

KerioWebStar5™

Users Guide

Kerio Technologies

© 1997-2006 Kerio Technologies. All rights reserved.

Release Date: June 8, 2006

This guide provides detailed description on *Kerio WebSTAR 5*, version 5.4. Any additional modifications and up-dates reserved.

For current product version, check <http://www.kerio.com/>.

Contents

- 1 Welcome to Kerio WebSTAR 5! 4**
- 2 Kerio WebSTAR 5 Overview 5**
 - 2.1 Testing the Kerio WebSTAR 5 Web Server 5
- 3 Setting up a Web Site 7**
 - 3.1 Installing your Web Site 7
- 4 The Admin Client Application 10**
 - 4.1 Using Administrative Access Levels 11
 - 4.2 The Admin Client Screen 12
 - 4.3 Admin Client Basics 16
 - 4.4 Entering and Editing Information 19
- 5 Adding Admin Users 23**
 - 5.1 Entering New Admin Users 23
 - 5.2 Limiting Admin Client Access with the Admin Server Allow/Deny Table 24
 - 5.3 Assigning Permissions to Host Administrators 24
- 6 Creating Web Virtual Hosts 26**
 - 6.1 Entering and Configuring Virtual Hosts 26
 - 6.2 Routing Requests to your Server Machine 28
- 7 Web Security 29**
 - 7.1 Overview 29
 - 7.2 Using a List as an Authenticator 33
 - 7.3 Setting up a Realm 37
- 8 Sharing Files with WebDAV 42**
 - 8.1 Setting up WebDAV Service 42
 - 8.2 Accessing the Web Folder using the Internet 43

Chapter 1

Welcome to Kerio WebSTAR 5!

Kerio WebSTAR 5 is the fastest and easiest to use web server available. The server applications are extremely fast Unix applications that take advantage of *Mac OS X*'s built-in multiprocessor support, faster networking, and the inherent stability of Unix. Your user interface is a separate Java application, *Admin Client*, that can be run from your server computer or any *Mac OS X* or *Windows* client computer with a TCP/IP connection to the server computer.

With the *Admin Client*, there is absolutely no need for you to learn and use a command-line interface, work with text-based configuration files, or deal with Unix commands.

The *User's Guide* is designed for the user who is new to *Kerio WebSTAR 5* and wants to publish a web site on the internet. It assumes that you have followed the instructions in the *Installation Guide* and have already installed the *Kerio WebSTAR* on your server computer and licensed your copy of *Kerio WebSTAR 5*.

We first review the process of porting your *WebSTAR 4* (or other) web site to *Kerio WebSTAR 5* and then introduce the *Admin Client* application. You will learn about:

- Establishing a connection to the server suite via *Admin Client*
- Working with the *Admin Client* interface
- Adding system admin users (people authorized to administer the server via *Admin Client*)
- Creating and managing web virtual hosts (a.k.a., web sites)
- Creating secure realms within a web site (i.e., password-protected areas)
- Sharing folders on the web using WebDAV

Chapter 2

Kerio WebSTAR 5 Overview

Kerio WebSTAR 5 actually consists of a group of utilities, plug-ins, and applications that work together.

- The web server application, *WSWebServer*, actually runs in the background and has no user interface. You start it by double-clicking the *Launcher*.
- The *Admin Client* application provides the main interface to the server suite. It can be run from either the server machine or other Mac OS X or Windows machines on your network.
- The *Admin Server* application manages communication between the *Admin Client* and the servers.
- The *Monitor* application enables you to monitor server activity from the server machine without using *Admin Client*.

2.1 Testing the Kerio WebSTAR 5 Web Server

The server suite includes a launcher utility whose main function is to start the server applications and the *Admin Server* utility. Its *File* menu allows you to access the utility applications that allow you to configure and monitor the server suite.

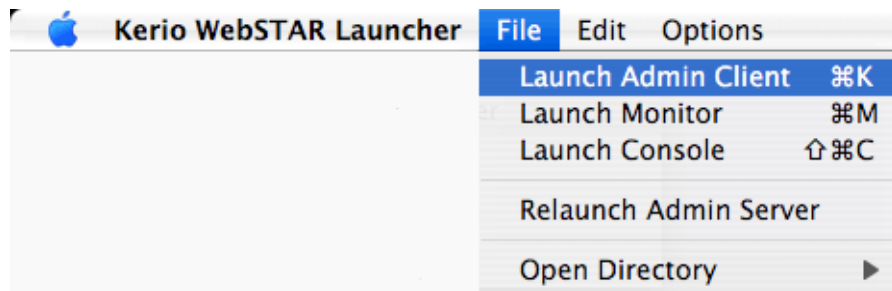
1. To start the *Kerio WebSTAR 5* servers, double-click the *Kerio WebSTAR Launcher* application.



Kerio WebSTAR Launcher

In a few seconds, its menu bar replaces the *Finder* menu bar. It launches the *WebSTAR Admin Server*, the servers, and loads the *WebSTAR* plug-ins located in the *Plug-ins* folder.

The Launcher's *File* menu lets you open the *Admin Client* application, the *Monitor* application, relaunch the *Admin Server* application, or open selected directories in the *Kerio WebSTAR* folder.



- The *Admin Client* is the utility application that enables you to configure and monitor all aspects of the server suite.
- The *Monitor* application enables you to monitor server suite activity. You can also access all of the *Monitor* application's windows via the *Admin Client*.

The *Kerio WebSTAR 5* servers also have no user interfaces. To verify that the *Web Server* is, indeed, running, open the *Process Viewer* application that is provided with Mac OS X. It should show the *WSWebServer* process running under the special "webstar" user that you created when you installed the server suite.

2. Open a web browser application on any computer that can see the server machine and connect to the server machine.

If your browser is on the Server machine, use `http://localhost/`. If it is on another machine, you can use the IP address of the server machine (e.g., `http://192.168.1.118`) or hostname (e.g., `http://www.mydomain.com`).

You will be able to browse the web site in the *DefaultSite* folder. You will see the default home page that ships with *Kerio WebSTAR 5*.

Once you verify that your web server is running, you are ready to reconfigure the *DefaultSite* folder so that *Kerio WebSTAR* will serve your site.

Chapter 3

Setting up a Web Site

Kerio WebSTAR 5 can serve a large number of web sites simultaneously. Each web site is called a web virtual host even if you are using *Kerio WebSTAR 5* to serve only one site.

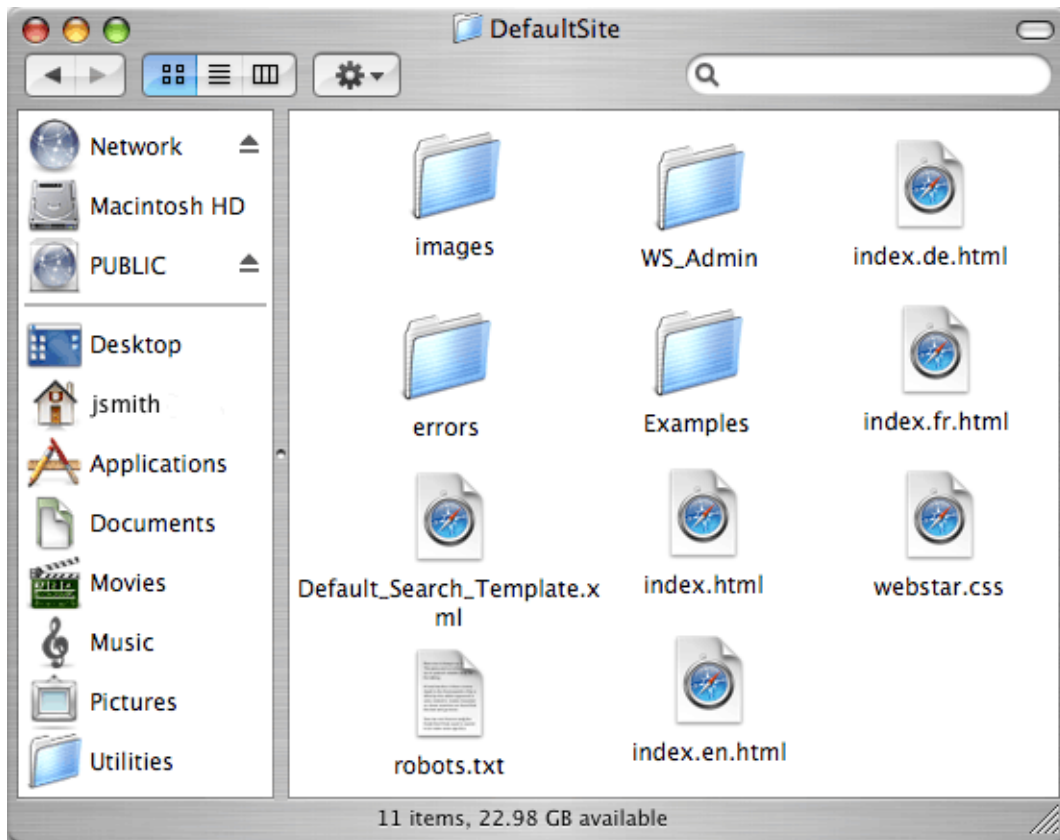
Each web virtual host has its own root folder. The root folder for a site contains all the files used by the entire web site.

Ordinarily you place all the root folders in the *WebServer* folder, which contains the web server application. Unlike OS 9 versions of *WebSTAR*, no `.html` files are placed at the same level as the webserver.

The Installer creates a “placeholder” root folder for you. It is called *DefaultSite*. You serve your site simply by replacing the default home page with yours and placing all the files for your site in this folder.

3.1 Installing your Web Site

The easiest way to install your web site is to replace the contents of the *DefaultSite* folder with your home page and the documents that make up your site.



The `index.html` file is the home page and the *Examples* and *images* folders contain documents that are used by the default site. The *errors* folder contains default `error.html` messages.

When you modify the contents of the *KerioWebStar* folder, you should do so logged on as the “webstar” user that you created during the installation process. This ensures that the web server will have the correct file permissions.

