



ApplianX IP Gateway User Guide

Version 2.0 – 05/10/2009

Contents

APPLIANX IP GATEWAY USER GUIDE.....	1
1.0 GETTING STARTED.....	4
1.1 How to use this guide	4
1.2 Prerequisites	4
1.3 L.E.Ds.....	4
1.4 Setting up the gateway	4
1.5 Logging in to the web interface.....	4
1.6 First time use.....	6
1.7 The Setup Wizard	7
1.8 The Main Menu	8
1.9 The Overview Page	9
1.10 Software Updates	10
1.11 Networking.....	11
1.11.1 Network settings via the web interface	11
1.11.2 Network settings via USB Flash Memory.....	13
2.0 CONFIGURING THE GATEWAY.....	14
2.1 Gateway Configuration	14
2.1.1 Gateway Configuration Page Descriptions	14
2.1.2 General Configuration Information.....	14
2.1.3 Editing Trunks	15
2.1.3.1 Editing a SIP Trunk	16
2.1.3.2 Editing a TDM Trunk	16
2.1.3.2.1 Editing a TDM Trunk Protocol.....	17
2.1.4 Endpoints	19
2.1.5 Groups	20
2.1.5.1 Adding or Editing a Group	20
2.1.6 Routes.....	22
2.1.7 Clocking	25
2.1.8 SIP.....	26
2.1.9 Codecs.....	28
2.1.10 Test.....	28
2.2. Backing up and Restoring Configurations	30

3.0 ADDITIONAL INFORMATION	32
3.1 Routing Overview	32
4.0 DIAGNOSTICS	33
4.1 Remote Logging	33
4.1 Diagnostic Log	34
5.0 TROUBLESHOOTING	35
5.1 Logging into the remote interface.....	35
5.1.1 I can't get access to the ApplanX Gateway Web Interface.....	35
5.1.2 I log on but the overview screen has errors at the top	35
5.1.3 I get a warning saying that the gateway can has not connected to the hardware.....	35
5.2 Making Calls through the Gateway	35
5.2.1 I can't make a call from the TDM side of the Gateway to an IP client.	35
5.3 Configuring the Gateway	37
5.3.1 I have made changes to the configuration but they don't seem to have any effect.....	37
5.3.1 I used the wizard to create an initial configuration but I have an error saying that there is no active configuration.....	37
6.0 GLOSSARY	38

1.0 Getting Started

1.1 How to use this guide

The ApplianX gateway interface has been designed to be intuitive. However we still recommend that new users read sections 1-3 of this guide before trying to set up a gateway for the first time. Sections 2 and 3 are a reference for those that have used the gateway before while sections 4 and 5, Diagnostics and Troubleshooting, should only be needed if problems have been encountered.

1.2 Prerequisites

The ApplianX gateway is configured via a Web Interface. Therefore a device with a web browser that supports TCP/IP will be needed to connect to the ApplianX. Also any networking cables and switches needed to allow this connection will be needed. Note that the Traffic connection of the IP Gateway needs to be connected to an Ethernet Switch and not to a Hub.

1.3 L.E.Ds

There are a number of LED's on the front of the ApplianX that are there to help during the installation and running of the ApplianX.

- Halted – This red LED indicates a serious error. If this has occurred in any circumstance other than restarting or shutting down the ApplianX then a serious error has occurred and a restart of the unit will be required.
- Error – This red LED indicates that the ApplianX has an error condition that may be resolved. Log into the ApplianX via the web interface to identify the nature of the problem
- Activity – This blue LED will flash when the ApplianX is starting up and also when the ApplianX is processing calls.
- Ready – This Green LED is lit when the ApplianX application is running.
- Startup/Initialising – This Yellow LED indicates that the ApplianX is starting. Note that user interaction may be needed via the web interface to complete startup.

1.4 Setting up the gateway

There are a number of steps that need to be carried out before the Gateway can be used to service calls. The **Setup Wizard** is designed to create a basic configuration.

1.5 Logging in to the web interface

The ApplianX Gateway should be powered up with LAN cables connecting the VoIP traffic port and the Admin port to the network. The ApplianX will take approximately one minute and twenty seconds to bring up the web interface.

Connect a PC to the same network that the administration port is connected to in order to allow access to the ApplianX's web interface. For Windows PC's type into the web browser, as the address for the Gateway, axnnnnnn, where nnnnnn is the 6 digit serial number for the ApplianX. Note that the serial number can be found on a label on the rear of the ApplianX and also on a label on the front left of the unit, if you are facing it.



