WEBAPPZ

bizDAV

User Guide

Version 3.1.1 – May 2005

For Java 1.4.2+ with WebObjects 5.2+ on Windows, Mac OS X, Solaris, and Linux

bizDAV User Guide (V3.1.1)

Introduction

Welcome to bizDAV

bizDAV is a powerful security and business management application to assist companies with maintaining their users, administering user access privileges to various e-business applications, configuring office-wide password and firewall settings, managing licences, and performing workplace audits when required. With bizDAV, system administration is easily handled, and the application's self-service options allow users to customize their personal application, password, and firewall settings, and to access their own audit information.

Who Can Use bizDAV?

bizDAV is ideally suited for companies that host or rent e-business applications, or those that manage large user groups.

For companies providing e-business applications, bizDAV can assist with client license administration for these applications. It can also be used for setting up the users for each application and assigning their individual access privileges.

For companies using several different web-based software applications, within their business, bizDAV can be used to manage the company's users and their access privileges to these various applications.

How Does bizDAV Work?

bizDAV is a flexible server application made accessible to the end user through an internet browser. No additional software is required. bizDAV can, however, work in conjunction with other J2EE applications.

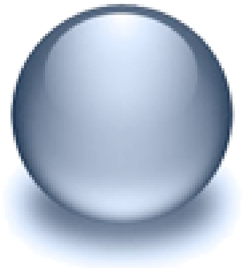
bizDAV provides online help to assist you with questions you may have when using the application. This online help consists of two components: bizDAV help and Application-Wide General help. bizDAV help provides information about all the features and functions of the application. To access this help component, click ? .

The Application-Wide General help component provides information about all the general function buttons and icons, which repeatedly appear in the search, list, or edit windows of the bizDAV application. To access this help component, click ?, which is usually found at the bottom right corner of a search, list, or edit window.

In the near future, the bizDAV help documentation will be formatted as "page-specific" help with integrated search functionality, as is already present in WEBAPPZ's 1TRACKER.

Glossary

Application - This refers to the bizDAV application, or any application managed by bizDAV; e.g. WEBAPPZ's 1TRACKER application.



Ball - Balls are used to restore/activate a Person's password in the Forgotten Password Restoration or Password Activation process. A ball consists of a ball id and ball password. In the aforementioned processes, the rolling of the ball represents an email being sent to you, regarding the ball password.

Business - This refers to the company's account or business registered to use bizDAV, or any subscribed to bizDAV-managed application.

Client Authentication Rules - A set of rules used to determine if a Business' or Person's firewall settings are configured to allow or deny various internet IP Addresses.

Function - An activity that is connected to an application and can be performed by one or more Persons. Persons are connected to functions through security groups.

HQ Person - This is the Person who functions as the system administrator for a specific business or office location of a business, and can administer office-wide attributes and permissions belonging to that business office.

IP Range - This refers to one or more computers whose client browsers are allowed or denied access to the applications managed by bizDAV. This could represent an entire office or an employee's/associate's remote location.

License - This is a fee or non-fee bearing "certificate" that details the maximum number of permitted users, price, start and end date, and assigned license key, for a business.

Person - A user (employee/associate) entered into bizDAV, and who may or may not be assigned to one or more security groups, having defined access functions within a business.

Security Group (Group) - Groups connect one or more Persons to one or more functions. Groups can be seen as ways to bundle Persons or functions together into one common group.

Home Page

bizDAV Home Page Icons

The bizDAV home page consists of a main icon bar at the top of the page. This bar displays a set of icons (functions) available to you, according to your access privileges. Rolling over any icon, here, will display the roll-over text describing the function associated with the icon.

The mini icon bar, located above the main bar, displays four icons. These icons are always present and correspond to general functions. Rolling over any icon, here, will display the roll-over text describing the function associated with the icon.

bizDAV User Access Levels

Depending upon how bizDAV is used within your company, different user access levels will apply.

If your company uses bizDAV to manage other e-business applications, the following user types will apply: Super User, Headquarter (HQ) Person, and General Users.

If your company uses bizDAV to manage a large pool of users and their access privileges to various e-business applications, the following user types will apply: HQ Person, and General Users.

If your company is using bizDAV in combination with the 1TRACKER application, the following user types will apply: HQ Person, and General Users.

bizDAV User Types	
Super User:	This Person has top level system administration privileges and can administer system wide attributes and permissions for all Persons and businesses managed by bizDAV.
HQ Person:	This Person functions as the system administrator for a specific business or office location of a business, and can administer office-wide attributes and permissions for all Persons belonging to that business office.
General User (Person):	This Person has no administrative functions for the business, but has access to several self-service options in bizDAV, which allow him to set personal security, password, and firewall management settings, and to customize his bizDAV-managed applications, according to various preset templates.

bizDAV Entities Table

The table appearing on the home page displays a list of entities (functions), with corresponding text explaining each of the entities available to you.

