



Bizfon 7000
System Administration Guide
(For Release 5.2)



Table of Contents

- 1 Introduction 1**
 - 1.1 Who Should Read This Guide 1
 - 1.2 What this Guide Is and What It Is Not 1
- 2 Connecting to Web Administration 2**
- 3 Configuring a New Bizfon 7000 3**
- 4 Upgrading Server Software 4**
 - 4.1 Step 1: Copy Files to the Update Area 4
 - 4.1.1 Alternative 1: Download from the Web 4
 - 4.1.2 Alternative 2: Use the FTP Window 5
 - 4.2 Step 2: Activate the Update 6
- 5 Network Configuration 7**
 - 5.1 Network Mode: Standard Router 8
 - 5.2 Network Mode: LAN Host 9
 - 5.3 Network Mode: NAT/Firewall 10
 - 5.4 Network Mode: NAT/Firewall with DMZ 12
 - 5.5 Network Mode: NAT/Firewall with Stealth DMZ 13
 - 5.6 Example 1: Secure Firewall 13
 - 5.7 Example 2: Secure Firewall with Internal Email Server 14
- 6 Adding Handsets 15**
 - 6.1 SIP Phones 15
 - 6.1.1 Plug-and-Play 15
 - 6.1.2 Manual Add 15
 - 6.2 Analog Phones 16
 - 6.3 Testing Phones 17
- 7 SIP Proxy 18**
- 8 Configuring Bizfon IP2 Phones 21**
 - 8.1 Introduction 21
 - 8.2 Programmable Function Keys (PFK's) 24
 - 8.2.1 Station Mode Selection 25
 - 8.2.2 PFK Function Selections 26
 - 8.3 Phone Options 28
 - 8.3.1 Description of Options 30
 - 8.4 Configuration Templates 31
 - 8.4.1 Default Templates 32
 - 8.4.2 Viewing a Template's Configuration 32
 - 8.4.3 Creating a New Template 32
 - 8.4.4 Applying a Template to a Phone's Configuration 32
 - 8.4.5 Deleting a New Template 32
 - 8.4.6 Changing a Template's Configuration 32
- 9 Dialing Rules and Service Groups 33**
 - 9.1 Background Information 33
 - 9.1.1 Dialing Rules 33
 - 9.1.2 Home Area Code 33
 - 9.1.3 Service Groups 33
 - 9.1.4 Exceptions 33
 - 9.2 Configuring Service Groups 33
 - 9.3 Configuring Home Area Code and Dialing Rules 35
 - 9.3.1 Dialing Rules, Home Area Code, and Dial 9 Service Groups 35



System Administration Guide

9.3.2	Dial 8 + PIN Service Group.....	36
9.4	Interaction Between Service Groups and Handset Outside Line Restrictions.....	37
10	Unified Messaging.....	38
10.1	Access Mechanisms	38
10.1.1	Forwarding Messages.....	38
10.1.2	POP Client.....	38
10.2	Access Examples.....	39
10.2.1	Example 1.....	39
10.2.2	Example 2.....	39
10.2.3	Example 3.....	40
10.2.4	Example 4.....	40
11	Backing up and Restoring Data	41
11.1	How to Create a Backup	41
11.2	How to Restore Data.....	42
12	Remote IP Phone.....	45
12.1	General Network Configuration Requirements	45
12.2	Bizfon Server Behind 3 rd Party NAT Firewall	45
12.3	Remote Bizfon IP2 Phone	46
12.3.1	Configuration	46
12.3.2	Limitations	47
12.4	Remote Non-Bizfon IP2 Phone	48
13	Call Routing.....	49
13.1	Call Routing Concepts.....	49
13.1.1	Introduction.....	49
13.1.2	Connection Attempt	49
13.1.3	Finally Clause	49
13.1.4	Primary Route, On-Busy Route, and Call Route	49
13.1.5	CallerID Dependant Call Routes	50
13.1.6	Presence	50
13.1.7	User Extensions and System Extensions.....	50
13.1.8	Concept Summary	50
13.2	View and Change a Call Route	51
13.3	Changing a User's Presence Setting.....	54
13.3.1	Changing Presence Via an Bizfon IP2 Phone	54
13.3.2	Changing Presence Via Any Phone.....	54
13.3.3	Changing Presence Via the User Intranet Web Site.....	54
13.3.4	Changing Presence Via the Administrative Web Page.....	55
13.4	Outside Line Call Routing.....	55
13.5	Example Call Route Configurations.....	56
13.5.1	Example 1: Ring 1 Phone, Then Voicemail.....	56
13.5.2	Example 2: Ring 1 st Phone, Then ring 2 nd Phone, Then Voicemail.....	57
13.5.3	Example 3: CO Line Rings 2 Phones, Then ring 3 rd Phone, Then Voicemail.....	57
14	Key System Behavior.....	58
14.1	Example Configuration	58
15	Direct Inward Dialing (DID)	59
15.1	Create a DID Block	59
15.2	Configure a Call Routing Plan for the DID Block.....	60
15.3	Create the DID Lines.....	61
16	Web, FTP, and CIFS	63
16.1	Web Sites.....	63



System Administration Guide

16.1.1	Internal Administration Web Site.....	63
16.1.2	Internal System Info Web Site.....	63
16.1.3	Internal Custom System Web Site	63
16.1.4	Internal Custom User Web Site.....	64
16.1.5	External Custom Web Site.....	64
16.2	Internal FTP Site	64
16.3	External FTP Site.....	64
16.4	Internal CIFS.....	64
17	Call Queues	65
17.1	Configuring a Queue	65
17.1.1	Managing Custom Queue Message Content	67
17.2	Servicing a Queue with an Bizfon IP2 Phone	68
17.2.1	Configuring the Phone	68
17.2.2	Agent Phone Configuration Example	70
17.2.3	Logging in and out of the Queue.....	71
17.3	Servicing a Queue with a Non-Bizfon IP2 Phone.....	71
17.4	Configuring Calls To Route To the Queue.....	71
17.4.1	Example 1: Call Routing To Auto Attendant and Then Call Queue	72
17.4.2	Example 2: Call Routing Directly to Call Queue	72
17.4.3	Example 3: Call Routing To AA, Live Answer User Extension, and Then Call Queue	72



1 Introduction

1.1 Who Should Read This Guide

This guide is to be read by people who will be installing and maintaining the Bizfon 7000 server. The technical background of the administrator is assumed to be greater than that of the system's end users. This is not an end user document. The reader is expected to have a sufficient computer networking and basic telephony background.

1.2 What this Guide Is and What It Is Not

The Bizfon 7000 web administration interface is designed to be easy to navigate and use. It has built in descriptions, help, and tips on many of its pages. This manual is not a duplication of that information, but is to be used in concert with that. This manual is intended to describe only those features or administration mechanics that are more complex and difficult to understand. Therefore, not all the features or all the parameters of each feature are discussed here. Again, this guide discusses only those features and parameters that require additional explanation beyond what is on the web pages.

This manual is not a tutorial on basic computer networking or telephone systems. Other sources may need to be consulted to supply that information.



2 Connecting to Web Administration

The administrative interface to the Bizfon 7000 is accessed using a web browser. Assuming the network settings are set to their factory defaults, the steps to connect to this interface are:

1. Plug your PC into one of the server's LAN ports.
2. Set up the PC's network interface to obtain an IP address automatically (using DHCP).
3. Verify that the PC has an IP address on the 192.168.2.x network.
You may need to release and renew the PC's IP address to get an address from the server.
4. Open your browser and enter the URL of <http://192.168.2.254:8080>.
5. When the "Welcome to Bizfon" page appears, login using the default password of "admin".



3 Configuring a New Bizfon 7000

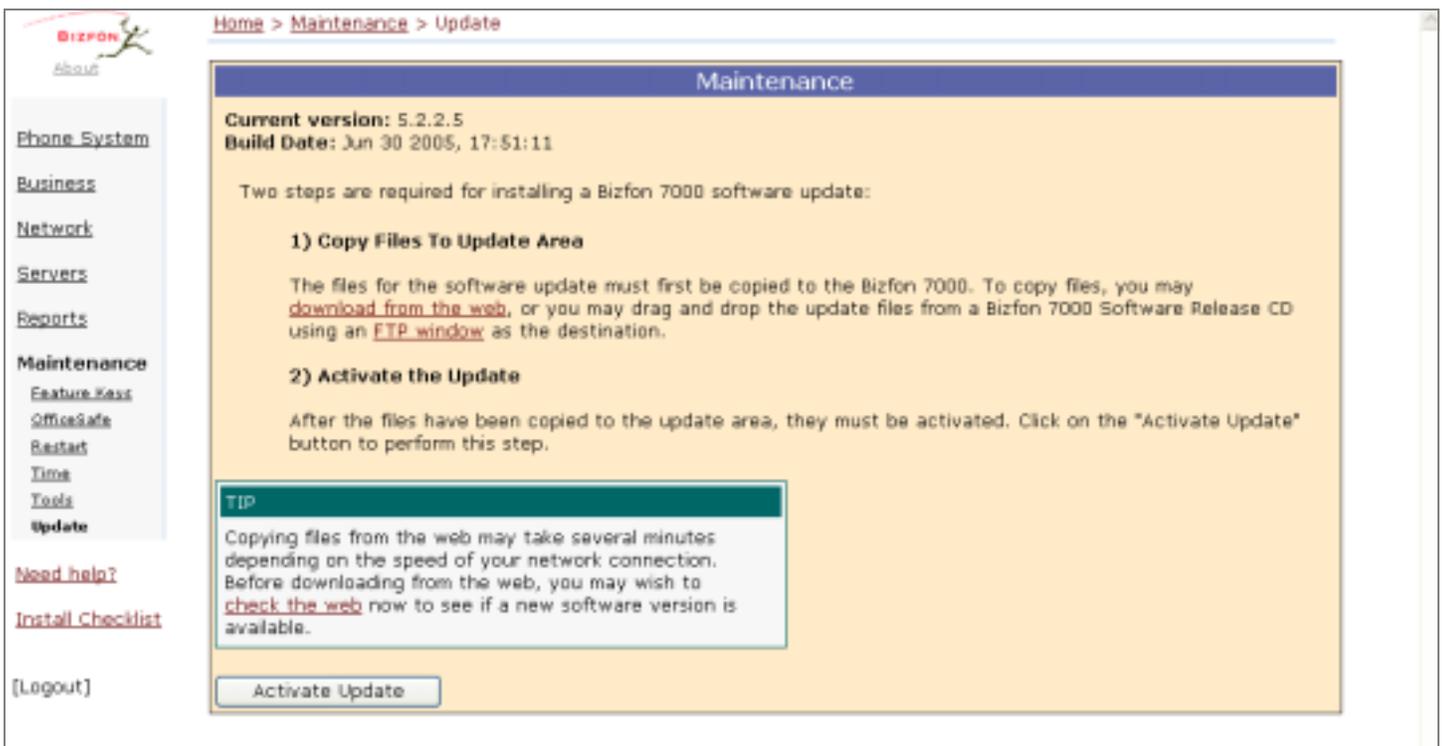
Login to the Bizfon 7000 web administration page. When the **Home** page appears, click on the **Install Checklist** link (on the left hand side) to bring up a new window containing steps necessary to set up a new system. Each brief step description is followed by a link to get to the appropriate administrative web page to execute the step. These steps are ordered to aid in a successful configuration. Most of the web pages to execute each step contain all the descriptions and help necessary to carry out the step. Use this guide to supplement the information on the web pages when necessary.

4 Upgrading Server Software

The software on the Bizfon 7000 server is upgradable. Before performing an upgrade, be aware that:

- It is highly recommended that you perform an OfficeSafe backup prior to performing the upgrade (see *Backing up and Restoring Data*).
- An upgrade will require a reboot of the server. So, the system should be idle (no phone or data users) when this is done.

To upgrade the software on the server, go to the **Maintenance / Update** web administration page. (In most cases the web administration pages can be viewed with various web browsers, but for this task it is recommended that you use the Microsoft Internet Explorer browser.) You will see a page like this:



As you can see, there are two steps involved: copying the files to the update area and activating the update.

4.1 Step 1: Copy Files to the Update Area

The copy step allows two alternatives: letting the sever download the software update files from the web or your copying update files that you already have to an FTP window. Let's look at each of these alternatives in more detail.

4.1.1 Alternative 1: Download from the Web

When you click on the **download from the web** link, the server makes a connection to a web site on the Internet that has the software and begins to download it to the server. Of course, if your server can't get to the Internet, this will fail. So, make sure that your Internet connectivity is working. Depending on the performance of your Internet connection, this will take awhile (as of this writing, the download is about 32M bytes). After the download is complete, the web browser will pop up a window like this:



You must continue with the Activate step to complete the software update.

If you do not get this dialog, do not activate the update. Your disk could get corrupted. Reboot the server and use alternative 2 described in the next section.

If this step doesn't seem to work, check the **Reports / System Events** page for any error information.

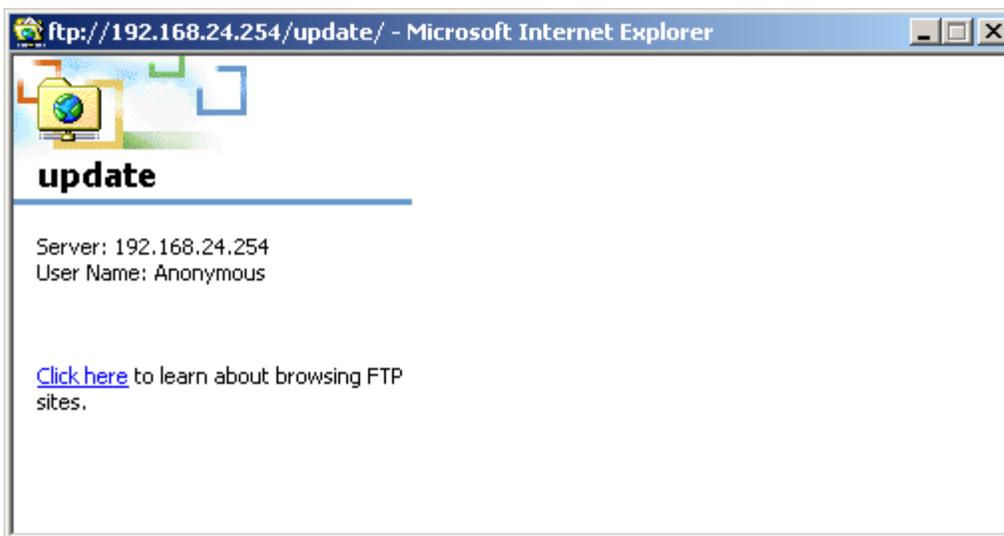
If the download took a long time to complete, your browser's connection to the server web administration may time out. If this happens, you will be asked to login again.

4.1.2 Alternative 2: Use the FTP Window

Instead of having the server download the software update files from the web, you may already have the files on a CD or your PC's hard drive. Ensure that you have these 6 files:

- installFiles.arc
- installFiles.ini
- newFlash.sre
- oisapp
- oisapp.sym
- upgrade.dat

Now you need to transfer them to the server. To do this, click on the **FTP window** link. A window similar to this will appear:



Using Windows Explorer, copy or drag the files from your PC (CD or hard drive) to this **update** window. This will cause the files to be transferred to the server.



After all the files have been copied, continue with the Activate step to complete the software update.

4.2 Step 2: Activate the Update

Once you have copied the software update files to the server, you are ready to tell it to update its software using those files. Just click the **Activate Update** button. This will cause the server to validate the files, install them, and reboot. The web administration will guide you as you wait for the update to be performed.



5 Network Configuration

The Bizfon server provides powerful and flexible network infrastructure capability. Much of this flexibility is configured by setting the **Network Mode** parameter on the **Network / Configuration** page. This page shows different parameter sets depending on the **Network Mode** setting. If the **Network Mode** is set to the factory default value of NAT/Firewall with DMZ, the page will be similar to that shown below.

