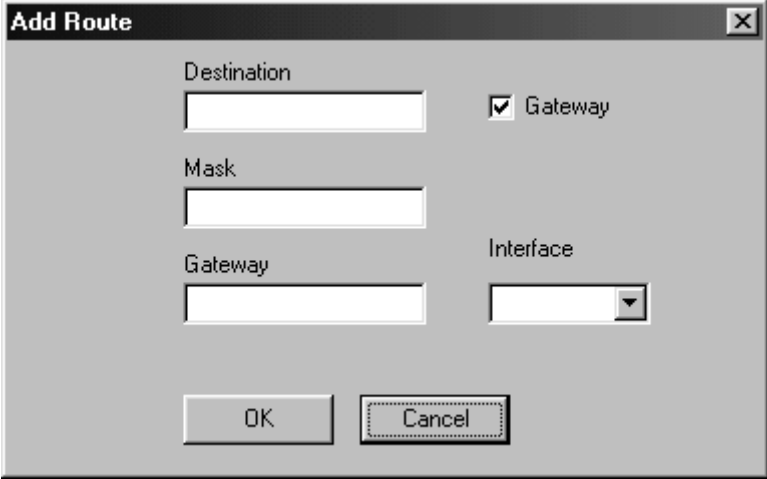
Add a Route Entry

> **Note:**
>
> Unless a specific Route is designated, add only ONE gateway per interface as adding more than one gateway per interface can cause conflicts when adding or deleting IP addresses.

Standard BRICKServer 2 configurations will use one gateway per NIC but route entries can be added if desired or specified by the network administrator. Add a Route Entry to the BRICKServer 2 by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2. When viewing the BRICKServer 2 Secure Config window (Figure 9), select Add Route and the Add Route window will open (Figure 15).

Figure 15. Add Route Window

3. Click to remove the check mark from the Gateway checkbox.

4. Type the destination IP address into the Destination field. Each computer and server on the Internet has at least one IP (Internet Protocol) address that uniquely identifies it from all other computers on the Internet. 10.1.1.2 is an example of an IP address. Your ISP or network administrator can provide you with you with the IP Address of your computer and/or BRICKServer 2.

> **Example:**
>
> `12.210.145.205`

5. Type the Subnet Mask into the Mask field. The Subnet Mask identifies the portion of the Internet Address that identifies the network and/or subnetwork for routing purposes. Subnetting is a technique used to allow a single IP

network address to span multiple physical networks. Your ISP or network administrator can provide you with the Subnet Mask of your computer and/or BRICKServer 2.

> **Example:**

`0.0.0.0`

6. Type the Gateway Address into the Gateway field. A gateway is a network point that acts as an entrance to another network. The Gateway Address is the address of the computer that connects your BRICKServer 2 to the Internet. Your network administrator or ISP can provide you with the Gateway address of your computer and/or BRICKServer 2.

> **Example:**

`255.255.255.0`

7. Type the interface into the Interface field. BRICKServer 2 knows the network interface card (NIC) as ETH. The interface naming convention is determined by how many network interface cards (NIC) are in the BRICKServer 2 and how many IP addresses (up to 64 per NIC) will be added to each NIC. The naming convention of ETHN:N is used to name the interface. The first interface, for example, would be named ETH0, and the second interface would be named ETH0:1.

8. Select OK, the BRICKServer 2 Secure Config window will appear (Figure 9). If all information was entered correctly, the Route entry will be listed in the Route Entries list box.

9. Select Save Configuration.

10. Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Remove a Route Entry

Delete a route entry by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2. When viewing the BRICKServer 2 Secure Config window (Figure 9); select the Route entry from the Route Entries list.

3. Select Remove Route to simultaneously remove the Route entry from the BRICKServer 2 and the Route Entries list box.

4. Select Save Configuration.

5. Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Shutdown Server

Shutdown Server is used to securely stop all services running on the BRICKServer 2, and turn off the power.

Shut down the BRICKServer 2 by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   When viewing the BRICKServer 2 Secure Config window (Figure 9), select Shutdown Server and the Server Shutdown window will appear (Figure 16).
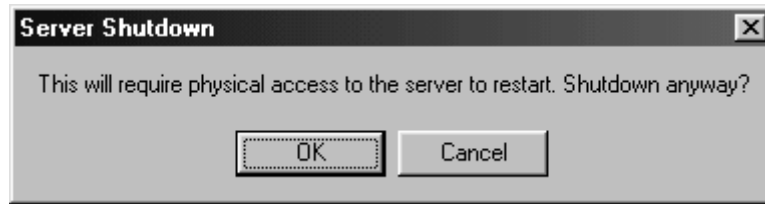

Figure 16. Server Shutdown Window

> **Note:**
>
> After using Shutdown Server, restart the BRICKServer 2 by physically going to the BRICKServer 2 and pushing the power button.

3.   Select OK to confirm that the BRICKServer 2 is to be shut down.

4.   Select Connection, Exit to close BRICKServer 2 Secure Config.

Reboot Server

Shutdown and restart the BRICKServer 2 without turning off the power by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   While viewing the BRICKServer 2 Secure Config window (Figure 9), select Reboot Server and the Reboot Server window will appear (Figure 17).

3.   Select OK to confirm the reboot.

Figure 17. Reboot Server Window

4.   Select Connection, Disconnect.

5.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Update Server

Updates to the BRICKServer 2 are done by the owner of the BRICKServer 2 or someone designated by the owner. This person would download self-extracting files from the BRICKServer 2 Web site and apply them to the BRICKServer.

Follow these steps to update the BRICKServer 2 with files that are downloaded from SAGE's Web site.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   Select Update Server and the Open window will appear (Figure 18).
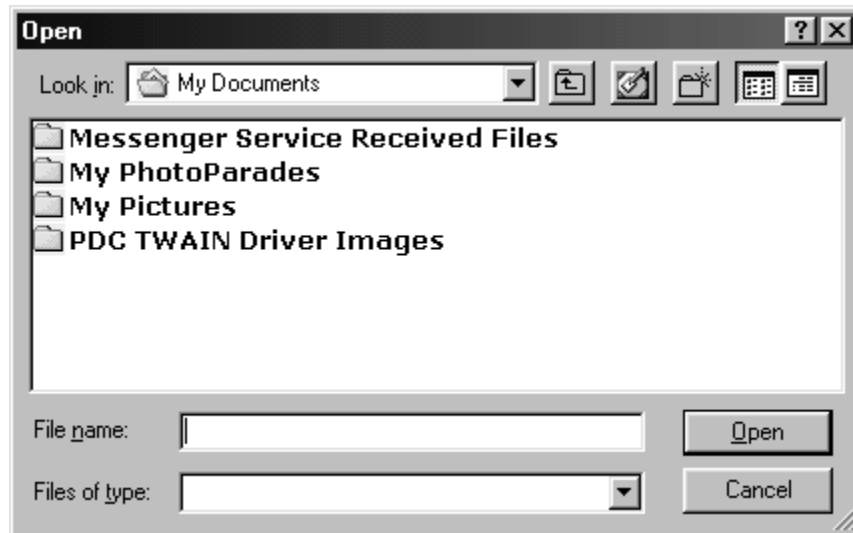

Figure 18. Open Window

3.   Go to the directory where the BRICKServer 2 update file is located.

4.   Click on the file name.

5.   Select Open to complete the process.

6.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Save Configuration

Save changes made to BRICKServer 2 the configuration by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2. Make the desired changes to the configuration.

3. Select Save Configuration and the Save window will appear (Figure 19).

Figure 19. Save Window

4. Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Clear Configuration

Clear Configuration is used to remove all the IP addresses, DNS entries, route entries and to stop all the services from running but does not remove domains.

> **Warning:**
>
> Use this feature wisely! Executing Clear Configuration will render the BRICKServer 2 unavailable to users.

> **Note:**
>
> Since changes are not cleared in memory, the IP addresses, DNS entries, and route entries can be reinstated and the services can be restarted by rebooting the BRICKServer 2, provided that Save Configuration had not been used.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2. Select Clear Configuration to remove all the IP Addresses, DNS Entries, and Route Entries, and to stop all Running Services.

3. If you are certain that the BRICKServer 2 is to be rendered unavailable to users, select Save Configuration. Otherwise, select Reboot Server.

4. Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Save/Load Local

Save/Load Local is used to save the configuration of the BRICKServer 2 to a text file on the client. The file can then be loaded onto subsequent servers using Load Local.

Save Local

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

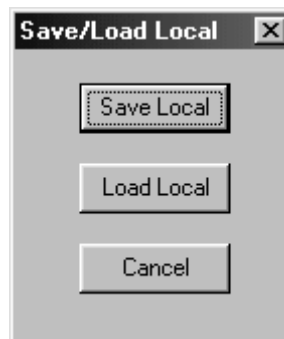2. Select Save/Load Local, the Save/Load Local window will appear (Figure 20).

Figure 20. Save/Load Local Window

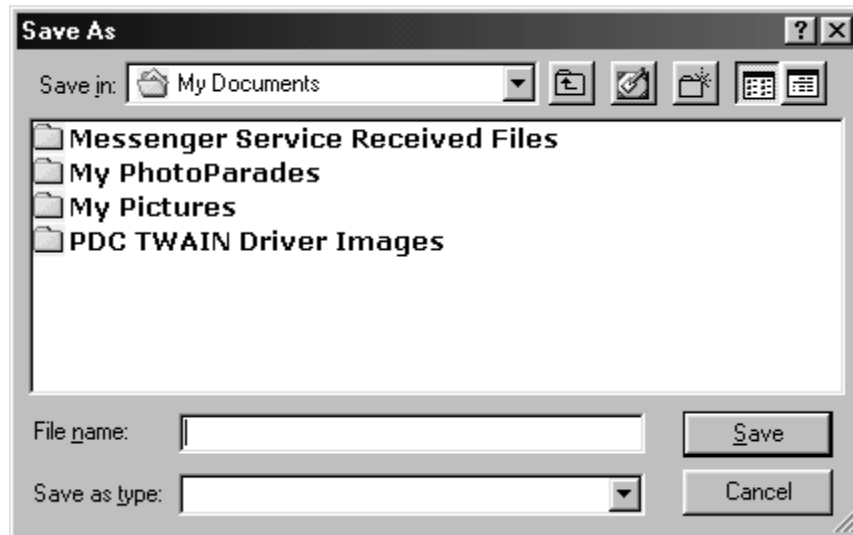3. Choose Save Local and the Save As window will appear (Figure 21).

Figure 21. Save As Window

4. Identify a folder on the client in which to store the text file.

5. Type a file name for the text file using the "**.txt**" extension.

6. Select Save to complete the process.

7. Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Load Local

> **Note:**
>
> Save Local saves the BRICKServer 2 configuration but, in the interest of security, excludes passwords. Before using Load Local, adding passwords by editing the text file is recommended

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2. Select Save/Load Local and the Save/Load Local window will appear (Figure 20).

Figure 22. Save/Load Local Window

3. Choose Load Local and the Open window will appear (Figure 23).
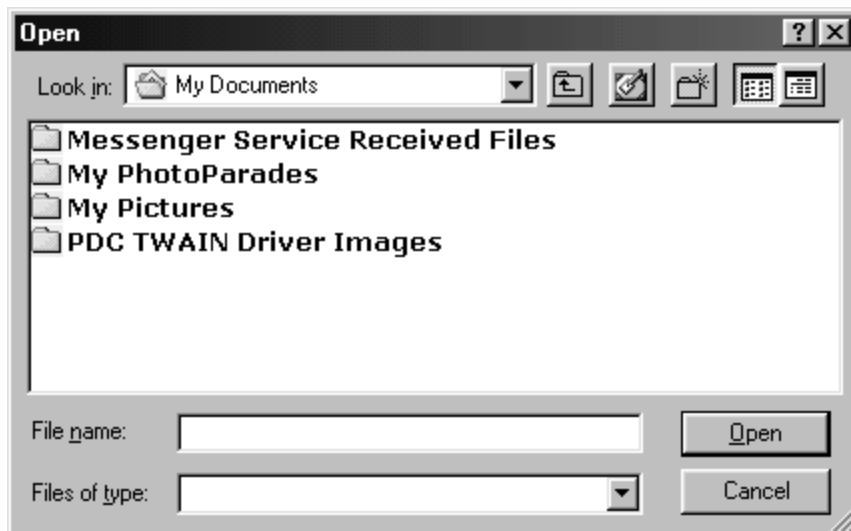
Figure 23. Open Window

4. Identify the folder on the client in which the text file created by using Save Local was stored.

5.   Select the file.

6.   Choose Open to complete the process.

7.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Add VHost/SSL

The prefix www is considered a virtual domain on the BRICKServer 2. The Add VHost/SSL feature links actual domains with virtual domains. When the actual domain is not linked with a virtual domain and a user types www.mydomain.com into a browser, it will not resolve.

This feature is used in tandem with Add Domain, refer to the section entitled Add a Domain on page 3-7 for additional information.

Change Date/Time

Use Change Date/Time to set the correct date and time for your time zone as demonstrated in the following steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

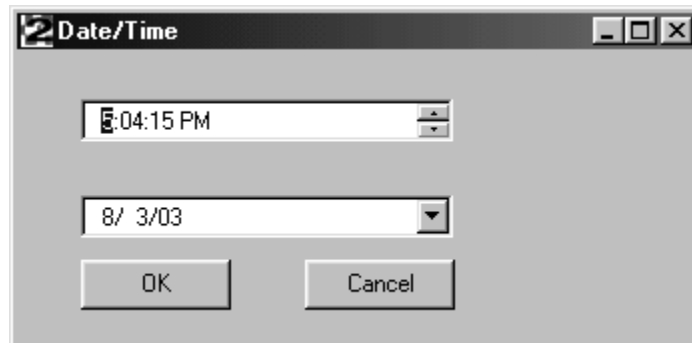2.   Select Change Date/Time and the Date/Time window will appear (Figure 24).

Figure 24. Date/Time Window

3.   Type the correct date and/or time into the appropriate fields.

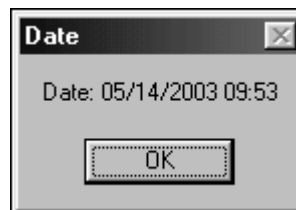4.   Select OK and the following Date window will appear (Figure 25).

Figure 25. Date Window

5.   Select OK, the BRICKServer 2 Secure Config window will appear (Figure 9).

6.   Select Save Configuration.

7.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Change Password

Change Password is used to change the password of the BRICKServer 2 and cannot be changed without having the original password.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   Select Change Password and the Change Password window will appear (Figure 26).

Figure 26. Change Password Window

3.   Type a new password into the New Password field.

4.   Type the password again into the Confirm New Password field.

5.   Select OK, the Password window will appear (Figure 26).

Figure 27. Password Window

6.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Running Services

The Running Services section of BRICKServer 2 Secure Config is used to identify which of the following services are allowed to run on the BRICKServer 2.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Config (refer to page 3-1).

2.   When viewing the BRICKServer 2 Secure Config window (Figure 9), select from the following service(s). A checkmark next to the service indicates that the service will start each time the BRICKServer 2 is rebooted.

   ● **Admin**—Allows the BRICKServer 2 to run admin services.

   ● **Web**—Allows the BRICKServer 2 to run Web services (HTTP).

   ● **Mail**—Lets the BRICKServer 2 send and receive Internet email using SMTP and POP3 protocols.

   ● **FTP**—Permits files to be uploaded to and downloaded from the designated FTP directories.

   ● **SSL**—A service for advanced users that allows the BRICKServer 2 to use the Secure Sockets Layer for transmitting data securely over the Internet. Before using SSL, it must be added to one of the domains. SSL can only be used with one domain per IP address. When using more than one NIC or more than one IP per NIC, ADDSSL/VHOST can be added to more than one domain but not to multiple domains on one IP, only multiple domains spread across multiple IPs.

3.   Use Connection, Disconnect when finished using BRICKServer 2 Secure Config, and Connection, Exit to close it.

Chapter 4.

BRICKServer 2 Secure Remote Admin

The **BRICKServer 2 Secure Remote Admin** is used to set up administrators and users for the domains on the BRICKServer 2. They can then work with any combination of areas, depending on their user rights, including Domain, HTTP, POP3, FTP, Log, Backup/Restore, and Certificates.

> **Note:**
>
> The BRICKServer 2 Secure Remote Admin is designed to log out the current user and shut down after periods of non-use.

> **Note:**
>
> The BRICKServer 2 Secure Remote Admin is designed in such a way that commands are executed in the background. In other words, the user can execute a command and go to another tab without waiting for the command to finish.