Generally, the HQ Person, of a business, will have the following entities appear in the table: My Business, My Profile, Persons, Groups, Audit Info, and Licenses.

For bizDAV General Users, the following entities will appear in the table: My Profile, and Audit Info.

Clicking on any of the links within the table is the same as clicking on the corresponding icons from the main icon bar.

Getting Started with bizDAV

HQ PERSON

This Person must enter the company's employees and associates (Persons) into the system and provide each of them with an initial user id and password for login access to bizDAV and any bizDAV-managed applications, made available to them. The HQ Person must also assign the Persons to groups, in order to provide those Persons with access to functions of a particular application. The HQ Person will also enter the business information of the company and configure office-wide password policies and firewall management settings. For EXT users, the HQ Person is the Person who clicked the 'Sign Up' button to register the business for the EXT services.

The general order of steps when first entering employees or associates into the system is as follows:

1. My Business - Enter general business information and configure office-wide password policies and firewall management rules.
2. Persons - Add Persons in or associated to your business, who require login access to bizDAV or any bizDAV-managed applications, made available to them.
3. Groups - Assign Persons to groups, according to different access level requirements for those persons. Create new groups, as needed to meet company needs.

GENERAL USERS (PERSONS)

Once they have been entered into the system and given an initial user id and password, by their company's designated HQ Person, these Persons will have access to bizDAV, and any bizDAV-managed applications, made available to them.

My Business (HQ Persons Only)

Please Note: This section applies to HQ Persons/HQ Security Group Persons only.

General

Here is where you can view and edit your company's general business information, and view the main Headquarters (HQ) Person for your business. This is also where you can establish firewall management rules for your business, and set up business-wide password management rules.

The page displays a detail-edit table, divided into three columns: the first column displays the name associated with each field; the second column displays the detailed information for each field; and the third column displays a brief explanation of each field, to assist you with entering details into this section. For fields requiring a more detailed explanation, it is provided under the associated heading. All fields marked by an asterisk are required.

Fields associated with a detail-edit icon indicate that information for those fields can be entered/edited by clicking the detail-edit icon. This action causes the detail-edit page, for that particular field, to appear.Details for these fields can only be entered once all other required information has been correctly entered and saved to the database. For Firewall Management and Password Management, you can also access these pages by clicking on the corresponding icons from the main icon bar or the Home page links.

HQ Person

This Person has full administrative privileges for your business. The Person assigned, here, has access to the following in your business:

> General business information,
> Firewall management,
> Password management,
> License management,
> Person management,
> Group mangement, and
> Business audit information.

Your business always has one HQ Person directly connected to the business. This is the designation assigned to the Person who signs up for the bizDAV application or an application managed by bizDAV. This Person is identified in the "HQ Person" field of the "Edit your Business" page.

You can, however, have one or more Persons from your business assigned to the "HQ Persons" group. These other Persons will have access to all the functions associated with the "HQ Person" group. These Persons are identified in the "Persons" field of the "Edit a Security Group" page. The "HQ Persons" group is especially useful for assigning administrative privileges to more than one Person in your business.

To enter/edit details for the designated "HQ Person":

1. Click the detail-edit icon ✎ in the "HQ Person" field. The "Edit Person Information" page will appear.
2. Enter/edit the details for the "HQ Person".
3. Click **Save**.

NOTES:

(1) All address, phone, and fax information for the HQ Person should be that of the HQ Person's business.

(2) All fields marked by an asterisk ★ are required.

Business’ Firewall Settings (HQ Persons Only)

Please Note: This section applies to HQ Persons/HQ Security Group Persons only.

bizDAV enables you to configure business-wide firewall settings. Here, you can specify which IP ranges are allowed to have access to bizDAV and any applications it manages. This feature helps to ensure that only authorized Persons have access to your business information.

To access the firewall managment page, where you can establish/change your business' firewall management settings:

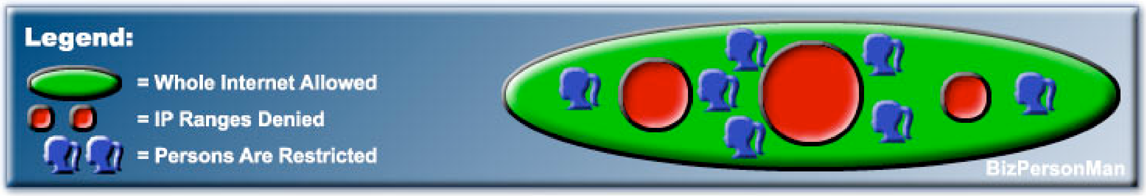
> Click the firewall management icon from the main icon bar, *or* click the firewall management link from the Home page, *or* click the firewall management link from the "My Business" detail-edit page.
>
> The "Firewall Management for your Business" page will appear, consisting of the following three sections:
>
> (1) **Firewall management defaults**
>
> These are the firewall management default settings that will be applied to your entire business. There are two settings to select here: the default rule and the Person's access. A brief explanation for each field setting is provided in the comments section. These defaults can be changed anytime, but it should be noted that changing these settings could affect Person access for your business. Any changes to the business' firewall management settings will be effective at the Person's next application login session.
>
> The default firewall management settings are as follows: Default Rule = Allow All, and Person's Access = Restrict.
>
> (2) **IP Range list**
>
> This section displays any IP Ranges which are allowed/denied access based upon the default rule selected. This feature is especially useful if you have employees or associates who work remotely. By specifying their IP Range, you can allow them to widen their internet access, so that they have access to the applications required by them. By default, no instances of IP Range are specified.