The screenshot shows the Bizfon web interface for Network Configuration. The breadcrumb trail is Home > Network > Configuration. The main content area is titled 'Network' and contains a table with the following data:

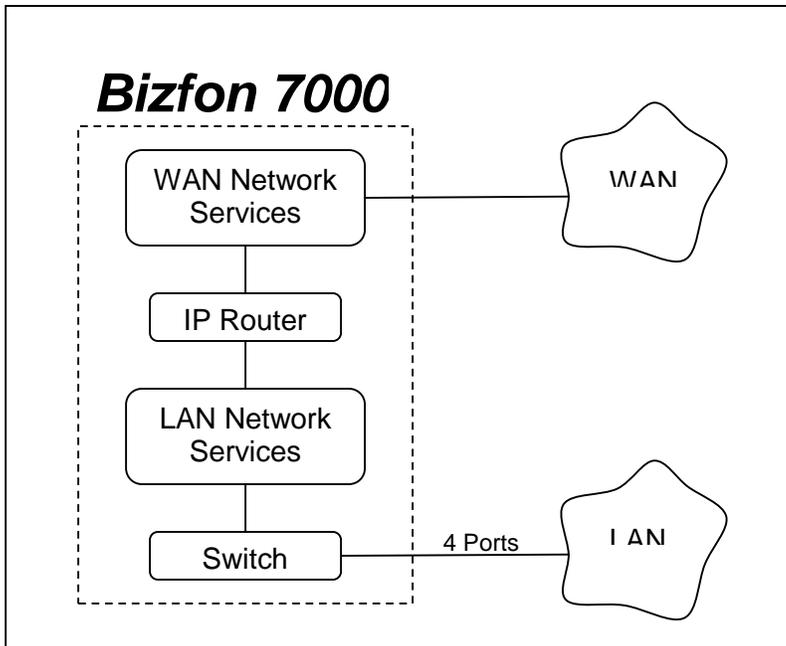
Configuration		
	Current Value	Action
Network Mode	NAT/Firewall with DMZ	Modify
LAN IP Address	192.168.2.254	
LAN Subnet Mask	255.255.255.0	
WAN Settings Method	Static	
WAN IP Address	192.168.1.1	
WAN IP Subnet Mask	255.255.255.0	
Gateway	192.168.1.254	
PPPoE Username		
PPPoE Service Name		
PPPoE MTU	1492	
LAN Addresses and Ports exposed through Firewall		
DNS (53,4069)	enabled	
FTP (20,21)	disabled	
HTTP (80)	enabled	
POP3 (110)	enabled	
PPTP (1723)	enabled	
Remote Bizfon 7000 Handsets (2088,8081)	enabled	
SIP (5060)	enabled	
SMTP (25)	enabled	
SNTP (4068)	enabled	
Host Name	MyHostName	
Domain Name (DNS)	MyHostName.MyDomainName.com	

The left sidebar contains navigation links: Phone System, Business, Network (with sub-links for Configuration, Static Routes, and VPN), Servers, Reports, Maintenance, Need help?, Install Checklist, and (Logout).

Each of the possible network mode values of this parameter are described below.

5.1 Network Mode: Standard Router

When the network mode is set to Standard Router, the logical network capability is as shown in the diagram below.

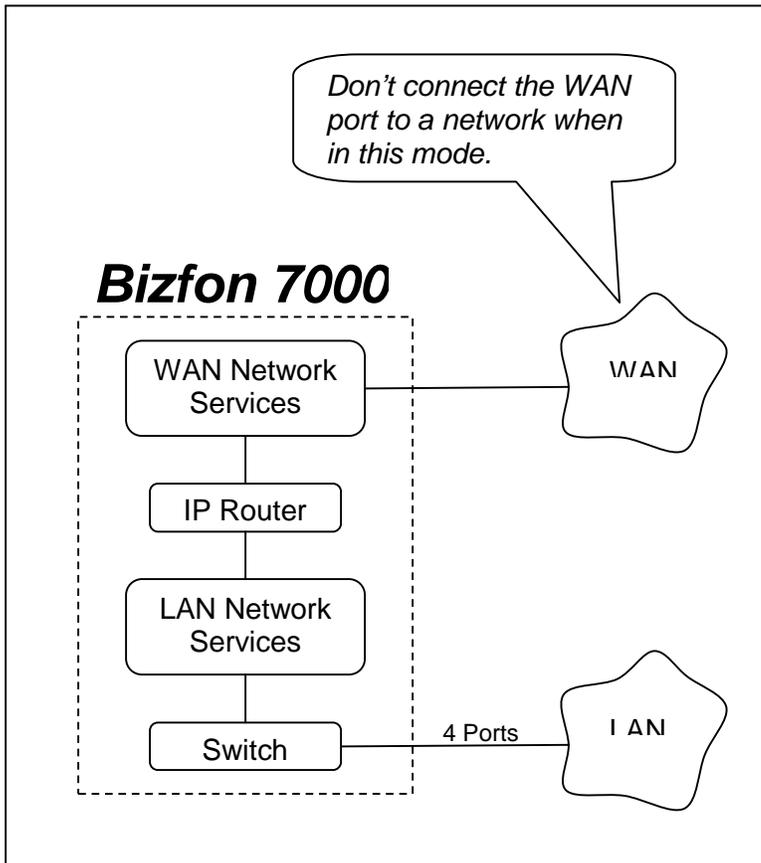


The server acts like an ordinary two port router with the server routing packets between the LAN and WAN interfaces. No NAT or firewall functionality is enabled. All LAN hosts are "visible" on the WAN. If the DHCP server is enabled (see the **Servers / DHCP Server** page), then the DHCP server will send its LAN IP address as the DHCP router (gateway) option so that LAN clients will know to use the Bizfon server as the router to the WAN. WAN hosts wanting to connect to LAN hosts will need to be configured with a network route using the Bizfon server's WAN address as a gateway to the LAN.



5.2 Network Mode: LAN Host

When the network mode is set to LAN Host, the logical network capability is as shown in the diagram below.



This mode is designed to be used when the Bizfon server is deployed as a peer (instead of as a router or firewall) on the local area network.

This mode is the same as Standard Router except that when the DHCP server is enabled, it will pass out the configured **Gateway** address (set on the **Network / Configuration / Modify** page) as the DHCP router (gateway) option (instead of giving out the Bizfon server's LAN address).

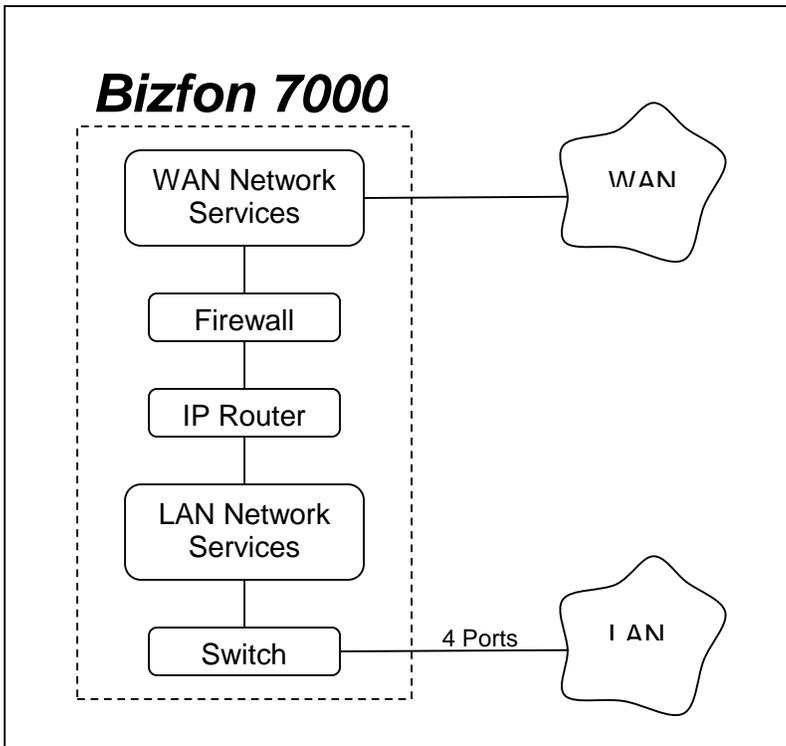
When in this mode, it is recommended that the WAN network port not be connected (ie. no network cable should be plugged in). Even though no network is plugged in, a WAN IP address and subnet mask must be assigned. A subnet number that is distinct from the LAN subnet number must be used when assigning the WAN IP address. Furthermore, a completely unused subnet number should be used to avoid any routing conflicts.

The WAN services (like FTP and HTTP) are still available via the LAN if the proper routes are configured on your network.



5.3 Network Mode: NAT/Firewall

When the network mode is set to NAT/Firewall, the logical network capability is as shown in the diagram below.



This mode's default setting permits only outbound connections from the LAN to the WAN; all WAN initiated connections are denied. In addition, all packets are subject to network address translation (NAT) such that no LAN addresses are "visible" on the WAN, yet have access to the WAN. These features reduce the ability of WAN hosts to attack LAN hosts.

WAN access to specific LAN network services can be allowed by exposing those specific LAN ports through the firewall. This configuration is made in the **Network / Configuration / Modify** page.



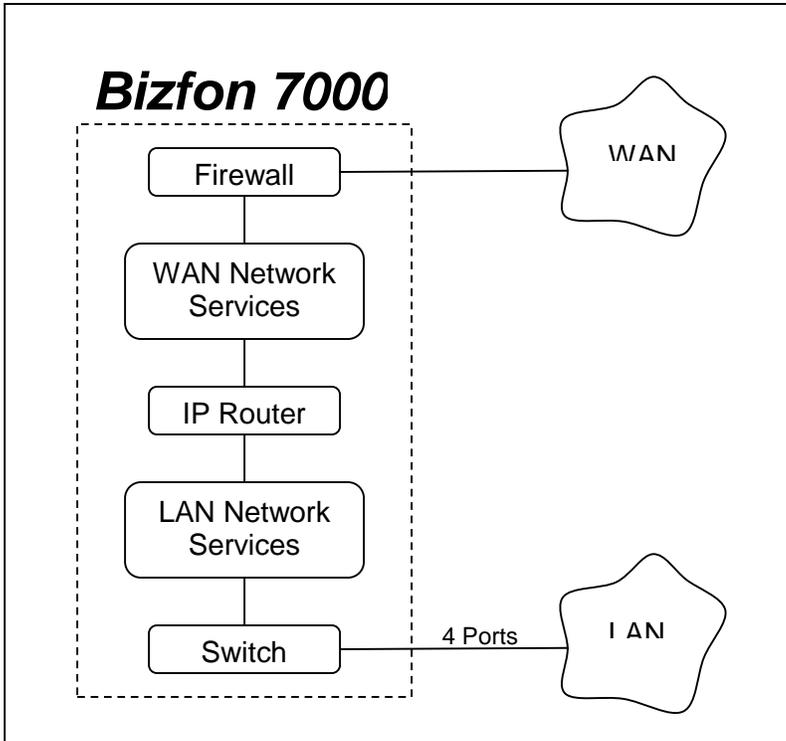
Firewall			
LAN Addresses exposed through firewall:			
WAN Port #	Protocol	IP Address	Local Port #
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP ▾	<input type="text"/>	<input type="text"/>

For example, a web server at port 80 is on a PC at 192.168.101.9. This is on the LAN. To permit access to this web server from the WAN at port 5000, create a new entry in the above table where the **WAN Port #** is 5000, the **Protocol** is TCP, the **IP Address** is 192.168.101.9, and the **Local Port #** is 80.

Due to security requirements, the Bizfon server's LAN IP address is not permitted as an **IP Address** in the table above. The server's VPN feature can be used to access Bizfon LAN network services from the WAN.

5.4 Network Mode: NAT/Firewall with DMZ

When the network mode is set to NAT/Firewall with DMZ, the logical network capability is as shown in the diagram below.



Turning on the DMZ moves the WAN network services behind the firewall. This means that even the Bizfon WAN services (POP, SMTP, FTP, HTTP, ...) are not available by hosts on the WAN. Making some of these services available can be done on the **Firewall** section of the **Network / Configuration / Modify** page.



Firewall			
LAN Addresses exposed through firewall:			
WAN Port #	Protocol	IP Address	Local Port #
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>
<input type="text"/>	TCP	<input type="text"/>	<input type="text"/>

Bizfon 7000 Services (ports) exposed through DMZ:

<input checked="" type="checkbox"/> DNS (53,4069)	<input checked="" type="checkbox"/> Remote Bizfon Handsets (2088,8081)
<input type="checkbox"/> FTP (20,21)	<input checked="" type="checkbox"/> SIP (5060)
<input checked="" type="checkbox"/> HTTP (80)	<input checked="" type="checkbox"/> SMTP (25)
<input checked="" type="checkbox"/> POP3 (110)	<input checked="" type="checkbox"/> SNTP (4068)
<input checked="" type="checkbox"/> PPTP (1723)	

Notice the checkboxes for specific Bizfon services. They are convenience shortcuts to filling in the form above them.

5.5 Network Mode: NAT/Firewall with Stealth DMZ

This mode is the same as NAT/Firewall with DMZ except that all ICMP services (echo, redirect, etc) are turned off. This makes it more difficult for attacks from the WAN to probe the server. It also makes it more difficult for the administrator to troubleshoot any network connectivity problems (since ping and traceroute won't work).

5.6 Example 1: Secure Firewall

Requirements:

The Bizfon server will be used as the router between a LAN and the Internet. Protecting the LAN from the Internet is a requirement. The server will be used as the local email server with email being sent to it from the WAN and LAN. The server will be the LAN time server. All other WAN services will be denied.

Configuration:

1. Set the **Network Mode** to NAT/Firewall with Stealth DMZ. Setting it to stealth mode will reduce the ability of Internet attacks to recognize the existence of the Bizfon server and its offered services.
2. In the **Firewall** section of the **Network / Configuration / Modify** page, change the **Bizfon Services (ports) exposed through DMZ** so that only SMTP, DNS, and SNTP are checked. SMTP is required to



receive email from the Internet for local users. DNS is required so the email server can resolve outbound mail addresses. SNTP is required to get accurate time from an Internet time server (configured on the **Maintenance / Time** page).

5.7 Example 2: Secure Firewall with Internal Email Server

Requirements:

The requirements are identical to *Example 1* except that instead of using the Bizfon server as the email server, another host (at 192.168.101.12) on the LAN will be used as the email server.

Configuration:

The configuration is identical to the above except for the following changes:

1. Uncheck the SMTP service from the list of exposed Bizfon services.
2. In the **Firewall** section of the **Network / Configuration / Modify** page, add an entry to **LAN Addresses exposed through firewall** where:
 - WAN Port # is 25.
 - Protocol is TCP.
 - IP Address is set to the LAN email server, 192.168.101.12
 - Local Port # is 25.



6 Adding Handsets

6.1 SIP Phones

6.1.1 Plug-and-Play

Some SIP phones are plug-and-play, which means that they will automatically register with the server when they boot up on the network. The following phones are capable of this:

- Bizfon IP2
- Cisco models 7905 and 7912 running SIP software versions 1.01 or greater
- Cisco models 7940 and 7960 running SIP software versions POS3-06-3-00 or greater

The means of configuring these phones varies depending on the DHCP configuration on their LAN:

1. If the phone is getting its IP address from the Bizfon 7000 DHCP server, the phone needs no manual configuration.
2. If the phone is getting its IP address from a non-Bizfon 7000 DHCP server and the DHCP server sends the phone the Bizfon server's IP address as the TFTP boot server (option #66), the phone needs no manual configuration.
3. If the phone is getting its IP address from a non-Bizfon 7000 DHCP server and the DHCP server doesn't send option #66 to the phone, then the Bizfon server's IP address needs to be manually set on the phone as its boot server.
4. If the DHCP server is sending the wrong (or no) option #66 IP address,
 - For Bizfon IP2, the manual setting on the phone will override the value sent by the DHCP server.
 - For Cisco phones, the alternate TFTP server should be set on the phone to override the value sent by the DHCP server.
5. If there is no DHCP server, then the phone needs to be manually configured with a static IP address (and netmask and gateway) and Bizfon server's IP address as its boot server.

TIP: If you are having trouble getting a phone configured, restore its factory defaults and reapply the desired settings.

When an Bizfon IP2 is booted on the network, the Bizfon server will automatically prompt you to upgrade its software when it has a newer version available.

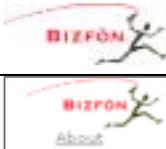
When a plug-and-play phone is registered with the server, it will appear on the **Phone System / Handsets** page in the SIP Handsets section. It will show the correct model and the MAC address will be displayed in the Identification column.

Note that a Cisco 7960 will be recognized as a 7940 and will have to be changed to 7960 via the **Phone System / Handsets** page by clicking on the **Modify** link next to the phone entry.

6.1.2 Manual Add

The Bizfon 7000 supports the manual adding of SIP phones to the system. This may be done because the SIP phone to be added is not a plug-and-play phone or you want to configure the phone without actually plugging it into the network (example, to pre-configure the server before an installation at the customer site).

To manually add a SIP phone, click on the **New SIP Handset** link in the **SIP Handsets** section of the **Phone System / Handsets** page.



Select the phone model and fill in the required fields.

If the phone isn't an Bizfon IP2 or one of the recognized Cisco phone types, then follow these steps:

1. Change the **Model** to Generic SIP.
2. Enter a **Login ID** and **Password** for the phone to use to authenticate with the server. Note that the Login ID must be unique; cannot use the same Login ID on multiple phones.
3. Click the **Program** button to add the new handset to server.
4. Configure the phone (following its particular configuration instructions) with the User ID (shown on the updated Phone System / Handsets page), Login ID, and Password.

If the phone is one of the supported plug-and-play types, then follow these steps:

1. Change the **Model** to the appropriate selection for the phone to be configured.
2. Enter a **Login ID** and **Password** for the phone to use to authenticate with the server. Note that the Login ID must be unique; cannot use the same Login ID on multiple phones.
3. Enter the correct **MAC Address** for the phone. Note if this isn't correct, then when the phone is booted on the network, the server will have a duplicate entry for this phone (because it will plug-n-play register itself with the system at the correct MAC address).
4. Enter the other parameters as necessary.
5. Click the **Program** button to add the new handset to server.

When the phone is registered with the server, its entry on the **Handsets** page will indicate that.