On a Linux or MAC OS X PC type axnnnnnn.local into the browsers address window. Please note that some older distributions of Linux may not support the technology needed for this method of logging on to the box. Also some web browsers may not support this mode of operation. This has been tested with Microsoft Explorer (versions 6, 7 and 8), Safari, Epiphany and Opera.

An alternative method of discovering the IP address assigned to the gateway is to use a Windows software application called *ApplianX Search Tool* (available from www.applianx.com/tools.aspx). Once installed, start *ApplianX Search Tool* from the *start* menu. The *ApplianX Search Tool* will search the local network for ApplianX products and report the IP address of any products it finds (see Figure 1-0 below). By selecting and right clicking on a listed device the search tool can launch the default web browser to open the administration page for the said ApplianX.

Serial Number	IP Address	ApplianX Model Type	Display Name
ax192459	10.202.200.69	IPGATEWAY	Mike F's Test Box
ax100209	10.202.15.201	DPNSSQSIGGATEWAY	
ax100205	10.202.205.68	IPGATEWAY	
ax100200	10.202.200.38	DPNSSQSIGGATEWAY	

Figure 1-0 The ApplianX Search Tool

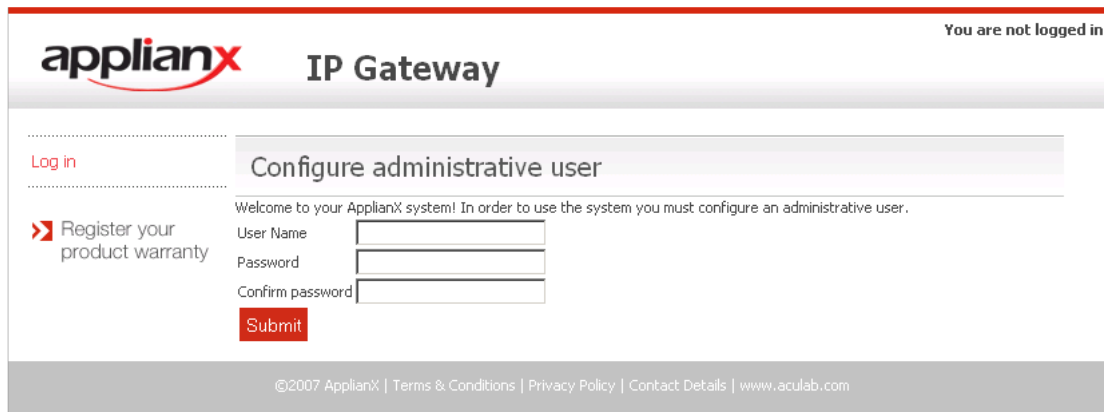
Please see the troubleshooting section if you cannot gain access to any ApplianX web pages.

1.6 First time use

On first use the Gateway Management Interface will display the page as in Figure 1-1 Configuring initial administrative user. The user is required to provide a user name and password for an administrative user for the Gateway.

Enter a user name, password and confirm the password. The user name and password cannot be left blank. Click **Submit** to create the account and login.

IMPORTANT: Until the Gateway has been configured, this user name and password will be the only means of accessing the gateway. Pressing the reset button on the front panel will delete any users and reset the gateway back to its factory default settings on a standard ApplianX chassis. For a Compact chassis please consult your support channel for information on returning the ApplianX to the factory defaults. If the user names and passwords are forgotten then this is the only way to gain access to the ApplianX via the web interface.



The screenshot shows the ApplianX IP Gateway web interface. At the top left is the ApplianX logo, and at the top right is the text "You are not logged in". Below the logo is the title "IP Gateway". On the left side, there is a "Log in" link and a link to "Register your product warranty". The main content area is titled "Configure administrative user" and contains a welcome message: "Welcome to your ApplianX system! In order to use the system you must configure an administrative user." Below this message are three input fields: "User Name", "Password", and "Confirm password". A red "Submit" button is located below the input fields. At the bottom of the page, there is a footer with the text: "©2007 ApplianX | Terms & Conditions | Privacy Policy | Contact Details | www.aculab.com".

Figure 1-1 Configuring initial administrative user

1.7 The Setup Wizard

The Setup Wizard is accessed from the Gateway menu. It is also automatically invoked the first time the Gateway is used. The setup wizard allows the creation of a basic configuration, prompting for the most commonly required and important configuration details. Default values or reasonable values are used wherever possible.