To add an IP Range:

1. Click the **Add** button. A new window will appear on the page, with the heading, "IP Range Properties". Here, you can enter the new IP Range details.
2. Click **Save** to capture the details of your new IP Range.

NOTE: Fields marked by an asterisk ★ are required.

(3) **Firewall Management Legend**



The legend displays the various elements that are represented in the associated firewall schematic. The schematic serves to visually demonstrate your selected firewall management settings. By default, the schematic demonstrates the "Allow All" & "Restrict" default settings.

To view a schematic for a different set of rules:

Select your new firewall settings and click **Save**. The schematic will display your most recently selected firewall settings.

Password Management (HQ Persons Only)

Please Note: This section applies to HQ Persons/HQ Security Group Persons only.

In bizDAV, you can set up password management rules, such as minimum total password length, minimum numberic/alphabetic characters, and password expiration that will apply to your entire business. The details column, next to the "Password Management" field, displays the password management rules specified for your business.

To access the password management page, where you can change the password management rules for your business:

1. Click the password management icon from the main icon bar, *or* click the password management link from the Home page, *or* click the password management link on the "My Business" detail-edit page. The "Password Management for all Persons in your Business" page will appear.
2. Enter the details for your business' password management.
3. Click **Save** to capture these details.

NOTE: Fields marked by an asterisk ★ are required.

You are free to change password management rules as often as you like. Your most recently selected settings will be applied to new Persons only. For existing Persons, the new settings will be applied at the Person's next required or self-service password change. If you wish that all your business' Persons abide by these new rules immediately, you must set the password expiry date to yesterday's date, which will result in a forced password change for all Persons.

License Management (HQ Persons Only)

Please Note: This section applies to HQ Persons/HQ Security Group Persons only.

bizDAV allows you to view the licenses applicable to your business. Specifically, you can view details such as maximum number of permitted users, assigned users, paid amount, start and end dates, license key, and license validity for each license.

To view the license/s available to your business:

> Click the license management icon from the main icon bar, *or* click the License link on the Home page.
>
> The license/s for your business will be displayed in the list. You can use the **Next** and **Previous** keys, if shown, to sort through the records, or you can opt to use the **Search** feature to narrow down your search for a specific license.

A license is defined by a date range, and once this date range expires, a new license must be obtained by your business to continue using the bizDAV application, or applications managed by bizDAV.

Application Service Provision Clients – e.g. 1TRACKER EXT

To purchase a new license:

> Click the **Buy** button and follow the instructions provided on screen. Please have a credit card ready.

1TRACKER BOX Clients

To purchase a new license:

1. Click the **Add** button. The "Edit a License" page will appear.
2. Please enter all fields on the page.
3. Click **Save**.

NOTE: An encrypted license key is required in order to create your new license. This license key will be provided to you by an authorized WEBAPPZ sales representative. Enter this key into the "license key" field.

Maintain Persons (HQ Persons Only)

Please Note: This section applies to HQ Persons/HQ Security Group Persons only.

In bizDAV, your employees and/or associates must first be entered into the system as "Persons". Once they have been added as Persons, you can assign them to groups, which define the functions/access privileges they will have, for the applications made available to them. There is no limit to the number of Persons you can add to your business; however, there is a limitation to how Persons are assigned to groups. Such assignments do not allow more Persons to have access to the applications than the number of users permitted in the license. In order for your users to have access to bizDAV or any bizDAV-managed applications, such as 1TRACKER, you must purchase a license for the expected number of users who will require access to these applications.

To view the list of Persons for your business:

> Click on the "Maintain Persons" icon from the main icon bar *or* click the Persons link on the Home page.
>
> The "Person (User) Management for your Business" page will appear, displaying a search and list window.
>
> *Search Window* - You can use one or more of the search categories, available in the search window, to look for specific Persons. By default, each of the search categories is minimized. To maximize a search category, click the maximize button ▶.
>
> To perform a search:
>
> 1. Click on the search categories you wish to use, and enter the details for those categories.
> 2. Click **Search**. The results will be displayed in the list window. If no matches to your search were found, the following message will appear, "Sorry, no instances of Person were found".
>
> *List Window* - The list window displays all of the Persons currently entered into the bizDAV system for your business. You can use the **Previous** and **Next** keys, if shown, to sort through the records, or you can opt to change the number of records in your list. The list also provides information on the Person's account status, groups he/she belongs to, last login date and other details, as obtained from the information entered for the Person's personal properties.