Administration Considerations

Is it possible to administer the BRICKServer 2 from across the Internet?
Administration can be performed on the BRICKServer 2 from across the Internet using BRICKServer 2 Secure Remote Admin. The connection will be fully encrypted, protecting the BRICKServer 2 against intruders.

Who should have administrative rights? The majority of computer system damage comes from insider mistakes and malicious attacks. For this reason, it is useful to limit BRICKServer 2 administrators. BRICKServer 2 Secure Remote Admin makes it easy to both administer and use the BRICKServer 2.

Administrative Assignments

The following Administrative Areas can be divided up amongst several people using BRICKServer 2 Secure Remote Admin.

- **Domain**—The domain administrator has rights to add, change, and delete administrator accounts, and change the primary backup/restore seed using the Users tab. The domain administrator also has ALL rights.

- **Web**—The Web administrator has rights to manage and transfer files between the client workstation and the BRICKServer 2 using the Web tab.

- **Mail Users**—The POP3 administrator, also called the Mail User administrator, has rights to add, change, and delete mail user accounts using the Mail Users tab.

- **FTP**—The FTP administrator has rights to add, change, and delete FTP user accounts.

- **Logging**—The Logging administrator has rights to save log files to the local workstation and clear log files on the BRICKServer 2.

- **Backup**—The Backup administrator has rights to create secure backup files and restore them to the BRICKServer 2.

- **Certificates**—The Certificates administrator has rights to set up and manage certificates on the BRICKServer 2.

Install the BRICKServer 2 Secure Remote Admin

Administrators who use BRICKServer 2 Secure Remote Admin will need to install it onto their desktop or laptop computer by following these instructions.

1. Insert the CD into the CD-ROM drive.

2. Follow the on-screen instructions for installing the BRICKServer 2 Secure Remote Admin.

Connect to the BRICKServer 2

1. Run the BRICKServer 2 Secure Remote Admin by selecting Start, Programs, BRICKServer 2, Admin (or the location specified during installation). The Administrator Login Screen will open (Figure 28).

Figure 28. Administrator Login Screen

2. Log into the BRICKServer 2 Secure Remote Admin using the Administrator Login Screen.

3.   Type either the IP address or the Host name of the domain on the BRICKServer 2.

4.   Type either the User name or Administrator Account name.

5.   Type the password of the user / administrator account into the Account Password field. As a security precaution, the password will be displayed as asterisks ("*").

6.   Select Login. The BRICKServer 2 Secure Remote Admin window will open (Figure 29). Tabs will be visible for Users, Web, Mail Users, FTP, Logging, Restore, Backup, and Certificates, based on the rights assigned to the user by the domain administrator.
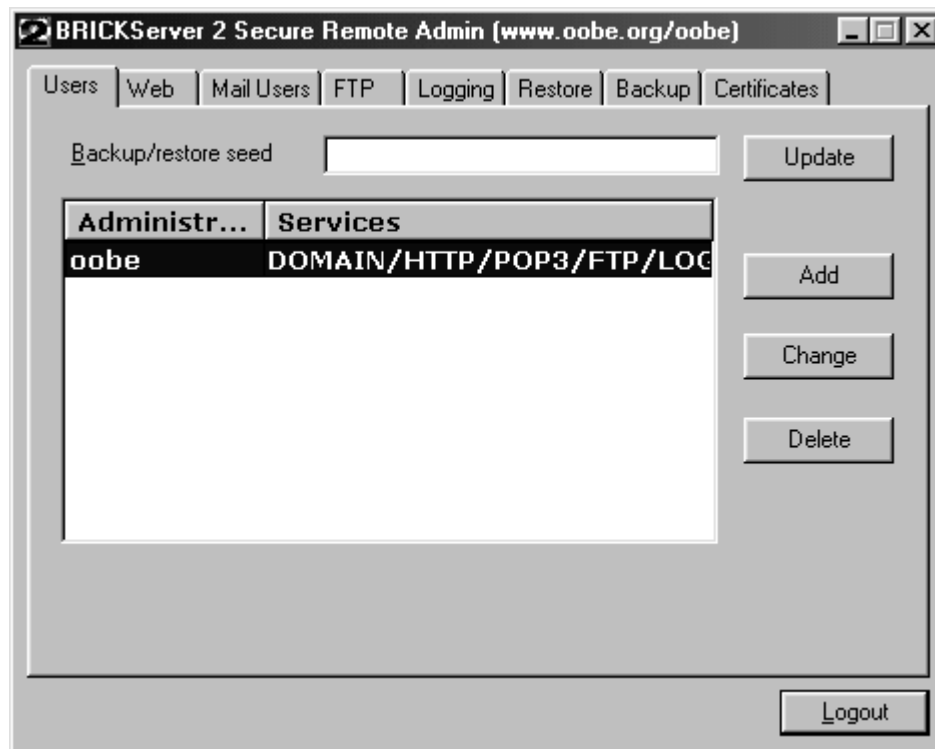
Figure 29. Users Tab

Disconnect from the BRICKServer 2

Use the following steps when finished with the BRICKServer 2 Secure Remote Admin.

1.   Choose Logout, located in the lower right corner of the BRICKServer 2 Secure Remote Admin window.

2.   Select Exit on the Administrator Login Screen.

Client Activity Log

The Client Activity Log window opens when using the BRICKServer 2 Secure Remote Admin showing a log of the results of the commands executed while using the BRICKServer 2 Secure Remote Admin.

Figure 30. Client Activity Log Window

Users Tab

The Users tab (Figure 29) allows the domain administrator to add, change, and delete administrator accounts, and change the primary backup/restore seed.

> **Note:**
>
> Only a Domain administrator can use the Users tab.

> **Note:**
>
> All users much be unique to each domain.

Add an Administrator

Add a new administrator by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Users tab (Figure 29), select Add and the Adding New Administrator window will open (Figure 31).
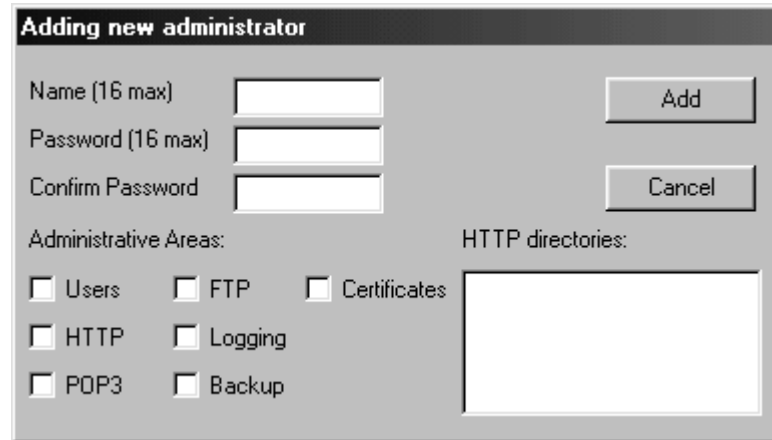
Figure 31. Adding New Administrator Window

3. Using their name or any combination of characters and numbers, type a unique name (up to 16 characters) for the new administrator in the Name field. Symbols and spaces are not permitted in the Name field, and case is irrelevant.

4. Type a password **at least 7 characters** for the administrator in the Password field using any combination of alphabetical characters, numbers, spaces, and symbols. As a security precaution, the password will be displayed as asterisks ("*").

5. Confirm the administrator's password by retyping it in the Confirm Password field.

    When adding an administrator, the password and confirmation password must be an exact match or the following error will occur.

Figure 32. Error Window

6. Select the Administrative Areas to which the administrator is assigned.

> **Warning:**
>
> **Giving a user Administrative rights to Users is the same as giving that user rights to ALL the Administrative areas!**

7. Specify the HTTP directories the administrator will access by typing each on a separate line in the HTTP Directories list box. Access automatically includes

all sub directories. The following example shows access granted to the administrator's web page directories.

> **Example:**

`/CGI-DATA/WEB_PAGE_FOR_ABC_COMPANY`

`/CGI-DATA/WEB_PAGE_FOR_XYZ_COMPANY`

The following example shows access granted to Joe's directory and includes all subdirectories.

> **Example:**

`/CGI-BIN/USERJOE`

The following example shows access granted to all directories.

> **Example:**

`/`

8.   Select Add, the BRICKServer 2 Secure Remote Admin window will appear (Figure 29). If all information was entered correctly, the new administrator will be listed in the Administrator column with the selected administrative areas listed under Services.

9.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Administrator with Rights to ALL Administrative Areas

Figure 33 shows an example of a setup for an administrator who would have rights to all the administrative areas of the BRICKServer 2. These administrators would see the window in Figure 34 upon login to BRICKServer 2 Secure Remote Admin.

Figure 33. Setup for an Administrator with Rights to all Administrative Areas
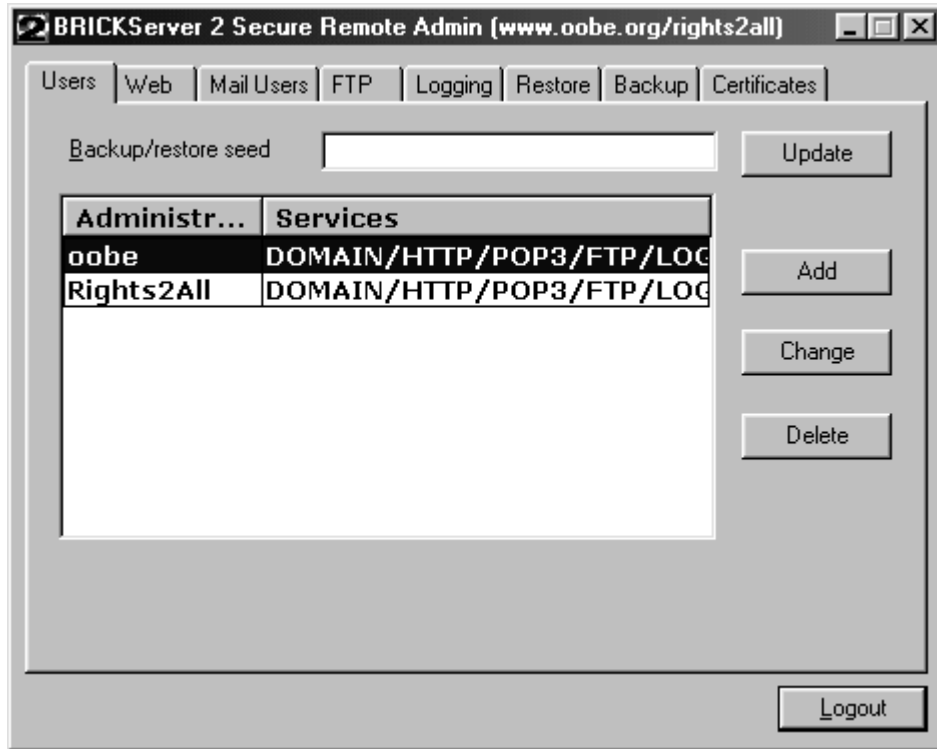
Figure 34. Administrator with all Rights

Administrator with HTTP Access

Figure 35 shows an example of a setup for an administrator who would have rights to only HTTP. These administrators would see the window in Figure 34 upon login to BRICKServer 2 Secure Remote Admin.
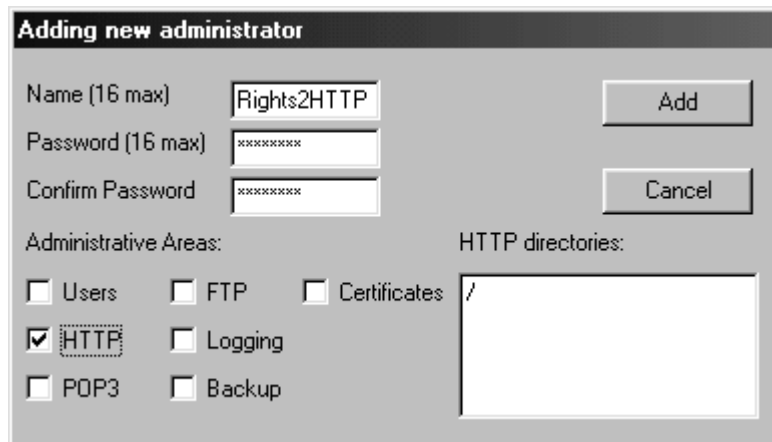

Figure 35. Setup for Administrator with Rights only to the HTTP Administrative Area
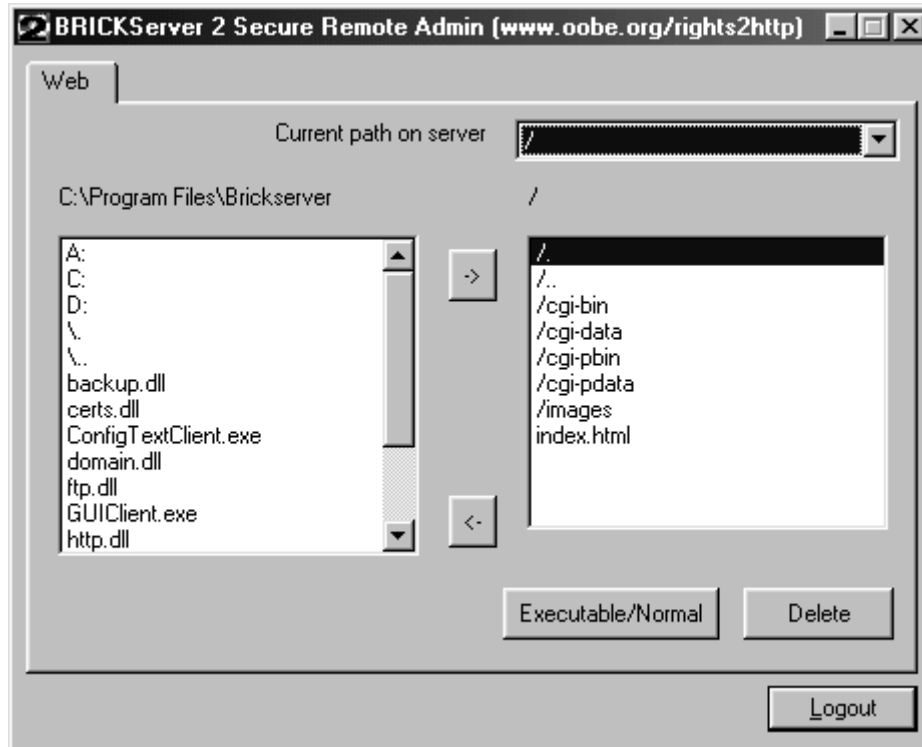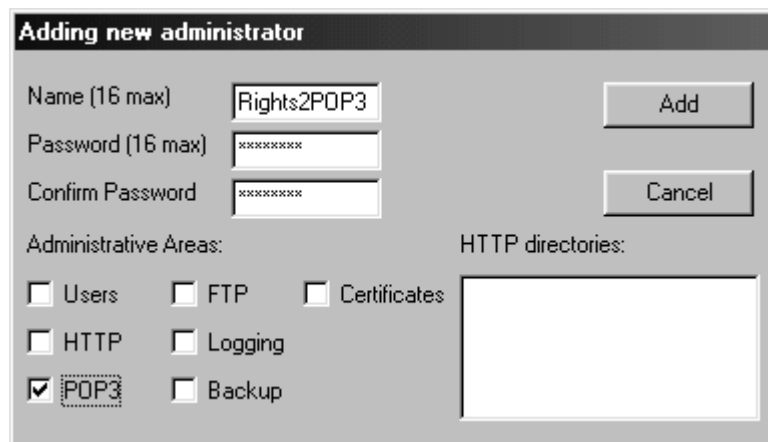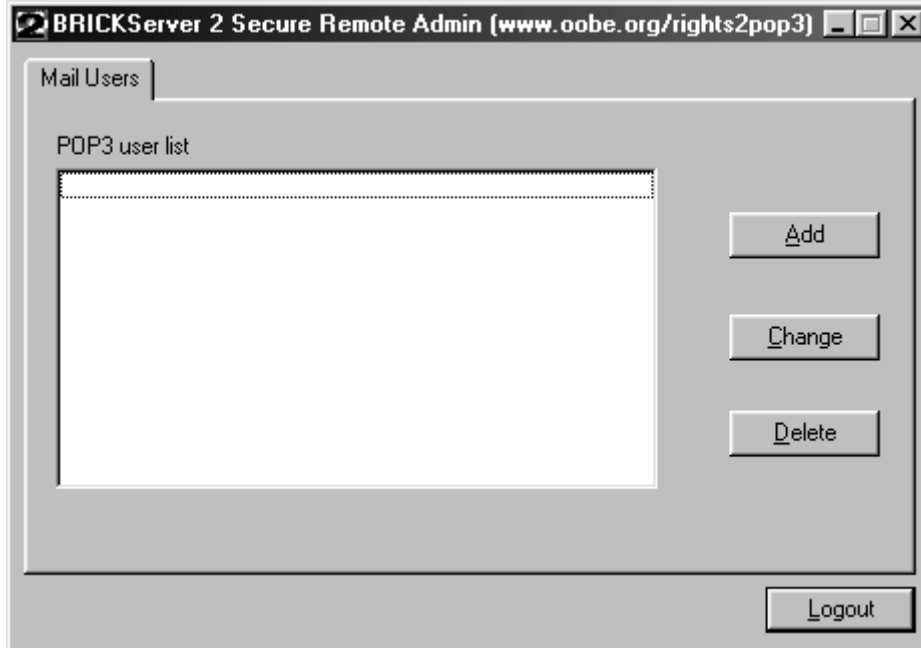
Figure 36. Administrator with Rights to only HTTP