1. If you are not currently logged in as the “webstar” user, choose *Log Out* from the *Mac OS X Apple* menu.
2. When prompted to log in, enter “webstar” as the user name and enter the webstar user’s password.
3. When the Mac OS X desktop appears, open the *WebServer* folder, which is in the *KerioWebSTAR* folder in your main *Applications* folder.

To replace the *DefaultSite* with your own site:

1. Open the *DefaultSite* folder, delete the `index.html` document and replace it with your home page. If your home page isn't already named `index.html` give it this name.
2. Place all the remaining files that make up your site inside the *DefaultSite* folder.

You can use the default error message files as is or replace them with your own. Be sure to name these `.html` files using the error numbers, e.g., `404.html` and store them in the `errors` folder.

If you need to perform tasks on the server machine that require Mac OS X Admin level privileges, you can log out and log in as an admin user. Be sure to remember to log in as “webstar” when you need to make changes to files that the web server will access.

Chapter 4

The Admin Client Application

You use the *Admin Client* application to configure and monitor the entire server suite.

Kerio WebSTAR 5 supports two levels of administration: Server-wide and Host-specific. Server-wide settings apply to the server suite as a whole and all hosts, while other aspects are configured separately for each host.

For administrative purposes a Settings Group combines access privileges to a web host.

Kerio WebSTAR 5 supports two levels of administrative user access, the full administrator level, which grants access to the server-wide settings and all hosts, and host admin, which grants access only to the host-specific settings for a selected *Settings Group*.

Server-Wide Settings

- Enter and set access privileges for *Kerio WebSTAR 5* administrators.
- Create and configure web virtual hosts.
- Set the *Default Document* loaded when browsers log onto your sites.
- Set the locations of the monitored servers, the ports used to communicate with *Admin Client* and the servers, and other server parameters.
- Set various web connections and web caching parameters.
- Configure encrypted connections using SSL.
- Set up and monitor FTP service.
- Edit the suffix mapping table.
- Set up a search index to support quick searches of your web site.
- Establish connections with *4th Dimension* databases to publish dynamic web sites.

Host-Specific Settings


- Configure web security. You can create secure realms within your web site and control access via a password system and or prohibit or allow specific hosts/IP addresses to connect.
- Set up shared folders using WebDAV and set permissions.
- Configure and monitor web logs.
- Configure CGI actions.

4.1 Using Administrative Access Levels

If you use *Kerio WebSTAR 5* to serve several (unrelated) web sites, it is possible for you to designate different individuals as administrators for each web site. If you grant host admin privileges to each site administrator and configure *Admin Server* so that each person can only see his web site, you can delegate certain administrative tasks to each person without compromising the security of the other web sites or the server as a whole.

How it Works

When a person connects to the *Admin Server* using the *Admin Client* application, the *Admin Client* firsts presents a Connect dialog box, in which the user must enter a valid user name and password.

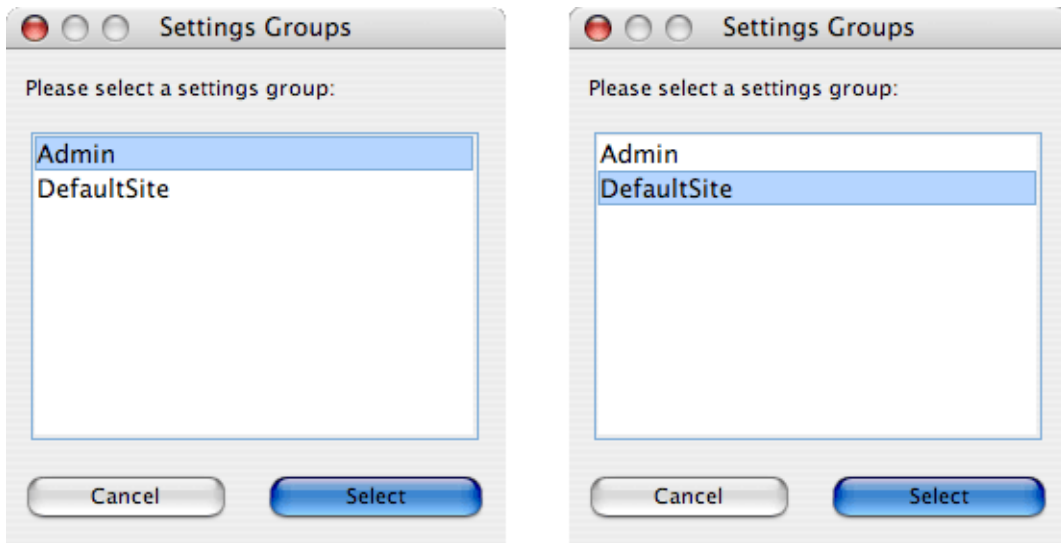


Using the *Server* and *Port* areas, the user must specify the server machine and the *Port* that the *Admin Server* is using to listen for requests from *Admin Clients*.

He or she must then provide a user name and password that has been entered into the system.

If the person enters a valid user name and password, the *Admin Client* application presents a list of *Settings Groups* that the user is authorized to administer.

Here is an example: On the left, a person with full admin privileges has just logged in. He can choose to access only the server-wide settings or the server-wide settings, plus the settings for the default web host. On the right, a person with host admin privileges for the *DefaultSite* has logged on. Only that *Settings Group* is presented.

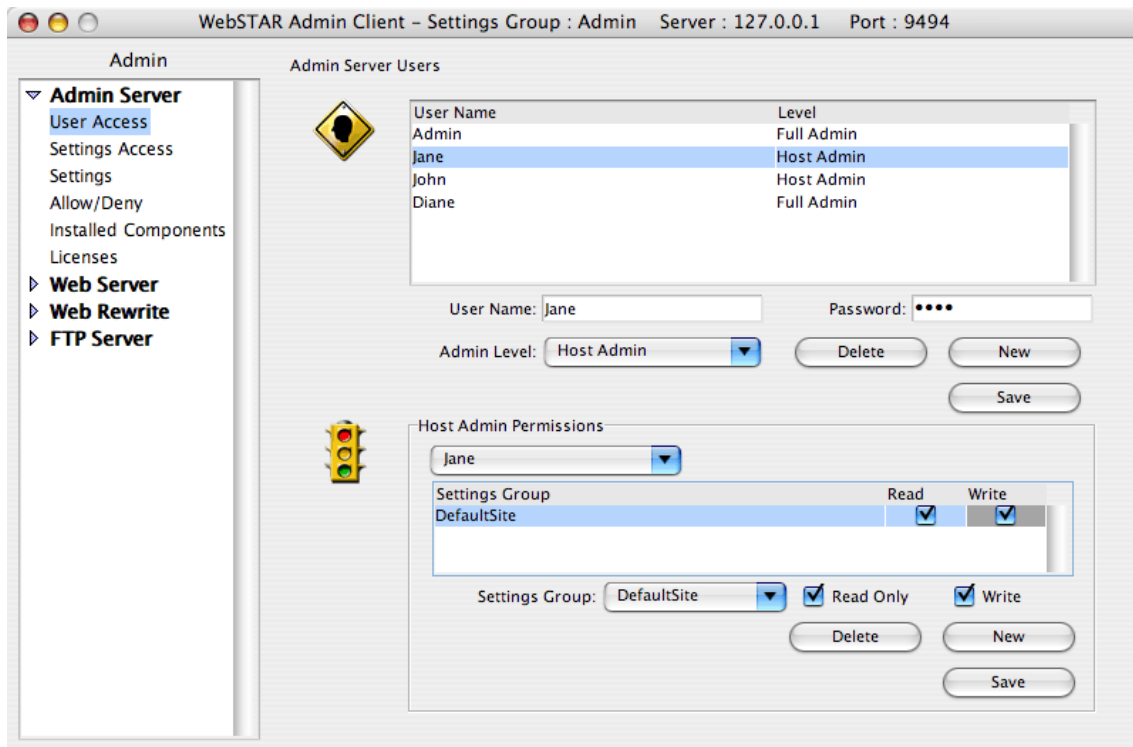


4.2 The Admin Client Screen

The *Admin Client* screen is divided into two areas: the browser area and the panel area.

You access a panel by clicking its name in the browser area. Panels are organized into groups and you can collapse or expand a group by clicking its disclosure triangle. You click on a panel name to display it in the panel area.

The server-wide panels are listed in the *Admin Server*, *Web Server*, *Web Rewrite*, and *FTP Server* groups. The host-specific panels are listed in the *Web Host*, *Web Security*, and *Web Rewrite* groups.



When you create a new admin user and give that person host admin privileges, the browser area will show only the host-specific panels that person has access rights for — omitting the serverwide panels and hiding the host admin settings for all other hosts served by your copy of *Kerio WebSTAR 5*.

If you create several hosts and log with full admin privileges, you will be asked to choose the *Settings Group* you wish to administer. The browser area will then show the serverwide panels and the host specific panels for only the host you chose, not other hosts for which you have access rights. You can open another window to gain access to other virtual hosts.