To view the personal details of any Person in your list:

Click the detail-edit icon ✎ associated with that Person record. The "Edit Person Information" page will appear displaying any details available for that Person.

To add a Person to your business:

1. Click the **Add** button, located at the bottom of the list window. The "Edit Person Information" page will appear, consisting of several personal information categories.
2. Select the information category you would like to enter details for, and click the associated min/max button to maximize the category window, if it is currently minimized. Enter the Person's details into the corresponding fields. Continue to enter the details into the various categories until you are done.
3. Click **Save**. If all information has been entered correctly, the newly entered Person will appear in your list of Persons. If any information was entered incorrectly, one or more error messages will appear.

NOTES:

(1) A brief explanation of each category field appears in the last column. Any further explanation necessary for a field will appear, below, under the associated category heading.

(2) All fields marked by an asterisk ★ are required.

(3) Information will be saved only if there are no errors.

Person Attributes

PERSON LOGIN PROPERTIES

Inactivity Timeout - The inactivity timeout is a security feature that allows you to specify the number of minutes of inactivity after which you will be automatically logged out of your current session. Since Persons may have different security requirements, this feature provides you the option to set this parameter to meet your individual needs. For example, a Person who spends most of her time using her desktop, could set the inactivity timeout ~25-30 minutes, as there is little risk that an unauthorized user would access her desktop. A Person who is in and out of his office, however, may wish to set his inactivity timeout to ~2-5 minutes, as there is greater potential here that an unauthorized user could access information he was working with. As the business' HQ Person, you can establish the initial session timeout for individual Persons. The timeout specified, here, can be changed by the Person, herself, when she logs into bizDAV, and clicks on "My Profile - My User Info".

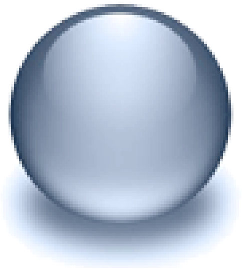
Account Suspension (Optional) - A Person's account may have a specified account suspension date. The account suspension date refers to the date that the Person will no longer be able to log in to bizDAV or any bizDAV-managed applications.

To restore a suspended account:

1. Enter a new account suspension date, manually, or automatically, using the **Pick** button. You can also delete the account suspension date and leave the field empty; i.e. no account suspension date.
2. Over-write the number of bad logins to zero.
3. Click **Save**.

Personal Firewall Management - The firewall management rules specified, here, will apply to that particular Person and specifically, at his next login session. These firewall settings will determine whether or not the user can specify wider or narrower internet access, under "My Personal Firewall Management", when he logs in to the bizDAV application.

FORGOTTEN PASSWORD RESTORATION PROPERTIES (OPTIONAL)



This property is optional; however, all fields for this category are required to create Balls, which are used in the forgotten password restoration process. The information, here, can be entered by the HQ Person or by the individual Person. If you are an HQ Person, this property will display one extra field, "Bad Ball Attempts". If a Person fails to generate a ball in the forgotten password restoration process, after five attempts, she will be required to contact her HQ Person, who will be able to clear the number of bad ball attempts, to zero. The Person will then be able to try the forgotten password restoration process, again.

Maintain Groups (HQ Persons Only)

Please Note: This section applies to HQ Persons/HQ Security Group Persons only.

bizDAV is pre-configured with security groups, known as factory presets. These factory presets have been created, as a convenience, to provide your business with some common security groups to assign your Persons to. Security groups determine the functions your business' Persons can perform. Each security group is associated with one or more functions. There is no limit to the number of security groups a Person can belong to; however, the license purchased by the business must support the number of actual users. For Persons who belong to multiple security groups, one or more functions may be repeated.

As an HQ Person, you can create security groups, specific to your business. You may wish to create security groups with different functions than the factory presets, or you may wish to create entirely new groups. There is no limit to the number of groups you can create.

To view the list of security groups (Groups) available to your business:

> Click the "Group Management" icon from the main icon bar *or* click on the "Groups" link on the Home page. The "Group Management for your Business" page will appear, displaying a search and list window.
>
> *Search Window* - You can use one or more of the search criteria, available in the search window, to look for a specific security group. By default, the search window is minimized. To maximize the search window, click the maximize button ▶.
>
> To perform a search:
>
> > Enter the details into the corresponding fields, for the search criteria you wish to use and click **Search**. The results of your search will be displayed in the list window. If no matches to your search were found, the following message will appear, "Sorry, no instances of SGroup were found".
>
> *List Window* - The list window displays all of the Groups currently entered into the system for your business. You can use the **Previous** and **Next** buttons, if shown, to sort through the records, or you can opt to change the number of records displayed in your list. The list also provides information regarding the functions associated with each group, and whether or not the group is a factory preset.