Administrator with POP3 Access

Figure 37 shows an example of a setup for an administrator who would have rights to only POP3. These administrators would see the window in Figure 38 upon login to BRICKServer 2 Secure Remote Admin.
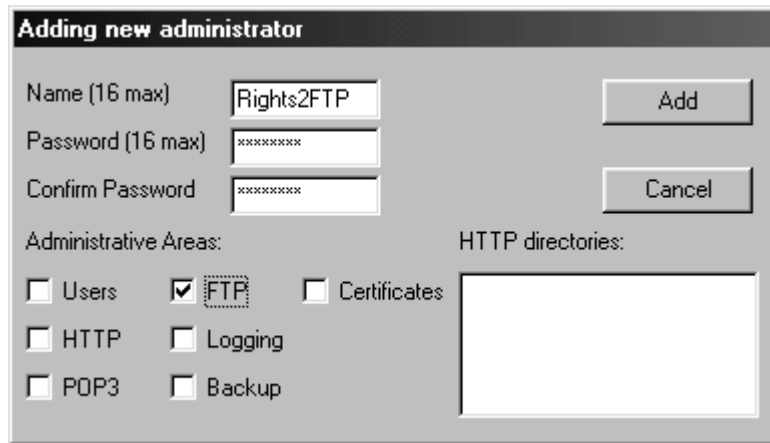

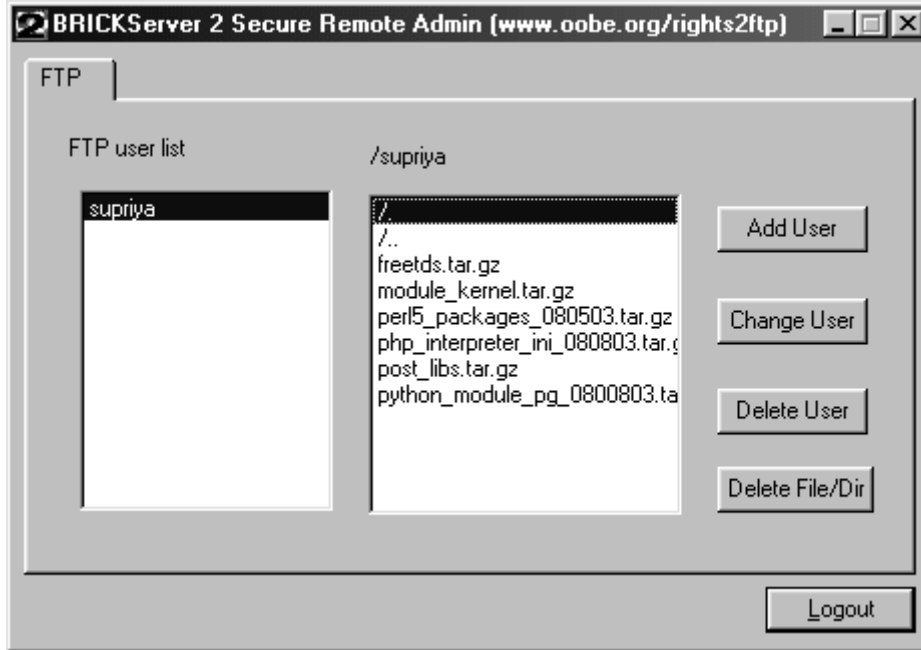*Figure 37. Setup for Administrator with Rights only to the POP3 Administrative Area*

Figure 38. Administrator with Rights to only POP3

Administrator with FTP Access

Figure 39 shows an example of a setup for an administrator who would have rights to only FTP. These administrators would see the window in Figure 40 upon login to BRICKServer 2 Secure Remote Admin.

Figure 39. Setup for Administrator with Rights only to the FTP Administrative Area

Figure 40. Administrator with Rights to only FTP

Administrator with Logging Access

Figure 41 shows an example of a setup for an administrator who would have rights to the Logging administrative area. These administrators would see the window in Figure 42 upon login to BRICKServer 2 Secure Remote Admin.
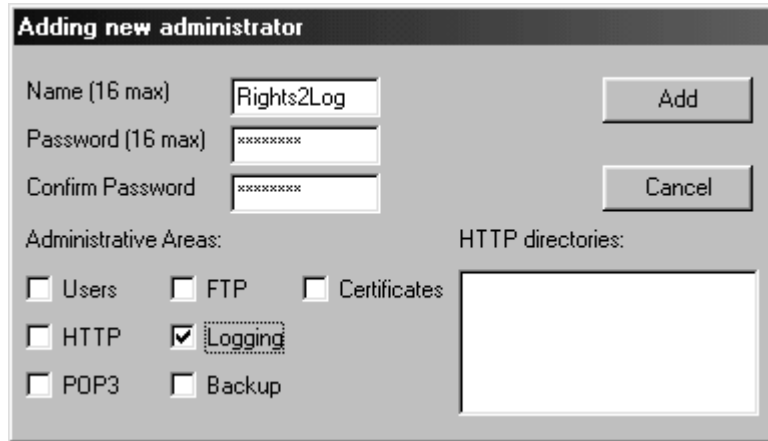

Figure 41. Setup for Administrator w/Rights to only the Logging Administrative Area

Figure 42. Administrator with Rights to only Logging

Administrator with Backup Access

Figure 43 shows an example of a setup for an administrator who would have rights to the Backup administrative area. These administrators would see the window in Figure 44 upon login to BRICKServer 2 Secure Remote Admin. Backup administrators, by default, also have the right to Restore and are the only administrators who can restore.
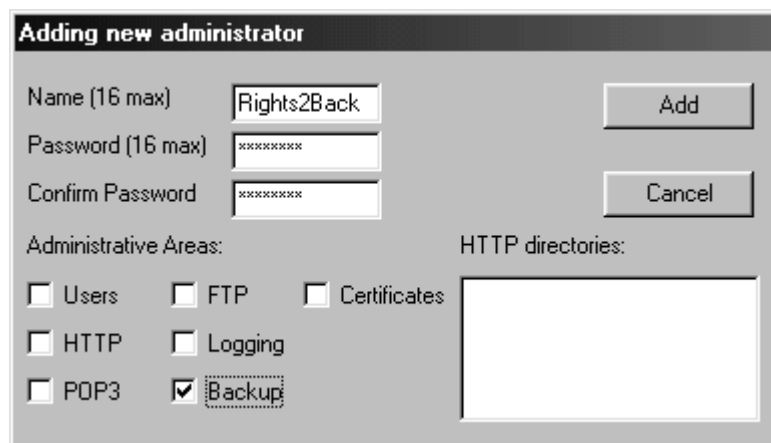

Figure 43. Setup for Administrator with Rights only to the Backup Administrative Area (includes Restore by Default)
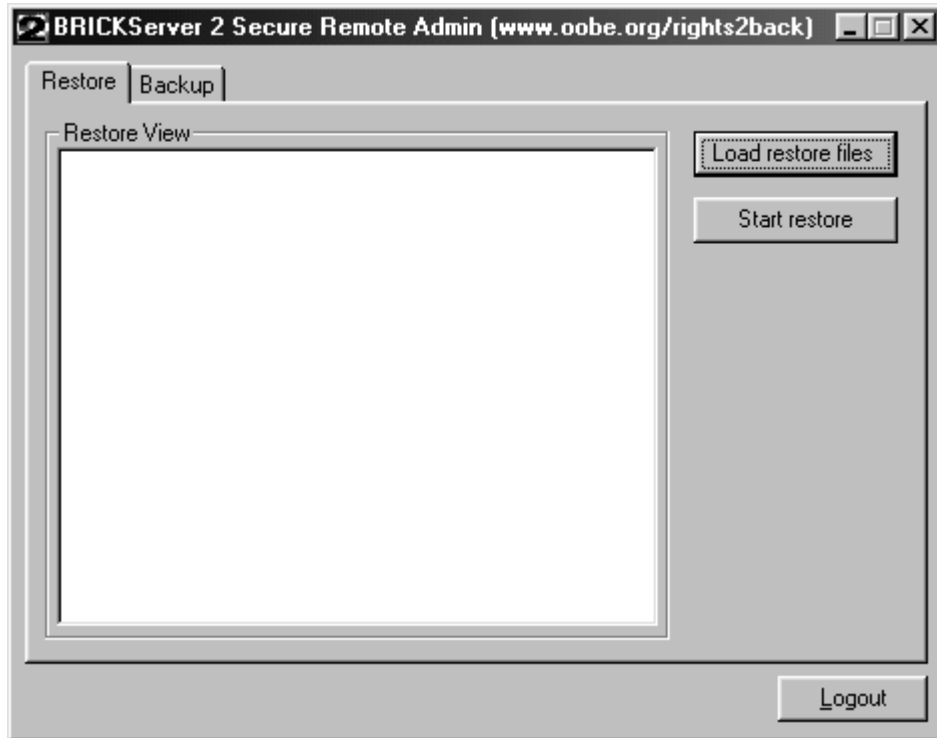
Figure 44. Administrator with Rights to only Backup (includes Restore)

Administrator with Certificates Access

Figure 45 shows an example of a setup for an administrator who would have rights to the Certificates administrative area. These administrators would see the window in Figure 46 upon login to BRICKServer 2 Secure Remote Admin.
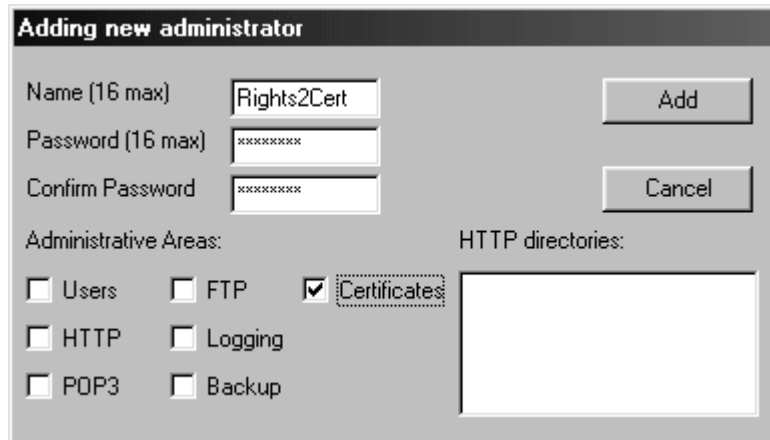

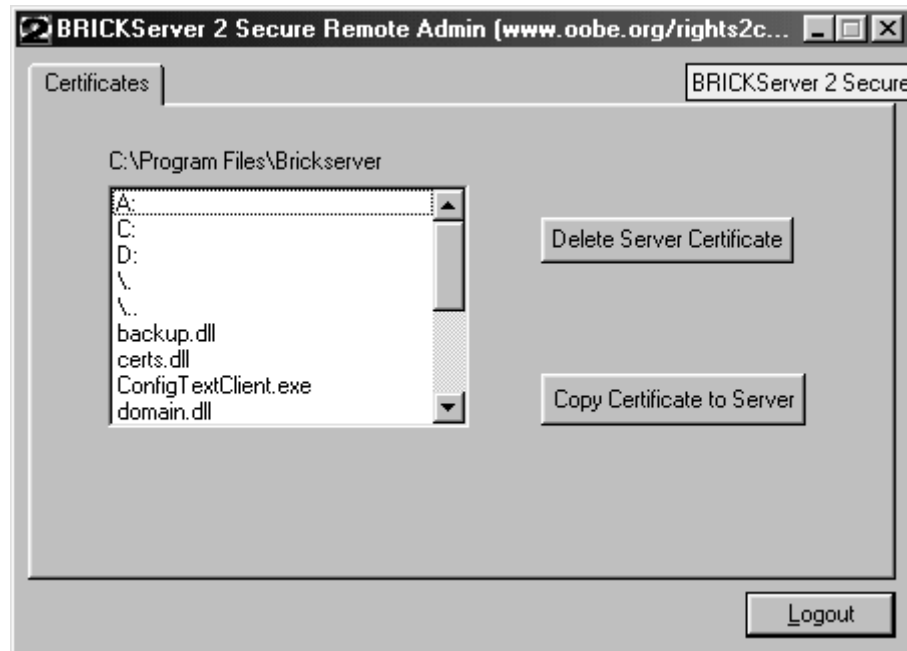*Figure 45. Setup for Administrator with Rights only to the Certificates Administrative Area*

Figure 46. Administrator with Rights to only Certificates

Administrator with Logging and Backup Access

Figure 47 shows an example of a setup for an administrator who would have rights to both the Logging and Backup administrative areas of the BRICKServer 2. These administrators would see the window in Figure 48 upon login to BRICKServer 2 Secure Remote Admin.
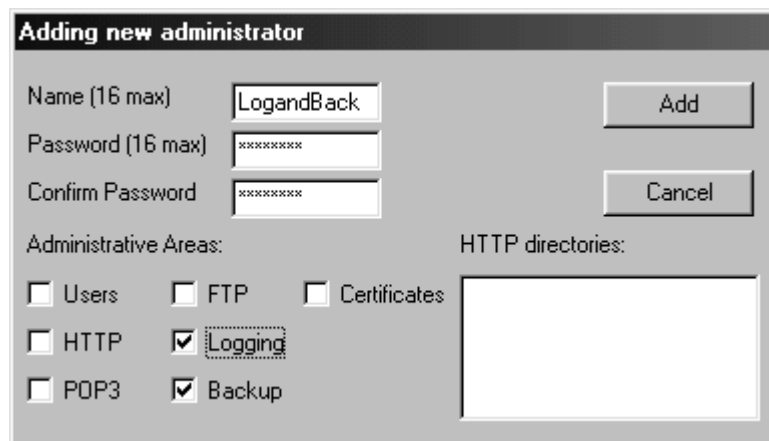

Figure 47. Setup for Administrator with Rights to both the Logging and Backup Administrative Areas
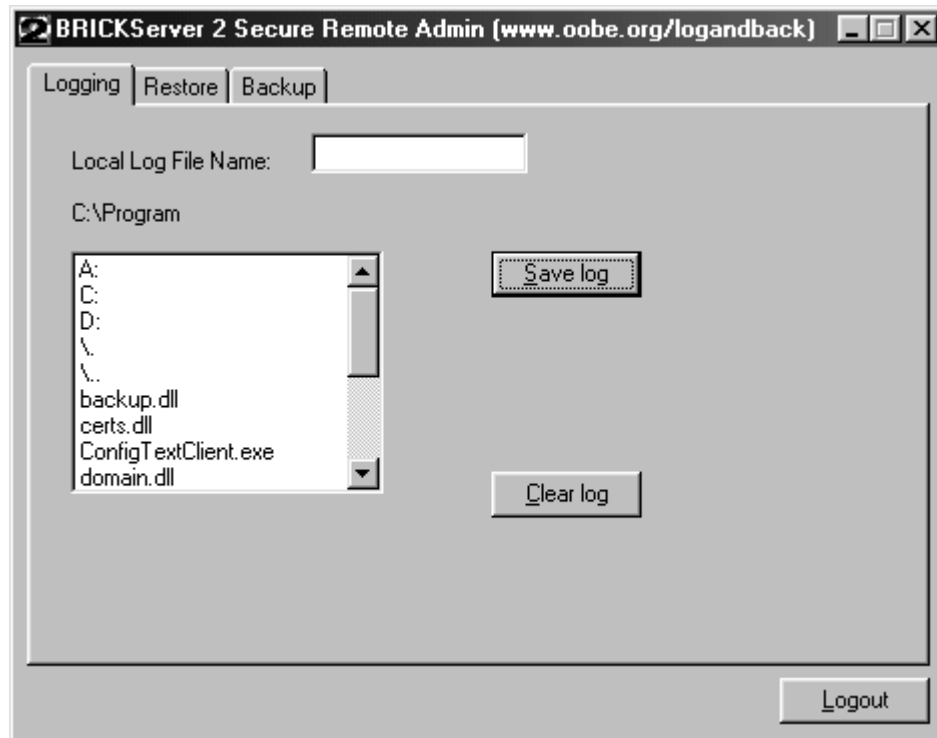
Figure 48. Administrator with Rights to both Logging and Backup