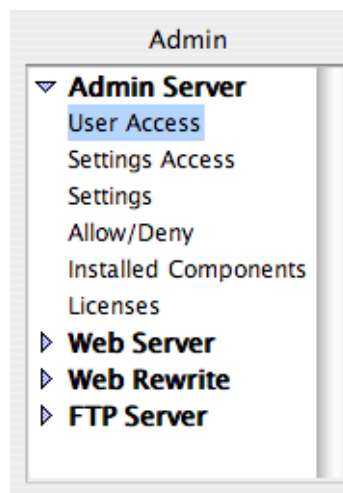
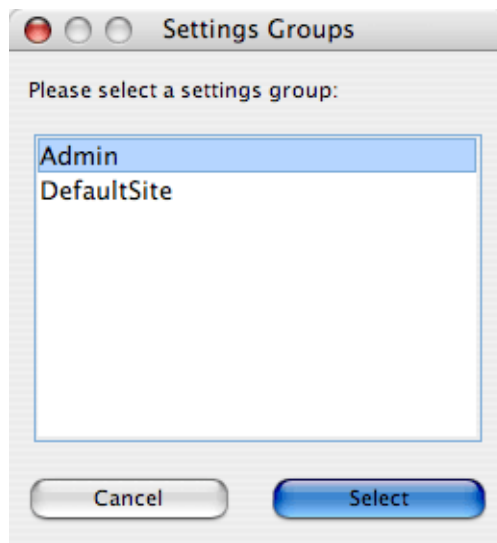
How to Regulate Administrative access to Kerio WebSTAR 5

- If you're a full administrator and you want to access only serverwide settings, choose *Admin* in the *Settings Groups* dialog.
- If you're a full administrator and you want to access settings for a web virtual host, choose that settings group in the *Settings Groups* dialog.
- If you're a full administrator and you want to access settings for two or more web virtual hosts, choose one settings group in the *Settings Groups* dialog and then choose

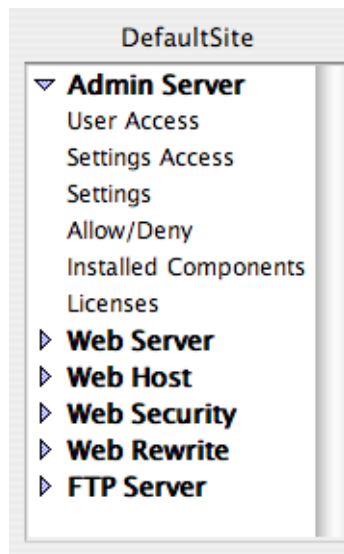
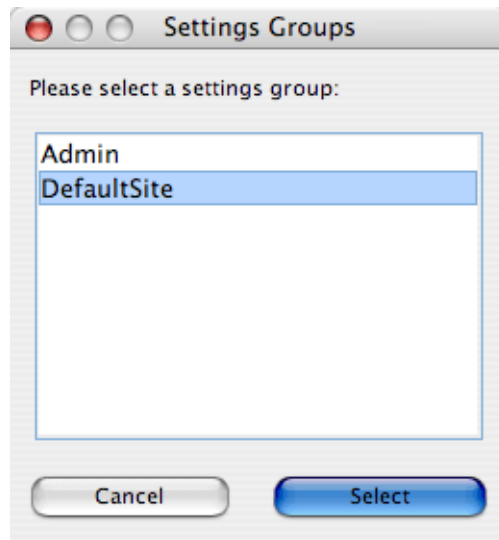
File. New and choose another settings group. The second settings are shown in the second window.

- If you're a host administrator, choose the settings group you want to access in the *Settings Groups* dialog.

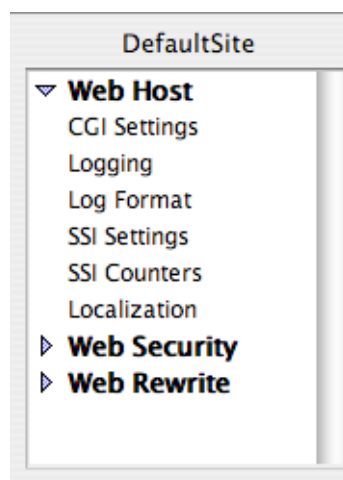
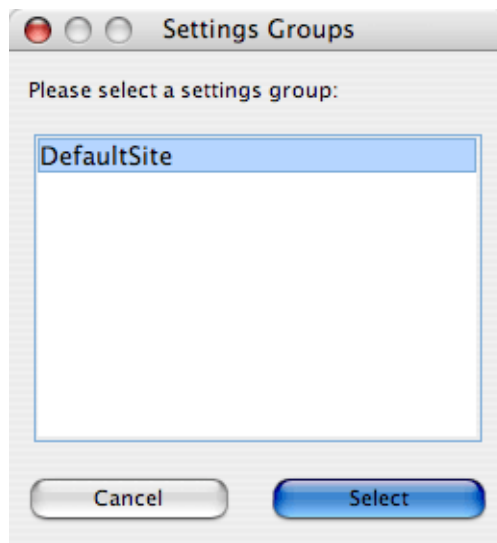
A full administrator selects the *Admin* group and sees only the Server-wide settings.



A full administrator selects a settings group and sees the Server-wide settings and the host-specific settings for that settings group. Both web site and mail settings appear.



A host administrator chooses a settings group and sees only the settings for that settings group.



4.3 Admin Client Basics

When you use the *Admin Client*, you log into the server suite using the server machine's IP address or hostname, port for communicating with the *Admin Client*, and an *Admin* user name and password.

If you are using the copy of *Admin Client* on the server machine, you can use `localhost` instead of the server machine's IP address or hostname.

After you access the *Admin Client*, you manage the server suite by selecting panels listed in the left panel and adding, modifying, or deleting data in the selected panel.

Establishing Contact with the Admin Server

To administer a *WebSTAR*, you need TCP/IP access from the client to the server machine. The default port used by the *WebSTAR Admin Client* and the *WebSTAR Admin Server* is 9494.

To configure your web virtual host:



1. Double-click your *Admin Client* application icon or choose *Launch Admin Client* from the Launcher's *File* menu.

In a few seconds, the *Connect* dialog box appears.

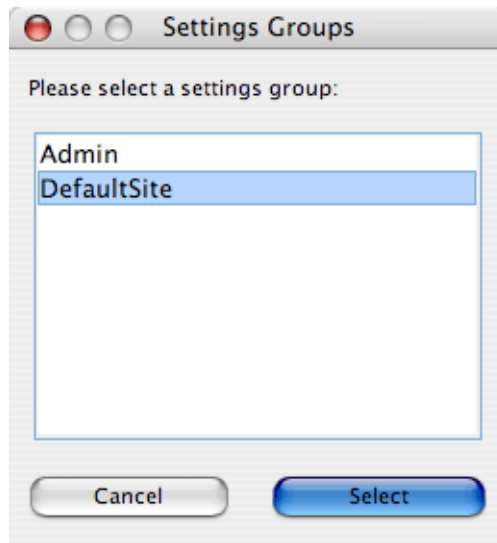
2. Enter the IP address or hostname of the computer that is running the *Kerio WebSTAR 5* server suite in the server entry area.

If you're running *Admin Client* on the server machine, enter `localhost` in the *Server* area.

3. Enter 9494 in the *Port* area.

This is the default port used by *WebSTAR Admin Client* to communicate with the *Admin Server* application. This port can be changed at a later time using *Admin Client*.

4. Enter a *User Name* and *Password* and click *Connect*.



The *Settings Groups* dialog box appears. The first *User Name* and *Password* that you enter will be the master *User Name* and *Password*. For that reason, be sure to choose a very secure password.

When you first log in, the *Admin* and *DefaultSite* settings groups are listed. The web hosts you create using the *Admin Client* application will appear in this list in subsequent logins.

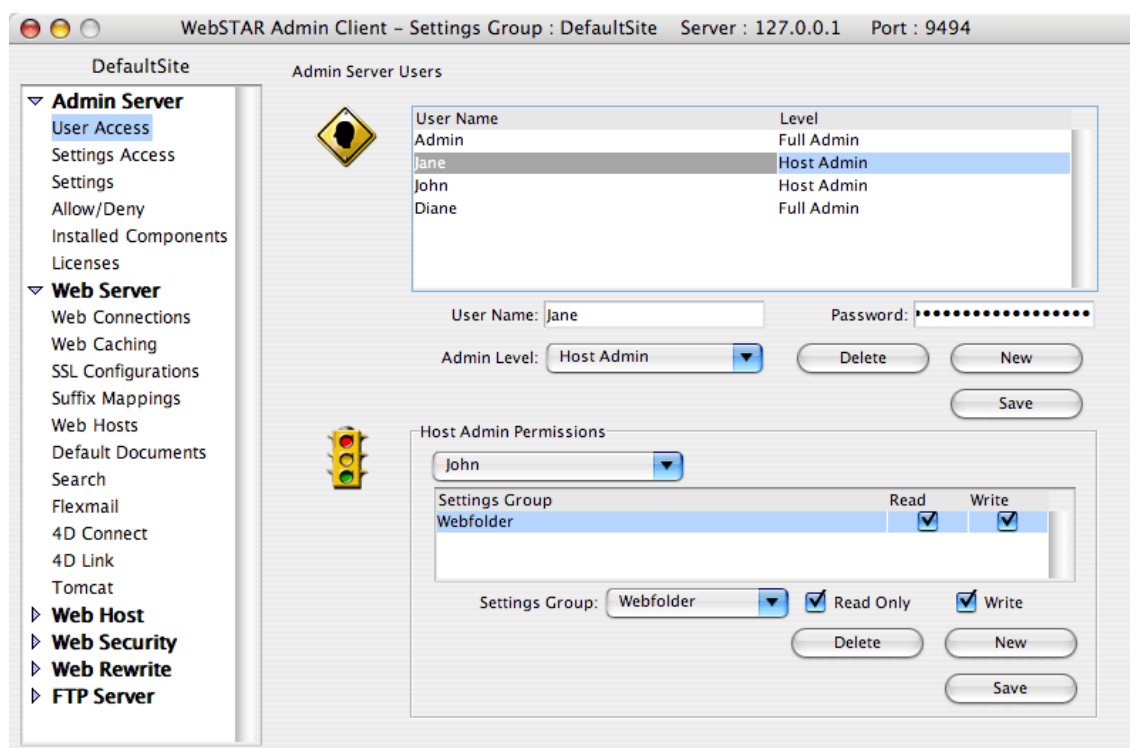
5. Highlight *DefaultSite* in the *Settings Groups* dialog box and click *Select*.

In a few seconds, the *Admin Client* window appears.

Working with the Admin Client

The *Admin Client* window uses a browser area on the left to allow you to display different panels and a panel area in which you view and configure *Kerio WebSTAR 5*. The title bar shows the current settings group, the IP address of the machine on which the *Admin Server* is running, and the port used to communicate with *Admin Client*. The current settings group is also shown just above the browser area.

The browser area organizes panel names by topic. The *Admin Server*, *FTP* and *Web Server* groups contain the server-wide settings and are shown only if you have full admin privileges. The *Web Host* and *Web Security* groups are host-specific. The settings in these groups of panels pertain to the settings group shown above the browser and in the title bar.