6.2 Analog Phones

Plug the phone into one of the server's phone ports reserved for Inside Phone Extensions. It is a good idea to plug the first phone into port 16, the next one into port 15, etc., working backwards toward port 4. Lift the



phone receiver so that the phone is "off hook." Click the **Scan For New** link on the **Phone System / Handsets** page in the **Analog Handsets** section. Your phone will now appear in the **Analog Handsets** section of the page. Hang up the phone receiver.

6.3 Testing Phones

Below are some suggested steps for verifying that a phone is set up correctly:

1. Dial 400 for auto attendant.
2. Enter '#7'. The auto attendant will play back information about the phone configuration.
3. Hangup. The phone will ring back.

If any of these steps fail, check:

- Physical wiring between phone and server
- Network settings
- Phone and server configuration

7 SIP Proxy

Note that this is an optional feature that requires a feature key.

Using a SIP Proxy, the Bizfon 7000 can use an Internet Telephony Service Provider (ITSP) to provide support for dialing and receiving outside calls. To configure the server for your ITSP, go to the **Phone System / Outside Lines** page. In the **SIP Proxies** section, you will see a list of all the SIP Proxies you have configured. To configure a new SIP Proxy, click the **New SIP Proxy** link. You will see a page like this:

Home > Phone System > Outside Lines > New SIP Proxy

Phone System

SIP Proxy

Description

User ID

Proxy Address (Domain Name or IP Address)

Proxy Port

SIP Proxy Server requires SIP registration

Login ID

Password

Registrar Address and Port are different from Proxy settings

Registrar Address (Domain Name or IP Address)

Registrar Port

Digits Sent (digits from the full number, 1-XXX-XXX-XXXX, to send to the proxy)

Maximum Active Calls

Default Auto Attendant

Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.

Call Route

Calls received from this SIP Proxy go to:

Extension

Auto Attendant

Voicemail for user

Routed using DID Block

Here is some additional info on particular parameters:

- **Description:** This can be any text useful to the server administrator. Example: "Starship".
- **User ID:** This is assigned by the ITSP. It is typically a phone number.



- **Proxy IP Address:** This is the IP address of the ITSP's server. Get this from the ITSP.
- **Proxy Port:** The default value is typical. Verify with the ITSP.
- If your **SIP proxy server requires SIP registration**, check the box indicating this and fill in the **Login ID** and **Password** assigned by the ITSP. If the ITSP uses a registrar server that is different than the SIP proxy server, check the appropriate checkbox and enter the address of this server in the **Registrar IP Address** field.
- **Digits Sent:** This is the number of dialed DTMF digits to be sent to the ITSP when making a call. If the number specified is less than the number dialed, the trailing digits are the ones sent. The default value is typical.
- **Maximum Active Calls:** The Bizfon server will use this number to limit the total of the incoming and outgoing active calls with this SIP Proxy. This is useful for controlling the network bandwidth used.

There are a few additional parameters that can be set after creating the new SIP Proxy and then clicking its **Modify** button on the **Phone System / Outside Lines** page. Here is the **Modify SIP Proxy** page:

Phone System

SIP Proxy

Description

User ID

Proxy Address (Domain Name or IP Address)

Proxy Port

Caller ID Name

Caller ID Number

SIP Proxy Server requires SIP registration

Login ID

Password

Registrar Address and Port are different from Proxy settings

Registrar Address (Domain Name or IP Address)

Registrar Port

Digits Sent (digits from the full number, 1-XXX-XXX-XXXX, to send to the proxy)

Maximum Active Calls

Default Auto Attendant

Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.

Advanced Settings

DTMF Payload (96 to 127, typically 96)

Pad DTMF RTP Packets

Call Transfer Method

Obtain DID number from

Call Route

Calls received from this SIP Proxy go to:

Extension

Auto Attendant

Voicemail for user

Routed using DID Block

The only difference between this page and the one for creating a new SIP Proxy is the **Advanced Settings** section.

The specifics of what values to enter for each of the advanced settings parameters vary with different ITSP's. Consult with your ITSP for this information.



8 Configuring Bizfon IP2 Phones

8.1 Introduction

To configure Bizfon IP2 phones, go to the **SIP Handsets** section of the **Phone System / Handsets** page.

SIP Handsets					
Handset	Line	Owner	Caller ID	Identification	Action
					New SIP Handset
BizTouch IP2					View Configuration Add Call Appearance Reboot Phone Replace Phone
First Middle Last	1	susan	First Middle Last	MAC: 00-0A-DD-81-07-DE User ID: 5100 Login ID: 5100 192.168.2.2:5060 (expires: AUG 10, 2005 06:23 PM)	Modify Delete Ring

This shows a list of all Bizfon IP2 phones known by the Bizfon server. As you can see, a number of functions are available by clicking on per phone links.

Per Phone Functions:

- **View Configuration** – This allows you to view and modify the phone configuration.
- **Add Call Appearance** – This allows you to create another call appearance for this phone. Multiple call appearances allow a single phone to handle calls for multiple extensions.

Example: Administrative Assistant

The office administrative assistant, Susan Bell, wants to be able to optionally answer the phones of two executives: Tom Brown and Joe Andrews. Here are the steps to accomplish this:

1. The assistant will already have one call appearance on her phone for her own calls. New call appearances will be added for each executive. The first new call appearance description could be changed from “Susan Bell (L2)” to “Susan Bell (Tom)”. The second description could be changed similarly.
2. The call routes for the executives would be set to ring their own handset and the assistant’s handset in parallel. However, by setting it to ring the call appearance on Susan’s phone that is designated for that executive, she’ll know who the call is for and can answer accordingly (“Good morning, Tom Brown’s office...”).

Note that the procedures in this example could be applied to other scenarios like one person answering calls to “sales” as well as “support”. By sending each of those calls to distinct call appearances, the answering person can greet the caller appropriately.

- **Reboot Phone** – Reboot the phone. The reboot will occur after a short delay on an idle phone. If the phone is in-use, the reboot will wait until the phone is idle.
- **Replace Phone** – This allows the phone to be replaced by another while automatically transferring all the configuration parameters and settings to the new phone. This is typically used when replacing a broken handset.
- **Modify** – This allows for the modification of handset call appearance parameters.



- **Delete** – Delete the phone (so the server no longer knows about it).
- **Ring** – Ring the phone. This is useful to verify connectivity.

The phones must be rebooted before any configuration changes will take affect.

The phone configuration parameters are available by clicking on the **View Configuration** link.



Home > Phone System > Handsets > View Configuration

Phone System

- [Audit PIN Codes](#)
- [Auto Attendants](#)
- [Call Blocking](#)
- [Call Forward](#)
- [Dialing Rules](#)
- [Extensions](#)
- [Handsets](#)
- [Outside Lines](#)
- [Speed Dial](#)

Business

Network

Servers

Reports

Maintenance

[Need help?](#)

[Install Checklist](#)

[Logout]

Phone System

BizTouch IP2

MAC: 00-0a-dd-81-07-de

Call Appearances:
Susan Bell

Programmable Function Keys

Station Mode: PBX Behavior

Key	Type	Action
12	(not defined)	
11	(not defined)	
10	(not defined)	
9	(not defined)	
8	(not defined)	
7	(not defined)	
6	(not defined)	Modify
5	(not defined)	
4	(not defined)	
3	(not defined)	
2	Call Appearance Susan Bell, Ring Type: AUTO	
1	Call Appearance Susan Bell, Ring Type: AUTO	

Template Options

save this handset configuration in a template

apply the selected template to this handset configuration

IP2 (Factory - Key) ▾

NOTE

It is necessary to reboot this Bizfon 7000 phone for changes to take effect.

Reboot phone now

Phone Options

Values marked with * may be overridden by the user of the phone. These values are restored when the user of the phone restores factory defaults.

	Value	Action
Call History Size	99 *	
Clock Mode	12 Hour *	
Codec Preference Order	G.711, G.729A	
Daylight Saving Time	use current server setting	
Hold Reminder Mode	Timer *	
Hold Reminder Timeout	300 *	
Jitter Buffer Size	80ms	
Message Waiting Indication	Visual	
Off Hook Digits Dialed		
Paging Mode	Pages always accepted *	
Paging Zones	0	
Radial Memory	Forever *	
RTP Media Port Range	16384 to 32767	
SIP NAT Keep-alive Interval	20	
SIP Port	5060	Modify
Time Zone	use current server setting	
Audible Dialing	enabled *	
Auto On Hold	disabled *	
Auto Retrieve Calls	enabled *	
Call Timer Display	enabled *	
Caller ID Display	enabled	
Configuration Menu	enabled	
DTMF Payout	enabled	
Intercom Auto Answer	enabled *	
Keypad Dialing	enabled	

This page contains a number of functional sections: Programmable Function Keys, Template Options, and Phone Options. Each one will be examined in the sections below.



8.2 Programmable Function Keys (PFK's)

Look at the Programmable Function Keys section on the View Configuration page.

Programmable Function Keys		
Station Mode: PBX Behavior		
Key	Type	Action
12	(not defined)	Modify
11	(not defined)	
10	(not defined)	
9	(not defined)	
8	(not defined)	
7	(not defined)	
6	(not defined)	
5	(not defined)	
4	(not defined)	
3	(not defined)	
2	Call Appearance Susan Bell, Ring Type: AUTO	
1	Call Appearance Susan Bell, Ring Type: AUTO	

This section is used to show and modify the configuration of the individual PFK's on a particular handset. To modify the configuration, click the **Modify** link.



Call Blocking
Call Queues
Dialing Rules
Extensions
Handsets
Outside Lines
Speed Dial

Business
Network
Servers
Reports
Maintenance

[Need help?](#)
[Install Checklist](#)

[Logout]

TIP

Outside Lines that are enabled for Line Appearance can be automatically assigned to Programmable Function Keys on the phone. Click the button below to assign the Outside Lines.

The server has no Outside Lines configured for Line Appearance at this time.

Programmable Function Keys

Station Mode PBX Behavior

Key	Type	Type
12	Not Used	
11	Not Used	
10	Not Used	
9	Not Used	
8	Not Used	
7	Not Used	
6	Not Used	
5	Not Used	
4	Not Used	
3	Not Used	
2	Call Appearance	Susan Bell Ring Type: AUTO change
1	Call Appearance	Susan Bell Ring Type: AUTO change

8.2.1 Station Mode Selection

Notice the **Station Mode** selection in the above figure. It can be set to **PBX Behavior** or **Key System Behavior**. This selection is used to change the way two areas of phone behavior:

- It varies how some of the PFK functions work. These changes will be specified below when the functions are described.



- It varies how the handset Hold button works. When in key system mode and the active call is on a Line Appearance PFK, the Hold button performs a system wide call park operation that allows the call to be picked up by a Line Appearance PFK on this or another handset. When in PBX mode or the active call is on a Call Appearance PFK, the Hold button performs a local hold operation that is local to the handset.

8.2.2 PFK Function Selections

Notice the numbered **Key** rows in the above figure. To set the function for a particular PFK, click the drop down arrow and choose one of the functions.

Busy Lamp Field (BLF) PFK Type – Monitors and dials another phone. The other phone is specified when setting up the BLF function. When the PFK is pressed, the behavior of this function is dependent upon the **Station Mode** selection.

- When **Station Mode** is set to **PBX Behavior**, the extension of the owner of the designated phone is dialed.
- When **Station Mode** is set to **Key System Behavior**, an intercom connection is made to the designated phone.

Call Appearance PFK Type – The PFK can be mapped to one of the phone’s call appearances. This allows calls to be placed or received using this call appearance. Additional notes:

- Recall that a phone can have multiple call appearances. This allows for each call appearance to be distinctly used in call routing and for those calls to be managed independently and concurrently on the same phone.
- Mapping more than one PFK to the same call appearance allows multiple calls to that call appearance to be active at the same time. The call appearance won’t appear busy to the call route (see *Call Routing*) until all the PFK’s defined for this call appearance are in use. This is akin to call waiting except the PFK’s are used to alert and select a new call.

Example: Busy Receptionist

Requirements:

Susan works as a receptionist at a busy office. She gets many phone calls each hour. She wants to be able to answer each call while minimizing the possibility of any caller getting a busy signal.

Phone Configuration:

She has one call appearance defined on her phone. She sets up 8 of her phone’s PFK’s so that they map to her phone’s call appearance. (She wants to use the remaining PFK’s for other functions).

Discussion:

When the first phone call comes in, her phone will ring and the first of the call appearance PFK’s blink green. While talking with the first caller, a second call comes in. Her phone rings again and the second of the call appearance PFK’s blinks green. She puts the first caller on hold by pressing the Hold button on her phone and picks up the second caller by pressing the second call appearance PFK. She continues to put callers on hold and answer new calls just as described. She terminates calls by switching to another call appearance PFK.



Function PFK Type – The PFK can be set to perform one of a specified set of functions. Allowable functions are:

- **Centrex Flash** – Sends a flash signal out the analog CO line. This is ignored if not connected to an analog CO line.
- **Headset** – Turns the headset (if one is plugged in) on and off. If a headset is plugged in and the handset is off-hook, then this button toggles the audio between the headset and the handset. (If a headset PFK isn't defined, the phone's speaker button will be used to operate the headset).
- **Personal Speed Dial** – Dials a Personal Speed Dial Number that is programmed directly on the phone. The mapping of Personal Speed Dial PFK's and Personal Speed Dial Numbers defined in the handset is as follows. Starting with the uppermost PFK on the phone, count each Personal Speed Dial PFK beginning with 0. This number determines which handset defined Personal Speed Dial Number the PFK dials.
- **Redial** – Redials the last dialed number. Unless the **Enable Line Appearance(s) Use of Dial Plan** phone option is enabled (see *Phone Options*), only call appearance (not line appearance) dialed calls can be redialed.

Line Appearance PFK Type – Monitor the status of an outside line, answer an incoming call on that line, and select the line for outbound calls. The line is specified when setting up this function for this PFK. For outside lines to be available for selection, they must be enabled on the **Phone System / Outside Lines / Modify** page by checking the **Enable Line Appearance** checkbox. Any number dialed on a line appearance bypasses dialing rules, service groups, call history, and the handset's **Outside Line Connection** parameters (**Phone System / Handsets / Modify Handset**).

Not Used PFK Type – No action. This function is selected when the PFK should be disabled.

Queue Appearance PFK Type – Monitor the status of a Call Queue and answer calls in the queue. See *Call Queues* for more information on configuring phones for this use.

Speed Dial PFK Type – Automatically dials an extension. The extension is specified when setting up the Speed Dial function for this PFK.



8.3 Phone Options

Look at the Phone Options section on the View Configuration page.

Phone Options		
Values marked with * may be overridden by the user of the phone. These values are restored when the user of the phone restores factory defaults.		
	Value	Action
Call History Size	99 *	Modify
Clock Mode	12 Hour *	
Codec Preference Order	G.711, G.729A	
Daylight Saving Time	on (U.S. rules)	
Hold Reminder Mode	Timer *	
Hold Reminder Timeout	300 *	
Jitter Buffer Size	80ms	
Message Waiting Indication	Visual	
Off Hook Digits Dialed		
Paging Mode	Pages always accepted *	
Paging Zones	0	
Redial Memory	Forever *	
RTP Media Port Range	16384 to 32767	
SIP NAT Keep-alive Interval	30	
SIP Port	5060	
Time Zone	use current server setting	
Audible Dialing	enabled *	
Auto On Hold	disabled *	
Auto Retrieve Calls	enabled *	
Call Timer Display	enabled *	
Caller ID Display	enabled	
Configuration Menu	enabled	
DTMF Payout	enabled	
Intercom Auto Answer	enabled *	
Keypad Dialing	enabled	
Line Appearance(s) Use Dial Plan	enabled	
Off Hook Ringing	enabled *	
On Hook Dialing	enabled *	
Visual Ringing	enabled *	

This section is used to show and modify the phone options for a particular handset. To modify the configuration, click the **Modify** link.



Home > Phone System > Handsets > Modify Handset

Phone System

BizTouch IP2

MAC: 00-0a-dd-81-07-de

Call Appearances:
Susan Bell

NOTE

It is necessary to reboot this Bizfon handset for changes to take effect.

Phone Options

Fields marked with * may be overridden by the user of the phone. These fields are restored when the user of the phone restores factory defaults.

Call History Size*	99	(0 - 99, calls kept in history)
Clock Mode*	12 Hour	
Codec Preference Order	G.711, G.729A	
Daylight Saving Time	use current server setting	
Hold Reminder Mode*	Timer	
Hold Reminder Timeout*	300	(1 - 600 seconds)
Jitter Buffer Size	80ms	
Message Waiting Indication	Visual	
Off Hook Digits Dialed		
Paging Mode*	Pages always accepted	
Paging Zones	0	(comma separated list of zones from 0 through 9)
Redial Memory*	Forever	(length of time last number dialed is stored)
RTP Media Range (Port to Port)	16384 to 32767	(typically 16384 to 32767)
SIP NAT Keep-alive Interval	20	(10 - 300 seconds) for remote phones behind NAT firewall
SIP Port	5060	(typically set to 5060, change if necessary for firewall)
Time Zone	use current server setting	

- Enable Audible Dialing* (tone heard when key pressed)
- Enable Auto On Hold*
- Enable Auto Retrieve Calls*
- Enable Call Timer Display*
- Enable Caller ID Display
- Enable Configuration Menu (CONF softkey enabled on phone)
- Enable DTMF Playout (DTMF sent in outbound RTP packet)
- Enable Intercom Auto Answer* (speakerphone activates automatically)
- Enable Keypad Dialing (typically enabled)
- Enable Line Appearance(s) Use of Dial Plan (typically enabled)
- Enable Off Hook Ringing* (phone rings when new call received while off hook)
- Enable On Hook Dialing* (speakerphone activated when number dialed)
- Enable Visual Ringing*

Update
Start Over
Cancel

Many of these options are easily understood from the web page. However, some of the more complicated ones will be described next.