Administrator with HTTP and Certificates Access

Figure 49 shows an example of a setup for an administrator who would have rights to both the HTTP and Certificates administrative areas of the BRICKServer 2. These administrators would see the window in Figure 50 upon login to BRICKServer 2 Secure Remote Admin.
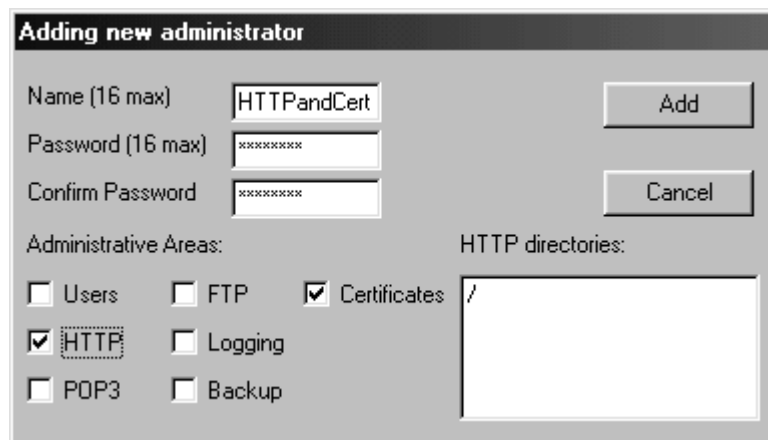

Figure 49. Setup for Administrator with Rights to both the HTTP and Certificates Administrative Areas
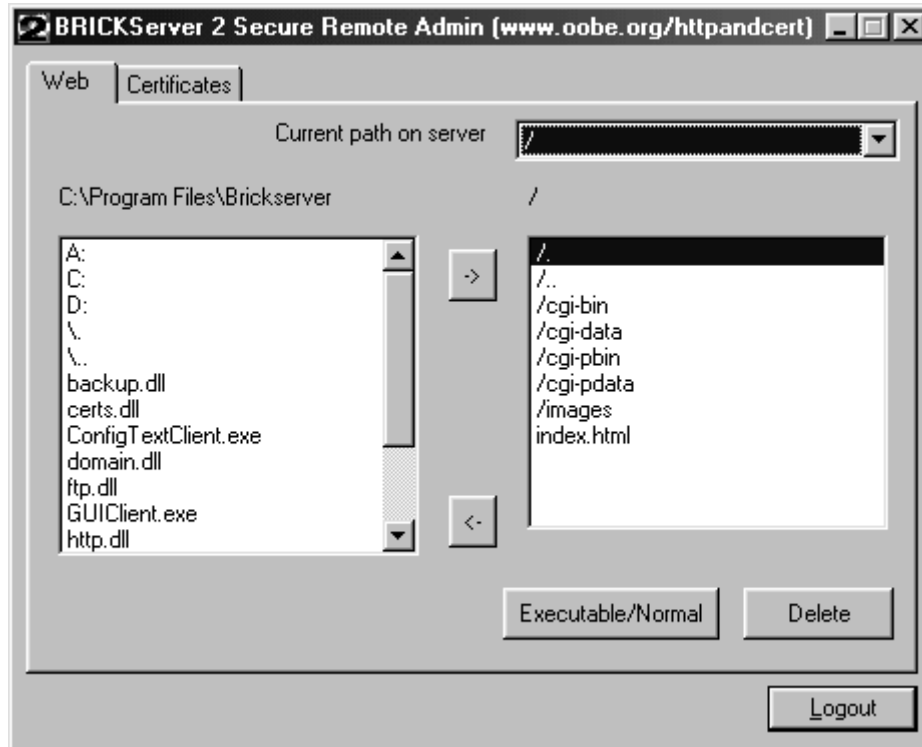
Figure 50. Administrator with Rights to both HTTP and Certificates

Change Administrator Rights

A list of the administrative users is shown on the Users tab, change an administrator's password or their administrative areas by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Users tab (Figure 29), select the Administrator from the Service Administrator(s) list.

3. Select Change, and the Changing an Existing Administrator window will open (Figure 51).
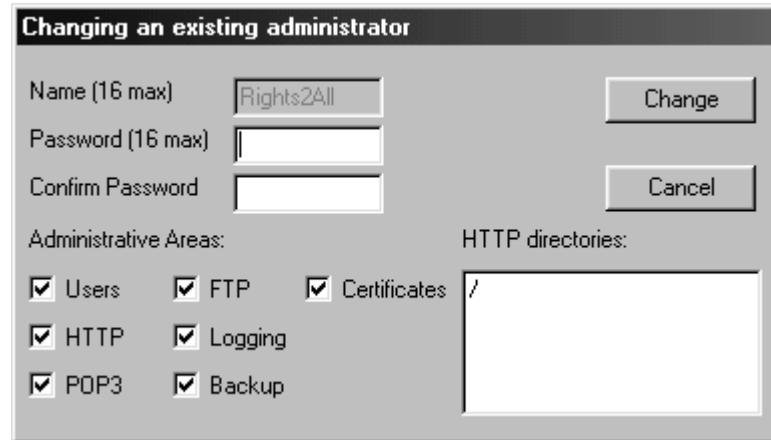
Figure 51. Changing an Existing Administrator Window

4. Make the desired changes to the Password, Administrative Areas and/or HTTP directories.

5. Select Change, the BRICKServer 2 Secure Remote Admin window will appear (Figure 29). Updates to the Administrative Areas will be visible in the Services column.

6. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Delete an Administrator

A list of the administrative users is shown on the Users tab, delete an administrator from the domain by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Users tab (Figure 29), select the Administrator name from the list.

3. Select Delete and the Deleting an Existing Administrator window will open (Figure 52).
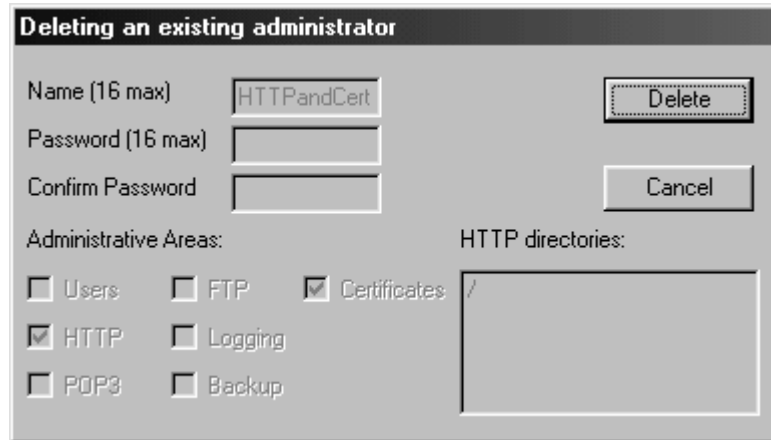
Figure 52. Deleting an Existing Administrator Window

4. Choose Delete, the BRICKServer 2 Secure Remote Admin window will appear (Figure 29). Confirm that the administrator was deleted by reviewing the names in the Administrator column.

5. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Change the Backup/Restore Seed

The Backup/Restore seed is an encryption code that is similar to a password. It can contain any combination of characters, numbers, and symbols. The seed is a security precaution that prevents anyone except the Backup administrator from being able to decrypt the backup file. As an additional security precaution, the Backup administrator can only decrypt the backup file on the BRICKServer 2.

In summary, only the designated Backup administrator can restore files to the domain, and they must type the seed when prompted.

Change the primary backup/restore seed by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Users tab (Figure 29), select the Administrator name from the list.

3. Type the seed into the Backup/Restore Seed field.

4. Select Update to complete the process.

5. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Web tab

> **Note:**
>
> Only HTTP administrators can view and use the Web tab.

The HTTP administrator has rights to manage and transfer files between the client workstation and the BRICKServer 2. Administrators with rights to only the HTTP administrative area would see the window in Figure 53 upon login to BRICKServer 2 Secure Remote Admin.
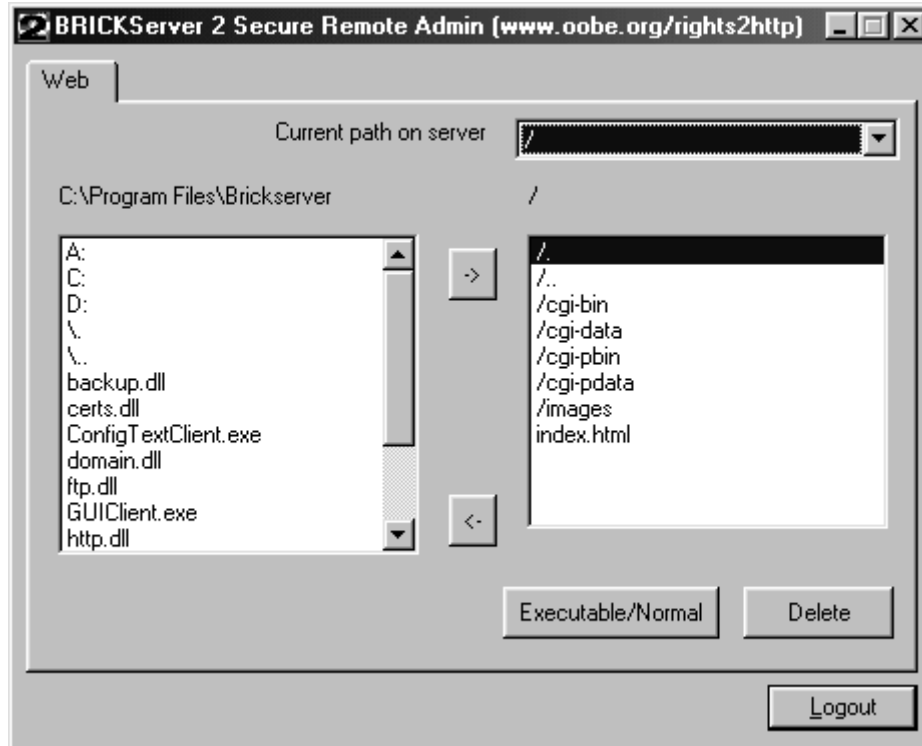

Figure 53. HTTP Administrators View of BRICKServer 2 Secure Remote Admin

When viewing the Web tab the directories and files located on the BRICKServer 2 are listed on the right side of the window and the client workstation's directories and files are listed on the left. The current directory name is shown above each list box.

> **Example:**
>
> **The directories represented in Figure 53 are:**
>
> **CLIENT DIRECTORY = C:\PROGRAM FILES\BRICKSERVER**
>
> **SERVER DIRECTORY = /CGI-DATA**

Transfer Directories and/or Files from Client to BRICKServer 2

Use the following steps as guidelines for transferring directories and files from the client to the BRICKServer 2.

> **Caution:**
>
> **Once started, transfers cannot be stopped!**

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Web tab (Figure 53), identify the directories and/or files to transfer from the client to the BRICKServer 2 by selecting the source directory/file(s) in the client list box (left-side), and then navigate to the destination directory in the server list box (right-side).

   - Double-click to select drives and directories.

   - Double-click the \.. to go back one level in the client workstation list box (like using in the *Windows* environment).

   - Double-click the \.. in the BRICKServer 2 list box to go back a level.

   - Select multiple files by clicking once on the first file on the list; hold the shift key on the keyboard while clicking once on the last file.

3. Locate the source directory or file(s) on the client (left list box).

4. Locate the destination directory on the BRICKServer 2 (right list box).

5. Use —> to complete the transfer process.

6. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Transfer Directories and/or Files from BRICKServer 2 to Client

Use the following steps as guidelines for transferring directories and files from the BRICKServer 2 to the client.

> **Caution:**
>
> **Once started, transfers cannot be stopped!**

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Web tab (Figure 53), identify the directories and/or files to transfer from the BRICKServer 2 to the client by selecting the source directory/file(s) in the BRICKServer 2 list box (right-side), and then navigate to the destination directory in the client list box (left-side).

   - Double-click to select drives and directories.

   - Double-click \.. to go back one level in the client workstation list box (like using in the *Windows* environment).

- Double-click \.. in the BRICKServer 2 list box to go back a level.
- Select multiple files by clicking once on the first file on the list; hold the shift key on the keyboard while clicking once on the last file.

3. Locate the source directory or file(s) on the BRICKServer 2 (right list box).

4. Locate the destination directory on the client (left list box).

5. Use <— to complete the transfer process.

6. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Delete Directories and Files

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Web tab (Figure 53), select a directory or file for deletion.

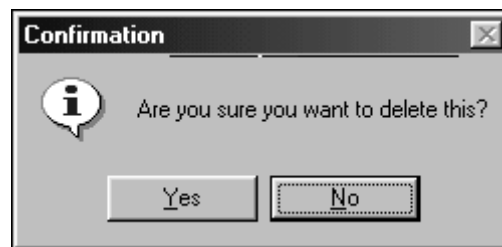3. Select Delete and answer Yes to the Confirmation window (Figure 54) to complete the process.

Figure 54. Confirmation Window

4. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Executable/Normal Files

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Web tab (Figure 53), use Executable/Normal to mark files in the CGI-BIN directory as executable.

> **Note:**
>
> Only files in the CGI-BIN will be recognized as executable, code must be adjusted accordingly.
>
> An asterisk next to the filename indicates an executable file.

3. Executable files can be returned to normal state by again selecting Executable/Normal.

4.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Customize the HTTP Banner

Customize HTTP banners such as the 404 and 500 errors by using the following steps (this example customizes the banner for the 404 error).

1.   Create a file on the client named "err404.html".

2.   On the BRICKServer 2, create a subdirectory in the HTTP directory named "errors".

3.   Transfer the file named "err404.html" from the client to the BRICKServer 2 using the BRICKServer Secure Remote Admin (refer to page 4-18 for instructions).

Prevent the Display of Directory Listings

Prevent directory listings from being displayed on the BRICKServer 2 by following these steps.

1.   Create a file on the client describing that the directory listing is denied named "index.html".

2.   Transfer the file named "index.html" from the client to the BRICKServer 2 using the BRICKServer Secure Remote Admin (refer to page 4-18 for instructions), placing it in each directory where directory listings are denied.

POP3 Tab

Note:

Only POP3 administrators can view and use the Mail Users tab.

The Mail Users tab (Figure 55) allows the POP3 administrator to add, change, and delete mail user accounts, and forward POP3 user's email. Administrators with rights to only the POP3 administrative area would see the window in Figure 55 upon login to BRICKServer 2 Secure Remote Admin.

Figure 55. POP3 Administrators View of BRICKServer 2 Secure Remote Admin

---

Note:

Incorrectly addressed email can be channeled by adding a default user, i.e., named *default*.

Add a POP3 User

Add a new POP3 user to the domain by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Mail Users tab (Figure 55), select Add and the Adding New POP3 User window will open (Figure 56).
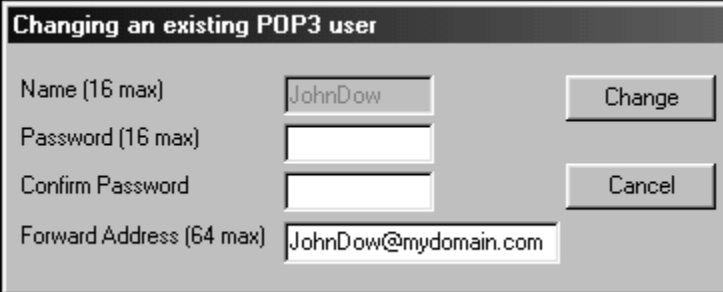

Figure 56. Adding New POP3 User Window

3.   Using their name or any combination of characters and numbers, type a unique name (up to 16 characters) for the new POP3 user in the Name field. Symbols and spaces are not permitted in the Name field, and case is irrelevant.

4.   Type a password **at least 7 characters** for the POP3 user in the Password field using any combination of up to 16 alphabetical characters, numbers, spaces, and symbols. As a security precaution, the password will be displayed as asterisks ("*").