To add a Security Group to your business:

1. Click the **Add** button, located at the bottom of the list window. The "Edit a Group for your Business" page will appear. Here, is where you enter the details for your new security group, including name, associated functions, and Persons assigned to this group.
2. Enter the details for your new security group, and click **Save**. If all information has been entered correctly, the new security group will appear in your list of security groups. If any information was entered incorrectly, one or more error messages will appear. You can easily identify any security groups created by your business in your list of security groups. These groups will have "No" in the Factory Preset column.

NOTES:

(1) A brief explanation of each field appears in the last column. Any futher explanation for a field, will appear, below, under the associated heading.

(2) All fields marked by an asterisk ★ are required.

(3) Any field displaying the detail-edit icon ✎ can only be entered, once all other required details have been entered and saved to the database. These details can be entered at a later time, if desired.

To assign functions to your new Security Group:

1. Click the detail-edit icon ✎ next to your new security group. The "Edit a Group for your Business", page will appear.
2. Click the "Functions" detail-edit icon ✎. The "Select Functions" page will appear, displaying a search and list window.

   Search Window - You can use the search feature to look for a specific function. Simply enter the details for your search into the corresponding field/s and click **Search**. The results of your search will be displayed in the list window. If no matches to your search were found, the following message will appear, "Sorry, no instances of SFunction were found".

   List Window - The list window displays all of the functions available to your business. You can use the **Next** and **Previous** buttons to sort through the records, or you can opt to change the number of records displayed in your list.

3. Select the function/s you wish to assign to your new security group, by clicking inside the corresponding box/es.
4. Click **Save Selected** to save your selection to the database. Your new security group now has your selected functions associated with it.

To assign Persons to a Security Group:

1. Click the detail-edit icon next to the security group you wish to add Persons to. The "Edit a Group for your Business" page will appear.
2. Click the "Persons" detail-edit icon. The "Select Persons" page will appear, displaying a search and list window.

   Search Window - You can use the search feature to look for a specific Person. Simply enter the details for your search into the corresponding field/s and click **Search**. The results of your search will be displayed in the list window. If no matches to your search were found, the following message will appear, "Sorry, no instances of Person were found".

   List Window - The list window displays all of the Persons currently entered into the system for your business. You can use the **Next** and **Previous** buttons to sort through the records, or you can opt to change the number of records displayed in your list.

3. Select the Person/s you wish to assign to your security group, by clicking the corresponding box/es.
4. Click **Save Selected** to save your selection to the database. You have now assigned your selected Persons to that security group.

My Profile (All Persons)

bizDAV allows you to edit your personal profile information and customize your application/system settings, which will be applied to any bizDAV-managed applications made available to you. You can select preferred date and number formats, specify your choice of application layout, change your password information, set personal firewall management rules, and update your user information. Changes to your settings can be made anytime, as often as desired , and will be effective at your next login session.

To enter/edit details for your personal profile:

1. Click the My Profile icon, from the main icon bar, *or* click the My Profile link on the Home page. The "My Profile Settings" page will appear, with the following options:

Date Formats - Here, you can choose your preferred date and time formats. Only one selection is allowed for each category.

Number Formats - Here, you can select your preferred currency and decimal formats. Only one selection is allowed for each category.

Languages - Here, you can choose your preferred language for your applications. Please note that only English is currently supported.

Layouts - Here, you can select a layout style from a set of available templates. The layout style you choose will be applied to all your applications managed by bizDAV, including all your PDF printouts.

**My User Info* - Here, you can enter/edit your personal user information, which consists of the following details:

- Your Login Properties, such as password, inactivity timeout, and personal firewall management,
- Your Name Properties,
- Your Forgotten Password Restoration Properties (You must enter all fields, here, if you wish to use the "Forgot" feature.),
- Your Role Properties, where you can specify your workplace job titles,
- Your Work Telecommunication Properties,
- Your Home Telecommunication Properties, and
- Your Work Address Properties.

*A further explanation of this option is provided, under the heading, "My User Info".

Detailed Settings (Optional) - Here, you can view a more technical summary of the settings you selected for Dates, Numbers, Languages, and Layouts. You can also make changes, here, to any of your detailed settings, individually.

2. Click on the option you would like to enter/edit details for, by clicking on the corresponding button or link. The associated page for that option will appear.
3. Enter/edit the details for that option and click **Save**. You will return to the main "My Profile" page.

My User Info

LOGIN PROPERTIES

Password - you can change your password anytime, as often as desired, using the self-serve password change feature.

To change your password:

1. Click the "My Profile" icon from the main icon bar, *or* the "My Profile" link on the Home page.
2. Click the "My User Info" options.
3. Click inside the "Password" field of the category, "Your Login Properties", and enter your new password.
4. Re-type your new password into the "Re-type Password" field.
5. Click **Save**.