8.3.1 Description of Options

Codec Preference Order – Sets the preferred codec order in the phone. The codec is the method of encoding/decoding the audio sent to and received by the phone. The two possible codec's are G.711 and G.729A. G.711 preserves voice quality, but takes more bandwidth. G.729A takes less bandwidth, but reduces voice quality. Note that this only sets the preferred codec order. Not all codec's are supported for all call types (for example, accessing the server auto attendant requires G.711). To maintain operability, the phone will use whichever codec is required to support the call. This means that your preferred codec won't always be the one used.

Jitter Buffer Size – Jitter is a variation in network audio packet latency experienced by the phone, resulting in a reduction in audio quality. The phone uses a jitter buffer to maximize the audio quality when jitter occurs. This configuration parameter can be used to alter the size of the jitter buffer.

Off Hook Digits Dialed – Enables the phone to automatically dial some digits whenever the phone is taken off hook.

- An example of this is a service phone placed at a locked door or loading dock where all dialing is disabled and want the phone to automatically dial a predefined number when it is taken off hook.
- Another example might be to have the phone automatically dial '9' (or '8' + PIN Code) to get an outside line. Note that these digits will always be dialed when the phone is taken off hook, so this might interfere with other uses of the phone. For example, if the phone is configured to automatically dial '9', the user will not be able to use PBX features that don't start with '9' (Call Park, Call Forwarding, etc.).

Paging Zones – Sets the list of paging zones that the phone will participate in. For example, if the sales team uses zone 3 for pages to the entire team, then this option on the team member's phones must be set to include zone 3.

SIP NAT Keep-alive Interval – Some NAT firewalls will automatically timeout connections. If a remote phone is behind such a firewall, then this setting allows a keep-alive packet to be sent from the phone to the Bizfon server at the frequency specified. When set to an interval more frequent than the firewall timeout, this will prevent the firewall from timing out the connection.

Enable Auto On Hold – When one call is active on the phone and another call comes in (with a free Call/Line Appearance PFK), if the PFK for the new call is pressed, the first call is automatically put on hold instead of terminated.

Enable Auto Retrieve Calls – When the phone is on hook and a call is on hold, then when the phone is taken off hook, the on hold call is automatically retrieved. When this is not enabled, the phone gets an open line (if available) when taken off hook.

Enable DTMF Playout – DTMF digits are allowed to be sent during an active call.

Enable Keypad Dialing – If not enabled, the keypad cannot be used to initiate or transfer a call. This does not prevent the keypad from functioning during an active call. It prevents the use of the keypad to initiate any functions directly with the Bizfon server (for example: dial number, Call Park, etc.).



Enable Line Appearance(s) Use of Dial Plan – If not enabled, the phone number dialed when a line appearance PFK is selected is not displayed by the phone, is not recorded in the phone’s call history, and is not available for redial. Reasons to disable are if the line doesn’t follow the North American Numbering Plan (including if the line connects to another PBX). The use of this feature requires the server’s dial plan to be configured (see *Dialing Rules and Service Groups*).

Enable On Hook Dialing – On hook dialing means that the handset doesn’t have to be picked up (nor the speakerphone button hit) before dialing a number on the keypad. When the phone is on hook and a digit is dialed on the keypad, the phone will automatically go off hook to the speaker phone.

8.4 Configuration Templates

Configuring many phones can be time consuming and error prone. To improve this, the Bizfon 7000 provides templates that store a phone configuration. The system provides a factory default template for each phone type. However, the administrator can create his own unique templates as well.

A list of all the templates known by the system is in the **Handset Configuration Templates** section of the **Phone System / Handsets** page.

Home > Phone System > Handsets

Analog Handsets				Scan For New	Handset Configuration Templates		
Handset	Owner	Caller ID	Port	Action	Model	Description	Action
			04	New Analog Handset	BizTouch IP2	IP2 (Factory - Key)	Activate
			05	New Analog Handset	BizTouch IP2	IP2 (Factory - PBX) * active *	
			06	New Analog Handset			
			07	New Analog Handset			
			08	New Analog Handset			
			09	New Analog Handset			
			10	New Analog Handset			
			11	New Analog Handset			
			12	New Analog Handset			
			13	New Analog Handset			
			14	New Analog Handset			
			15	New Analog Handset			
			16	New Analog Handset			

SIP Handsets					
Handset	Line	Owner	Caller ID	Identification	Action
					New SIP Handset
BizTouch IP2					View Configuration Add Call Appearance Reboot Phone Replace Phone
Susan Bell	1	susan	Susan Bell	MAC: 00-0A-00-81-07-0E User ID: 5100 Login ID: 5100 192.168.2.2:3060 (expires: AUG 11, 2005 05:00 PM)	Modify Delete Ring



8.4.1 Default Templates

The current default template for each phone type is listed as * **active** * in the list of **Handset Configuration Templates**. To make another template the default, click its **Activate** link. The current active templates are used for configuring phones during plug-n-play.

8.4.2 Viewing a Template's Configuration

To view a template's phone configuration, click on the template **Description** in the list of **Handset Configuration Templates**.

8.4.3 Creating a New Template

New templates can be created from any phone's configuration. Creating a new template has a few steps:

1. Click **View Configuration** on an existing phone.
2. Change the configuration according to the requirements for the new template.
3. Save the current configuration as a template.

To perform the last step, notice the **Template Options** section of the **View Configuration** page.



When you click the **Save** button, a pop-up window prompts you to enter the description for the new configuration. After clicking **OK** in the pop-up window, the template is saved and will now appear in the list of **Handset Configuration Templates**.

8.4.4 Applying a Template to a Phone's Configuration

To apply a template to a phone's configuration, follow these steps:

1. Click **View Configuration** on the phone to be changed.
2. Using the **Template Options** section, select the template to be applied from the drop down list.
3. Click the **Apply** button.

8.4.5 Deleting a New Template

The factory provided templates cannot be deleted. To delete an administrator created template, click its **Delete** link in the **Handset Configuration Templates** section of the **Phone System / Handsets** page.

8.4.6 Changing a Template's Configuration

Templates can be saved, applied, and deleted. To change a template's configuration, a combination of those operations must be used. The template configuration cannot be edited directly. The required steps to change a template are to: delete the template you want to change, edit a phone's configuration that reflects the template you want to change, and then save the template with the original name.



9 Dialing Rules and Service Groups

9.1 Background Information

9.1.1 Dialing Rules

As a user dials digits on a phone, the system collects the digits one at a time. How does it know when it should wait for more digits (because the user is dialing slowly) or when it should take the digits it has and try to make a call with them? The server's rules for this are called Dialing Rules. Dialing rules specify to the Bizfon server what digit sequences are valid to be dialed out on the public phone network.

Examples:

- When dialing a "local" number, you don't normally dial 1 and the area code. So, the system should collect the first 7 digits dialed and then try to make the call. It shouldn't wait for more.
- When you dial a long distance number, you normally dial 1 plus the area code and then the 7 digit local number. The system needs to recognize this case distinctly from the "local" number case and know to collect all 11 digits before trying to make the call.

In addition, some local calling areas require an area code to be dialed without the 1 prefix in order to properly dial some numbers. This implies that these rules may vary dependant on the local calling area where the Bizfon server is installed.

9.1.2 Home Area Code

Some features of the Bizfon server and phones (example: redial from call history) require the knowledge of the home area code. So this information is a required part of the dialing rules.

9.1.3 Service Groups

The server can use a variety of services to place outside calls: CO lines, SIP Gateways, and SIP Proxies. Some of these services may be optimum for particular types of calls. For example, your SIP Proxy might be the least expensive way to make long distance calls, yet your CO lines are best for local calls.

A Service Group is a collection of services that can be used to place outside calls. Three service groups are created automatically by the server:

- All CO Lines
- All CO Lines & SIP Gateways
- All CO Lines, SIP Gateways, and SIP Proxies

9.1.4 Exceptions

Dialing rules and service groups are only used for call appearance calls, not for line appearance calls. (This is because line appearance calls access the outside line directly).

Only the North American Numbering Plan (NANP) is supported by the server dialing rules. If your Bizfon server is located in an area that does not support NANP, then you can gain direct access to an outside line by using a line appearance PFK or dialing '9#'.

9.2 Configuring Service Groups

Dialing rules, home area code, and service groups are all configured using the **Phone System / Dialing Rules** page.



Home > Phone System > Dialing Rules

Phone System

Dial 9 - Service Groups

Area Code	Dial Method	Service Group	Action
any	1 + Area Code dialed	All CO Lines & SIP Gateways	Modify

Dial 8+PIN - Service Group

Service Group	Action
All CO Lines	Modify

NOTE

When 8+PIN is dialed, only CO Lines may be used to complete the call. Please verify that Service Group you select only contains CO Lines or the system may not complete call as expected.

Service Groups

Group	Service(s)	Action
		New Service Group
All CO Lines		
All CO Lines & SIP Gateways		
All CO Lines, SIP Gateways & SIP Proxies		

Phone System

- [Audit PIN Codes](#)
- [Auto Attendants](#)
- [Call Blocking](#)
- [Call Queues](#)
- [Dialing Rules](#)**
- [Extensions](#)
- [Handsets](#)
- [Outside Lines](#)
- [Speed Dial](#)

Business

Network

Servers

Reports

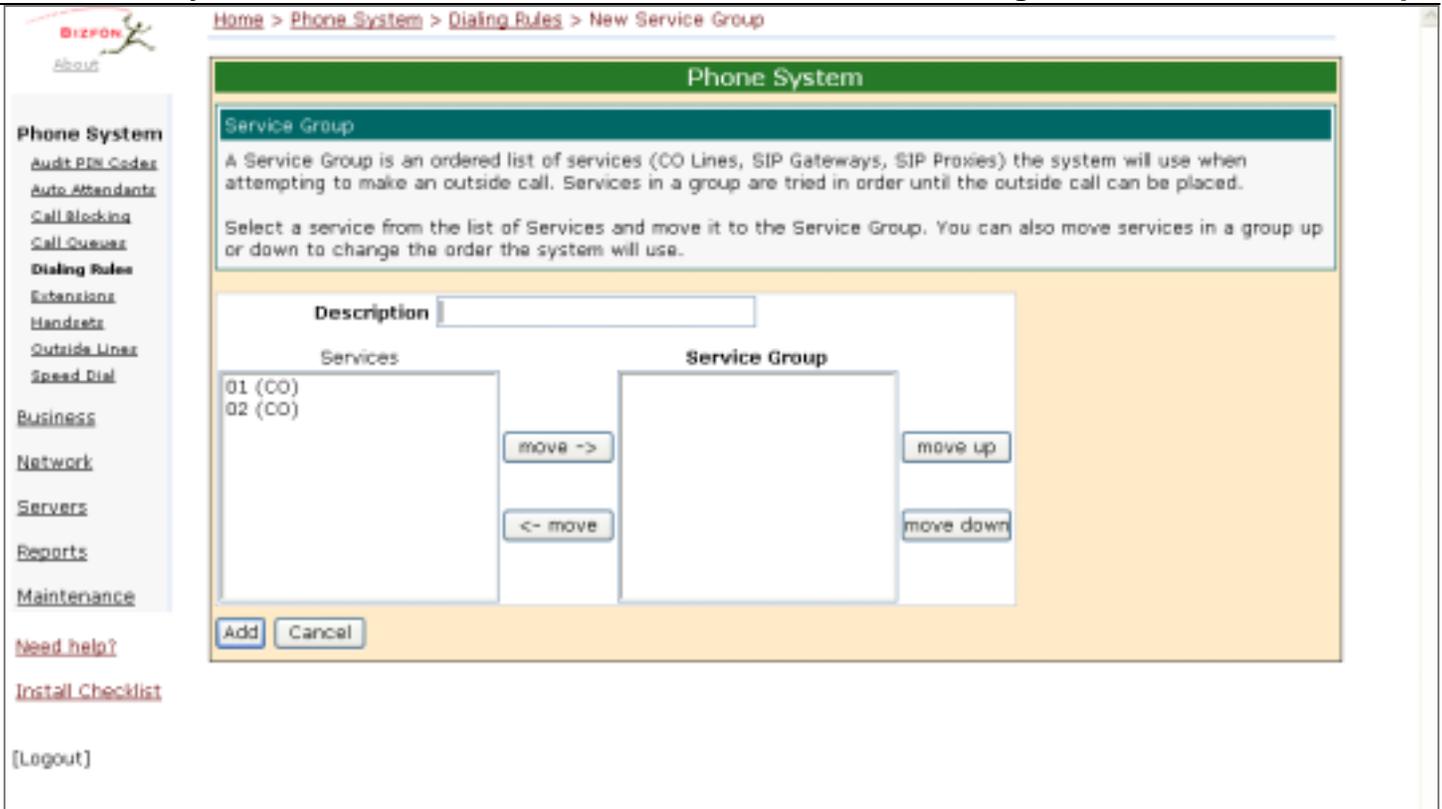
Maintenance

[Need help?](#)

[Install Checklist](#)

[Logout]

The first step in configuring this area is to set up the desired service groups. If one of the pre-configured service groups satisfies your requirements, you have nothing more to do. If not, click **New Service Group** to create your own.



Enter a **Description** for this service group. Then, move the services required for this group into the new service group.

When an outbound call is initiated using the service group, the services in the group will be tried in top-down order until an idle service is found. The call will be made using the first idle service in the list. So, the last step in setting up a service group is to ensure that the order of the services reflects your preferred priority of use. Regarding service selection when one of the services in the group is a SIP proxy, the SIP proxy will continue to be considered idle until its maximum active calls setting has been reached.

9.3 Configuring Home Area Code and Dialing Rules

The configuration of dialing rules, home area code, and dial 9 service groups are all done together. The dial 8 + PIN service group is done separately.

9.3.1 Dialing Rules, Home Area Code, and Dial 9 Service Groups

To configure the dialing rules, home area code, and dial 9 service groups, click on the **Modify** link in the **Dial 9 – Service Groups** section of the **Phone System / Dialing Rules** page.



Home > Phone System > Dialing Rules > Modify Dial 9

Phone System

Area Code	Dial Method	Service Group
Home <input type="text"/>	1 + Area Code dialed ▼	All CO Lines & SIP Gateways ▼
<input type="text"/>	1 + Area Code dialed ▼	All CO Lines & SIP Gateways ▼
<input type="text"/>	1 + Area Code dialed ▼	All CO Lines & SIP Gateways ▼
<input type="text"/>	1 + Area Code dialed ▼	All CO Lines & SIP Gateways ▼
all others	1 + Area Code dialed	All CO Lines & SIP Gateways ▼

NOTE

Seven digit phone numbers (###-###) and phone services such as 911, 411, etc. will be routed using the Home Area Code Service Group if the Home Area Code has been set. These numbers and services will be routed using the "All CO Lines, SIP Gateways & SIP Proxies" service group if the Home Area Code has not been set.

TIP

Additional Area Codes can be added by filling in all the Area Codes entries on this page, clicking on Update, then clicking Modify to return to this page. Area Codes can be deleted by clearing the Area Code box then clicking on Update.