In this screen, a full administrator has logged onto the *DefaultSite* settings group. The *Admin Server Users* table shows that a second full administrator has been added plus two host admins. The *Host Admin Permissions* table shows the access permissions granted to one of the host admins.

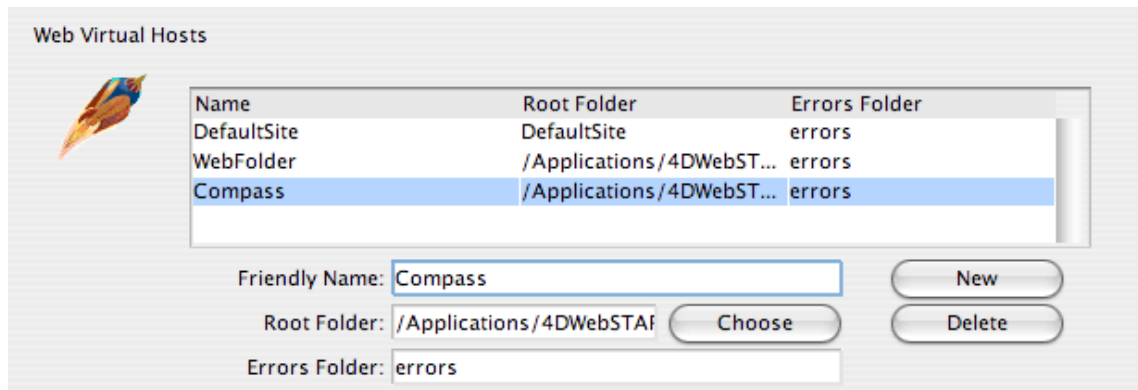
4.4 Entering and Editing Information

Although each *Admin Client* panel allows you to manage different settings, they all use the same types of interface elements and share the same conventions for adding, modifying, and deleting data.

These pages show the basic principles that you will use to enter, modify, delete, and import or export information.

Working With Tables

Many panels allow you to create a new entry in a table. For example, this table is a list of web virtual hosts:



You follow the same basic procedure for entry and editing of all tables.

- To create a new entry: Click the *New* button associated with the table. (Some panels contain two tables, each with their own set of buttons.) This creates a new, blank row in the table. You can enter information by typing directly into the new row. Often there are separate entry areas below the table in which you can also enter information. There is one area per column in the table. When you type into one area, your text is mirrored in the other area.

If you need to enter a path to a folder (as is the case for the root folder in this example), click the *Choose* button to select the folder using a *Select Folder* dialog box.

Add as many rows as needed by clicking the *New* button to add each new row. Click *Save* to save all your changes to the table. Some tables have their own *Save* button; other panels have only one *Save* button, located at the bottom of the screen.

Although the areas below a table that accept text are sometimes enterable, the information will not be added to the table unless a row is selected.

- To modify an entry: Double-click in a table cell to get an insertion point. Type the new text in the cell or modify the contents of the corresponding entry area below the table. Click the *Save* button to save your modifications to the table.
- To delete an entry: Double-click in a row to select the row. Click the *Delete* button to remove the row. Deleting a row is not undoable.

The Admin Client Menubar

Use the items in the *File* menu to establish connections to the *Admin Server*:

- *New* — Allows you to open another window to establish a new connection. For example, if you are a Full Admin and want to access the settings for a second Web Virtual Host, choose *New* to access that host.

- *Connect* — Enabled only when the frontmost window is not connected to the Admin Server. It allows you to use that window to access the Admin Server.
- *Disconnect* — Allows you to end the connection to the Admin Server.

Use the *Windows* menu contains menu items that display the server monitoring windows:

- *Admin Activity* — Shows the number of Admin user connections.
- *Admin Log* — Shows the history of Admin connections.
- *Web Log* — Shows the history of web usage.
- *Web Activity* — Summarizes web connection activity.

Table Pop-up Menus

Some tables use pop-up menus to control the contents of the table. For example, the contents of this table is controlled by the pop-up menu just above it.

Settings Group	Read	Write
Webfolder	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

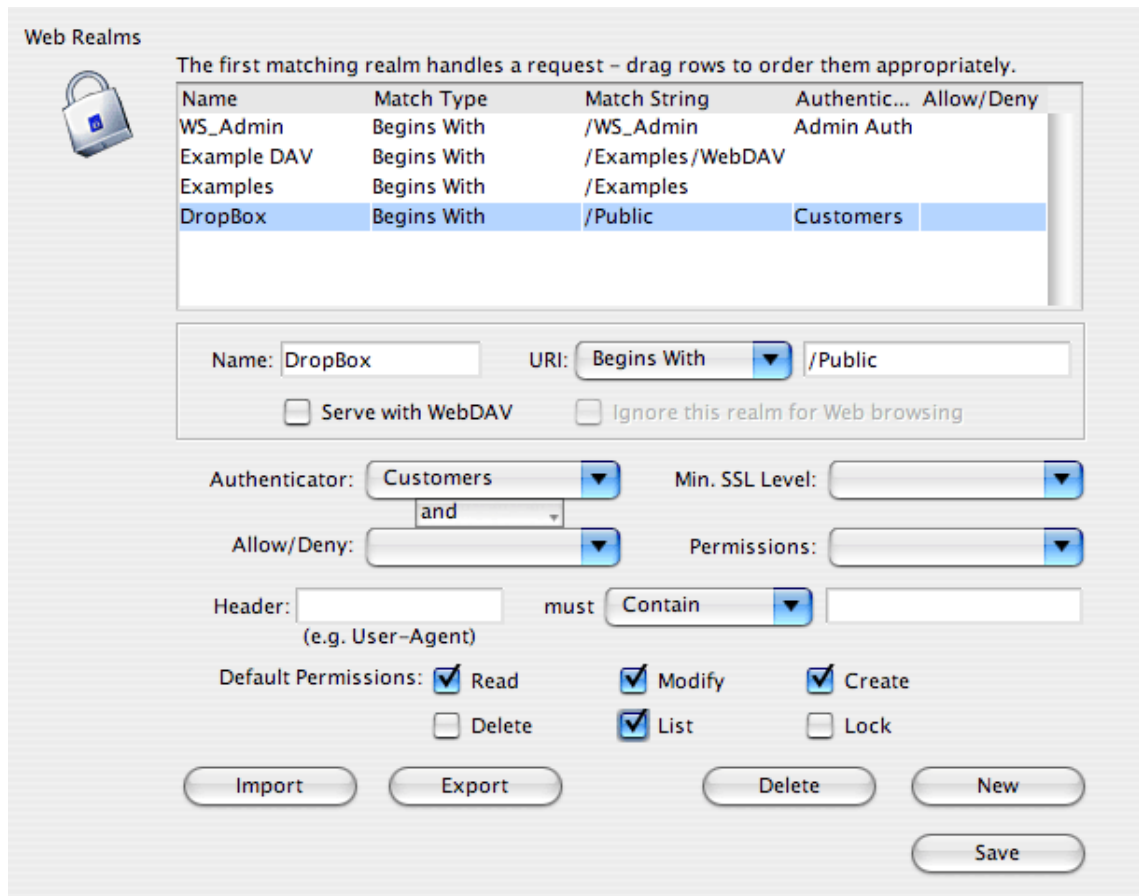
Settings Group: Read Only Write

Buttons: Delete, New, Save

When you chose another name from the pop-up, the table is populated with the items that belong to that person.

Reordering the Rows of a Table

In some tables the order in which the rows appear is important. For example, when you define a realm, the first realm definition that matches a user's request is executed. You change the order by dragging a row up or down in the table.



In this example, the realm definition at the bottom of the table is being moved higher in the order. The red bar indicates where the dragged row will be dropped if you release the mouse button.

Import and Export

Some tables have import and export functionality. Clicking the *Export* button exports the contents of the table as a tab-delimited text file and the *Import* button allows you to import a file in that format.

Chapter 5

Adding Admin Users

After you get your web site up and running, you will want to add your name to the list of persons who are authorized to administer *Kerio WebSTAR 5*. If other people will also be doing administrative work on the server, their names should also be entered.

If it is appropriate, you can give some users full admin privileges and others only host admin privileges.


You do this work using the *Admin Client* application.

5.1 Entering New Admin Users

If you are not already running the *Admin Client* application, establish a connection with *Admin Server* by following the steps described earlier in the section 4.3.

1. Highlight the User Access item in the Admin Server topic.
The Admin Users area shows only the default user, "Admin."
2. Click the New button to add a new user.
A blank row in the Admin Users table appears.
3. Enter your user name and password either in the new row or in the two entry areas below the table.
4. Use the Admin Level pop-up menu to assign yourself Full Admin access privileges.
This allows you to configure both the server-wide and host-specific *Kerio WebSTAR 5* settings.
5. (Optional) If you want to give other users Admin access, repeat these steps.
A completed Admin Users table with four new users is shown below. One new user is a Full Admin and the other three are Host Admins. In the next section, you will specify the Settings Groups that they are permitted to administer.

Admin Server Users



User Name	Level
Admin	Full Admin
Diane	Full Admin
John	Host Admin
Jane	Host Admin

User Name: Password:

Admin Level:

5.2 Limiting Admin Client Access with the Admin Server Allow/Deny Table

In addition to the user name and password system described here, you can also restrict administrative access by setting up the *Allow/Deny* table. An *Allow/Deny* table restricts access to specified host names or IP addresses of individual machines.