5.   Confirm the POP3 user's password by retyping it in the Confirm Password field.

6.   Type the user's Name (up to 64 characters) in the Forward Address field.

7.   Select Add, the BRICKServer 2 Secure Remote Admin window will appear (Figure 55). If all information was entered correctly, the new POP3 user will be listed on the POP3 user list.

8.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Change a POP3 User's Account

Change the POP3 user's password and/or forward address by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2.   When viewing the Mail Users tab (Figure 55), select the POP3 user from the list.

3.   Select Change, and the Changing an Existing POP3 User window will open (Figure 57).

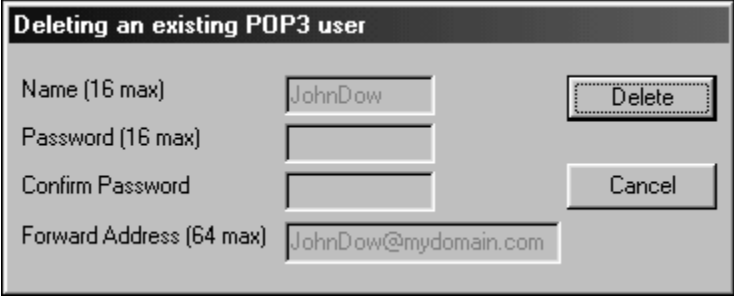*Figure 57. Changing an Existing POP3 User Window*

4.   If changing the POP3 user's password, type a password of **at least 7 characters** in the Password field using any combination of up to 16 alphabetical characters, numbers, spaces, and symbols. As a security precaution, the password will be displayed as asterisks ("*").

5.   Confirm the password by retyping it in the Confirm Password field.

6.   Type the user's Name (up to 64 characters) in the Forward Address field.

7.   Select Change, the BRICKServer 2 Secure Remote Admin window will appear (Figure 55).

8.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Delete a POP3 User

Delete a POP3 user from the domain by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2.   When viewing the Mail Users tab (Figure 55), select the POP3 user name from the list.

3.   Select Delete and the Deleting an Existing POP3 User window will open (Figure 58).

Figure 58. Deleting an Existing POP3 User Window

4.   Choose Delete, the BRICKServer 2 Secure Remote Admin window will appear (Figure 55). Confirm that the POP3 user was deleted by reviewing the names on the POP3 user list.

5.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Email Clients Quick Setup

A quick way to configure the client email application to work with POP3 and SMTP is to use the Domain Name (i.e. MYDOMAIN.COM) as the POP3 and SMTP server. The BRICKServer 2 SMTP server requires authentication and uses NTLM, Plain, CRAM MD5, and APOP authentication methods.

FTP Tab

Note:

Only FTP administrators can view and use the FTP tab.

The FTP tab (Figure 59) allows FTP administrators to add, delete and change the passwords of users who are authorized to transfer files to/from the BRICKServer 2. FTP users can use any FTP program to transfer files to/from the BRICKServer 2. Files can only be uploaded to the Web site by using BRICKServer 2 Secure Remote Admin.

Administrators with rights to only the FTP administrative area would see the window in Figure 59 upon login to BRICKServer 2 Secure Remote Admin.
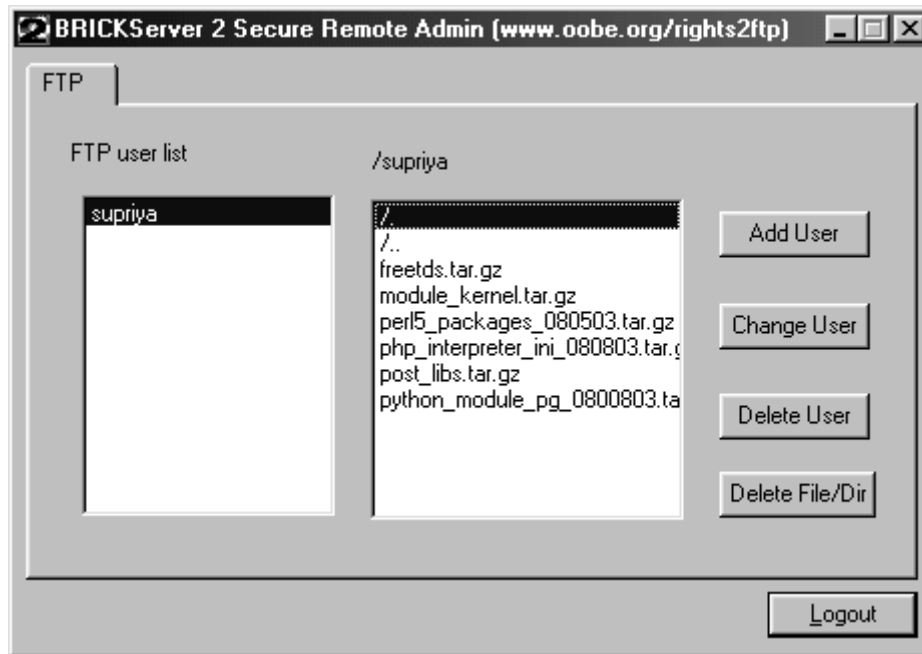

Figure 59. FTP Administrators View of BRICKServer 2 Secure Remote Admin

Add a New FTP User

Add a new FTP user to the domain by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the FTP tab (Figure 59), select Add and the Adding New FTP User window will open (Figure 60).
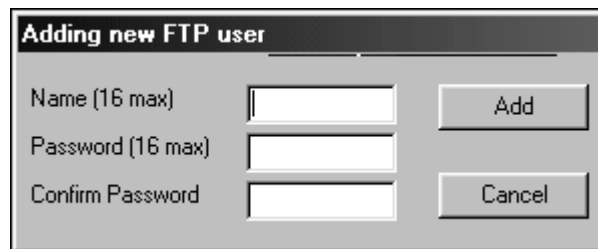

Figure 60. Adding New FTP User Window

3. Using their name, or any combination of characters and numbers, type a unique name (up to 16 characters) for the new administrator in the Name field. Symbols and spaces are not permitted in the Name field, and case is irrelevant.

4. Type a password **at least 7 characters** for the administrator in the Password field using any combination of alphabetical characters, numbers, spaces, and symbols. As a security precaution, the password will be displayed as asterisks ("*").

5. Confirm the administrator's password by retyping it in the Confirm Password field.

6. Select Add, the BRICKServer 2 Secure Remote Admin window will appear (Figure 59).

7. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Change an Existing FTP User

Change an existing FTP user's password by following these steps.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the FTP tab (Figure 59), select the user from the FTP user list.

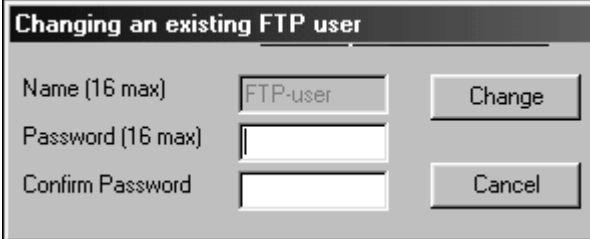3. Select Change, and the Changing an Existing FTP User window will open (Figure 61).

Figure 61. Changing an Existing FTP User Window

4. Type a new password of **at least 7 characters** in the Password field using any combination of up to 16 alphabetical characters, numbers, spaces, and symbols. As a security precaution, the password will be displayed as asterisks ("*").

5. Confirm the new password by retyping it in the Confirm Password field.

6. Select Change, the BRICKServer 2 Secure Remote Admin window will appear (Figure 59).

7. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Delete an FTP User

Delete an FTP user from the domain by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2.   When viewing the FTP tab (Figure 59), select the user from the FTP user list.

3.   Select Delete, and the Deleting an Existing FTP User window will open (Figure 62).
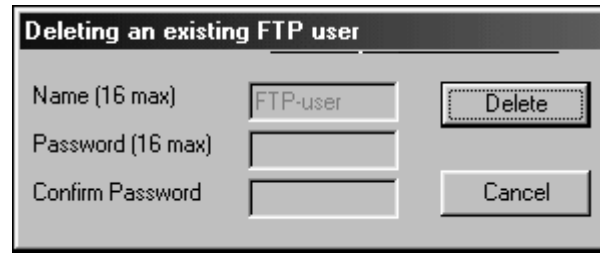

Figure 62. Deleting an Existing FTP User Window

4.   Choose Delete, the BRICKServer 2 Secure Remote Admin window will appear (Figure 59). Confirm that the administrator was deleted by reviewing the names in the Administrator column.

5.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Delete a Directory or File

Delete a directory or file by following these steps.

1.   If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2.   When viewing the FTP tab (Figure 59), identify the directory or file to delete by selecting it in the Server list box (right side).

   ●   Double-click to select drives and directories.

   ●   Double-click the \.. to go back one level in the client workstation list box (like using in the *Windows* environment).

   ●   Double-click the \.. in the BRICKServer 2 list box to go back a level.

   ●   Select multiple files by clicking once on the first file on the list; hold the shift key on the keyboard while clicking once on the last file.

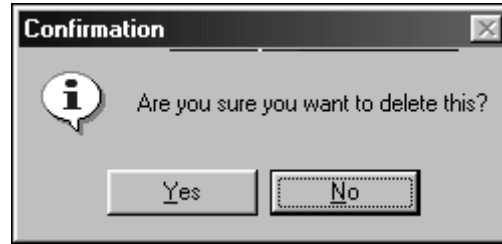3.   Select Delete File/Dir, and the Confirmation window will open (Figure 63).

Figure 63. Confirmation Window

4.   Choose Yes, the BRICKServer 2 Secure Remote Admin window will appear (Figure 59). Confirm that the file / directory was deleted by reviewing the Server list box.

5.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Anonymous File Uploads and/or Downloads

Permit anonymous file uploads and/or downloads by creating an FTP user with no password.

Logging tab

> **Note:**
>
> Only Logging administrators can view and use the Logging tab.

The Logging tab (Figure 64) allows Log administrators to securely save log files to the local workstation and clear log files on the BRICKServer 2. Administrators with rights to only the Logging administrative area would see the window in Figure 64 upon login to BRICKServer 2 Secure Remote Admin.

Figure 64. Log Administrators View of BRICKServer 2 Secure Remote Admin

Save Log

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Logging tab (Figure 64), type a name for the log file in the Local Log File Name text box.

3. Identify the destination directory using the list box.

    ● Double-click to select drives and directories.

    ● Double-click the \.. to go back one level (like using in the *Windows* environment).

4. Select Save log to complete the process.

> **Note:**
>
> The Log file is a line separated text file containing information regarding web traffic on the domain. It can be viewed or printed by using a text editor such as *Notepad* or *WordPad*.

5. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Clear Log

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Logging tab (Figure 64), select Clear log.

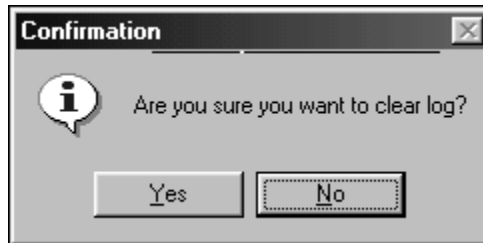3. The clear log Confirmation window will open (Figure 65).

Figure 65. Confirmation Window

4. Select Yes to complete the process.

5. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Restore Tab

> **Note:**
>
> Only Backup administrators can view and use the Restore tab.

The Restore tab (Figure 66) allows Backup administrators to securely restore backup files. Administrators with rights to only the Backup administrative area would see the window in Figure 66 upon login to BRICKServer 2 Secure Remote Admin.
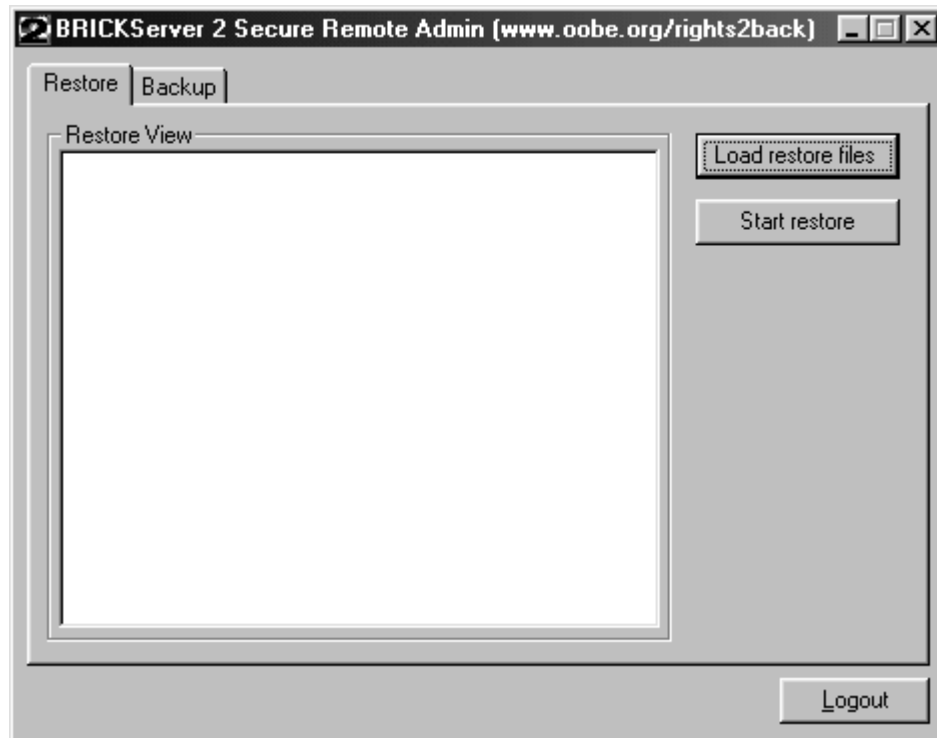
Figure 66. Backup Administrators View of BRICKServer 2 Secure Remote Admin

Note:

A backup cannot be restored onto a different domain.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Restore tab (Figure 66), select Load restore files.

3. Choose the restore file using the Backup Image to Load dialog box.

4. Select Open and the file name will be displayed in the Restore view list box.

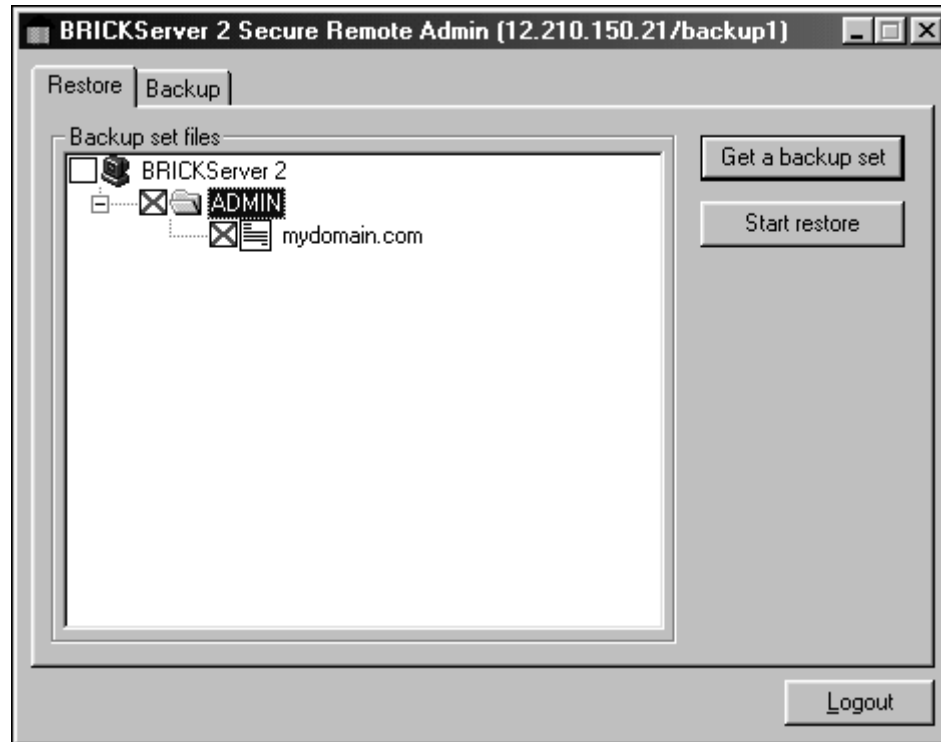5. Click on the square to the left of the file name to insert an X (Figure 67).

Figure 67. Restore Tab after using Get a Backup Set

6.   Select Start Restore to complete the process.

7.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Backup Tab

> **Note:**
>
> Only Backup administrators can view and use the Backup tab.