At any time, **Cancel** can be selected to return to the main Gateway Overview page. No configuration is stored until the user selects **Apply** on the final wizard page.

A wizard created new configuration will have:

- 3 Endpoints
 - Default SIP Endpoint (Will have no associated IP address initially)
 - ApplianX IP Gateway Self (will match calls from the ApplianX to itself, e.g. as sometimes made during SIP transfer)
 - Proxy (Will have an address if given in the wizard)
- 3 Groups
 - “TDM Trunks” containing all the TDM trunks
 - “Default Incoming SIP group”
 - “Proxy group”
- No routing rules defined and the “Use same rules for all groups” option turned on.
- The “Accept calls from unknown endpoints” option will be turned off.
- TDM clocking configured to use any good available TDM trunk or otherwise to fallback to local clocking
- SIP listening on UDP and TCP ports 5060
- using UDP for outgoing calls
- enabling DTMF as RFC2833
- G.711 a-law and G.711 mu-law codecs enabled

At the end of the wizard your web browser will be redirected to the “Edit Configurations” page. Here you have a list of all configurations that have been setup on the ApplianX. Note that if this is the first time a configuration has been created then the new configuration will be listed in the “Available configurations” list. The configuration must be activated to bring it into use. This is done by selecting **Use** for the required configuration.

1.8 The Main Menu

On the left of the screen at all times, apart from when the wizard is running, you will be able to access all the configuration and status pages.

- **Status**
 - **Overview** – A page with some basic gateway call counts and a list of actions required of the gateway administrator.
 - **Alarms** – This page will display any Layer 1 or Layer 2 alarms on the TDM trunks. It will also allow the masking of these alarms.
 - **Calls** – A graphical display of all the call activity on the ApplianX Gateway.
 - **Call Log** - A recent history of calls that the gateway has attempted to route. This page can be very useful for diagnosing issues during the set up phase for the gateway.
 - **Trunk Status** – This has detailed information on the SIP and TDM trunks

- **System Configuration**
 - **Global Configuration** – This allows the box to be named
 - **System Time** – This allows the setting of the clock to local time and NTP configuration.
 - **Software Update** – From this page a check can be made for software updates. See section 1.8 for more information.
 - **System Users** – This allows the addition of new administrators to the ApplianX and the setting of their privileges.
 - **Backup and Restore** – This allows configurations to be saved and restored to the ApplianX.
 - **Networking** – This allows the user to choose static IP addresses or DHCP mode
 - **SNMP** – This allows the configuration of the SNMP settings. From here you can enter the IP address of the host you wish to send traps to and enable them. Also here you can turn on the traps for the disconnecting of the Ethernet ports. Similar options are available for the TDM ports through the TDM configuration options.
 - **Setup Wizard** – This allows the setup wizard to be run to create a skeleton configuration
 - **SIP Credentials** – This allows the configuration of details to allow the gateway to respond appropriately when challenged for authorisation information.

- **Gateway Configuration**
 - **Edit Configurations** – This takes you to the main configuration overview where different gateway configurations can be selected and edited. All aspects of the gateway from Codecs and SIP set up to routing rules and groups can be edited here.
 - **Cause Mappings** – Here the clearing causes between SIP, QSIG and DPNSS can be changed from their default values.

- **Diagnostics**
 - **Remote Logging** – This allows the administrator to point the syslog output from the ApplianX to an external syslog client or ApplianX Trace Tool. This is for advanced users and support teams.

- **Watchdog Status** – This reveals the status of the “watchdogs” running on the ApplianX. They are here to look for any elements that have failed or are reporting problems. This is for advanced users and support teams.
 - **Restart** – This is used to “reboot” the ApplianX. Note that rebooting will cause all contact to be lost with the ApplianX through the user interface.
 - **Diagnostic Log** – This provides a high level overview of gateway process and can be used for debugging purposes.
 - **About** – This gives build information on the ApplianX.
 - **Endpoint Status** – This page will list the status of those IP endpoints that have been configured for monitoring
 - **Hardware** – This gives on the version and status of the hardware used in the ApplianX.
- **Account**
 - **Log Out** – This allows the current user to log out of the ApplianX administration screens.
 - **Change Password** – This allows the current administration user to change their password.

1.9 The Overview Page

The overview page gives some basic stats for the gateway such as total incoming and outgoing call counts. At the bottom of this page will be a list of actions that the gateway is flagging for the administrator.