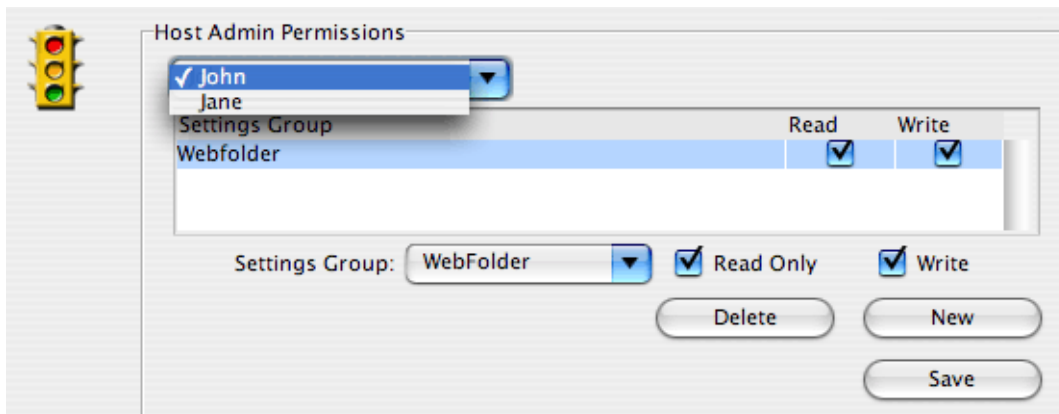
With the *Allow/Deny* table, you can block admin access to your web server from someone on the outside who has stolen a valid user name and password. All you need to do is tell *Kerio WebSTAR 5* which machines are valid Admin machines. All other attempts to access the web server are automatically blocked.

You use the *Allow/Deny* panel in the *Admin Server* group to set up such a system. Please refer to the *Technical Reference* for more information.

5.3 Assigning Permissions to Host Administrators

Of course, every full administrator can access any settings group. If you have created any host admins, you also need to grant access privileges to each host admin. Otherwise, *Kerio WebSTAR* wouldn't know which web virtual hosts a host admin has access rights to.

If you haven't created any web virtual hosts yet, you can postpone this task until you take care of that detail.



When you assign a person host admin privileges, his/her name automatically appears in the *Host Admin Permissions* pop-up menu at the bottom of the *Admin User Access* screen. In the table on the left, two host admin users have been added. Their names appear in the pop-up menu shown here.

To assign them permissions, you select each such host admin from the *Host Admin Permissions* pop-up menu and then assign read only or both read and write permissions, as appropriate.

1. In the *Host Admin Permissions* area, choose a *Host Admin User* from the pop-up menu above the table.

2. Click *New* in the *Host Admin Permissions* area.

A new row is added to the *Host Admin Permissions* table. Each row is for a different settings group.

3. Choose a settings group from the *Settings Group* pop-up menu below the table and click the *Read Only* or *Write* checkboxes, as appropriate.

By default, only read access is allowed. This enables a host admin to view settings but not create, modify, or delete them.

4. Repeat steps 2 and 3 for each settings group that this host admin has access rights to.
5. (Optional) If there are more host admin users, repeat this process for each host admin user.

Chapter 6

Creating Web Virtual Hosts

In *Kerio WebSTAR 5*, you organize your sites by creating one folder per web virtual host. Ordinarily, you place the folders in the *WebServer* folder. After you organize the documents in this fashion, you can tell *Admin Server* about them. There are two basic tasks:

- Tell *Admin Server* which folders are the root folders for your web virtual hosts and enter any necessary routing information.
- (Optional) Establish host admin access privileges for others.

You would need to do the second task only if you plan to delegate any administrative responsibilities to others. If you are going to administer all the web virtual hosts yourself, you only need to give yourself full admin privileges.

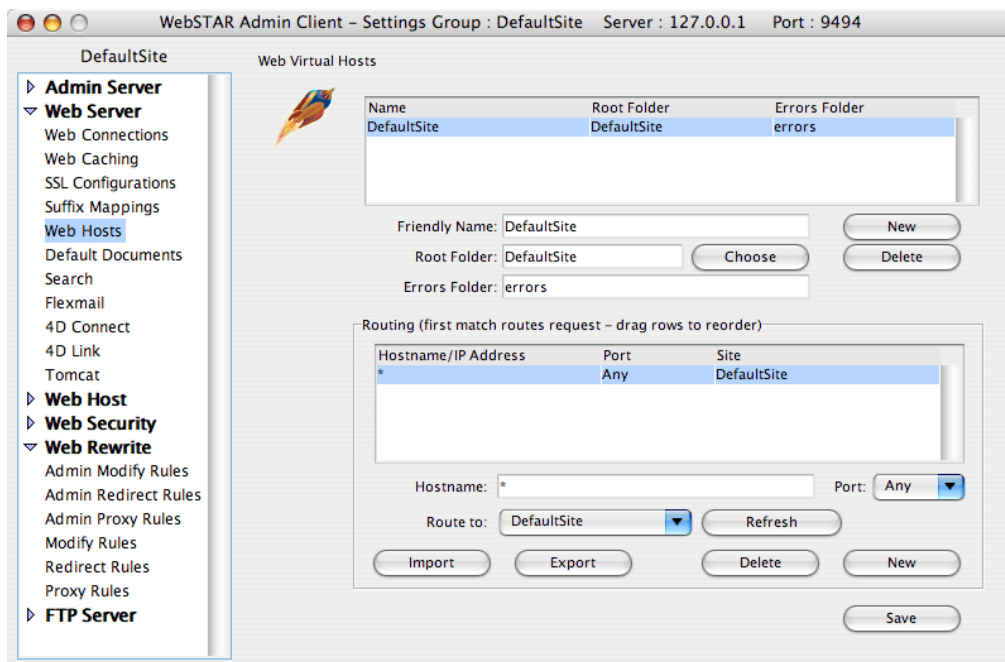
6.1 Entering and Configuring Virtual Hosts

A default virtual host folder, *DefaultSite*, has been placed in the *WebServer* folder by the installer. If you want to rename this site or add additional sites, you need to use the *Web Hosts* panel.

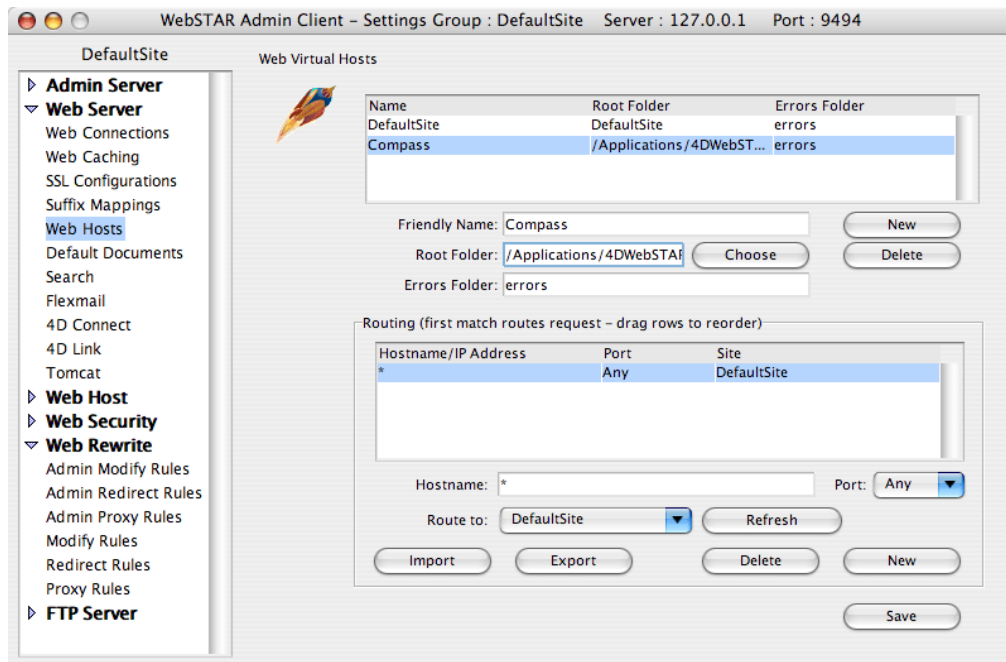
If you are going to use the server to serve more than one site, you can create new folders in the *WebServer* folder and move the relevant documents into those folders. Be sure to log into your Mac OS X system as the special *webstar* user while you are working with web host files.

If you create administrators with host admin privileges, return to the *User Access* panel in the *Admin Server* topic to grant them the appropriate permissions after creating the new web virtual hosts.

1. In the *Admin Client* application, click the *Web Hosts* item in the *Web Server* group.
Use the *Web Virtual Hosts* list at the top to enter information about the each virtual host folder that you have created.



- The *Friendly Name* is the name of the web virtual host that appears in the *Settings Groups* dialog when you log in to the *Admin Server* application.
 - The *Root Folder* is the relative path from the web server to the root folder for the web virtual host (i.e., the folder where all the documents making up the site are stored). Click the *Choose* button to locate the folder via a *Select Folder* dialog box.
 - The *Errors Folder* is the relative path from the *Root Folder* to the folder containing the error messages. You should put the *Errors* folder inside the *Root* folder. If you do so, you can simply enter the name of the *Errors* folder here.
2. To edit the default host, double-click in the text to be edited in either the text in the table or the entry areas below the table.
 3. To add a new web virtual host, click the *New* button below the *Virtual Hosts* table. A new row in the *Web Virtual Hosts* table appears. Default values are provided. You can enter or edit text directly into each field in the line or enter information into the entry areas below the table. If you are entering directly into the table, press the Tab key to move to the next field.
 4. Repeat these steps for each web virtual host you want to create. A *Web Virtual Hosts* panel with a new web virtual host looks like this:



6.2 Routing Requests to your Server Machine

If you are serving several web sites simultaneously, you probably need to route incoming requests to different virtual hosts. This is done using the *Routing Table* that appears below the *Virtual Hosts* table on this panel.

By default, all incoming requests are directed to the default web virtual host. If you serve your web site using the default host, you do not need to change this — except if you change the *Friendly name* of *DefaultSite*, the entry in the *Routing Table* should match.

The *Routing Table* allows you to direct requests by hostname/IP address or port to a specific hosts. If needed, enter a new line in the table for each distinct hostname or IP address.

Chapter 7

Web Security

The term web security refers to the ability to control access to the material on your web sites.

With *Kerio WebSTAR 5*, you can control access by requiring the browser to supply a valid user name and password. You can also control access by creating an *Allow/Deny* table that restricts access by hostname or IP address. Moreover, you can set default permissions for authorized users (e.g., read only, modify, list, and so forth).