Inactivity Timeout - The inactivity timeout is a security feature that allows you to specify the number of minutes of inactivity after which you will be automatically logged out of your current session. Since users may have different security requirements, this feature provides you the option to set this parameter according to your individual needs. For example, a Person who spends most of her time using her desktop, could set the inactivity timeout to ~25-30 minutes, as there is little risk that an unauthorized user would access her desktop. A Person who is in and out of his office, however, may wish to set his inactivity timeout to ~2-5 minutes, as there is greater potential here that an unauthorized user could access information he was working with. If your HQ Person specified your initial inactivity timeout, you are free to change it here. You can change the value for this setting, at any time, and as often as desired.

To change your inactivity timeout setting:

1. Click the "My Profile" icon from the main icon bar, *or* click the "My Profile" link on the Home page.
2. Click the "My User Info" option.
3. Click inside the "Inactivity Timeout" field of the category, "Your Login Properties", and enter a value here, between 2 and 30 minutes.
4. Click **Save**.

Personal Firewall Management

This feature allows you to define your personal client authentication rules, in accordance with the firewall management rules specified for your business. The client authentication rules generally represent a combination of two sets of rules - those configured office-wide by your business' HQ Person, and those specified by you, for your individual firewall settings.

You can view your current firewall management settings under the "Your Login Properties" category, of the "Edit Person Information" page, or under "Client Authentication Rules", of the "My Personal Firewall Management" page.

You can configure your firewall settings to meet individual security and access needs, which may change depending upon your work environment and location. For example, if you are working remotely, you may need to add/deny IP ranges, beyond those specified in your business. You can change your personal firewall management settings anytime.

To ensure that your firewall settings are configured properly, bizDAV provides you the convenience to test your firewall with a specific IP address. This test is instantaneous and will give you a "Pass" or "Fail" result. If a tested IP address fails, this means that from that location, a client browser would not be able to log in, with your user id and password. If the test results are not to your satisfaction, then you must re-configure your firewall settings, or you may have to contact your business' HQ Person, if the former does not resolve the problem.

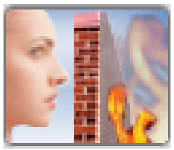
NOTES:

(1) You are strongly recommended to test your firewall prior to logging out of the bizDAV application, to ensure that your settings will allow you to log back into the bizDAV application, at your next login. If you fail to do so, you may not be able to log in to the application from your current IP address.

(2) All fields marked by an asterisk ★ are required.

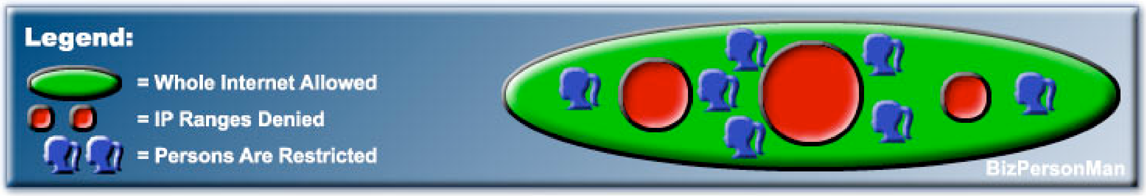
For information on editing your personal firewall management settings, and for an explanation of the seven firewall (IP address) authentication rules, please refer to the help section - My Personal Firewall Settings.

My Personal Firewall Settings (All Persons)



bizDAV allows you to manage your personal firewall settings. This feature enables Persons of a business to configure their firewall settings to meet their individual security and access needs. The HQ Person establishes office-wide firewall management rules for the business. The Persons of the business can then establish their personal client authentication rules, in accordance with the firewall management rules specified for the business.

You can view a graphic on the top of the "My Personal Firewall Management" page, which depicts the default firewall management rules, established for your business. The associated legend indicates what each element of the graphic represents.



Below the graphic, you will see the following table headings:

Use Default IP Ranges from your business: Any IP ranges specified by your business' HQ Person will be listed here. To apply your business' IP ranges to your firewall settings, ensure that the checkbox is checked. If the checkbox remains unchecked, any of your business' IP ranges listed here will not be applied to your firewall settings.

IP Ranges for (Your Name): Here, you can view/add IP ranges specific to you, only. The rule (Allow/Deny) applied to these IP ranges, will be displayed in the table.

To add an IP range to your list:

1. Click the **Add** button. A detail-edit window will appear below the list table.
2. Enter the details for your new IP range into the corresponding fields.
3. Click **Save**.

NOTE: All fields marked by an asterisk ★ are required.

Client Authentication Rules: Here, you can view the client authentication rules that are used to determine if your firewall settings are configured properly for a particular IP address. These rules represent a combination of the firewall settings established by your business' HQ Person, and those settings specified by you. The seven (7) possible client authentication rules are described below.