Overview	
Status	Running
Incoming Calls	0
Outgoing Calls	0
Unroutable Calls	0
Clock source	Local

Required Actions	
Error	Trunk 1 - Layer 1 Errors (Possibly cabling, clocking, layer1 configuration (e.g. CRC on/off) or wrong firmware)
Error	Trunk 2 - Layer 1 Errors (Possibly cabling, clocking, layer1 configuration (e.g. CRC on/off) or wrong firmware)
Error	Trunk 3 - Layer 1 Errors (Possibly cabling, clocking, layer1 configuration (e.g. CRC on/off) or wrong firmware)
Error	Trunk 4 - Layer 1 Errors (Possibly cabling, clocking, layer1 configuration (e.g. CRC on/off) or wrong firmware)

Figure 1-2 The Overview page

As you can see in the above example the Gateway is telling us that we have Layer 1 errors on all trunks. In this case it is because we have not connected any TDM trunks to the gateway yet.

1.10 Software Updates

The Software Updates page can be accessed by firstly selecting Global Configuration, which then expands the menu, followed by selecting Software Updates. A page similar to the one below in figure 1-3 will be displayed.

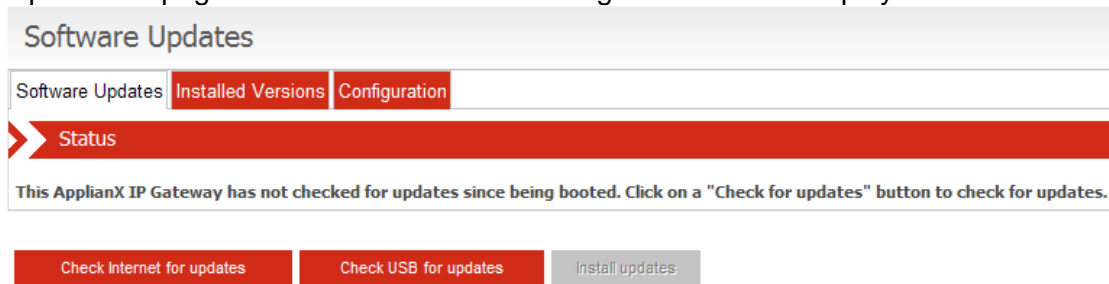


Figure 1-3 Software Updates page

Select "Check Internet for new updates" to get the latest update information from the ApplianX server. Note that Internet access is needed for this option. To update from USB please see the documentation for the ApplianX USB Update Tool on the ApplianX web site. Once the updates have been identified select "Install updates".

Note that when the software updates are applied the ApplianX will download the updated software packages and will install them. At the end of the update the user will be asked to reboot the box so that the updates can take full effect.

Selecting the **Installed Versions** tab will give a list of all the software packages that make up the ApplianX and their version number. This may help advanced users to diagnose issues.

The **Configuration** takes you to the page shown below in figure 1-4. Here you can set up any local HTTP proxy information that is needed to give the ApplianX access to the ApplianX update archive.

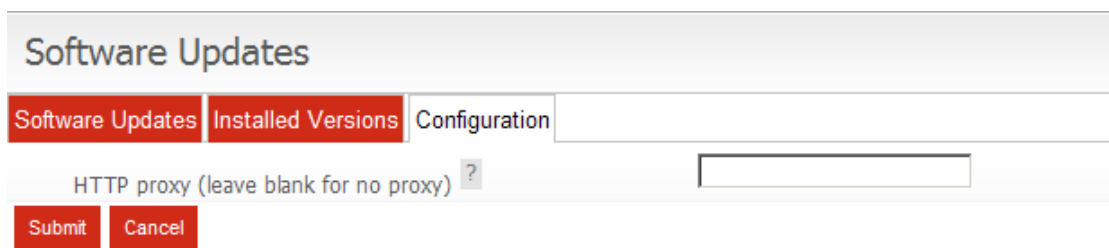


Figure 1-4 Software Updates page

1.11 Networking

The AplianX IP Gateway needs to have 3 IP addresses for the standard gateway and 2 for the Compact AplianX. By default these are set to DHCP for setting up the device only. The gateway should only actually be deployed using static IP addresses. Note that if DHCP is selected and there is no DHCP server on the network the AplianX will use Zeroconf technologies to get IP addresses and to provide access to the unit. There are 2 methods to change the IP settings. One via the web interface and one that can be done via a USB flash memory device.

1.11.1 Network settings via the web interface

The IP addresses can manually be set to static addresses by selecting **Networking** from the menu on the left. Here the 3 interfaces can be selected to be set up via DHCP or can be manually set to static IP addresses as shown below in figure1-5.