In *Kerio WebSTAR 5*, web security is based on the concept of a realm. A realm is usually a folder or file within a web virtual host's root folder. The realm is actually defined by a string that is contained within a request. A request that contains the string that defines the realm is intercepted by the security system and the requesting browser's credentials are challenged.

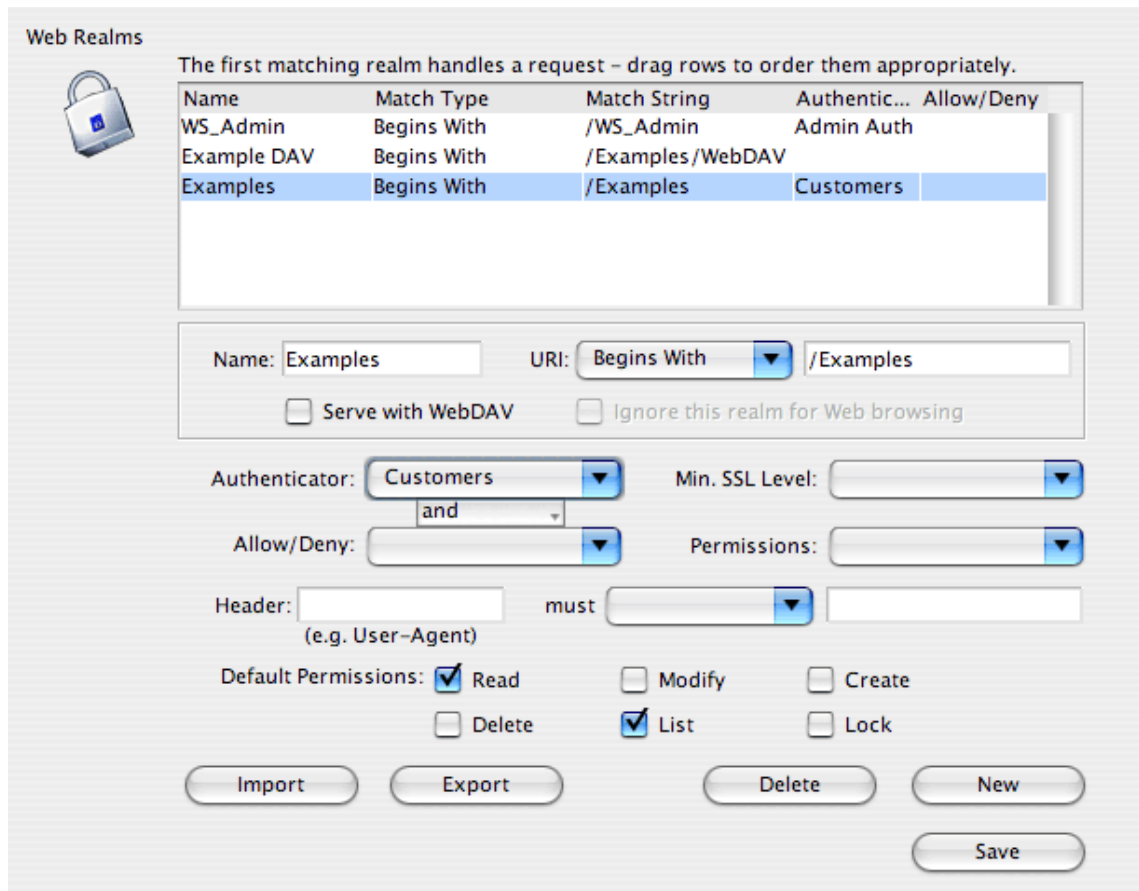
7.1 Overview

The panels in the *Web Security* topic work together to provide a sophisticated and flexible web security system. Most likely, it provides more flexibility than you will ever need.

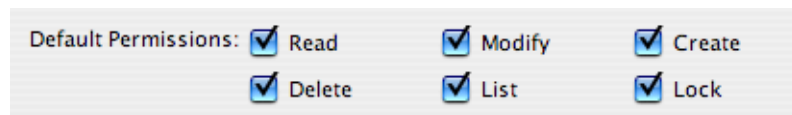
You use the *Web Realms* panel to define the string that defines each realm.

The *Web Realms* table on the *Web Realms* panel is the list of realms that pertain to this host (remember, web security is specified separately for each host).

For each realm:



- You can link an authenticator. An authenticator is one or more lists of authorized user names and passwords. The user names and passwords are entered in the *Built-in User Lists* panel and an authenticator (one or two user lists) is defined in the *Authentication* panel. When a browser attempts to access the realm, a *User Name/Password* dialog box is automatically displayed.
- You can also link an *Allow/Deny* table. It contains a list of domains or IP addresses that are either permitted or not permitted access.
- You specify *Default Permissions* which apply to all authorized individuals (i.e., listed on the authenticator and/or are using permitted domains/IP addresses).



- Optionally, you can link a *Permission* table when you want to specify different permissions for people on the authenticator. Usually, default permissions are sufficient.

Realms, User Lists, Allow/ Deny Tables, and Permissions

Although it might appear complicated at first, *Kerio WebSTAR 5's* implementation of web security makes it very flexible and powerful.

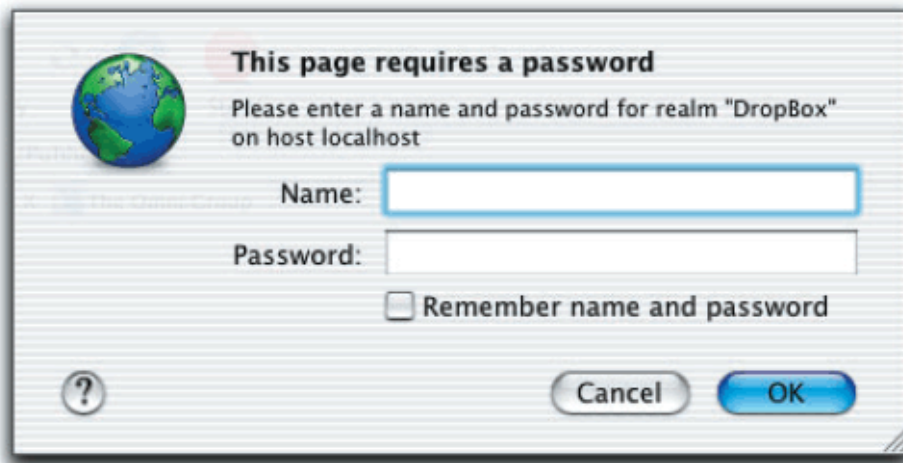
By separating *User Lists* and *Allow/Deny* tables from realms, *Kerio WebSTAR 5* makes these lists and tables reusable.

A user can be on several user lists and, thus, different groups can be granted access to different realms. And, since permissions (e.g., *List*, *Modify*, etc.) are separate from user lists, a person can have different permissions for different realms.

When you specify a realm, you link lists of users and/or an *Allow/Deny* table to the realm. This means that you first define the users who have access to the realm (or list of eligible computers) separately.

Setting up a User List

With the *User Lists* panel in the *Web Security* topic, you can set up any number of lists and enter the user names and passwords for each authorized user.



When you use this form of security, the user is confronted with a dialog box that requests a valid name and password whenever access to a protected realm is attempted.

To add a new user list:

1. Click the *New List* button.
A new row appears in the *Built-In User Lists* table.
2. Type the new list name directly into the table.
3. Click *Save* in the *Built-in User Lists* area to save the list.

When you save the list name, it is added to the pop-up menu in the *User List Configuration* area.

To add users to a user list:

1. Choose the name of the list from the *User List Configuration* pop-up menu.
2. Click *New* in the *User list configuration* area.
A new enterable area appears in the *User List Configuration* table.
3. Enter the *User Name* and *Password* either into directly into the table or in the two entry areas below the table.

User List Configuration

✓ Admin List
Customers

User Name	Password
john
jane
diane
paul

User Name: john Password:

Import Export Delete New

4. Repeat this process for each user.
5. Click *Save* to save your changes to the user lists.

7.2 Using a List as an Authenticator

Once you have created a user list, you need to indicate that you wish to use the list as an authenticator. An authenticator is the object that challenges a browser's access rights to a realm.

Using an authenticator as the object that is linked to a realm allows you to use more than one list. Even if you don't need this feature, you still need to define an authenticator and link it to your user list.

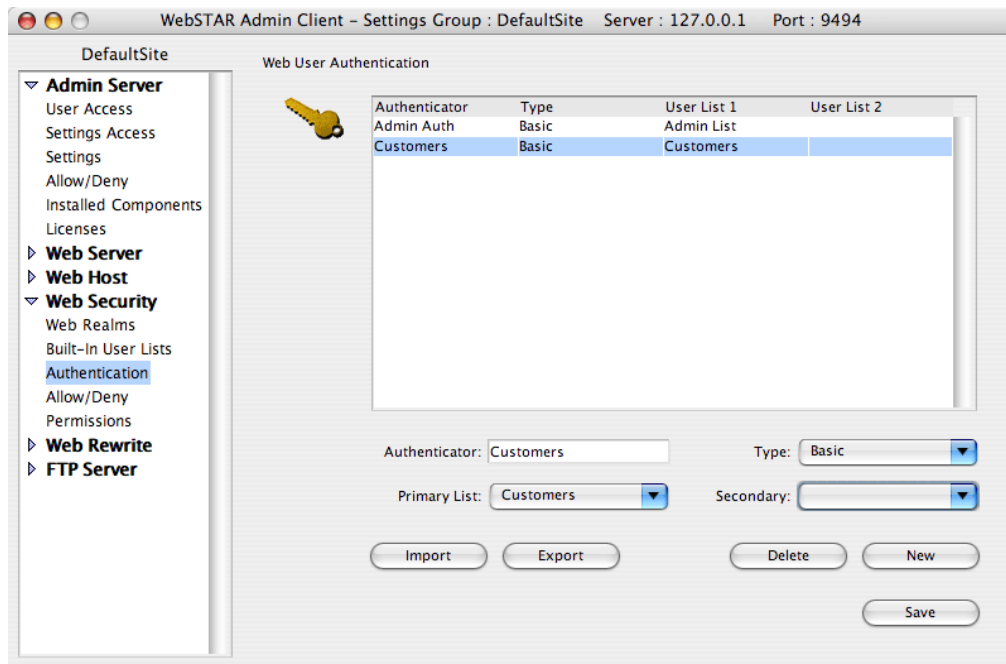
Creating a Realm Authenticator

The *Authentication* panel allows you to define up to two user lists as an authenticator. Later, using the *Web Realms* panel, you link the authenticator — not the user lists themselves — to the realm definition.