RULE 1 - © WEBAPPZ Web Application Firewall Technology	
Validation:	1: Browser/Client (B/C) Address may not be part of Business' Denied IP Ranges. 2: B/C Address may not be part of Personal Denied IP Ranges. 3: B/C Address must be part of Business' Allowed IP Ranges. Ignored: Personal Allowed IP Ranges.
Explanation:	Your business has established that the entire internet is unaccessible to its Persons, except for any allowed IP ranges, specified. Your business does not allow you to widen your internet access, beyond the allowed IP ranges it has specified. You have selected to apply the default IP ranges established by your business. You may deny any IP range from your business' allowed IP ranges by adding that IP range to your personal list.
Example:	Your business has denied access to the entire internet, except from Locations A, B, and C. Due to security issues with Location A, you decide to deny IP ranges from that location; therefore, only IP ranges from Locations B and C will be able to log in with your user id.

RULE 2 - © WEBAPPZ Web Application Firewall Technology	
Validation:	1: Browser/Client (B/C) Address may not be part of Business' Denied IP Ranges. 2: B/C Address may not be part of Personal Denied IP Ranges. 3: B/C Address must be part of Business' Allowed IP Ranges. 4: B/C Address must be part of Personal Allowed IP Ranges.
Explanation:	Your business has established that the entire internet is unaccessible to its Persons, except for any allowed IP ranges, specified. Your business does not allow you to widen your internet access, beyond the allowed IP ranges it has specified. You have selected *not* to apply the default IP ranges established by your business; therefore, no IP ranges currently have access. You may allow any IP range from your business' allowed IP ranges, by adding that IP range to your personal list.
Example:	Your business has denied access to the entire internet, except from Locations A, B, and C. You will be working from Location B, therefore, you must permit access for IP ranges from that location. From Locations A and C, you will still be unable to log in with your user id, since you ignored the business' default IP ranges.

RULE 3 - © WEBAPPZ Web Application Firewall Technology	
Validation:	1: Browser/Client (B/C) Address may not be part of Business' Denied IP Ranges. 2: B/C Address may not be part of Personal Denied IP Ranges. 3: B/C Address must be part of Business' Allowed IP Ranges OR Personal Allowed IP Ranges.
Explanation:	Your business has established that the entire internet is unaccessible to its Persons, except for any allowed IP ranges, specified. Your business allows you to widen your internet access, beyond the allowed IP ranges it has specified. You have selected to apply the default IP ranges established by your business. You may add IP ranges other than those specified by your business.
Example:	Your business has denied access to the entire internet, except from Locations A, B, and C. You are working from Location D; therefore, you must allow IP ranges from this location to give you the required access. From Locations A, B, and C, you will still be able to log in with your user id, since you applied the business' default IP ranges.

RULE 4 - © WEBAPPZ Web Application Firewall Technology	
Validation:	1: Browser/Client (B/C) Address may not be part of Personal Denied IP Ranges. 2: B/C Address must be part of Personal Allowed IP Ranges. Ignored: Business' Denied IP Ranges and Business' Allowed IP Ranges.
Explanation:	Your business has established that the entire internet is unaccessible to its Persons, except for any allowed IP ranges, specified. Your business allows you to widen your internet access, beyond the allowed IP ranges it has specified. You have selected *not* to apply the default IP ranges established by your business; therefore, you currently have no IP ranges with access. You may add IP ranges other than those specified by your business.
Example:	Your business has denied access to the entire internet, except from Locations A, B, and C. You are working from Location D; therefore, you must add the IP ranges from this location to give you the required access. From Locations A, B, and C you will no longer be able to log in with your user id, since you ignored the business' default IP ranges.

RULE 5 - © WEBAPPZ Web Application Firewall Technology	
Validation:	1: Browser/Client (B/C) Address may not be part of Business' Denied IP Ranges. 2: B/C Address may not be part of Personal Denied IP Ranges. Ignored: Business' Allowed IP Ranges and Personal Allowed IP Ranges.
Explanation:	Your business has established that the entire internet is accessible to its Persons, except for any disallowed IP ranges, specified. Your business does not allow you to widen your internet access. Since you are restricted, there is no choice, here, to apply/ignore the default IP ranges specified by the business. You may, however, deny more IP ranges, than those specified by your business.
Example:	Your business has allowed access to the entire internet, except from Locations A, B, and C. You wish to limit access from Location D also; therefore, you must add the IP ranges from this location to ensure denied access. From Locations A, B, C, and D, you will not be able to log in with your user id, since you are restricted.

RULE 6 - © WEBAPPZ Web Application Firewall Technology	
Validation:	1: Browser/Client (B/C) Address may not be part of Business' Denied IP Ranges. 2: B/C Address may not be part of Personal Denied IP Ranges. Ignored: Business' Allowed IP Ranges and Personal Allowed IP Ranges.
Explanation:	Your business has established that the entire internet is accessible to its Persons, except for any disallowed IP ranges, specified. Your business allows you to widen your internet access, beyond the disallowed IP ranges it has specified. You have selected to apply the default IP ranges established by your business; therefore, these IP ranges are not allowed by you, unless you add them back to your personal list.
Example:	Your business has allowed access to the entire internet, except from Locations A, B, and C. You will be working from Location B; therefore, you must add the IP ranges from this location to ensure you will have the access required. From Locations A and C, you will not be unable to log in with your user id, since you applied the business' default IP ranges.