Networking

Administration interface

DHCP

IP address

Netmask

Gateway

Signalling interface

DHCP

Media interface

DHCP

Name resolution settings

Name server source Enter settings manually
 DHCP on the signalling interface

Name server

Name server

Search domains

Save Configuration Cancel Changes

Figure 1-5 Networking

Note that changing the IP addresses will affect the box and its internal and external communications. When changing the administration port and saving the configuration you will immediately lose connection between the web browser and the Appliance. The browser should be manually redirected to the new IP address. Also when changing the other IP addresses the internal communications will need to be re-established. This should take around a couple of minutes to resolve. You will see the message below, in figure 1-6, on the Overview page.

Required Actions

Warning The Gateway is waiting for hardware to become available. This is to be expected when the system has just been started or when the network configuration has changed. The hardware should be detected within a couple of minutes.

Figure 1-6 Warning

Finally the options for name resolution can be setup on this page. Servers may be manually entered or DHCP on the signalling interface may be selected.

1.11.2 Network settings via USB Flash Memory

The ApplianX will check for the presence of a USB device when it is booting up. If it finds one then it will look on this device for User Defined IP settings and will configure the unit to come into service with those settings. Note that using this method it takes a few minutes longer for the unit to come up and change the IP addresses to those configured.

On the USB flash device create a directory called `applianx_net` in the root. Place 3 files in this directory called `admin`, `media` and `signalling`. Note that these files have no extensions so be careful with the editor you are using in case it adds an extension for you.

Within each of these files you need to put the information to set the static IP address.

[Config]

```
ip = 10.202.165.169  
netmask = 255.255.0.0  
gateway = 10.202.100.254
```

or to set an interface to DHCP use.

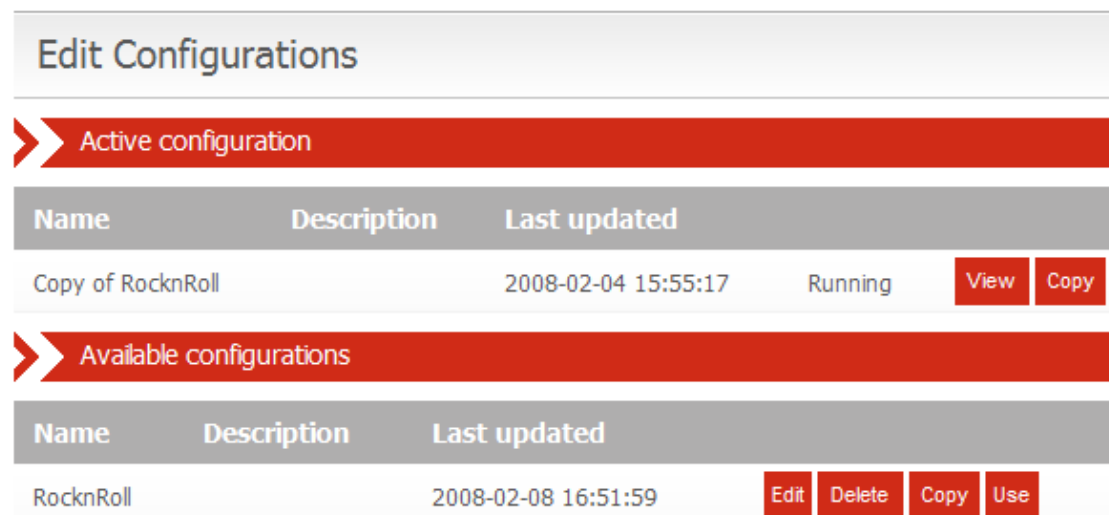
[Config]

```
dhcp = 1
```

2.0 Configuring the Gateway

2.1 Gateway Configuration

All Gateway configurations are managed from the Figure 2-1 Edit configurations page. The currently active configuration is listed first. This may not be directly edited, but may be examined by selecting **View**. To modify the active configuration, it is first necessary to click **Copy** next to the active configuration entry. When you are happy with edits made to a new or copied configuration you can select this to be the active configuration by selecting the **Use** button on the right of the configuration.



The screenshot shows a web interface titled "Edit Configurations". It is divided into two sections: "Active configuration" and "Available configurations".