To create a *User List Authenticator*:

1. Click the *User Authentication* item in the *Web Security* topic.
2. Click *New* to create a new item in the *Web User Authentication* table.
A new blank row appears in the table.
3. Enter the name of the *Authenticator* directly into the table or into the *Authenticator* entry area below the table.
4. Choose a user list from the *Primary User list* pop-up menu.
5. (Optional) Choose another list from the *Secondary List* pop-up.
6. (Optional) Repeat the process to create additional authenticators.
7. Click *Save* to save the authenticator.

Here is an *Authentication* panel with one user-defined authenticator, *Customers*.



Linking an Allow/Deny table to a Realm

This *Allow/Deny* table specifies that only three machines will be allowed access to a realm. To use this table, it must be linked to a realm.

Allow/Deny Table Name

Web Folder

New Table

Delete

Save

Allow/Deny Table Configuration

Web Folder

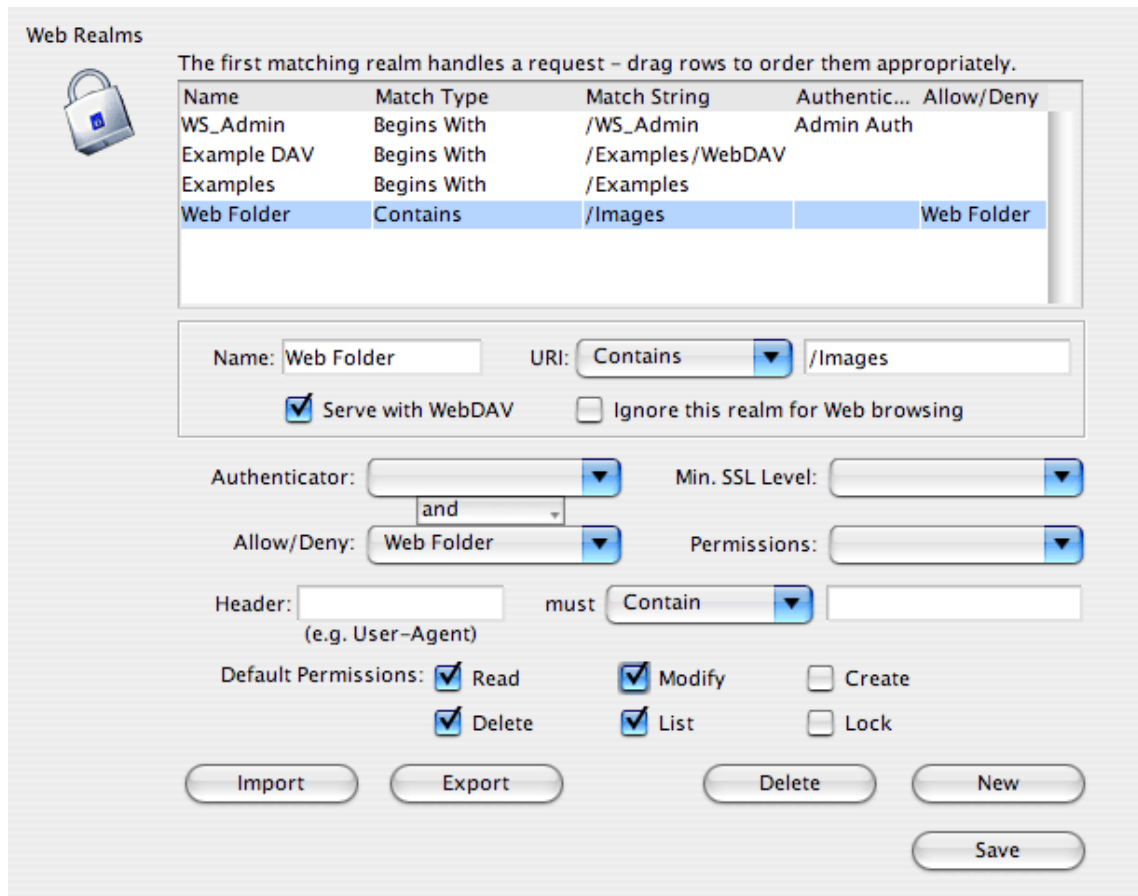
Allow/Deny	Hostname/IP Address
Allow	192.168.44.169
Allow	192.168.44.155
Allow	192.168.1.1

Allow/Deny: Allow

Address: 192.168.1.1

Import Export Delete New

In the screen below, the *Web Folder Allow/Deny* table is linked to a realm:



Using an Allow/Deny Table to Restrict Access

You can also limit access to realms by entering a list of authorized or unauthorized IP addresses or host names. For example, you can use an *Allow/Deny* table to allow in browsers using computers within your company and outside contractors, but keep everyone else out.

You do this by setting up an *Allow/Deny* table using the *Allow/Deny* panel in the *Web Security* topic. An *Allow* entry means that requests for data in the realm will be accepted if they come from a computer with a matching domain name, host name, or IP address. A *Deny* entry means that all browser requests for data in the realm the *Allow/Deny* table is linked to will be rejected if they come from a computer with the domain name, host name, or IP address.

If an unauthorized browser attempts to access the protected realm, the Access Forbidden error (the 403.html file in that host's *Errors* folder) is served.

To set up an *Allow/Deny* table:

1. Click the *Allow/Deny* item in the *Web Security* topic.
2. Click *New Table* and enter the name of the *Allow/Deny* table.
3. Click *Save* to save the table name.
When you save the table name, it is added to the *Allow/Deny Table* configuration pop-up menu.
4. Choose the new table from this pop-up menu.
5. Click *New* to add an entry to the table.
6. Choose either *Allow* or *Deny* from the *Allow/Deny* pop-up menu below the table and enter a hostname or IP address in the Address area.
7. (Optional) Repeat steps 5 and 6 for each hostname/IP address to be added.
8. (Optional) Repeat steps 2 through 6 to create additional *Allow/Deny* tables.
9. Click *Save* to save the *Allow/Deny* table.

When you define a realm, you can link one *Allow/Deny* table to the realm.

7.3 Setting up a Realm

After you have set up the desired authentication and permissions objects, you can proceed to define a realm. The realm consists of:

- The *Realm definition* — the string that is found in the request which indicates that the security system must intercept the request and challenge the requestor's credentials.
- An *Authenticator* and/or *Allow/Deny* table. The authenticator presents a *User Name and Password* dialog box and requires that the browser enter valid credentials before *Kerio WebSTAR 5* serves the requested page. The *Allow/Deny* table checks to see that the request has come from an authorized computer. Either or both can be used.
- *Default Permissions*, which specify the access rights granted to eligible browsers.

Creating the Realm Definition

Your first task is to specify the string in the request that defines the realm.

To define the realm:

1. Click the *Web Realms* item in the *Web Security* topic.
2. Click the *New* button to create a new realm.
3. Enter the realm name in either the new row in the *Web Realms* table of the entry area below the table.
4. Use the URI pop-up menu to select the search criterion.
Your choices are *Contains*, *Begins with*, *Ends with*, or *Matches Regular Expression*. The latter allows you to use standard regular expressions to define the search string.
5. Enter the string to search for in the *Match String* column or entry area.

In this example, a public folder has been added to the root folder of *DefaultSite*.

When a request that begins with */Public* is received, the user is asked to supply a user name and password. Only the users on the *Customers* authenticator are accepted. The *Default Permissions* enable them to read, list, modify, and create items.

Web Realms

The first matching realm handles a request – drag rows to order them appropriately.

Name	Match Type	Match String	Authentic...	Allow/Deny
WS_Admin	Begins With	/WS_Admin	Admin Auth	
Example DAV	Begins With	/Examples/WebDAV		
Examples	Begins With	/Examples		
DropBox	Begins With	/Public	Customers	

Name: URI:

Serve with WebDAV Ignore this realm for Web browsing

Authenticator: Min. SSL Level:

and

Allow/Deny: Permissions:

Header: must
(e.g. User-Agent)

Default Permissions: Read Modify Create
 Delete List Lock

Permissions Lists

If you need to grant different levels of access to people within an authenticator, you can create a *Permissions List* and use it instead of *Default Permissions*.

Although you can create a one permissions list for each user list (consisting, for example, of all the people on each user list), there is no requirement for you to do so. A permissions list is a logically separate object from a user list. For example, you can only add the user names of people for whom the *Default Permissions* are not appropriate.

A permissions list can also mix people from several user lists.

If a person should have different levels of access to different realms, then you can create several permissions lists in which the person has different levels of access on each list. You then link the different permissions lists to the different realms.

In other words, you use the *Permissions* panel only when you need to “fine tune” access rights.

Linking an Authenticator or Allow/Deny table to the Realm

To protect a realm, all you need to do is specify an *Authenticator* and/or an *Allow/Deny* table and set default permissions.

1. Highlight a realm definition in the *Web Realms* table.
2. Choose an authenticator from the *Authenticator* pop-up menu and/or an Allow/Deny table from the *Allow/Deny* pop-up menu.
3. Use the *Default Permissions* checkboxes to set permissions for all eligible browsers.

In this example, the contents of the *Examples* folder will be displayed only to browsers who can supply a valid user name and password. Those user names and passwords can be found on the user lists that are linked to the *Customers* authenticator. An *Allow/Deny* table could also be linked to the realm definition but it is not necessary.

The first matching realm handles a request – drag rows to order them appropriately.