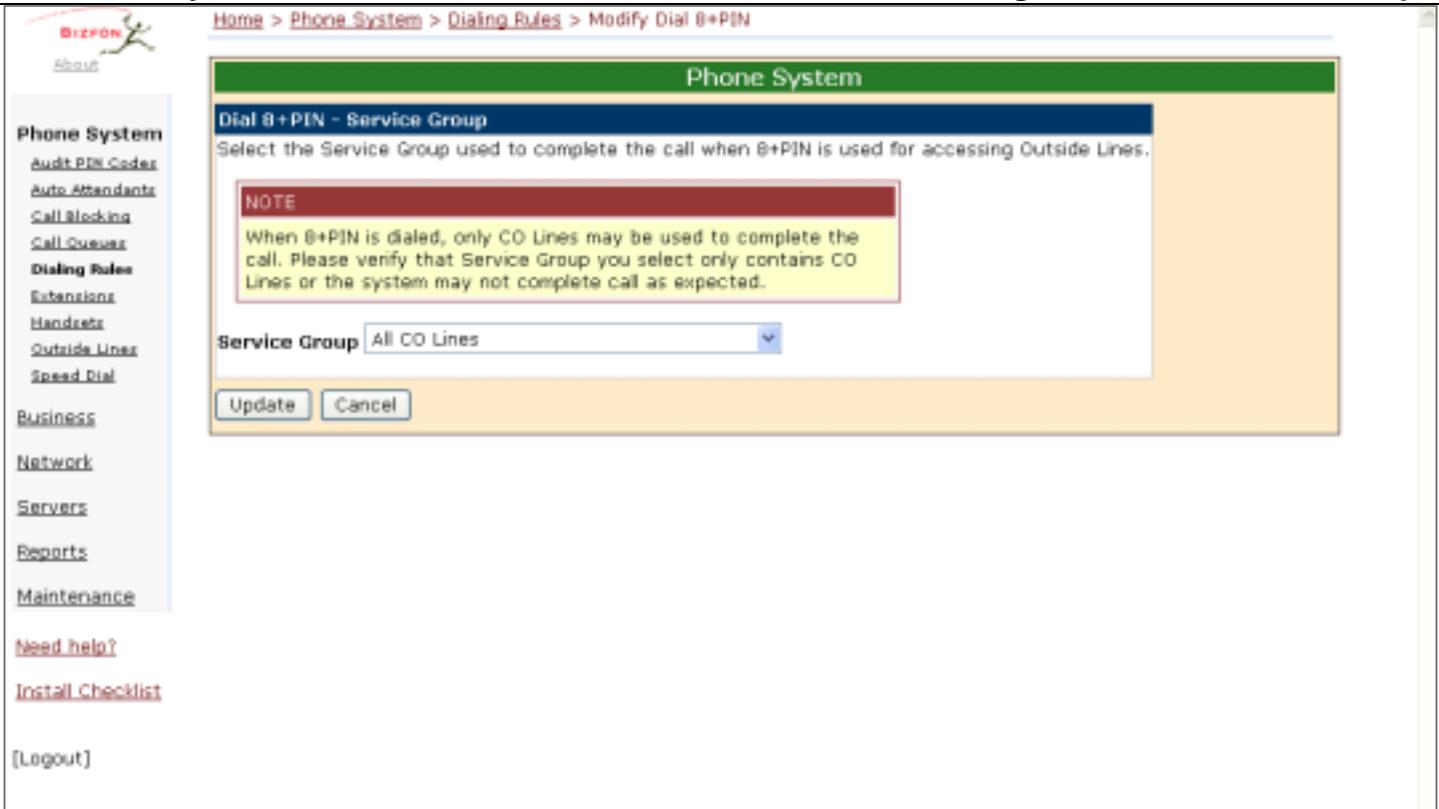
Home Area Code: This is the implied area code for 7 digit phone numbers.

Configuration Steps

1. Enter your Home Area Code and set the Dial Method. Most local calling areas will set the Dial Method to Area Code NOT dialed (i.e. 7-digit dialing). This sets up the dialing rule for local calls.
2. Notice the all others area code entry. Its Dial Method is permanently set to 1 + Area Code dialed. This sets up the dialing rule for most long distance calling.
3. Set up any additional area codes where you must dial the area code, but not a 1 prefix.
4. Choose the desired Service Group for each of the area code entries.
5. If there are any additional area codes with unique service group requirements, enter it in an empty Area Code row, select its Dial Method, and choose the Service Group.

9.3.2 Dial 8 + PIN Service Group

To configure the **Dial 8 + PIN Service Group**, click on the **Modify** link in the **Dial 8 + PIN – Service Group** section of the **Phone System / Dialing Rules** page.



Choose the desired **Service Group** to use for all 8 + PIN calls. Be sure to select only service groups that contain only CO lines.

9.4 Interaction Between Service Groups and Handset Outside Line Restrictions

As stated above, service groups are used to direct the placement of outbound calls to particular services and the service chosen for a particular call is the first idle service in the group. There is one exception to this. A handset can be configured to restrict its use of any CO Line, SIP Gateway, or SIP Proxy when placing an outside call. The rule for resolving this is as follows:

1. According to the number dialed, the configured service group is found for a particular outbound call.
2. When the first idle service in the group is found, the list of handset restrictions is checked. If the found service is restricted for the handset, then the next idle service is found and the handset check is made again. This continues until a non-restricted idle service is found to place the call. If none is found, the caller hears a fast busy signal indicating that no available outside lines were found.



10 Unified Messaging

The Bizfon 7000 supports unified messaging such that a user's voicemail and email messages are combined into one "inbox" in the system. Because voicemail and email are stored together and because voicemail can be accessed both as voicemail on the phone and as email on a PC, unified messaging may behave in unexpected ways. Here are some of the important properties of the unified messaging feature:

- Voicemail and email are stored in one inbox on the server (hence, "unified" messaging!). Messages from this inbox can be forwarded to another email account or POP'd to an email client.
- Using a phone, the voicemail and email messages can be listened to, deleted, etc. When a voicemail or email message is deleted via a phone, it is deleted from the inbox on the server
- When unified messages are deleted off the server because of a POP or a mail forward, the voicemail is deleted as well. So it is no longer available on a phone.

10.1 Access Mechanisms

The two main mechanisms to access your voicemail and email messages from the server are:

- Forwarding messages to another email account
- Using a POP email client to transfer the messages to your PC.

10.1.1 Forwarding Messages

Using the server message aliases feature (**Business / Message Aliases** page), you can forward any incoming message (voicemail or email) for a user to an external (non-Bizfon 7000) email account. This is done by entering the user's Bizfon login name as the email alias and the external email address in the members list. If you want to save a copy of the message on the Bizfon server, also enter the user's login name in the members list.

If you save a copy on the server, eventually the user may exceed his inbox quota on the server. To avoid this, the user's messages must be periodically deleted from the server.

Common Error

A common error is assigning the Bizfon server's domain name to be that of an existing domain name.

Example:

MyCompany pays an Internet hosting service to provide email for all their employees at user@mycompany.com. The employees get their email by configuring their email application to POP the email off the hosting service's email server. When the Bizfon server is installed, it is given a domain name of mycompany.com.

This creates a problem where the Internet DNS servers are configured such that mail for user@domainname is to be sent to the external hosting service's IP address, but the Bizfon DNS server has been configured to think it is responsible for handling email for the same domain name. Then when putting user@domainname in the members list, the Bizfon server says "that's me!" and sends the email to himself instead of to the external IP address. The solution is to not use the same domain name for both.

10.1.2 POP Client

Using the **POP3 Mail Transfers** section of the **Business / Users / Modify User** page, each Bizfon user can be configured so that a POP request to transfer email to a POP client will transfer: email and voicemail messages; email messages only; or no messages. Only the first option will transfer voicemail messages to the PC email application's inbox.



Each user's PC email application needs to be configured so it can talk to the Bizfon server to send and receive messages. The precise details depend on the application, but here is the required server information:

- Enter the IP address of the Bizfon 7000 server's **LAN TCP/IP Address** (from the **Network / Configuration** page) as the incoming POP3 server address.
- Enter the same address as the outgoing SMTP server address.
- Enter the user's server login name and password as the POP3 user and password.
- Do not use Secure Password Authentication (SPA).
- Do not use SSL to communicate with the Bizfon 7000 server.
- Do not use authentication for the outgoing server.

In addition, most popular email applications allow the messages to be left on the server when they are transferred to the PC. Using this feature, the user may eventually exceed his inbox quota on the server. To avoid this, it is recommended that you enable your email application to either delete all the server email after N days or to delete it when it is deleted on the PC.

10.2 Access Examples

10.2.1 Example 1

Requirements:

Tom (login name "tom") doesn't expect to get email at his Bizfon 7000 address, but instead uses an external email account (tom@yahoo.com). His Bizfon 7000 voicemail should be sent to the external email account. Voicemail should also be available from his phone.

Configuration:

Set up an Bizfon 7000 message alias for Tom to forward all his messages to his external email account as well as keep a copy on the Bizfon server. Create a new message alias such that:

- **Email Alias** is set to "tom".
- **Members** is set to "tom" and "tom@yahoo.com".

Commentary:

Tom will use his phone to delete old voicemail messages. If any email is sent to his Bizfon 7000 account, it will be forwarded to his external account, leaving a copy on the Bizfon server. If email accumulates on the server, he will need to periodically connect with a POP email client to delete those old email messages.

10.2.2 Example 2

Requirements:

Tom is a remote user of the system. He doesn't have a phone. His extension is configured to send all calls directly to his voicemail. He doesn't want to call in to get his voicemail, but instead wants all email and voicemail messages to be sent directly to his external email account (tom@yahoo.com).

Configuration:

Set up an Bizfon 7000 message alias for Tom to forward all his messages to his external email account. Create a new message alias such that:

- **Email Alias** is set to "tom".
- **Members** is set to "tom@yahoo.com".



Commentary:

Tom will get all his email and voicemail messages using his external email account. Since the system will delete the messages off the server as soon as they are forwarded, he doesn't need to periodically delete anything left there.

10.2.3 Example 3

Requirements:

Tom will use the Bizfon 7000 for his email. He wants to use his phone to listen to voicemail messages, but doesn't want those messages sent to his email account.

Configuration:

- Set up Tom's Bizfon 7000 **POP3 Mail Transfers** configuration to transfer only email messages.
- Set up Tom's PC email application to POP email off the Bizfon 7000 without leaving a copy on the server.

Commentary:

Tom's email messages will be deleted off the server as soon as they are POP'd to his PC email application. Voicemail messages will be kept on the server until he deletes them via his phone.

10.2.4 Example 4

Requirements:

Tom will use the Bizfon 7000 for his email. He wants to use his phone to listen to voicemail messages and wants those messages sent to his email account as well.

Configuration:

- Set up Tom's Bizfon 7000 **POP3 Mail Transfers** configuration to transfer both email and voicemail messages.
- Set up Tom's PC email application to POP email off the Bizfon 7000 while leaving a copy on the server until he deletes the message on his PC.

Commentary:

Tom will be able to listen to his voicemail messages on his phone or on his PC (via email). If he deletes a voicemail message using his phone, it will not be deleted on his PC. However, if he deletes a voicemail from his PC, it will be deleted from the server, making it no longer available on his phone. He will have to periodically delete messages from his PC so that he doesn't exceed his message quota on the server.



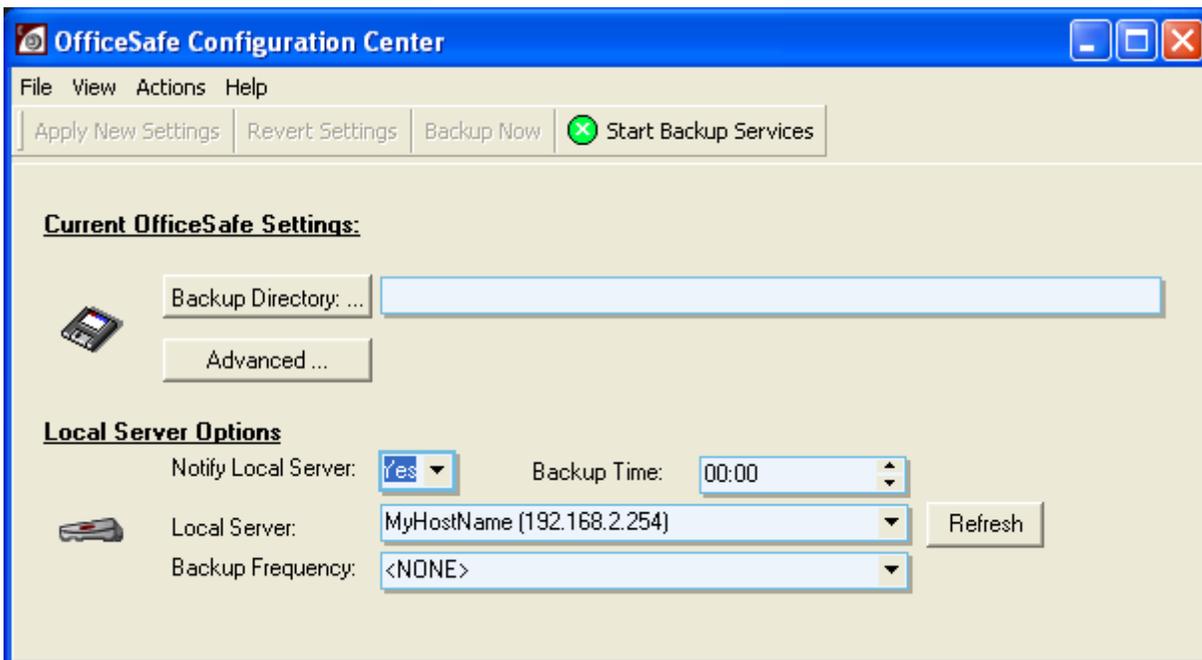
11 Backing up and Restoring Data

It's a good idea to back up your Bizfon 7000 server data. In the event of a server failure, you can restore your data from the backup. You can set up the Bizfon OfficeSafe Application to create the backup as frequently as you need. Take a few minutes to assess how much data you would be willing to lose in case you need to restore the system from a backup.

OfficeSafe is optimized for restoring the entire Bizfon server disk. It is not possible to restore only a particular file.

11.1 How to Create a Backup

1. Double-click **OfficeSafe** on your desktop or select **Programs>Bizfon>OfficeSafe**.



2. Click **Backup Directory** to select where the backup should be created.
NOTE: Using the Advanced button, you can set the Bizfon port for the backup server connection and the maximum size of the backup file. It is recommended that you call Customer Support before using these features.
3. Select **Yes** for **Notify Local Server**.
4. Select a **Backup Time** to have the backup performed automatically at the same time every day.
5. Select the **Local Sever** to backup. Click **Refresh** to scan the network for Bizfon 7000 servers.
If your Bizfon server is not found, you can “ping” the server to make sure it is connected and/or on the same local subnet.
6. Select the **Backup Frequency**. More frequent updates mean that, in case of a disk failure, you will lose less data when you restore from the last backup.
NOTE: You must select a Backup Frequency even if the frequency you want is already selected (If this is the case, select it again).

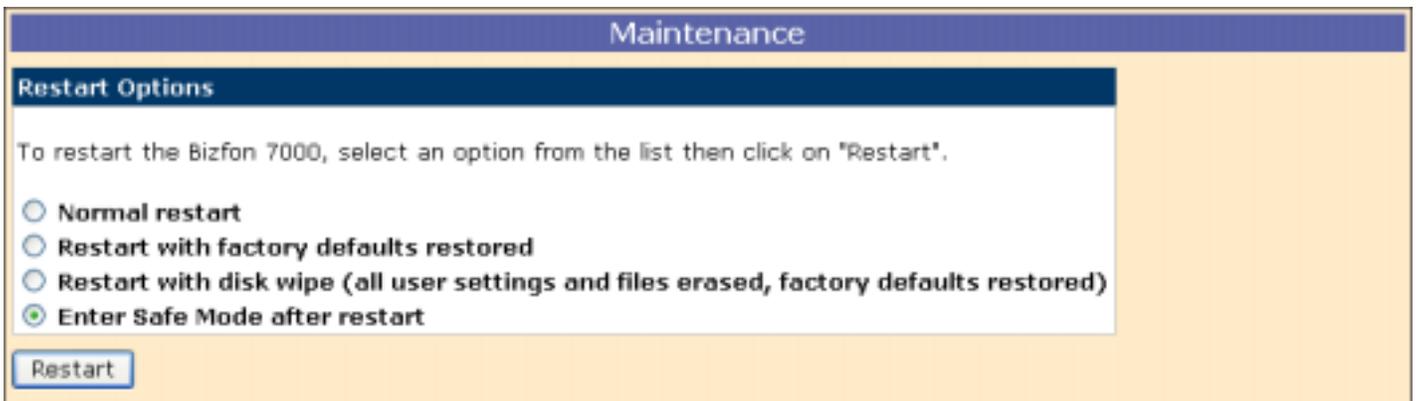


7. Click **Apply New Settings** to save your changes.
8. Click **Backup Now** or click **Start Backup Services** for the backup to begin at the time you selected. **Do not exit the OfficeSafe application. The OfficeSafe application must be running on the PC whenever a backup is performed.** You may, however, minimize the window.
9. When the backup has completed, a message appears: "Backup operation completed normally." You can save the Backup Log (as it appears in the OfficeSafe window by selecting **File>Save as**).

11.2 How to Restore Data

Use this procedure to restore backed up data to the Bizfon 7000 server. The procedures described here assume that your server can still boot. You must restore the data while the Bizfon server is in Safe Mode. When in Safe Mode, the server will always use the factory default IP address (192.168.2.254) with DHCP enabled. In order to avoid IP address conflicts on the network, it is recommended that all the LAN connections be unplugged and to plug in only the OfficeSafe PC used for configuring the restore.

10. Expand **Maintenance** and click **Restart**.



11. Select **Enter Safe Mode after restart**.
12. Click **Restart**.
13. Type "SAFEMODE" into the pop-up browser window.



14. The Bizfon server will power down and then power back up in Safe Mode.

The Bizfon 7000 is currently in **Safe Mode**. [Open System Events Window](#)

Status:

OfficeSafe

IP Address of OfficeSafe PC:

Port #: 5001

[Restore from OfficeSafe](#)

Disk Operations

[Mount](#) [Format](#)

If you have just installed a new or empty *Primary Disk*, you must *Format* it before you *Update* the software. Alternatively, you can *Restore from OfficeSafe*.