The Backup tab (Figure 68) allows Backup administrators to create secure backup files for the HTTP, FTP, and POP3 directories as well as for the Log data. Once again, backup administrators are the only administrators who have restore rights. Administrators with rights to only the Backup administrative area would see the window in Figure 68 upon login to BRICKServer 2 Secure Remote Admin.
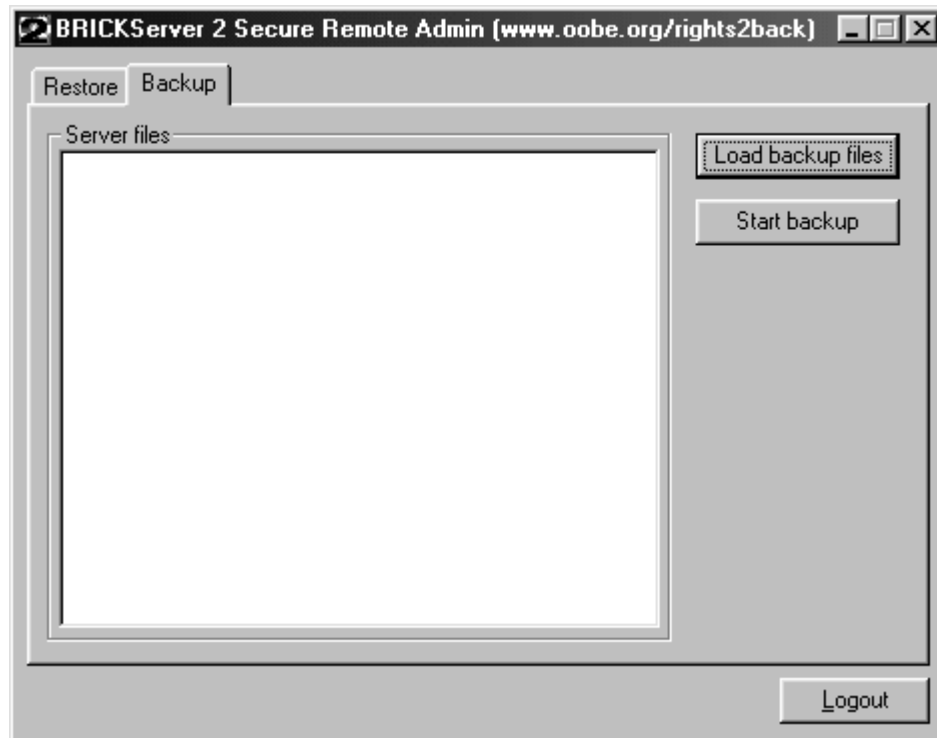
Figure 68. Backup Administrators View of BRICKServer 2 Secure Remote Admin

Note:

A backup cannot be restored onto a different domain.

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Backup tab (Figure 68), select Load backup files to view a list of files to backup in the Server files list box (Figure 69).
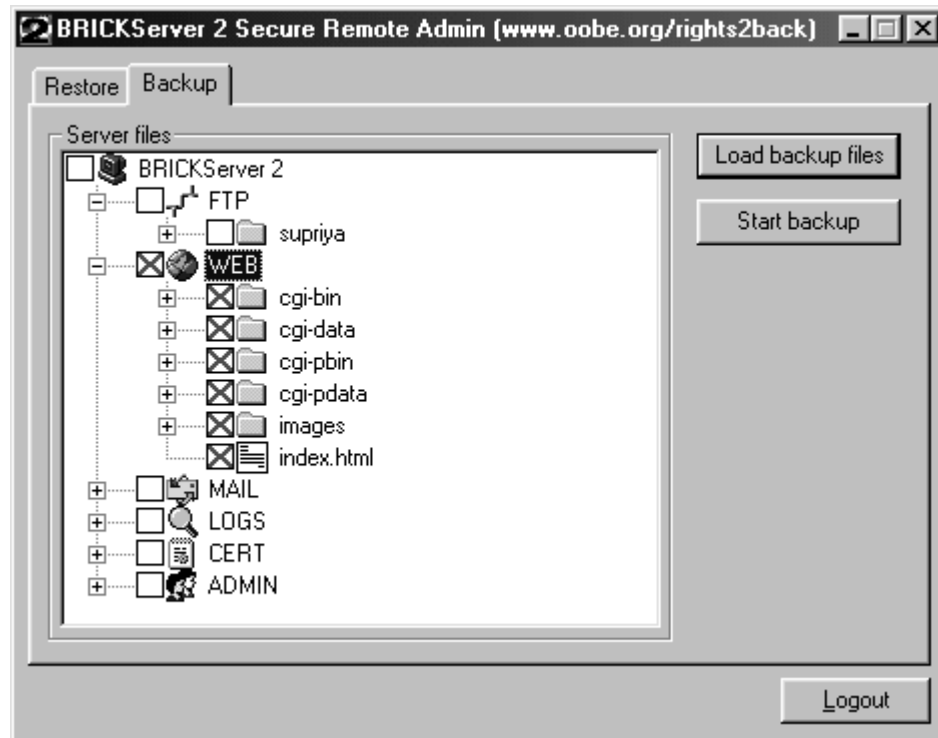
Figure 69. Server Files List

3. Choose from the BRICKServer 2 files by clicking on the square, thereby inserting an X (see Figure 69).

- **BRICKServer 2**—Backup all files on the BRICKServer 2.

- **FTP**—Backup all FTP directories and files on the BRICKServer 2.

- **WEB**—Backup all HTTP directories and files on the BRICKServer 2.

- **MAIL** —Backup all POP3 directories and files on the BRICKServer 2.

- **LOGS**—Backup all Logging directories and files on the BRICKServer 2.

- **CERT**—Backup all Certificates directories and files on the BRICKServer 2.

- **ADMIN**—Backup all Admin directories and files on the BRICKServer 2.

The Server files list can be expanded or condensed by using the ⊞ and ⊟ buttons.

4. Select Start backup and the Where to Save the Backup Image dialog box will appear (Figure 70).
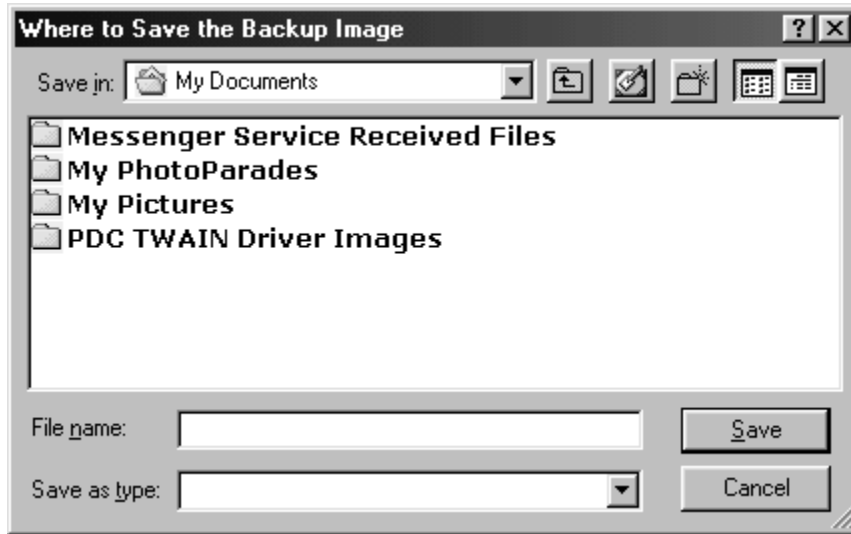
Figure 70. Where to Save the Backup Image Window

5.   Designate a directory, type a file name, and select Save to complete the process. The Client activity log will show the status of the backup (Figure 71).

Figure 71. Client Activity Log after Completed Backup

6.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Certificates Tab

Note:

Only Certificates administrators can view and use the Certificates tab.

The Certificates tab (Figure 72) allows Certificates administrators to set up and manage digital certificates on the BRICKServer 2.
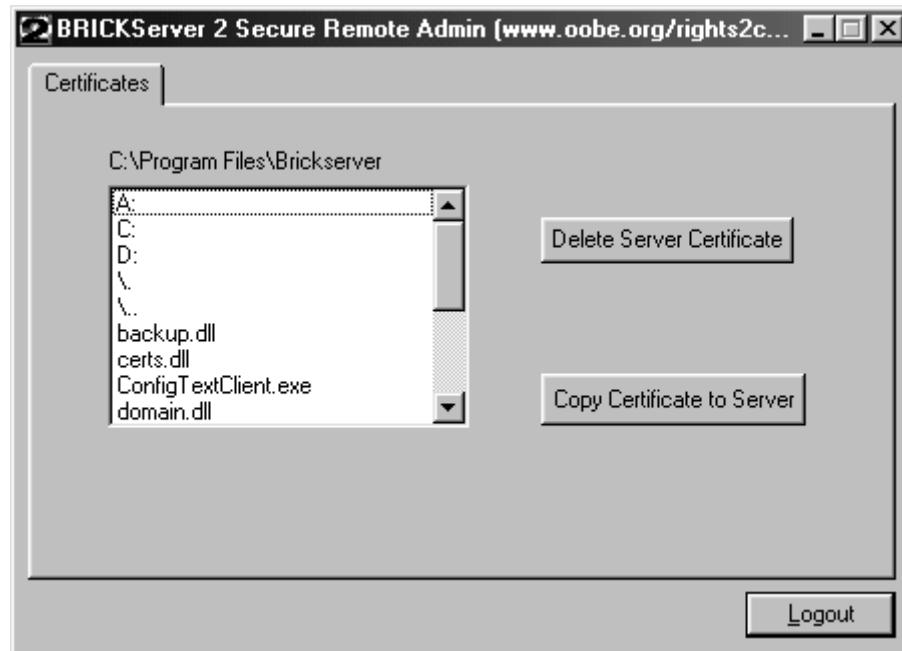
Figure 72. Certificates Administrators View of BRICKServer 2 Secure Remote Admin

Note:

Only a Certificates administrator can use the Certificates tab.

SSL is available only to the default domain.

Each IP Address is assigned one Certificates administrator.

A certificate is an electronic attachment that is used for security purposes, primarily used with email. It verifies that the sender of a message is who they claim to be, and provides the ability for the recipient to send an encoded reply.

Certificates can be self-made or obtained by anyone from a Certificate Authority (CA). Using a CA guarantees that the two parties exchanging information are really who they claim to be. VeriSign is the leading provider of digital authentication products and services. Other CAs include the following.

- Thawte Consulting
- Internet Publishing Services
- Certisign Certification Digital Ltda
- BelSign

The CA issues an encrypted digital certificate containing the applicant's public key along with other identification information (the CA's own public key is available on the Internet). The recipient of an encrypted message uses the CA's public key to

decode the digital certificate attached to the message, verifies it as issued by the CA and then obtains the sender's public key and identification information held within the certificate. With this information, the recipient can send an encrypted reply.

It is best to obtain a certificate from a valid Certificate Authority if interaction will take place with a 3rd party client such as *Netscape* and *Microsoft Internet Explorer*, who have hard coded lists of acceptable Certificate Authorities. Otherwise, users will experience dialog boxes on the first, or all, connections.

> **Note:**
>
> The BRICKServer 2 will allow one certificate per domain.

Create a Certificate

> **Note:**
>
> When a self-signed certificate is used, error and/or warning messages will occur when attempting to connect to SSL.

1. Create a private key by typing the following on a Linux or Unix server, which creates a Certificate Request file named certreq.pem.

   `OPENSSL REQ -NEW -DAYS 365 -NODES -OUT CERTREQ.PEM -KEYOUT YOURFILE.PEM`

2. Submit the certreq.pem file, along with a request for the certificate, to one of the CAs along with any other information they may need.

3. After processing, the CA will send a certificate in following format to be appended to yourfile.pem. *Windows Notepad* can be used to append the information into the file.

   ```
   -----BEGIN CERTIFICATE-----

   CERTIFICATE DATA HERE

   -----END CERTIFICATE-----
   ```

Copy the Certificate to the BRICKServer 2

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Certificates tab (Figure 72), identify the directory where the certificate file is located.

   ● Double-click to select drives and directories.

- Double-click the \.. to go back one level (like using ⬆ in the *Windows* environment).

3. Select the certificate file.

    Certificates named with file extensions of pem will be copied to the BRICKServer 2 and automatically placed in the correct directory on the Certificates administrator's domain. The BRICKServer 2 does not recognize certificates with extensions other than pem. The following example shows a certificate named with the correct extension.

    ┌───┐
    │ **Example:**   │
    └───┘

    YOURFILE.PEM

    The BRICKServer 2 has no way of knowing if a certificate is in the valid certificate format. Invalid certificates with the pem extension will be copied to the BRICKServer 2 but users who try to connect will see a message indicating the certificate is not valid.

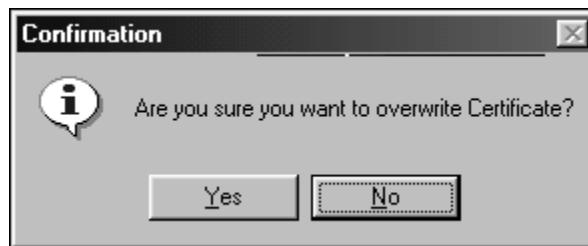4. Select Copy Certificate to Server and the Confirmation window will open (Figure 73).

Figure 73. Confirmation Window

5. Choose Yes to complete the process, the certificate will be automatically placed in the correct directory on the domain, and the BRICKServer 2 Secure Remote Admin window will appear (Figure 59).

6. Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Delete the BRICKServer 2 Certificate

1. If not already connected to the BRICKServer 2, connect to it using BRICKServer 2 Secure Remote Admin (refer to page 4-2).

2. When viewing the Certificates tab (Figure 72), select Delete Server Certificate.

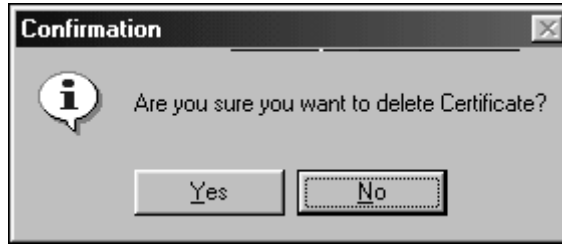3. The Confirmation window will open (Figure 74).

Figure 74. Confirmation Window

4.   Choose Yes to complete the process, the certificate will be deleted from the domain, and the BRICKServer 2 Secure Remote Admin window will appear (Figure 59).

5.   Use Logout when finished using BRICKServer 2 Secure Remote Admin.

Chapter 5.
BRICKServer 2 Secure Config – Remote Command Line Interface

The BRICKServer 2 offers a remote command line interface that can be used by advanced users to run the BRICKServer 2 commands from anywhere on the Internet, provided that the BRICKServer 2 has an active Internet connection.

Install the BRICKServer 2 Secure Config

Install the BRICKServer 2 Secure Config remote command line interface on a client by following these instructions.

1. Insert the CD into the CD-ROM drive.

2. Follow the on-screen instructions for installing the BRICKServer 2 Secure Config remote command line interface.

Connect to the BRICKServer 2

1. Run the BRICKServer 2 Secure Config remote command line interface by selecting Start, Programs, BRICKServer 2, BRICKServer 2 Secure Config. The BRICKServer 2 Secure Config remote command line interface window will open (Figure 75).
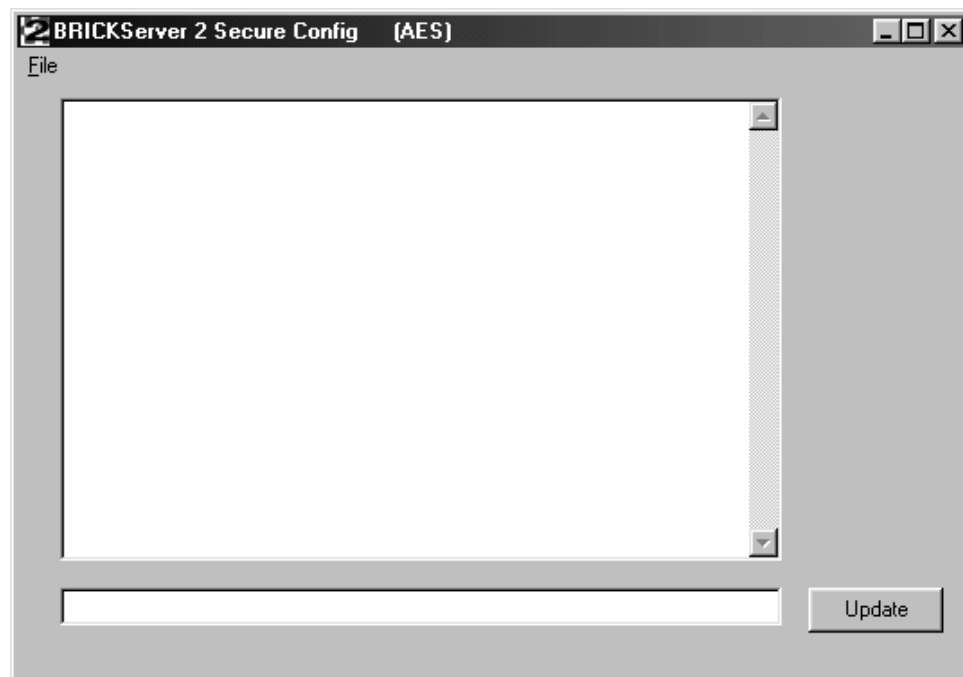

Figure 75. BRICKServer 2 Secure Config Window before Login

2.   Select File, Connect and the Login window will open (Figure 76).

Figure 76. Login Window

3.   Type the IP Address or domain name of the BRICKServer 2 into the Address field.

4.   Type the Password of the BRICKServer 2 into the Password field.

5.   Select OK and the Host Machine Available window will appear (Figure 77).

Figure 77. Host Machine Available Window

If an incorrect password is typed, a window will appear (Figure 78).