Name	Match Type	Match String	Authentic...	Allow/Deny
WS_Admin	Begins With	/WS_Admin	Admin Auth	
Example DAV	Begins With	/Examples/WebDAV		
Examples	Begins With	/Examples	Customers	

Name: URI:

Serve with WebDAV Ignore this realm for Web browsing

Authenticator: Min. SSL Level:

and

Allow/Deny: Permissions:

Header: must

(e.g. User-Agent)

Default Permissions: Read Modify Create
 Delete List Lock

In this example, the *Default Permissions* show that users can read and list the files but cannot modify or delete them, nor can they create files or lock files.

Chapter 8

Sharing Files with WebDAV

WebDAV (Web Distributed Authoring and Versioning) is a new protocol that extends the http protocol to provide file sharing over the internet. WebDAV allows geographically separated people to work together by sharing files via the internet.

A WebDAV client application or WebDAV aware operating system provides access to a *WebDAV* folder. The contents of the shared folder appear either as a mounted volume on the desktop or in a new window.

Kerio WebSTAR 5's implementation of WebDAV provides all the security features that are offered in standard http browsing. This makes it the most secure and convenient way to share files over the Internet.

8.1 Setting up WebDAV Service

To set up WebDAV service, you need to create a web virtual host that references a folder to be published on the web via WebDAV. Typically, a folder within a host's Root folder is used. After you've created this folder, the process is very similar to creating an ordinary realm. The realm is the shared folder.

You define the shared folder as a realm and use a user list or an Allow/Deny table to limit access to the realm. Using *Default Permissions* on the *Web Realms* panel, you can restrict access rights to the shared folder.

To publish a folder on the web using WebDAV:

1. Create a folder within your *WebServer* folder that you wish to share over the internet and place the files you want to share in the folder.

The shared folder can be a folder within a virtual host.

2. Click the *Web Realms* item in the *Web Security* topic and create a realm that corresponds to the shared folder.
3. Click the *Serve with WebDAV* checkbox.
4. Choose the authenticator and/or Allow/Deny table that you want to use to restrict access to the shared folder and set *Default Permissions* for the shared folder.

Web Realms

The first matching realm handles a request – drag rows to order them appropriately.

Name	Match Type	Match String	Authentic...	Allow/Deny
WS_Admin	Begins With	/WS_Admin	Admin Auth	
Example DAV	Begins With	/Examples/WebDAV		
Public Folder	Begins With	/Examples/Public	Customers	

Name: URI:

Serve with WebDAV Ignore this realm for Web browsing

Authenticator: Min. SSL Level:

and

Allow/Deny: Permissions:

Header: must

(e.g. User-Agent)

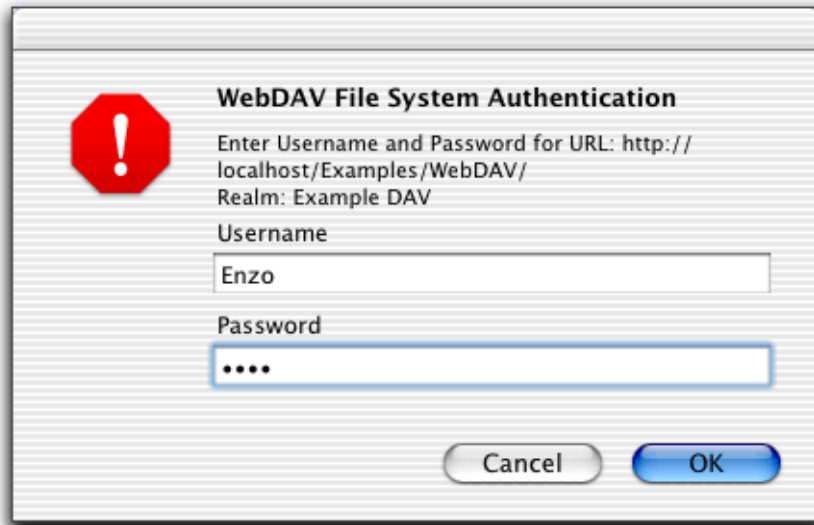
Default Permissions: Read Modify Create
 Delete List Lock

In this example, the shared folder in the virtual host's folder is named *Public*. Only the persons associated with the *Customers* authenticator can access the items in the folder. *Default Permissions* grant them read and list privileges.

8.2 Accessing the Web Folder using the Internet

A folder published using WebDAV can be accessed on Macintosh OS classic, Mac OS X, and Windows computers.

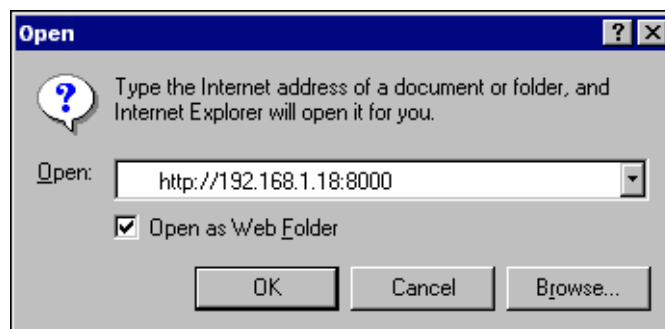
- On Mac OS X, support for WebDAV is built right into the *Finder*. Choose the *Go . Connect to Server* menu item and enter the URL for the shared folder. In a few moments, an *Authentication* dialog box will appear. Enter a valid user name and password. If authorized, the folder will appear as a mounted volume on your desktop. A separate application such as *Goliath* can also be used under Mac OS X.



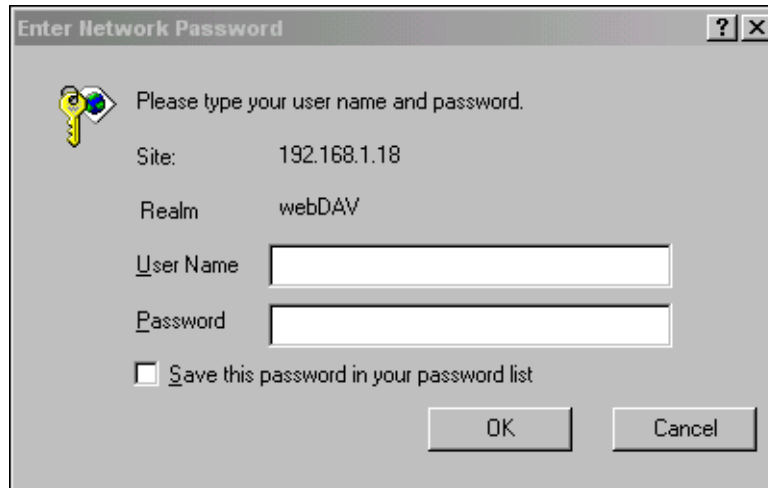
- On Mac classic, use a WebDAV client application such as *Goliath*. Enter the URL as well as a valid user name and password in the dialog box. If authorized, the contents of the folder will be listed in a new window.



- On Windows, use *MS Internet Explorer* (or another Office application) as the client. For example, from *Internet Explorer*, choose *File* → *Open* and enter the URL of the shared folder. Be sure to check the *Open as Web Folder* checkbox.

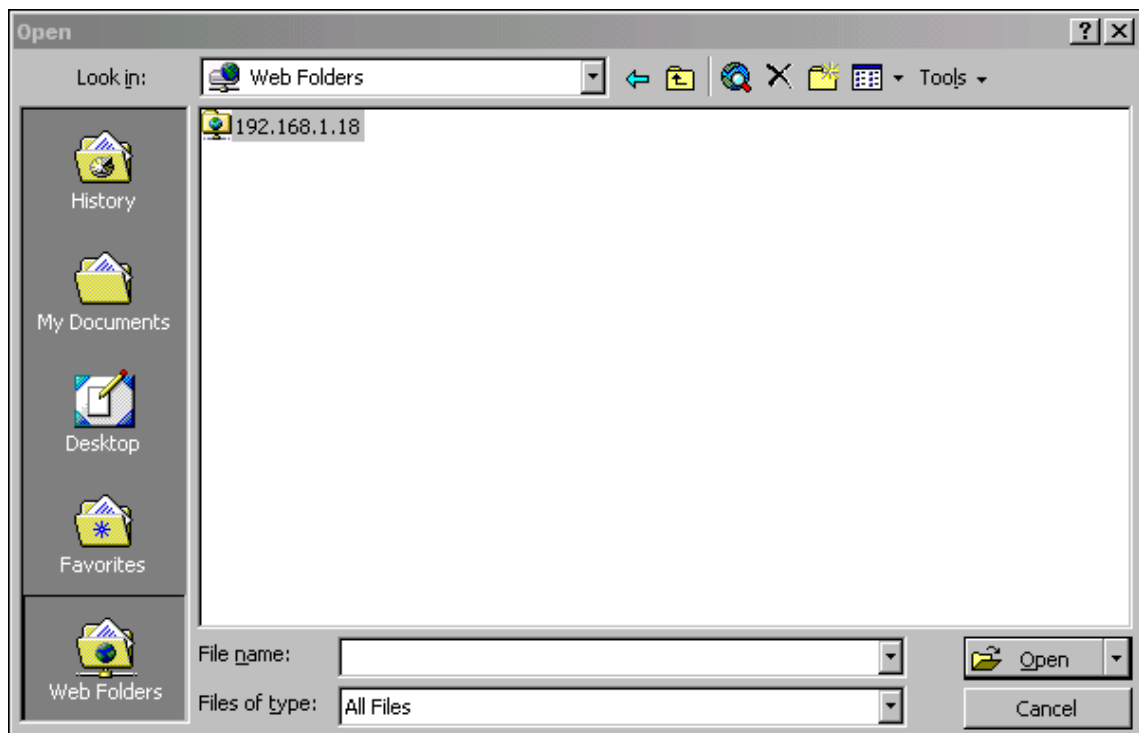


When the *Authentication* dialog box appears, enter a valid user name and password. As with *Goliath*, the contents of the shared folder appear in a new window.



WebDAV Client Applications

Windows: All Microsoft Office applications support WebDAV. In a *Microsoft Office Open* dialog box, you can click the *WebFolder* icon to view a list of WebDAV folders. Select the desired folder, click *Open*, and enter your user name and password to open the file directly into the application.



Macintosh Classic: Macintosh users who are not using Mac OS X can download *Goliath* from <http://www.webdav.org/goliath>.