If you have just installed a new *Mirror Disk*, you should *Mount* the disks now. The mirroring will be performed during the mount. **NOTE:** Make sure you have installed the disks correctly. The *Primary Disk* (the disk that will be copied) **MUST** be installed on left side as you look at the front of the server. The *Mirror Disk* must be installed to the right of the *Primary Disk*.

Reboot Operations

The *Reboot in Normal Mode* options have been disabled because the disk (s) have not been mounted. You must first *Mount* the disk(s) before you can boot the Bizfon 7000 in Normal Mode.

Reboot in Normal Mode
 Reboot in Normal Mode with Factory Defaults restored
 Reboot in Normal Mode with Factory Defaults restored AND all user settings and files erased
 Reboot in Safe Mode

[Reboot](#)

Software Update

Two steps are required for updating the software!

- Copy Files To Bizfon 7000**

The files for the software update must first be copied to the server. To copy update files to the server, you may drag and drop the update files from an Bizfon 7000 Software Release CD using an [FTP window](#) as the destination.

- Activate the Update**

After the files have been copied to the server, they must be activated. Select the "Update" button below to perform this step.

[Update](#) (disk(s) must be mounted first!)

NOTE: If the FTP Window fails to open, you can FTP the files directly to the Bizfon 7000 system. FTP to address **192.168.2.254**. Change to directory 'update'. Make sure FTP is set to perform 'binary' transfers. See the Bizfon 7000 System Administration manual for more information.

- 15. In the **OfficeSafe** section, enter the **IP Address of OfficeSafe PC** (and where the backup data is located).
- 16. Select the **Restore from OfficeSafe** button.



17. Depending on the size of the backup data (and the performance of your network and OfficeSafe PC), it may take several minutes or longer for the backup to be restored. You will see a **Restore was successful** message in the **Status** pane when complete.
18. Select **Reboot in Normal Mode** and click the **Reboot** button.
CAUTION: Do NOT select Reboot the Bizfon 7000 in Normal Mode with Factory Defaults restored.
19. When the Bizfon server has restarted, log in.
20. Verify that the data has been restored successfully.



12 Remote IP Phone

A remote IP phone is one where the phone's local area network (LAN) is not the same as the Bizfon server's LAN. An example of this scenario is where the Bizfon server is set up at the company's main office, but an employee wants to be able to have an office phone at home such that calls to/from that phone work just as though the employee was at the company's main office.

12.1 General Network Configuration Requirements

In support of remote IP phone usage, several remote phone and Bizfon server network configurations are possible.

1. The Bizfon server can be directly connected to the Internet via its WAN port. However, the WAN cannot be in "Use PPPoE" mode.
2. The Bizfon server can be behind a single 3rd party NAT firewall. This requires specific server configuration that is described below.
3. The remote phone can be directly connected to the Internet.
4. The remote phone can be behind a single 3rd party NAT firewall.

Note: Bizfon cannot guarantee proper operation of 3rd party networking products. However, Bizfon expects this to work with typical firewalls and tests against several brands. Some NAT/Firewall configuration may be required.

12.2 Bizfon Server Behind 3rd Party NAT Firewall

To support remote IP phone usage when the Bizfon server is behind a single 3rd party NAT firewall, the server's Network Mode must be in LAN Host Mode. This can be set on the **Network / Configuration / Modify** page.

When set to LAN Host Mode, the page contains a **Public IP Address** section as shown below:

Public IP Address

If you are using a third party NAT Firewall to map a Public IP Address to the Bizfon 7000 LAN IP Address, then enter that address here, otherwise leave this field blank.

Public IP Address

NOTE

The Public IP Address is used by Bizfon 7000 VOIP services to encode the proper IP Addresses when communicating with remote SIP services or devices (such as IP Phones) when a third party NAT Firewall is between the Bizfon 7000 and the Internet.

Most third party NAT Firewalls require specific access rules to enable this functionality. Refer to your firewall documentation to map the ports shown in the table below from the Public IP Address to the Bizfon 7000 LAN IP Address:

Port(s)	Protocol
2088	UDP
5060	UDP
8081	TCP
15000-15511	UDP



As instructed on the page, enter the firewall's public internet address as the **Public IP Address**. Furthermore, the firewall must be configured to statically map specific ports through the firewall to the Bizfon server. This is described in the **NOTE** section on the page.

12.3 Remote Bizfon IP2 Phone

12.3.1 Configuration

Configuration of the remote phone requires setting two configuration parameters in the phone itself. Both are found in the **Config / Network Settings** menu on the phone.

The first is **Boot Server IP**. This is normally the IP address of the Bizfon server's WAN port which can be obtained from the server's **WAN TCP/IP Address** parameter on the **Network / Configuration** page. However, if the Bizfon server network mode is set to LAN Host, then this value will be the **Public IP Address** parameter on the **Network / Configuration** page.

The second is **Remote Plug and Play Key** (called **Remote Plug 'n' Play** on the phone menu). This key is also obtained from the Bizfon server. Go to the **Servers / VOIP Server** page. You will see a page like this:

VOIP Server		
	Current Value	Action
BLF Port	2088	
BLF Secure	disabled	
Plug 'n' Play Secret Key	3395714248	
Maximum Active Remote Calls	8	Modify
Paging Base IP Addr	239.255.10.0	
Paging Port	56586	
Paging Max Hop Count	1	
RTP Base Port	15000	

The **Plug 'n' Play Secret Key** is what should be entered into the phone.

After entering these two parameters into the phone, save the settings (the phone will automatically prompt you to do that when you exit out of the configuration menu) and then reboot the phone.

At this point the remote phone generally operates the same as any other phone on the server's LAN.

TIP: If this doesn't seem to work, restore the phone's factory defaults and re-apply the required settings.



12.3.2 Limitations

While connecting the Bizfon IP2 phone to a network behind a NAT firewall works well, there are a few limitations.

1. While intercom works fine, paging functions usually do not. More specifically, sending pages from the remote phone always works, but neither zoned nor overhead pages will be heard at the remote phone.

Solution:

Paging is implemented using IP multicasting. If all the routers between the Bizfon server and the remote phone can be configured to pass multicast packets, then this limitation can be eliminated. Setting up a VPN between the Bizfon server and the remote phone may be used to enable this functionality. A full discussion of the general networking details and the configuration of various router brands is beyond the scope of this document. However, here are the Bizfon server details necessary to accomplish this.

On the **Servers / VOIP Server** page of the Bizfon server, there are three parameters used to configure where the server transmits zoned pages:

Paging Base IP Addr – This is the multicast base IP address used by the system. Each paging zone uses the base address plus an offset. Zone 0 (the overhead zone), uses an offset of 0, zone 1 uses an offset of 1, etc. For example, if the base address was set to 239.255.10.0, then zone 2 would use multicast IP address 239.255.10.2.

Paging Port – This is the UDP port number that the packets are sent to. All zones use the same port number (but each have their own multicast IP address).

Paging Max Hop Count – This value controls the time-to-live (TTL) count in the IP header of all paging UDP/RTP frames. Typically this value is set to 1 such that the packet won't be sent beyond the local subnet. However, if you have multiple subnets with phones on them, this value will need to be increased.

2. When there are multiple phones each at different remote locations and all behind their own NAT firewalls, there may be problems passing audio between them when one calls another.

Solution:

Statically map (one to one) the remote phone's RTP ports through the NAT firewall. This requires two steps.

The first step is to identify and possibly change the RTP ports used by the phone. Normally, a large range of ports are used. Because setting up a one to one mapping in the firewall may be a time consuming manual operation, you will want to reduce the number of ports used.

Go to the **Phone Options** section of the **Phone System / Handsets / View Configuration** page for the Bizfon IP2 remote phone. The **RTP Media Port Range** parameter is the range of ports to be used by this phone.

This is configurable. Two ports are required for each active "conversation" on the phone. The phone's intercom capability counts as a "conversation". A conference call uses two ports for each remote caller.



There are reasons why having a bigger range than absolutely necessary is good. However, when you have to manually map the ports through a firewall, you'll want to dramatically reduce the large default range to something you are willing to type into your firewall configuration. A suitable number would be 10 ports.

Modify the **Phone Options** to change the **RTP Media Port Range** parameter to reduce the maximum range.

The second step is to modify the NAT firewall configuration. You want to one-to-one map each of the RTP ports through the firewall such that packets arriving at those ports on the firewall's WAN interface are routed to the phone that is inside the NAT firewall. The directions for doing this are unique to each NAT firewall product and therefore beyond the scope of this description.

3. Internet Telephony Service Provider (ITSP) services configured on the Bizfon server may not be accessible from remote phones that are behind NAT firewalls.

Solution:

Statically map (one to one) the remote phone's RTP ports through the NAT firewall. This requires the same two steps as described in limitation 2 above.

12.4 Remote Non-Bizfon IP2 Phone

In addition to support for the Bizfon IP2 phone, the Bizfon server supports other remote SIP phones as well. Steps for configuring these are unique to each phone model and brand.

13 Call Routing

13.1 Call Routing Concepts

13.1.1 Introduction

When we think of calling an extension, we think of the system causing a particular phone to ring. Thus, if I tell you that my office extension is 106, you expect my office phone to ring when you dial it. Yet, we can imagine some circumstances under which my phone will not ring when you dial 106. For example, if I'm already on the phone, the system may send your call directly to my voicemail rather than give you a busy signal. The Bizfon 7000 call routing feature allows a call to an extension to be flexibly directed in this as well as other ways.

Some of these other ways are:

- Two phones might ring at the same time with either being able to answer the call.
- One phone might ring for 4 rings; then if no answer, another phone will ring.
- The call will be sent to a particular user's voice mail.
- The call will be sent to an auto attendant.
- The call will be sent to a call queue.
- The call will be routed differently depending on who the caller is (using CallerID).
- The call will be routed differently if the person being called is in their office vs. at a meeting.

In this section, we will explain the concepts necessary to understand how to configure these capabilities.

13.1.2 Connection Attempt

Suppose that I have an administrative assistant, that I am expecting an important phone call, and that I don't want the caller to have to leave a voicemail message. I'd like to tell the system to first attempt to reach me by ringing my office phone. If I don't answer in 4 rings, then I want the system to call my assistant's phone (using a distinctive ring so she'll know it is a call for me). The Bizfon 7000 calls each of these attempts to reach someone a "connection attempt." In this example, the system will be instructed to make two connection attempts. The first connection attempt is to ring my office phone 4 times. If no answer, then it should initiate a second connection attempt that will call my assistant.

One connection attempt can ring more than one phone. Suppose that during my work day, I often move back and forth between my office and my lab. I don't want to miss any calls, so I would like the system to ring both phones at the same time and let me answer the call from either one. This would be set up as one connection attempt, but with two phones in it.

13.1.3 Finally Clause

If the system can't get someone to answer the phone in any of the connection attempts, then we might like the call to be directed to our voicemail (or the auto attendant or to another dialed number or ...). This last direction for the call is called the "finally" clause. It tells the Bizfon server what to finally do after all connection attempts have failed. If no connection attempts are defined, then the call is immediately directed to the finally clause.

13.1.4 Primary Route, On-Busy Route, and Call Route

We have seen how the system seeks to find someone to answer a call. It does this by following the directions specified in a series of connection attempts and a finally clause. The Bizfon 7000 refers to this as a "primary route".



What should the system do with the call if a particular connection attempt in a primary route is busy (the phone is busy)? Normally, the system will consider the attempt failed and go on to the next connection attempt (or the finally clause). This is the same action taken as if the phones weren't answered. What if I want to take a different action if the phones are busy? This can be specified via an optional "on-busy route". Just like the primary route, it is made up of connection attempts and a finally clause. The system uses it to direct a call whenever a connection attempt in the primary route is busy.

The combination of a primary route and an optional on-busy route forms a "call route".

13.1.5 CallerID Dependant Call Routes

Suppose that I want to ensure that all calls from a VIP reach me. If my office phone doesn't answer, I want the system to call my cell phone. I can set the finally clause to dial my cell phone, but can I do this only if the VIP is calling? The Bizfon 7000 supports multiple call routes where the call route to use for a given call can depend on a CallerID pattern match. For example, if the VIP's phone is 585-123-4567, then I can create a unique call route that will only be used when the incoming CallerID matches that number. One call route is always designated to be used for non-CallerID-dependant calls.

13.1.6 Presence

I would like to easily change my call route depending on where I am. If I'm on vacation, I don't want to waste my caller's time waiting for my phone to ring 4 times when I know I won't be there to answer it. If I'm on a business trip, I may want my calls to immediately call my cell phone. The Bizfon 7000 remembers each user's presence. Each presence can have one or more call routes associated with it. So, when I tell the server that my presence has changed, it immediately begins to use the call routes that are set for my new presence. I don't need to take the time to reconfigure my call routes, just change my presence.

13.1.7 User Extensions and System Extensions

The Bizfon 7000 has two types of extensions: user and system. Only a user has a presence. A system extension has call routes without any presence setting.

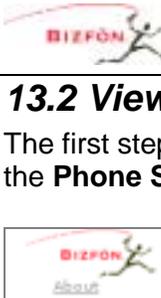
13.1.8 Concept Summary

User Extension

- Every user extension has a presence setting.
- Each possible presence has one or more call routes associated with it.
- The selection of which call route to use can depend on the incoming call's CallerID. One call route is independent of the incoming call's CallerID.
- Each call route contains a primary route and an optional on-busy route.
- Each route contains a series of zero or more connection attempts followed by a finally clause.
- Each connection attempt can ring one or more phones.
- The finally clause is executed when all connection attempts have failed to find someone to answer the call. It directs the call to voicemail, the auto attendant, dial a new number, etc.

System Extension

- Each system extension has one or more call routes associated with it. There is no presence setting to choose a set of call routes.
- In all other ways, it behaves exactly like a user extension.



13.2 View and Change a Call Route

The first step to changing a call route is to select the extension whose call routes you wish to change. Go to the **Phone System / Extensions** page.

The screenshot shows a web interface for 'Phone System' with a breadcrumb trail 'Home > Phone System > Extensions'. A table titled 'Extensions' is displayed with the following data:

Ext.	Description	Action
		Add New Extension
0	Operator	View Call Routes
100	Susan Bell (susan)	View Call Routes
101	Thomas Brown (tom)	View Call Routes
102	Joseph Andrews (joe)	View Call Routes
199	System Administrator (admin)	View Call Routes

The left sidebar contains a navigation menu with categories: Phone System (Audit PBX Codes, Auto Attendants, Call Blocking, Call Queues, Dialing Rules, Extensions, Handsets, Outside Lines, Speed Dial), Business, Network, Servers, Reports, and Maintenance. At the bottom of the sidebar are links for 'Need help?' and 'Install Checklist', and a '(Logout)' button.

Click on the **View Call Routes** link of the extension you want to change.