Figure 78. Connection Error Window

Disconnect from the BRICKServer 2

When finished using BRICKServer 2 Secure Config remote command line interface, disconnect to ensure security by using the following steps.

1.   Select Connection, Disconnect (Figure 5) to disconnect from the BRICKServer 2.

2.   Close the BRICKServer 2 Secure Config remote command line interface by selecting Connection, Exit.

Using the BRICKServer 2 Secure Config

Commands can be typed into the text entry field at the bottom of the BRICKServer 2 Secure Config dialog box and updates can be applied to the BRICKServer 2 using the Update button. Figure 79 shows an example of what is seen when the HELP command is typed; a list of the available BRICKServer 2 commands.
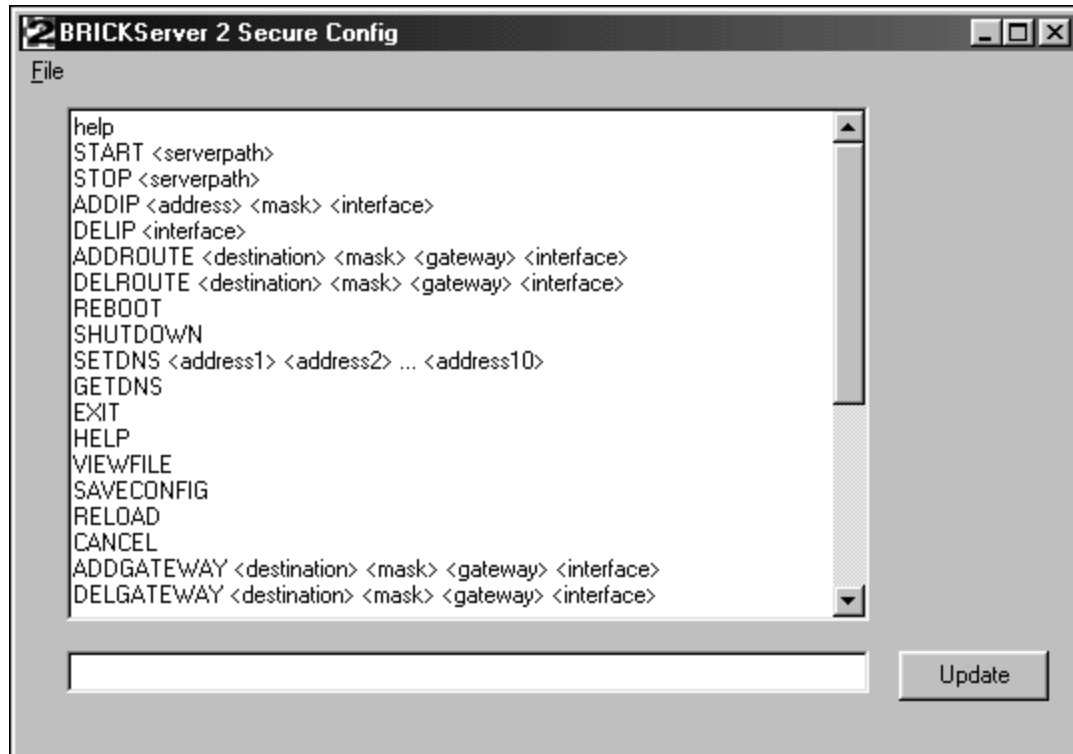

Figure 79. BRICKServer 2 Secure Config Window after Login

Command parameters can be viewed by typing the desired command without any parameters. Figure 80 shows the command parameters for the ADDROUTE command.
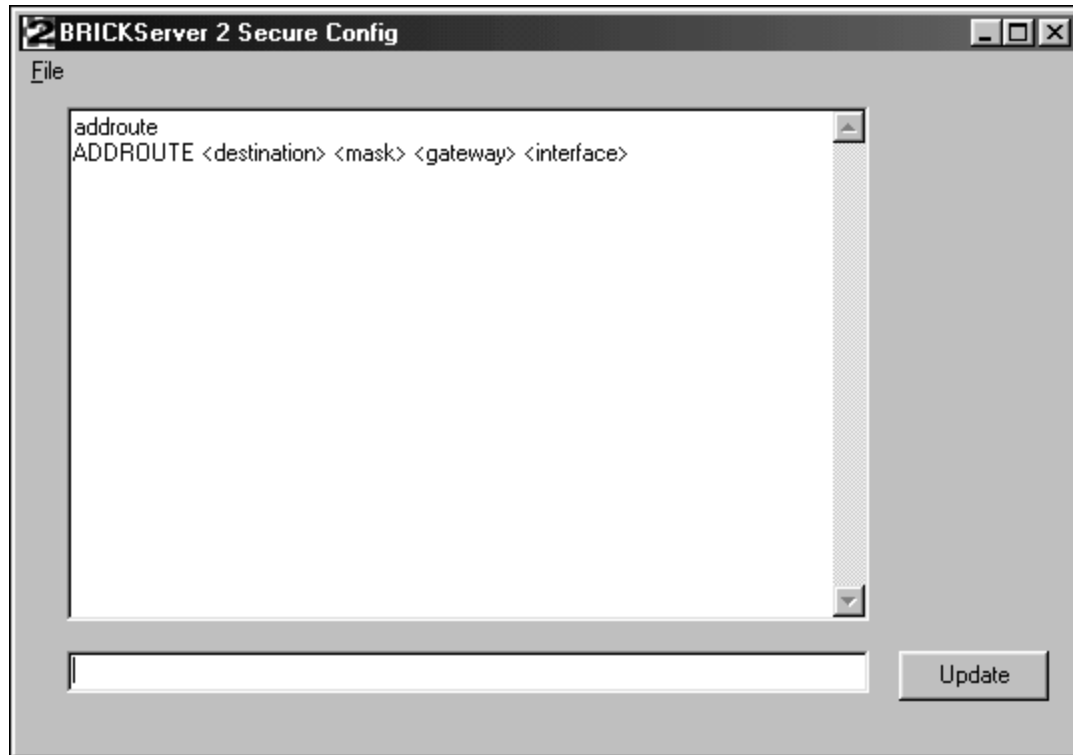
Figure 80. BRICKServer 2 Secure Config with ADDROUTE Command Parameters

BRICKServer 2 Commands

The following BRICKServer 2 commands can be executed directly on the BRICKServer 2 using a keyboard connected to the BRICKServer 2 or remotely using the BRICKServer 2 Secure Config remote command line interface. They are listed here in alphabetical order for ease of reference.

ADDDOMAIN

ADDDOMAIN is used to add virtual hosts. The limitation to the number of domains / virtual hosts that can be added is dictated by the amount of available disk space on the BRICKServer 2.

The basic command syntax for ADDDOMAIN is to type the command followed by the desired domain name, the default administrator's name, and then the administrator's password as in the following command example.

Command:

`ADDDOMAIN <DOMAIN> <ADMIN'S USERNAME> <ADMIN'S PASSWORD ON THE DOMAIN>`

In the following example, ADDDOMAIN is used to add a domain named MYWEBSITE.COM with ADMINUSER as the administrator name and ADMINPASSWORD as the administrator's password.

```
ADDDOMAIN MYWEBSITE.COM ADMINUSER ADMINPASSWORD
```

ADDGATEWAY

A gateway is a network point that acts as an entrance to another network. The Gateway Address is the address of the computer that connects your BRICKServer 2 to the Internet. Your network administrator or ISP can provide you with the Gateway address of your computer and/or BRICKServer 2. Set up the gateway by executing the following ADDGATEWAY command, replacing NNN.NNN.NNN.NNN with the destination, SSS.SSS.SSS.SSS with the subnet mask, GGG.GGG.GGG.GGG with the gateway address, and ETHN with the interface as in the following command example.

Command:

```
ADDGATEWAY <NNN.NNN.NNN.NNN> <SSS.SSS.SSS.SSS> <GGG.GGG.GGG.GGG> <ETHN>
```

Use the following example to add a gateway for a non-complex network or other type of network connection such as broadband, DSL, etc. The zeros denote there is no other route, other than the gateway.

Example:

```
ADDGATEWAY 0.0.0.0 0.0.0.0 12.210.115.1 ETH0
```

The following example shows how to route the gateway for a more complex network, for instance, one that uses a firewall. The IP address of 12.210.115.190 is the firewall, 255.255.255.0 is the Subnet Mask of that firewall, and 12.210.115.1 is the Gateway address to the firewall.

Example:

```
ADDGATEWAY 12.210.115.190 255.255.255.0 12.210.115.1 ETH0
```

> **Note:**
>
> Unless a specific Route is designated, add only ONE gateway per interface as adding more than one gateway per interface can cause conflicts when adding or deleting IP addresses.
>
> Always add the IP address first and then the Gateway address. When removing an IP address, always remove the Gateway address first and then the IP address. Use SAVECONFIG and then VIEWCONFIG after executing each command.

ADDIP

The ADDIP command is used to add the IP address to the BRICKServer 2. The following ADDIP command is executed by replacing NNN.NNN.NNN.NNN with the IP address, SSS.SSS.SSS.SSS with the subnet mask, and ETHN with the interface.

Each computer and server on the Internet has at least one IP (Internet Protocol) address that uniquely identifies it from all other computers on the Internet. 10.1.1.2 is an example of an IP address. Your ISP or network administrator can provide you with the IP address of your computer and/or BRICKServer 2.

The Subnet Mask identifies the portion of the Internet Address that identifies the network and/or subnetwork for routing purposes. Subnetting is a technique used to allow a single IP network address to span multiple physical networks. Your ISP or network administrator can provide you with the Subnet Mask of your computer and/or BRICKServer 2.

The Interface is the physical connection to the network and is also referred to as a NIC (Network Interface Card). The BRICKServer 2 knows the NICs as ETH. Depending on the number of NICs in the BRICKServer 2, they are known as ETH0, for the first, and ETH1 as the second.

Command:

```
ADDIP <NNN.NNN.NNN.NNN> <SSS.SSS.SSS.SSS> <ETHN>
```

Example:

```
ADDIP 12.210.115.190 255.255.255.0 ETH0
```

Note:

Always add the IP address first and then the Gateway address.
When removing an IP address, always remove the Gateway
address first and then the IP address. Use SAVECONFIG and then
VIEWCONFIG after executing each command.

The following example shows how to add two IP addresses.

Example:

```
ADDIP 206.61.52.2 255.255.255.192 ETH0

ADDIP 206.61.52.3 255.255.255.192 ETH0:1
```

ADDROUTE

ADDROUTE is used to direct clients to a network using a truncated IP
Address, thereby reducing access time. The basic command syntax for
ADDROUTE is to type the command followed by the destination IP address, a
mask that determines how much of the address is needed before it is
recognized, the Gateway address, and then the interface as in the following
command example.

Command:

```
ADDROUTE <DESTINATION> <MASK> <GATEWAY MASK> <INTERFACE>
```

The following example shows how to add a route for IP address
12.210.115.190 to the Gateway of 255.255.255.0 using the ETH1 interface.

Example:

```
ADDROUTE 12.210.115.190  255.255.255.0 12.210.115.1 ETH1
```

ADDSSL

ADDSSL is used to link the IP address to a domain, making it the default
domain for that IP. The basic command syntax for ADDSSL is to type the
command followed by the IP address, and then the domain name as in the
following command example.

Command:

```
ADDSSL <IP ADDRESS> <DOMAIN>
```

The following example shows how to add an SSL connection for IP address 12.210.115.190 to the domain of mywebsite.com.

Example:

`ADDSSL 12.210.115.190 MYWEBSITE.COM`

ADDVHOST

The ADDVHOST command is used to link virtual domains to the actual domain. Using the following ADDVHOST command, replace VIRTUAL HOST/DOMAIN with the ACTUAL HOST/DOMAIN name.

Command:

`ADDVHOST <VIRTUAL HOST/DOMAIN> <ACTUAL HOST/DOMAIN>`

In the following example, people who look for WWW.BRICKSERVER.COM on the Internet can find BRICKSERVER.COM.

Example:

`ADDVHOST WWW.BRICKSERVER.COM BRICKSERVER.COM`

Subdomains are added the same way. After adding a subdomain using the Domain section of the BRICKServer 2 Secure Config, use the ADDVHOST command to direct a virtual domain to it. In the following example, people who look for WWW.MY.TESTING.BRICKSERVER.COM on the Internet can find MY.TESTING.BRICKSERVER.COM.

Example:

`ADDVHOST WWW.MY.TESTING.BRICKSERVER.COM MY.TESTING.BRICKSERVER.COM`

DATE

DATE is used to change the date and time on the BRICKServer 2.

DELDOMAIN

DELDOMAIN is used to remove the domain, the administrator, and all users, as well as all directories and all related files. The basic command syntax for DELDOMAIN is to type the command followed by the desired domain name as in the following command example.

Command:

`DELDOMAIN <DOMAIN>`

In the following example, DELDOMAIN is used to remove a domain named MYWEBSITE.COM from the BRICKServer 2.

Example:

```
DELDOMAIN MYWEBSITE.COM
```

DELGATEWAY

DELGATEWAY is used to remove a gateway from the BRICKServer 2. The basic command syntax for DELGATEWAY is to type the command followed by the destination IP address, the mask that determines how much of the address is needed before it is recognized, the Gateway address, and then the interface as in the following command example.

Command:

```
DELGATEWAY <DESTINATION> <MASK> <GATEWAY MASK> <INTERFACE>
```

The following example shows how to remove the gateway from the ETH1 interface.

Example:

```
DELGATEWAY 0.0.0.0 255.255.255.0 0.0.0.0 ETH1
```

Command:

```
DELGATEWAY <DESTINATION> <MASK> <GATEWAY> <INTERFACE>
```

Note:

Always add the IP address first and then the Gateway address. When removing an IP address, always remove the Gateway address first and then the IP address. Use SAVECONFIG and then VIEWCONFIG after executing each command.

DELIP

DELIP is used to remove an IP address from a NIC on the domain. The basic command syntax for DELIP is to type the command followed by the interface as in the following command example.

Command:

```
DELIP <INTERFACE>
```

The following example shows how to remove the IP address on the ETH0 interface.

Example:

```
DELIP ETH0
```

Note:

Always add the IP address first and then the Gateway address. When removing an IP address, always remove the Gateway address first and then the IP address. Use SAVECONFIG and then VIEWCONFIG after executing each command.

DELROUTE

DELROUTE is used to remove a route from the BRICKServer 2. The basic command syntax for DELROUTE is to type the command followed by the destination IP address, the mask that determines how much of the address is needed before it is recognized, the Gateway address, and then the interface as in the following command example.

Command:

```
DELROUTE <DESTINATION> <MASK> <GATEWAY> <INTERFACE>
```

The following example shows how to remove a route from the ETH1 interface.

Example:

```
DELROUTE 12.210.115.190 255.255.255.0 12.210.115.1 ETH1
```

DELSSL

DELSSL is used to remove a secure connection between BRICKServer 2 and client(s). The basic command syntax for DELSSL is to type the command followed by the IP address as in the following command example.

Command:

```
DELSSL <IP ADDRESS>
```

The following example shows how to remove an SSL connection for IP address 12.210.115.190.