RULE 7 - © WEBAPPZ Web Application Firewall Technology	
Validation:	1: Browser/Client (B/C) Address may not be part of Personal Denied IP Ranges. Ignored: Business' Denied IP Ranges, Business' Allowed IP Ranges, and Personal Allowed IP Ranges.
Explanation:	Your business has established that the entire internet is accessible to its Persons, except for any disallowed IP ranges, specified. Your business allows you to widen your internet access, beyond the disallowed IP ranges it has specified. You have selected *not* to apply the default IP ranges established by your business; therefore, only personally denied IP ranges will apply here. So, if your personal list is empty, you may log in from anywhere.
Example:	Your business has allowed access to the entire internet, except from Locations A, B, and C. Since you have selected to ignore any disallowed IP ranges for the business, you may select to deny any location/s. You choose to deny access from Locations A and D. Therefore, Locations B and C would still have access.

Test your firewall with any specific IP Address: Here, you can test any browser/client IP Address with your current firewall settings. The test will provide you with a PASS or FAIL result. If the entered IP passes, then, from that browser/client IP address, you will be able to log in with your user id. If the tested IP address fails, then you will not be able to log in with your user id from that location. You must then adjust your firewall settings to allow that IP Address, or you must contact your HQ Person to assist you with your firewall settings.

NOTE: The IP Address which appears here, by default, is your current browser/client IP.

To test a specific IP Address:

1. Enter the IP address into the corresponding field. Your IP address must consist of 12 digits. Use the Tab key to move through each cell.
2. Click the "test" button, which appears as an asterisk . This test is instantaneous and your result will be immediately displayed as PASS or FAIL.

Audit Info (All Persons)

bizDAV enables all Persons to access their personal audit information, and for HQ Persons to access audit information for all Persons in their business. The audit log provides information about when and what applications were used, who used the applications, what activities were performed, what entity the activities were performed on, and with what instance. For all other Persons, this information provides them with a record of all activities performed from their browser/client IP address. For HQ Persons, the information serves as an administrative tool to assist them with troubleshooting and/or maintaining accurate activity logs for their business.

ALL PERSONS

To view your personal audit log:

1. Click the "Audit Log" icon *or* click the "Audit Info" link, from the bizDAV Home page. The "View Audit Log Information: Search (1/3)" page will appear, consisting of several search categories, one or more of which you may use, depending upon your search. Entering information into more than one search category will narrow your search and reduce database fetching time.
2. Select your search categories and enter the information into the associated fields. To maximize a search category window, click the maximize button ▶ at the top left corner of that search window.
3. Click **Search**. The results of your search will be displayed on a new page, "View Audit Log Information: List (2/3)". Here, you can view a list of all the activities that match your search criteria. You can use the **Prev** and **Next** buttons, if shown, to scroll through the information.
4. Click the "Disp" icon to view the details for a specific record from the list. The page, "View Audit Log Information: Detail (3/3)", will appear, with detailed information for each entity captured by the audit log, specific to that record.

HQ PERSONS

As an HQ Person, you have the same search categories available to you as those mentioned for All Persons, except, that you have one additional category - Search by Person (user) information. This category allows you to view all recorded activity for each of the Persons in your business.

To view your business' audit log, please refer to the steps referenced under the heading, "Audit Info - All Persons".

NOTES:

(1) If your search is very open and a large date range has been specified, the resulting list may require a long response time to be generated.

(2) If needed, you can determine the client domain name and/or the server IP address associated with a particular IP address (record), by clicking "Resolve". We strongly advise, however, that this process is performed on lists of less than 50 records, only, as it may take a few seconds to resolve each IP address.

The Developer

bizDAV was developed by WEBAPPZ Systems, Inc., a Canadian-based software development company, specializing in the delivery of innovative, secure, web-based applications for the different needs of businesses today.

bizDAV is WEBAPPZ's solution to assist internet-integrated companies with security management issues related to web-based applications, used within their companies and the users of those applications.

With the internet becoming a regular part of doing business, most companies are interested in ways to ensure their business information is kept secure and their networks are protected from unauthorized access. bizDAV incorporates a number of security measures to address these concerns and more. Whether it be defining user access levels, managing passwords, issuing licenses, or ensuring the confidentiality of business and personal information, bizDAV offers the functionality, security, and quality that your business wants from an enterprise-class application. When it comes to security for your business, why settle for anything less?

Our team of developers is committed to delivering robust business applications that meet the reliability, flexibility, and scalability required by companies today. We want to ensure that, as a customer, you are not buying just another piece of software; but instead, are part of the internet age community of businesses enjoying the benefits and competitive advantages that the internet and WEBAPPZ have made possible.

At WEBAPPZ, we are always welcome to any comments or suggestions for improvements, regarding any of our products. You can send us your comments to info@webappz.com.

For more information about WEBAPPZ or its product line, please see www.webappz.com.