Home > Phone System > Extensions > View Call Routes

Phone System

Call Routes For Extension 100 - Susan Bell (susan)

Presence: In Office --- Active ---		New Call Route
On calls from (603) 555-1212		
transfer to Voice Mail for Joseph Andrews (joe)		Modify Delete
On calls from all other callers		
transfer to Voice Mail for Susan Bell (susan)		Modify

Presence: At A Meeting		New Call Route
On calls from all callers		
First connection attempt: Susan Bell (Login ID:5100) for 4 rings (Ring Type 5)		Modify
Finally: transfer to Voice Mail for Susan Bell (susan)		

Presence: On Vacation		New Call Route
On calls from all callers		
transfer to Voice Mail for Susan Bell (susan)		Modify

Presence: On Business Trip		New Call Route
On calls from all callers		
transfer to Voice Mail for Susan Bell (susan)		Modify

Presence: At Home		New Call Route
On calls from all callers		
transfer to Voice Mail for Susan Bell (susan)		Modify

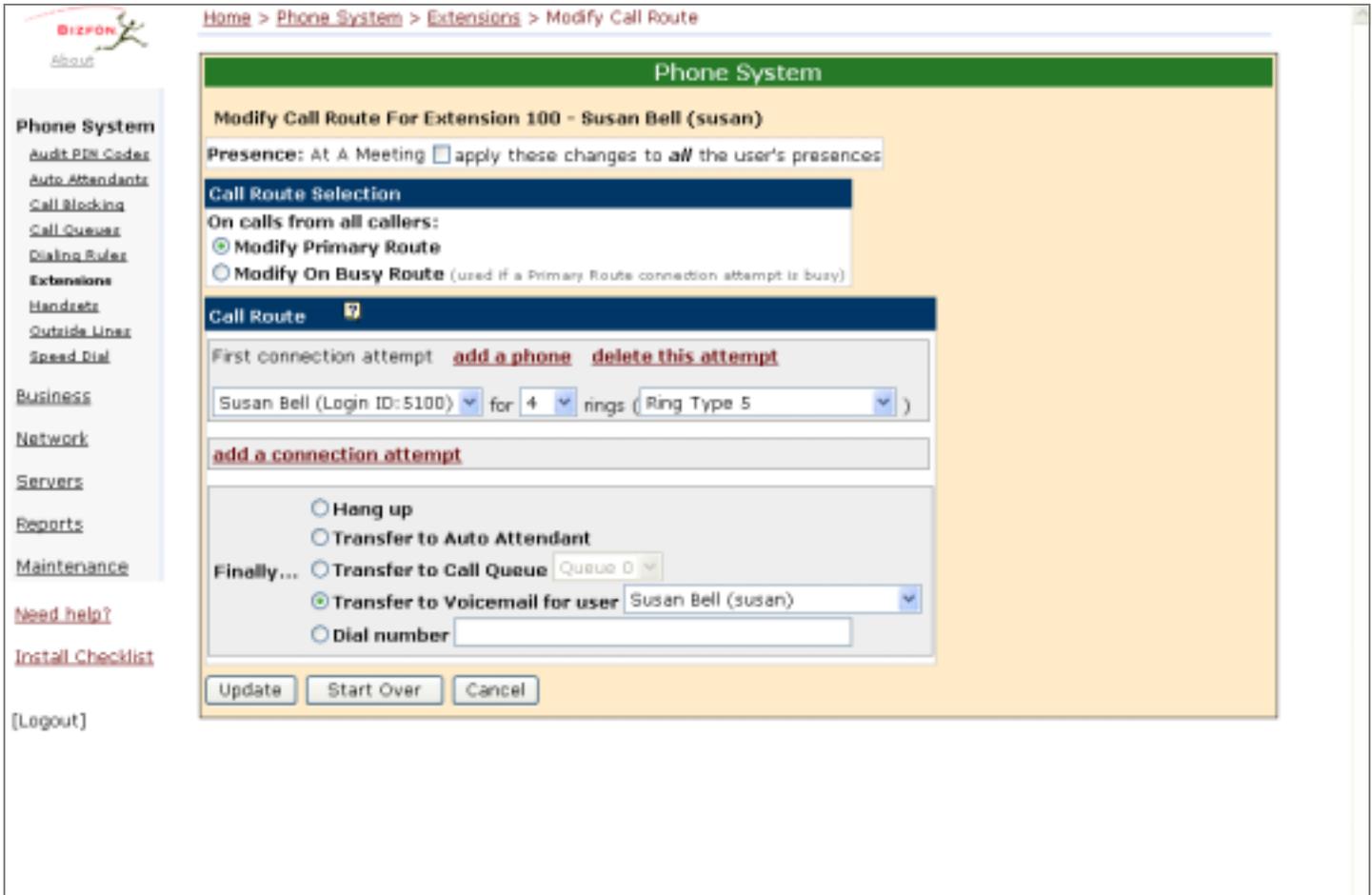
Presence: Away		New Call Route
On calls from all callers		
transfer to Voice Mail for Susan Bell (susan)		Modify

Presence: Busy		New Call Route
On calls from all callers		
transfer to Voice Mail for Susan Bell (susan)		Modify

Notice that each presence has its own set of call routes. If there is only one call route defined for a presence, it applies to all incoming calls. If more than one is defined, all but one has a CallerID pattern to match incoming calls against.

The system must always have a call route that is independent of the incoming call's CallerID. It creates a default call route for this when the extension is created. This call route may not be deleted (notice that no **Delete** link is offered). There can only be one call route like this for each presence. So, when creating a new call route, it must be one that is CallerID dependent. These call routes can be deleted.

To change a particular call route, click its **Modify** link.



Home > Phone System > Extensions > Modify Call Route

Phone System

Modify Call Route For Extension 100 - Susan Bell (susan)

Presence: At A Meeting apply these changes to **all** the user's presences

Call Route Selection

On calls from all callers:

Modify Primary Route

Modify On Busy Route (used if a Primary Route connection attempt is busy)

Call Route

First connection attempt [add a phone](#) [delete this attempt](#)

Susan Bell (Login ID: 5100) for 4 rings (Ring Type 5)

[add a connection attempt](#)

Hang up

Transfer to Auto Attendant

Finally... Transfer to Call Queue Queue D

Transfer to Voicemail for user Susan Bell (susan)

Dial number

Most of the configuration options on this page should be comprehensible after reading the *Call Routing Concepts* section above. Some additional explanation follows.

Notice the presence setting displayed near the top of the page. Next to it is a checkbox to apply changes made here to all presences. If this call route has no CallerID pattern specified (it is the “all calls” call route), then this call route is copied to the “all calls” call route in all the other presences. If this call route has a CallerID pattern specified, it is copied to the same CallerID patterned call routes in the other presences, creating new call routes if necessary.

To delete a phone from a connection attempt, choose “no selection” from the call appearance drop down list.

To set up a connection attempt so it properly participates in the ringing of a line appearance PFK on an Bizfon IP2 phone, select “Key System Ring Delay” from the call appearance drop down list. See XXX for more information.

Recall that the on-busy route is optional. An inactive on-busy route is one with no connection attempts and a finally clause set to **Hang up**. To make it active, add one or more connection attempts and/or change the finally clause. To make it inactive again, just change it back to the inactive state (delete all connection attempts and set the finally clause to **Hang up**).



13.3 Changing a User's Presence Setting

13.3.1 Changing Presence Via an Bizfon IP2 Phone

A user's presence can be changed via an Bizfon IP2 phone. When the **Mute/DND** button is held down for greater than 1 second, a presence menu will appear. See the "User Guide – Bizfon IP2" for more information.

13.3.2 Changing Presence Via Any Phone

A user's presence can be changed using any phone connected to an Bizfon 7000 by accessing the user's message center inbox. See the "Phone and Voice Mail Guide" for more information.

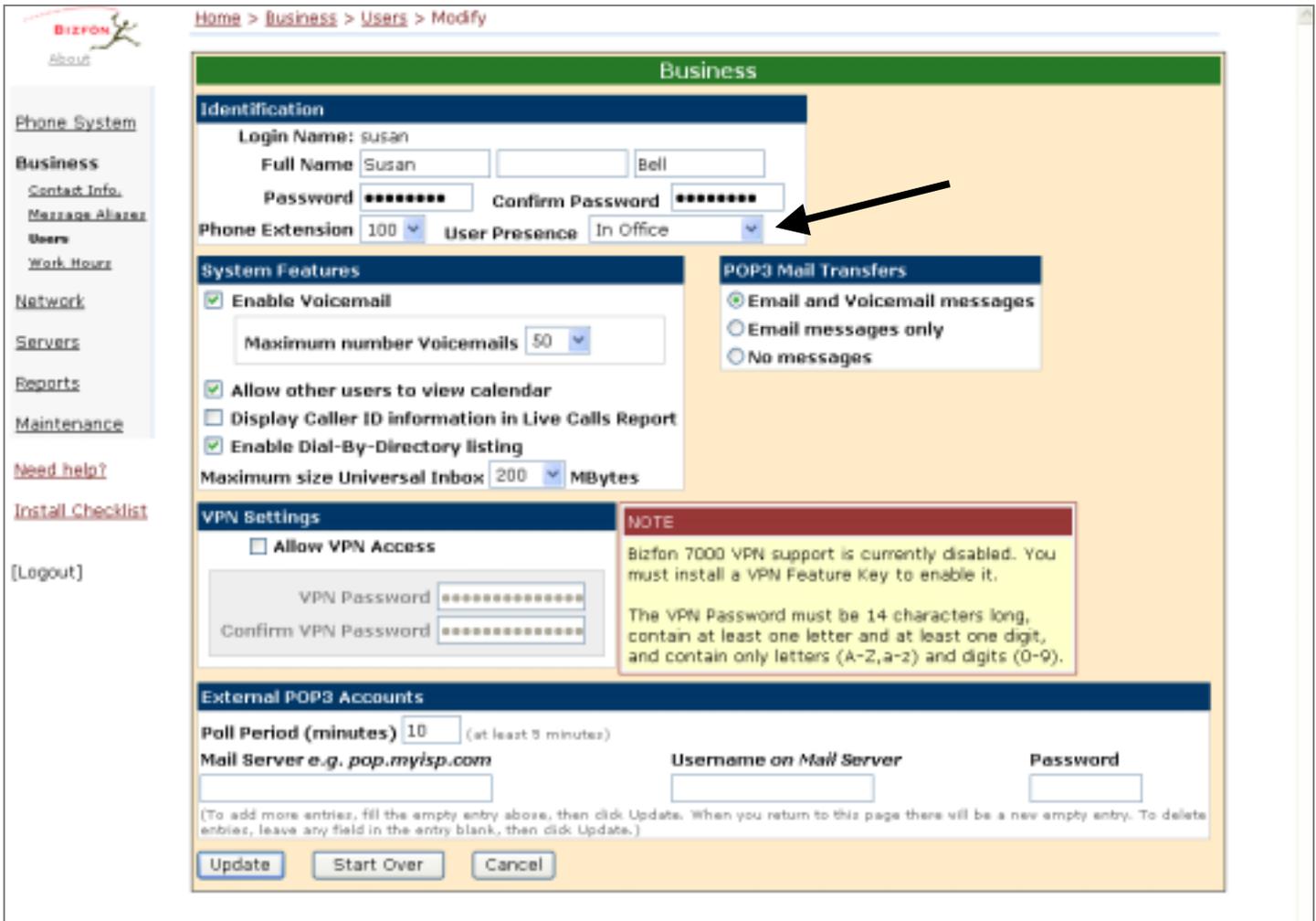
13.3.3 Changing Presence Via the User Intranet Web Site

A user can login to the Bizfon server's intranet web site to change her own presence setting. The URL is the server's LAN IP address or "corp." followed by the server's configured domain name (example, corp.myBizfon.com).



13.3.4 Changing Presence Via the Administrative Web Page

Although users can change their own presence setting, the Bizfon 7000 system administrator can change a user's presence by going to the **Business / Users** page, clicking on the **Modify** link of the user to change, and changing the **User Presence** setting.



13.4 Outside Line Call Routing

Outside lines (of any type: CO line, SIP Proxy, SIP GW, DID Block) have a call route associated with them. Go to **Phone System / Outside Lines** and click the **Modify** link on one of the CO lines.



Home > Phone System > Outside Lines > Modify Outside Line

Phone System

Outside Line

Description (typically enter phone number of line connected to the Bizfon 7000)

Port: 01

Enable Line Appearance

Features

Line has Caller ID service

Enable Loop Filters (typically checked, unchecked to improve echo performance on short loops)

Prefix Digits (digits dialed by the Bizfon 7000 after it seizes the line, before user dials)

CPC timer milliseconds
(Open Loop Disconnect)

Default Auto Attendant

Select the attendant used to answer when calls received from this source are routed to an Auto Attendant.

Call Route

Calls received from this CO line go to:

Extension

Auto Attendant

Voicemail for user

The Call Route section determines how a call coming into the system on this CO line is directed. The options shown are mostly self-explanatory. Below is some additional information.

The Bizfon 7000 supports multiple auto attendants. When a call is routed to an auto attendant, it goes to the designated default auto attendant for this outside line.

To use the full flexibility of the Bizfon 7000 call routing for any call from an outside line, set the outside line's call route to go to a system extension. Then configure whatever routing is desired for the system extension. Using this, outside calls can be directed in ways such as:

- Route to one phone and then another
- Route to multiple phones concurrently
- Route to a call queue

13.5 Example Call Route Configurations

13.5.1 Example 1: Ring 1 Phone, Then Voicemail

Requirements:

When Susan is in her office and a call is made to her extension, her phone should ring distinctively for inside vs. outside calls (an inside call makes a single ring and an outside call makes a double ring). If she doesn't answer in 4 rings, the call should be directed to her voicemail.

Configuration:

Modify the CallerID independent call route associated with Susan's In Office presence such that it has:

- One connection attempt where:



- The phone is Susan's office phone
- The number of rings is 4
- The ring type is **Single (int), Double (ext)**
- Finally clause set to transfer the call to Susan's voicemail

13.5.2 Example 2: Ring 1st Phone, Then ring 2nd Phone, Then Voicemail

Requirements:

Irregardless of Susan's presence, when a call is made to her extension, her phone should ring. If she doesn't answer in 4 rings, then her administrative assistant's phone should ring with a distinctive ring so he knows it is a call for Susan. If he doesn't answer in 4 rings, the call should be directed to Susan's voicemail.

Configuration:

Modify the CallerID independent call route associated with Susan's In Office presence such that it has:

- First connection attempt where:
 - The phone is Susan's office phone
 - The number of rings is 4
 - The ring type is **Single (int), Double (ext)**
- Second connection attempt where:
 - The phone is Susan's assistant's office phone
 - The number of rings is 4
 - The ring type is **Ring Type 4**
- Finally clause set to transfer the call to Susan's voicemail
- Select the checkbox to apply these changes to all Susan's presences

13.5.3 Example 3: CO Line Rings 2 Phones, Then ring 3rd Phone, Then Voicemail

Requirements:

Instead of having calls from a CO line go to the auto attendant, the calls should be answered live whenever possible. Tom and Joe work in telephone sales and are responsible for talking with customers. Their manager, Susan, will talk with customers if both Tom and Joe are busy. If no one answers the call, it should be transferred to Tom's voicemail.

Configuration:

Create a system extension for sales. Change the CO line's call route so that incoming calls go to the sales extension. Modify the sales extension call route such that it has:

- First connection attempt where 2 phones are specified:
 - The 1st phone is Tom's office phone, 4 rings, ring type is **Ring Type 4**
 - The 2nd phone is Joe's office phone, 4 rings, ring type is **Ring Type 4**
- Second connection attempt where:
 - The phone is Susan's office phone, 4 rings, ring type is **Ring Type 4**
- Finally clause set to transfer the call to Tom's voicemail



14 Key System Behavior

The Bizfon server and Bizfon IP2 phones can be configured to behave like a key system.

14.1 Example Configuration

Requirements:

An insurance agent called Best Insurance is provisioned with 3 CO lines. The office is staffed by 5 employees, with each having an Bizfon IP2. The system will behave like a key system with a PFK on each phone mapped to each of the CO lines. Using the PFK, each user will be able to monitor and directly answer each of the CO lines. If not answered, an incoming call should ring 6 times before routing to a central (not individual user) voice mail for the office.

Configuration:

1. Create a generic user on the system to receive the central voice mail for the office. Call the user "Best Insurance".
2. Create a system extension to route all incoming calls. Set up the call route so that it has one connection attempt with Key System Ring Delay as the call appearance (phone) that will ring 6 times. Configure the call route Finally clause to transfer to voice mail for user "Best Insurance".
3. For each CO line, check the **Enable Line Appearance** checkbox on the **Phone System / Outside Lines / Modify** page. Configure the call route for each CO line so all calls go to the created system extension.
4. For each Bizfon IP2, configure a line appearance PFK for each CO line. See *PFK Function Selections*.

15 Direct Inward Dialing (DID)

Direct inward dialing (DID) is a service offered by a local telephone company that provides a block of phone numbers for calling into a PBX without requiring a physical line for each number. In cooperation with the PBX, each number is mapped to a PBX extension so that each PBX user has a unique outside number that can be used to ring the user's phone directly rather than directing the incoming call to an auto attendant.

Configuring the Bizfon server for DID service involves 3 steps:

1. Creating a DID block.
2. Configure the call routing plan for the DID block.
3. Create a DID line for each DID trunk line plugged into the server.

15.1 Create a DID Block

Click on the **New DID Block** link on the **Direct Inward Dial Blocks** section of the **Phone / Outside Lines** page.



The screenshot shows the Bizfon web interface for creating a new DID block. The breadcrumb trail is "Home > Phone System > Outside Lines > New DID Block". The main content area is titled "Phone System" and contains a "DID Block" form. The form has three input fields: "Starting Phone Number", "Total number of phone numbers in the DID Block", and "DID Routing Plan" (a dropdown menu currently set to "make new Routing Plan"). Below the form are "Add" and "Cancel" buttons. On the left side, there is a navigation menu with categories: "Phone System" (containing links for Audit PIR Codes, Auto Attendants, Call Blocking, Call Queues, Dialing Rules, Extensions, Handsets, Outside Lines, and Speed Dial), "Business", "Network", "Servers", "Reports", and "Maintenance". At the bottom of the menu are links for "Need help?", "Install Checklist", and "[Logout]".

Enter the **Starting Phone Number** and **Total number of phone numbers in the DID Block** as specified by the telephone company. Unless you already have an existing **DID Routing Plan** that you want use, leave it as the default to make a new routing plan. As it says, this creates a new routing plan for use by this DID block.



15.2 Configure a Call Routing Plan for the DID Block

After the DID block is created, look at the **Direct Inward Dial Blocks** section on the **Phone System / Outside Lines** page to see the routing plan associated with the block.

Direct Inward Dial Blocks	
Block	Action
	New DID Block
(585) 865-1100 Numbers: 10 Plan: Routing Plan 1	Modify Delete

Note the **Plan** parameter value. Find it in the **Direct Inward Dial Routing Plans** section on the **Phone System / Outside Lines** page. To configure the routing plan, click on the **Details** link associated with the routing plan.

Home > Phone System > DID Routing Plan

Phone System

Routing Plan Information

Description	Routing Plan 1	
Default Extension	0 - Operator	Modify
DID Blocks using this plan	(603) 893-1100 / 10 numbers	

Phone Number to Extension Mapping

Phone Number	Extension	Action
		Add New Entry

TIP

Phone Numbers that do not appear in the table to the left use the Default Extension for this DID Block as defined above.

To remove a phone number from the table, select [Modify](#), then change the number to use the default extension.