> **Example:**

```
DELSSL 12.210.115.190
```

EXIT

The EXIT command is used to log off the BRICKServer 2, thereby securing it.

GETDNS

The GETDNS command lists the DNS entries made by using SETDNS.

GETDOMAINS

GETDOMAINS lists the domains created using ADDDOMAIN.

GETVHOSTS

The GETVHOSTS command shows a list of the domains on the BRICKServer 2.

HELP

The command HELP is used to view a list of the available BRICKServer 2 commands. Command parameters can be viewed by typing the desired command without any parameters. The following example shows the results of typing the command PASS on the BRICKServer 2.

> **Command:**

```
PASS <PASSWORD>
```

PASS

PASS is used to change the password that was established during the initial setup of the BRICKServer 2. The basic command syntax for PASS is to type the command followed by the desired password as in the following command example.

> **Command:**

```
PASS <PASSWORD>
```

The following example shows how to change the password to mypassword.

> **Example:**

```
PASS MYPASSWORD
```

REBOOT

If it is ever necessary to restart the BRICKServer 2 without turning off the power, execute the REBOOT command, which will shutdown and restart the BRICKServer 2 without turning off the power.

> **Command:**

```
RESTART
```

SAVECONFIG

The SAVECONFIG command saves the active configuration. New commands are appended to the configuration file when the command is executed.

SETDNS

Set the DNS server by executing the following SETDNS command, replacing NNN.NNN.NNN.NNN with the IP address.

> **Command:**

```
SETDNS <NNN.NNN.NNN.NNN>
```

> **Example:**

```
SETDNS 12.210.115.50
```

Up to 10 DNS entries can be added sequentially. The following command shows how 10 DNS entries would be added.

> **Command:**

```
SETDNS <NNN.NNN.NNN.NNN> <NNN.NNN.NNN.NNN> <NNN.NNN.NNN.NNN>
<NNN.NNN.NNN.NNN> <NNN.NNN.NNN.NNN> <NNN.NNN.NNN.NNN> <NNN.NNN.NNN.NNN>
<NNN.NNN.NNN.NNN> <NNN.NNN.NNN.NNN> <NNN.NNN.NNN.NNN>
```

SHUTDOWN

If it is ever necessary to turn off the power to the BRICKServer 2, execute the SHUTDOWN command, which stops all services running on the BRICKServer 2, and turns off the power.

Command:

`SHUTDOWN`

START

The START command is used to start a service on the BRICKServer 2. Available services include:

- **Admin**—Administration
- **FTP**—File transfer protocol
- **HTTP**—Webserver
- **Mail**—Starts mail services below SMTP, POP3, and TURN
- **SMTP**—Server that sends mail
- **POP3**—Server that retrieves mail
- **TURN**—Server that relays mail going outside the BRICKServer 2
- **SSL**—Secured socket layer

The basic command syntax for START is to type the command followed by the service name as in the following command example.

Command:

`START <SERVER NAME>`

The following example shows how to start FTP.

Example:

`START FTP`

STOP

STOP a service currently running on the BRICKServer 2 by using the STOP command. The basic command syntax for STOP is to type the command followed by the service name as in the following command example.

Command:

`STOP <SERVER NAME>`

The following example shows how to STOP the FTP service.

Example:

`STOP FTP`

VERSION

The VERSION command lists the version running on the BRICKServer 2, the available languages, and the languages on the system.

VIEWCONFIG

The VIEWCONFIG command displays the current active configuration on the screen.

VIEWFILE

VIEWFILE shows the current saved configuration file.

Chapter 6.

Advanced Web Topics

Default Web Pages

When a user types a URL into their web browser window (e.g., myserver.com or myserver.com/mydirectory) the BRICKServer 2 will show them the index.html file. If the index.html file is not found, the BRICKServer 2 will look for the next file on the following list (index.htm) to show the user. This process continues until one of the following files is found.

- index.html
- index.htm
- index.shtml
- default.htm
- index.cgi

If none of the files is found in the CGI-BIN or CGI-PBIN directories, the 500 Internal Error will occur (Figure 81). Follow the steps found on page 4-21, under the topic heading Customize the HTTP Banner to show something other than the 500 Internal Error.

500 Internal Error

There was an unusual problem serving the requested URL '/'.

thttpd/2.20c 21nov01 on a Brickserver 2

Figure 81. 500 Internal Error

Script Files

Script files are put into the CGI-BIN or CGI-PBIN directory and must be marked as executable using Executable/Normal on the Web tab (Figure 53) in the BRICKServer 2 Secure Remote Admin. CGI-BIN has create / read / write / delete access to CGI-DATA as well as execute rights in the CGI-PBIN but has no rights to the CGI-PDATA. CGI-PBIN has create/append writes to CGI-PDATA and create / read / write / delete access TO CGI-DATA as well as execute rights within CGI-BIN. CGI-PDATA can only have files created/appended.

> **Note:**
>
> Only files in the CGI-BIN and CGI-PBIN directories will be recognized as executable, code must be adjusted accordingly.
>
> An asterisk next to the filename indicates an executable file.

Scripts are named according to their language, as shown in the following table.

Script Language	File Extension
PHP	.php
PERL	.pl
PYTHON	.py
TCL	.tcl
JAVA	.java

Java, JavaScript, VBScript, and ActiveX

Java, *JavaScript*, *VBScript*, and *ActiveX* are usually used as client-side languages, meaning they are programs that run on the browser of the Web site visitor. These client-side applications can also run with your BRICKServer 2.

> **Note:**
>
> BRICKServer 2 does not come with a *Java* compiler.

JavaScript and *VBScript* are languages originally written to run on *Netscape* and *Microsoft Internet Explorer* browsers, respectively. As long as older versions of these languages are used, most but not all browsers will run these programs. *ActiveX* can encapsulate almost any application or applet into your web pages. However, it is not compatible with many browsers.

Java is bytecode complied on a *Java* compiler and then sent from the webserver to be run on the visitors' *Java*-enabled browsers. The <APPLET> HTML element is needed to add a *Java* applet to a page on your webserver.

> **Example:**
>
> ```
> <APPLET CODE="myapplet.class" WIDTH=250 Height=250> </APPLET>
> ```

This code would activate a visitor's browser to run the applet "myapplet.class" in a box 250 pixels on a side.

Use the <APPLET CODEBASE> format to run an applet located on another webserver. The general format is shown in the following example.

Example:

```
<APPLET CODEBASE="http://a_web_site_with_complied_Java_applets.com"
CODE="TestApplet.class" width=400 height=75 align=center >

<PARAM NAME="text" VALUE="This is the Applet Viewer.">

</APPLET>
```

The format for calling *Java* applets given in the following example with optional elements shown in brackets.

Example:

```
<APPLET

[CODEBASE = "http:the_URL_where_the_compiled_applet_resides"]

CODE = "myapplet.class"

[ALT = "Alternate text the viewers see if their browser can't run
Java"]

[NAME = "Applet instance name"]

WIDTH = pixels desired HEIGHT = pixels desired

[ALIGN = alignment desired]

[VSPACE = pixels desired]

>

[<PARAM NAME = appletAttribute1 VALUE = value>]

[<PARAM NAME = appletAttribute2 VALUE = value>]

…and so on for the desired number of PARAM NAMES…

[alternateHTML]

</APPLET>
```

Go to http://java.sun.com/applets/jdk/1.0/ to download a zip file with free complied applets and web pages that run on a *Java*-enabled browser to test *Java* on your webserver.

Basic PERL Script Example

```
#!/ext/pl

my $i=10;

print <<EHTML;

Content-Type:text/html

<html><head><title>TESTPAGE</title></head>

<body>

<h2>HELLO WORLD - BASIC PERL</h2>

$i

<h2>From your friends at SAGE</h2>

</body></html>

EHTML

exit;
```

PERL MYSQL Example

```
#!/ext/pl

use DBI;

my $host    = "192.168.0.188";

my $port    = "3306";

my  $dsn     = 'dbi:mysql:test:192.168.0.188:3306';

my $db_user = "root";

my $db_pw   = "";

my $dbh;

my $sth;

$dbh = DBI->connect($dsn,

                    $db_user,

                    $db_pw,
```

```
                        { RaiseError => 1, AutoCommit => 1 });

$sth = $dbh->prepare( q{ INSERT INTO SAGE (name) VALUES( ? )} );

$sth->execute('Perl User');

$dbh->disconnect;

exit;
```

Basic PHP Example

```
<HTML>

<HEAD>

<TITLE>

PHP TEST - echo test

</TITLE>

</HEAD>

<BODY>

<?

echo "Testing Echo - Very Basic Test";

?>

</BODY>

</HTML>
```

PHP MYSQL Connection Example

```
<?

    // ******************** Change this Title *************************

    $title = "Test \"connect_db\" function";

?>

<html>

<head>

<title><? echo($title); ?></title>
```

```
<h3><? echo($title); ?></h3>

</head>

<body>

<?

    // *************** Put your "Body" code in here *******************

    echo "connect_DB.php TOP now<br>";

     $link = mysql_connect("192.168.0.188:3306", "joe")

        or exit("Could not connect<br>");

    echo ("Connected successfully<br>");

        $db_connect=mysql_select_db("test",$link)

            or exit("Could not Select Table<br>");

    echo ("Connected to Table Successfully<br>");

    mysql_query("INSERT INTO SAGE (name) VALUES ('PHPMYSQL')");

    mysql_close($link);

?>

</body>

</html>
```

Basic PYTHON Example

```
print "Content-type: text/html\n\n"

print "<html>\n"

print "<Head>"

print "<Title>Obligatory Python Test Script</Title>"

print "</Head>\n"

print "<Body>\n"

print "<H3>Hello</H3>"

print "<b>This is the obligatory<br> Python 'Hello\' test
script<br></b>"
```

```
print "<i>Ta-da</i>"

print "</body>\n</html>"
```

PYTHON MYSQL Connection Example

```
#!/ext/py

import MySQLdb

print "Content-Type: text/html"

print # End of Headers!

print "<TITLE>Test Form Output</TITLE>"

print "<H1>Test Form Output</H1>"

db = MySQLdb.connect(db='test', host='192.168.0.3', user='SAGE',
passwd='')

if db is not None:

print "<LI>YEAH DB"

if db is None:

print "<LI>NOOOOOO DB"

cursor = db.cursor()

if cursor is None:

print "<LI>NOOOOO"

if cursor is not None:

print "<LI>YEAH CURSOR"

cursor.execute("""INSERT INTO SAGE (name) VALUES ("PythonMysql")""")

print "</UL>"

print "</BODY>"

print "</HTML>"
```

TCL Basic Example

```
puts "Content-Type: text/html\n\n"
```

```
puts "<html>"

puts "<body>"

puts "<h1>hello tcl world!</h1>"

puts "</body>"

puts "</html>"
```

Chapter 7.

Additional Information

BRICK*server* **2**

h a c k - p r o o f   w e b   s e r v e r

Interface Naming Convention

The interface naming convention is determined by how many network interface cards (NIC) are in the BRICKServer 2 and how many IP addresses (up to 64 per NIC) will be added to each NIC. The naming convention of ETHN:N is used to name the interface. The first interface, for example, would be named ETH0, and the second interface would be named ETH0:1.

FTP Password Security

Logins, uploads and downloads to FTP are not protected by encryption. Sending FTP passwords in the clear is dictated by the specifications for FTP protocol.

Use special caution when setting FTP and mail passwords on the BRICKServer 2. In order to be compatible with other FTP and email programs, these passwords are not encrypted while in transit over your network or the Internet making it easy for a computer criminal to "sniff" them. So if you choose FTP and/or email passwords that are identical to any of your Web administration passwords, you are leaving your BRICKServer 2 wide open for an attacker to deface or shut down your Web site.

FTP Security

Since FTP client programs do not encrypt communications, any files uploaded or downloaded using FTP are vulnerable to "sniffing" (i.e., eavesdropping by computer criminals).

Securing Files on the Webserver

Files placed in the CGI data directory are difficult to read without a CGI program. Some webmasters take advantage of that by placing confidential files such as user names and passwords, or credit card information in that directory. However, CGI-DATA files are only as safe as the CGI programs that read from them and consequently visitors are sometimes able to read confidential files. The solution is to never use the CGI-DATA directory to hold files you absolutely do not want visitors to see.

ActiveX

A loosely defined set of rules developed by *Microsoft* for how applications should share information. ActiveX controls use *ActiveX* technology. Programmers can develop *ActiveX* controls in a variety of languages (i.e., C++, Visual Basic, *Java*) for automatic download and execution by a Web browser.

Administrator

The user who controls and maintains the accounts of other system users. The administrator has access to settings and functions that a typical user cannot modify.

AES

A block cipher used for encryption of data transfers. It is free for all uses.

Client

A computer connected either to the Internet or the same network as the BRICKServer 2.

DNS

Domain Name Service. Internet service that translates domain names into IP addresses.

Ethernet Port

The Ethernet Port is the interface connecting the BRICKServer 2 to the Internet or network is also referred to as a NIC (Network Interface Card). It uses a cable known as a patch, CAT-5 or Ethernet cable, having a RJ-45 connection. BRICKServer 2 knows the NIC as ETH. The interface naming convention is determined by how many network interface cards (NIC) are in the BRICKServer 2 and how many IP addresses (up to 64 per NIC) will be added to each NIC. The naming convention of ETHN:N is used to name the interface. The first interface, for example, would be named ETH0, and the second interface would be named ETH0:1.

FTP

File transfer protocol. The protocol used on the Internet for sending files.

Gateway

Network point that acts as an entrance to another network.

Gateway Address

Address of the computer connecting your BRICKServer 2 to the Internet. Your network administrator or ISP can provide you with the Gateway address of your computer and/or BRICKServer 2.

HTTP

Hypertext Transfer Protocol. The underlying protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands.

IP Address

Each computer and server on the Internet has at least one IP (Internet Protocol) address that uniquely identifies it from all other computers on the Internet. 10.1.1.2 is an example of an IP address. Your ISP or network administrator can provide you with the IP Address of your computer and/or BRICKServer 2.

Java

A high-level, object-oriented programming language developed by Sun Microsystems. It is similar to C++, but simplified to eliminate language features that cause common programming errors.

JavaScript

A scripting language developed by Sun Microsystems to enable Web authors to design interactive sites.

Linux

A freely-distributed open source operating system that runs on a number of hardware platforms. Can be downloaded from the Internet (www.linux.org) at no charge.

Mail Domains

Used to identify the name of the BRICKServer's mail service. It must be the same name that the ISP or DNS administrator used to set up the DNS record for your mail server.

MD5 Digital Signatures

An algorithm used to create digital signatures for initial authentication.

Network Mask

Often referred to as the netmask, provided by your ISP or network administrator.

NIC

Network Interface Card. A board inserted into a computer so it can be connected to a network.

OS

Operating System (Windows, Unix, etc.). The most important program that runs on a computer. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

PERL

A general-purpose programming language that can be downloaded from the Internet (www.perl.com) at no charge.

PHP

Short for PHP: Hypertext Preprocessor. A general-purpose programming language that can be downloaded from the Internet (www.php.net) at no charge.

POP3

Post Office Protocol. Protocol for retrieving email between servers.

PYTHON

A general-purpose programming language that can be downloaded from the Internet (www.python.org) at no charge.

SMTP

Simple Mail Transfer Protocol. Protocol for sending email between servers.

SSI

Server Side Include. A powerful tool for web developers used to execute programs and insert the results. Directs Web servers to dynamically generate data for the Web page whenever it is requested.

SSL

Secured socket layer. Protocol used to transmit private documents via the Internet.

Subnet Mask

The Subnet Mask identifies the portion of the Internet Address that identifies the network and/or subnetwork for routing purposes. Subnetting is a technique used to allow a single IP network address to span multiple physical networks. Your ISP or network administrator can provide you with the Subnet Mask of your computer and/or BRICKServer 2.

TCL

A general-purpose programming language that can be downloaded from the Internet (tcl.sourceforge.net) at no charge.

THTTPD

A portable, fast and secure HTTP Web server.

Unix

A popular multi-user, multitasking operating system.

VBScript

Simpler version of the Visual Basic programming language developed by *Microsoft*. Enables Web authors to include interactive controls, such as buttons and scrollbars, on their Web pages.

Chapter 9.

List of Figures

Chapter 10.

Index

T

U

V

W

SAGE, Inc.

Telephone...806-354-8185 or 800-580-0025

Email...support@sage-inc.com

Website...www.sage-inc.com