Phone System navigation menu:
[Audit PIR Codes](#)
[Auto Attendants](#)
[Call Blocking](#)
[Call Forward](#)
[Dialing Rules](#)
[Extensions](#)
[Handsets](#)
[Outside Lines](#)
[Speed Dial](#)
[Business](#)
[Network](#)
[Servers](#)
[Reports](#)
[Maintenance](#)
[Need help?](#)
[Install Checklist](#)
 [Logout]

The routing plan specifies a mapping for each DID phone number to an Bizfon server extension. The **Default Extension** will be used as the mapping for any phone numbers not explicitly specified in the **Phone Number to Extension Mapping** list.



15.3 Create the DID Lines

The last step in configuring the Bizfon server to use DID lines is to configure each of the analog lines that have DID trunk lines plugged into them. Look at the **Analog Outside (CO) Lines** section of the **Phone System / Outside Lines** page.

Analog Outside (CO) Lines			Scan For New
Outside (CO) Line	Type	Port	Action
01	FXO	01	Modify Delete
02	FXO	02	Modify Delete
	---	03	New FXO Line
	---	04	New FXO Line New DID Line
	---	05	New FXO Line New DID Line
	---	06	New FXO Line New DID Line
	---	07	New FXO Line New DID Line
	---	08	New FXO Line New DID Line
	---	09	New FXO Line New DID Line
	---	12	New DID Line
	---	13	New DID Line
	---	14	New DID Line

Click on **New DID Line** for each port where a DID trunk line is plugged in.



The **Number of digits sent by CO to identify DID number** must be as specified by the telephone company. Select the **DID Block** created earlier.



16 Web, FTP, and CIFS

16.1 Web Sites

The Bizfon server supports a variety of web sites: administrative and user, internal (LAN) and external (WAN), auto-generated and customized content, system information and user information. These will be described below.

The custom content must be HTML only. No server side scripting languages (ASP, server side Java, Cold Fusion, CGI) are supported.

LAN side Web servers are protected from WAN access when the Bizfon server is in one of the network modes that turns on the firewall.

The following terms will be used in the URL and UNC specifications:

- **DomainName:** This is the DNS domain name specified for the Bizfon server on the **Network / Configuration** page.
- **LANSideServerName:** This is the DNS name of the Bizfon server at the LAN address, *corp.DomainName*. Alternatively, it can be the LAN IP address.
- **WANSideServerName:** This is the DNS name of the Bizfon server at the WAN address, *www.DomainName*. Alternatively, it can be the WAN IP address
- **HostName:** This is the host name specified for the Bizfon server on the **Network / Configuration** page.
- **LoginName:** This is the login name of a user on the Bizfon server.

16.1.1 Internal Administration Web Site

The Bizfon server supports an internal (LAN) web site that provides the administrative interface to the server. Two versions of this are available.

- Normal Mode Administrative Web Site: Access to this web site is gained via **http://LANSideServerName:8080**.
- Safe Mode Administrative Web Site: Access to this web site is gained via **http://192.168.2.254:8080**. The safe mode administrative web site is only available when the server boots up in safe mode.

16.1.2 Internal System Info Web Site

The Bizfon server hosts an internal (LAN) company web site that shows a variety of company information including a directory of users, a phone feature guide, distribution lists, a live calls report, etc. From the directory of users, a link to more specific information for each user is available.

To view the web site, go to **http://LANSideServerName**.

16.1.3 Internal Custom System Web Site

The Bizfon server hosts an internal (LAN) company web site composed of custom HTML content.

To view the web site, go to **http://LANSideServerName/export/public/website/**.

To add, delete, and modify the files for the web site, use **ftp://LANSideServerName/public/website** or use Windows file sharing (CIFS) to **\\HostName\public\website**.



16.1.4 Internal Custom User Web Site

The Bizfon server hosts internal (LAN) per-user web sites composed of custom HTML content.

To view the web sites, go to **http://LANSideServerName/export/users/LoginName/website/**.

To add, delete, and modify the files for the web site, use **ftp://LANSideServerName/users/LoginName/website** or use Windows file sharing (CIFS) to **\\HostName\users>LoginName\website**.

16.1.5 External Custom Web Site

The Bizfon server hosts an external (WAN) company web site composed of custom HTML content.

To view the web site, go to **http://WANSideServerName**.

To add, delete, and modify the files for the web site, from a PC on the LAN use **ftp://WANSideServerName** or Windows file sharing (CIFS) to **\\HostName**.

16.2 Internal FTP Site

The Bizfon server supports an internal (LAN) FTP site that can be used to store and retrieve files from the LAN. No FTP user/password is required to gain access. The URL for the FTP site is **ftp://LANSideServerName**.

16.3 External FTP Site

The Bizfon server supports an external (WAN) FTP site that can be used to retrieve files from the WAN. This site is read-only from the WAN. No FTP user/password is required to gain access. The URL for the FTP site is **ftp://WANSideServerName**.

To add or delete files from the site, use **ftp://WANSideServerName** from a PC on the LAN.

16.4 Internal CIFS

When the file server is enabled on the **Servers / File Server** page, the Bizfon server supports an internal CIFS file server. No file permissions are supported. Access is via the UNC path **\\HostName**.



17 Call Queues

Note that this is an optional feature that requires a feature key.

Call queues are useful when incoming calls may not be able to be immediately answered “live”, but will be able to be answered after some delay. The incoming calls go into a “hold” queue and agents (people responsible for answering calls from a queue) can answer each call in first-in-first-out (FIFO) order. The Bizfon IP2 phone provides rich support for working with call queues. All other phones provide only very limited ability to work with this feature.

Some of the available features are:

- The caller will hear an initial greeting message when entering the queue. In addition, a status message will replay periodically to all calls in the queue. The replay interval can be configured. These messages can be system default messages or custom messages.
- Using an Bizfon IP2 phone, an agent can login (or logout) his phone to the group responsible for handling a particular call queue. Once logged in, his phone may ring when calls are in the queue, he can monitor the status of the queue, and he can answer calls in the queue. The conditions under which the agent’s phone will ring can be configured, thus providing significant flexibility in managing the call queue.
- A queue can be configured with a maximum call wait time after which a call can be hung up, transferred to an auto attendant, or transferred to a specified user’s voice mail.

To be able to use call queues:

- The feature key must be installed.
- The queue must be configured.
- The agent’s Bizfon IP2 phone must be configured.
- The agent must login his phone and answer calls in the queue.
- The system must be configured to route calls to the queue.

17.1 Configuring a Queue

The first step in using call queues is to configure one of the queues. Go to the **Phone System / Call Queues** page. You will see a page like this:



Home > Phone System > Call Queues

Phone System

The table below displays the current settings for the Call Queues.
You can also [manage the content](#) of the messages played by the Call Queues.

NOTE

The Call Queue Feature Key has not been installed on this system. You may configure the queues, but they will not function until the feature key has been installed.

Call Queues				
Queue	Replay Status Message (secs)	Max. Wait (minutes)	After maximum wait is reached, or caller presses 0, then...	Action
0 Queue 0	60	30	transfer caller to Default Auto Attendant	Modify
1 Queue 1	60	30	transfer caller to Default Auto Attendant	
2 Queue 2	60	30	transfer caller to Default Auto Attendant	
3 Queue 3	60	30	transfer caller to Default Auto Attendant	
4 Queue 4	60	30	transfer caller to Default Auto Attendant	
5 Queue 5	60	30	transfer caller to Default Auto Attendant	
6 Queue 6	60	30	transfer caller to Default Auto Attendant	
7 Queue 7	60	30	transfer caller to Default Auto Attendant	
8 Queue 8	60	30	transfer caller to Default Auto Attendant	
9 Queue 9	60	30	transfer caller to Default Auto Attendant	

[Logout]

The system supports 10 queues. To configure a queue, click the **Modify** link. Then click the **change** link on the queue you want to configure. This brings up a browser pop-up like this:



Queue Termination Option - Microsoft Internet Explorer

Call Queue

Description

Replay Status Message (30 - 600 seconds, 0 = no status)

Maximum Wait (1 - 120 minutes, 0 = wait forever)

After maximum wait time, then:

Hang up

Auto Attendant

Voice mail for user

[Done](#) [Cancel](#)

Change **Description** to something meaningful to you as the system administrator (example: "Customer Support"). The number in the **Replay Status Message** parameter is the interval, in seconds, between replays of the queue status message to waiting callers. The **Maximum Wait** parameter is the maximum time, in minutes, that a call will wait in the queue (unanswered) before moving to one of the final dispositions shown.

Note that if the caller presses 0 while in the queue, the call exits the queue just as if the maximum wait time was reached. This is especially useful if the final disposition of a call is **Auto Attendant** or **Voice mail** since the caller can exit the queue early without hanging up. When recording a custom queue greeting or status message (see *Managing Custom Queue Message Content*), you may want to mention this feature so your callers know about it.

When finished with the configurations on this page, click the **Done** link and then the **Update** button on the previously waiting page (**Phone System / Call Queues / Modify**).

17.1.1 Managing Custom Queue Message Content

The server comes with default messages for the initial greeting when a call enters a queue and the status message that is replayed periodically. To customize these messages, you can either record new messages directly into the server using the phone or record them via some other means and transfer the audio files to the server. The instructions for doing this can be found by clicking on the **manage the content** link near the top of the **Phone System / Call Queues** page.



17.2 Servicing a Queue with an Bizfon IP2 Phone

17.2.1 Configuring the Phone

An Bizfon IP2 phone can be configured such that one of its programmable function keys (PFK) can monitor the status of a queue and allow the user to answer a waiting call. This type of PFK is called a “queue appearance”. To configure the PFK, go to the **Phone System / Handsets** page and click on the **View Configuration** link for the phone you want to configure. You will see a page like this:

Home > Phone System > Handsets > View Configuration

Phone System

BizTouch IP2
 MAC: 00-0a-dd-81-07-de
 Call Appearances:
 Susan Bell

Template Options

Save save this handset configuration in a template
 Apply apply the selected template to this handset configuration
 IP2 (Factory - Key) ▼

NOTE
 It is necessary to reboot this Bizfon 7000 phone for changes to take effect.
[Reboot phone now](#)

Programmable Function Keys
 Station Mode: PBX Behavior

Key	Type	Action
12	(not defined)	Modify
11	(not defined)	
10	(not defined)	
9	(not defined)	
8	(not defined)	
7	(not defined)	
6	(not defined)	
5	(not defined)	
4	(not defined)	
3	(not defined)	
2	Call Appearance Susan Bell, Ring Type: AUTO	
1	Call Appearance Susan Bell, Ring Type: AUTO	

Phone Options

Values marked with * may be overridden by the user of the phone. These values are restored when the user of the phone restores factory defaults.

	Value	Action
Call History Size	99 *	
Clock Mode	12 Hour *	

Click the **Modify** link in the **Programmable Function Keys** section. You will see a page like this:



Home > Phone System > Handsets >

Phone System

BizTouch IP2
 MAC: 00-0a-dd-81-07-da
 Call Appearances:
 Susan Bell

NOTE
 It is necessary to reboot the Bizfon 7000 handset for changes to take effect.

TIP
 Outside Lines that are enabled for Line Appearance can be automatically assigned to Programmable Function Keys on the phone. Click the button below to assign the Outside Lines.

 The server has no Outside Lines configured for Line Appearance at this time.

Programmable Function Keys
 Station Mode: PBX Behavior

Key	Type
12	Not Used
11	Not Used
10	Not Used
9	Not Used
8	Not Used
7	Not Used
6	Not Used
5	Not Used
4	Not Used
3	Not Used
2	Call Appearance Susan Bell Ring Type: AUTO change
1	Call Appearance Susan Bell Ring Type: AUTO change

Select a PFK to designate for this queue, click the drop down arrow, and select **Queue Appearance** for this PFK's function. Then click the **define** link that appears. This will bring up a browser pop-up like this:



On this page, the first selection is to choose the particular **Call Queue** to be designated for this PFK. Next is a checkbox to specify that the phone should automatically **Login** to the agent group responsible for servicing the queue. The **Ring Type** might be set to a unique type for this phone so that the agent can easily distinguish calls in the queue from other calls to his phone.

As you can see, the page contains a description of most of the parameters. These parameters control the ring behavior for this agent's phone when a call is in the queue. Using this, you can configure the handling of calls in a flexible manner.

17.2.2 Agent Phone Configuration Example

Requirements:

Suppose you have 3 agents to handle calls in a Customer Support queue. You desire Agent 1 and Agent 2 to answer most of the calls, while allowing calls to “overflow” to Agent 3 when necessary. Furthermore, you want to give each agent 2 minutes to finish updating a log about the previous call before their phone will ring with a new call in the queue. You can achieve this by configuring each of the agent's phones as follows:

Agent Phone Configurations:

	Wait Period	Number of Callers	Rest Time
Agent 1	0 seconds	1	120 seconds
Agent 2	0 seconds	1	120 seconds
Agent 3	180 seconds	5	120 seconds



Commentary:

Agent 3's phone will ring when any call has been in the queue for 3 minutes (or 5 or more callers are in the queue). This might happen because Agents 1 and 2 are:

- Already talking to other callers in the queue.
- Away from their desk.
- Have finished with their previous call, but are in their 2 minute rest interval.
- Are ignoring their ringing Customer Support queue appearance because they are on another phone call, talking with someone in their office, etc.

17.2.3 Logging in and out of the Queue

When an agent's phone is not logged in to the agent group responsible for handling calls from a queue, the queue appearance button will be red and the agent's phone will not ring when a call is in the queue.

While not logged in to the agent group for the queue, the queue appearance PFK will flash red when a call is in the queue. If the agent momentarily hits the queue appearance PFK while flashing red, he can answer the next call in the queue.

To login to the agent group for that queue, hold down the queue appearance button for 1 ½ seconds. The light on the button will then either go out if there are no calls in the queue or flash green if there are waiting calls.

To logout, hold the queue appearance button for 1 ½ seconds and the button will change to red indicating that you are logged out.

Note that the auto-login checkbox can be checked on the queue appearance PFK configuration page so that the agent's phone is automatically logged in when the phone is rebooted. Then, unless the agent logs out, his phone will always be in the agent group responsible for handling calls in that call queue.

17.3 Servicing a Queue with a Non-Bizfon IP2 Phone

As stated earlier, the call queue feature is designed to be used with Bizfon IP2 phones and all other phones provide only a very limited ability to work with this feature. The only function a non-Bizfon IP2 phone can participate in is answering a call that is in the queue. Any phone can do this by dialing 441X, where the last digit is the queue number (0-9). The phone will never ring indicating that a call is waiting in the queue.

17.4 Configuring Calls To Route To the Queue

A call enters a call queue when it is routed from a system or user extension. Therefore, configuring the server so that inbound calls enter a call queue is little different from configuring it for any inbound call routing. The same features for the handling of any inbound call can be used to route a call to a call queue:

- The outside call can be sent to the auto attendant or route directly to the queue extension.
- If the call goes to the auto attendant, an auto attendant menu short cut can be set up to route the call to the queue extension.

See the *Call Routing* section in this document for information on setting up call routes. Both user extensions and system extensions can be set up so the call will route to a call queue.

Go to the **Auto Attendant – Menu Shortcuts** section of the **Phone System / Auto Attendants** page to set up an auto attendant menu shortcut.



17.4.1 Example 1: Call Routing To Auto Attendant and Then Call Queue

Requirements:

The inbound call will come in to the auto attendant. The custom auto attendant greeting will include, "For customer support, press 2." When the caller presses 2, they will hear the customer support queue greeting and be placed in the queue.

Configuration:

1. The inbound call will come in on an outside line. The outside line's call route is set to route calls to the auto attendant.
2. A system extension is created for customer support. Its call route is configured so that calls are immediately transferred to the customer support call queue.
3. An auto attendant custom greeting is recorded that tells the callers to press 2 to reach customer support.
4. An auto attendant menu shortcut is configured so that digit 2 calls the customer support system extension.

17.4.2 Example 2: Call Routing Directly to Call Queue

Requirements:

The inbound call will come in directly to the queue.

Configuration:

1. A system extension is created for customer support. Its call route is configured so that calls are immediately transferred to the customer support call queue.
2. The inbound call will come in on an outside line. The outside line's call route is set to route calls directly to the customer support system extension.

17.4.3 Example 3: Call Routing To AA, Live Answer User Extension, and Then Call Queue

Requirements:

The inbound call will come in to the auto attendant. The custom auto attendant greeting will include, "For customer support, press 2." When the caller presses 2, the customer support person's phone will ring. This allows the call to be answered live, if possible, rather than hearing the queue greeting message. If the call isn't answered after 4 rings, the call will route to the customer support queue and the caller will hear the customer support queue greeting and be placed in the queue.

Configuration:

1. The inbound call will come in on an outside line. The outside line's call route is set to route calls to the auto attendant.
2. An auto attendant custom greeting is recorded that tells the callers to press 2 to reach customer support.
3. A system extension is created for customer support. The call route for this is set so the call:
 - Rings the customer support person's phone 4 times.
 - Then if no answer, the call is transferred to the customer support call queue.
4. An auto attendant menu shortcut is configured so that digit 2 calls the customer support system extension.