Active configuration section:

Name	Description	Last updated	
Copy of RocknRoll		2008-02-04 15:55:17	Running View Copy

Available configurations section:

Name	Description	Last updated	
RocknRoll		2008-02-08 16:51:59	Edit Delete Copy Use

Figure 2-1 Edit configurations page

2.1.1 Gateway Configuration Page Descriptions

Configuration information is presented as a set of inter-related tabbed pages, some of which lead to further more detailed pages. At any time, selecting **Cancel Changes** will cause all changes to be discarded. Selecting **Save Configuration** will save the changes made. In either case, the main Edit Configurations page is redisplayed.

2.1.2 General Configuration Information

This page, shown in Figure 2-2, enables the setting of a configuration name and description. A configuration may be renamed by changing the **Configuration name**. The **Configuration description** allows any notes or important information to be stored along with a configuration.

Editing: My configuration

General **Trunks** Endpoints Groups Routes Clocking SIP Codecs Test

>> General Configuration Information

Configuration name

Configuration description

>> Network Unique ApplanX IP Gateway Call Identity

First callid for this ApplanX IP Gateway

Range of callids for this ApplanX IP Gateway

Save Configuration Cancel Changes

Figure 2-2 General

2.1.3 Editing Trunks

All available trunks are listed on the Trunks page as in Figure 2- 3 Trunks **page**. SIP Trunks and TDM Trunks are listed separately. Settings for an individual trunk can be changed by selecting **Edit** next to the trunk.

Editing: My configuration

General **Trunks** Endpoints Groups Routes Clocking SIP Codecs Test

>> SIP trunks

Name	Description	Type	Group	
Trunk 5		SIP	No group	Edit

>> TDM trunks

Name	Description	Type	Group	
Trunk 1		TDM	TDM trunks	Edit
Trunk 2		TDM	TDM trunks	Edit
Trunk 3		TDM	TDM trunks	Edit
Trunk 4		TDM	TDM trunks	Edit

Save Configuration Cancel Changes

Figure 2- 3 Trunks page

2.1.3.1 Editing a SIP Trunk

Each Trunk requires a name distinct from all other Trunks. Changing the name of a Trunk causes all references to the Trunk to also change. The time at which the speech path is opened for calls on this trunk can be selected. Often it is required to open up speech paths before the call is connected to allow the signalling of in band information. If a call comes in on a trunk it is possible to select how the gateway deals with that call. Also SNMP traps can be activated for the signalling network Interfaces.

Apply Cancel	
General settings	
Trunk name	Trunk 5
Trunk description	
Open inward speech path before answer ?	<input checked="" type="checkbox"/>
Response to unroutable incoming calls ?	Release
SNMP configuration	
Enable SNMP traps	<input checked="" type="checkbox"/>

Figure 2- 4 Edit SIP Trunk Page

2.1.3.2 Editing a TDM Trunk

Each Trunk requires a name distinct from all other Trunks. Changing the name of a Trunk causes all references to the Trunk to also change. The Group for this Trunk can be selected from the list of Trunk Groups. NOTE: Mixing different types of Trunk in the same Trunk Group is not supported. All Trunks in a Group must be of the same type. The time at which the speech path is opened for calls on this trunk can be selected to be prior to the call be connected. This is useful for the passing of in-band information related to the call. In contrast to a SIP trunk, it is possible to block a TDM trunk from participating in call activity. The strategy for allocating outgoing timeslots can be selected from a list of options. The minimum digit count allows the gateway to attempt routing when a certain number of digits have arrived. The inter-digit timeout in milliseconds can be specified. This is the time that the gateway waits for another digit before deciding it has got them all. For CAS protocols this defaults to 5 seconds. The strategy for dealing with calls that cannot be routed can be selected here also. The currently configured protocol is displayed. This can be changed or configured by selecting **Edit**. In particular supplementary features are enabled and disabled through this edit option. Finally the SNMP trap can be enabled for this trunk.

Apply Cancel

General settings

Trunk name	Trunk 1
Trunk description	
Open inward speech path before answer ?	<input checked="" type="checkbox"/>
Routing group	TDM trunks
Block trunk from call activity ?	No
Outgoing timeslot allocation strategy ?	Highest available
Minimum digit count ?	1
Interdigit timeout (milliseconds) ?	5000
Interdigit timeout for virtual calls (milliseconds) ?	1000
Send sending complete on outgoing calls ?	<input checked="" type="checkbox"/>
Send overlap digits on outgoing calls ?	<input checked="" type="checkbox"/>
Response to unroutable incoming calls ?	Release

SNMP configuration

Enable SNMP traps	<input checked="" type="checkbox"/>
-------------------	-------------------------------------

Protocol configuration

Protocol	DPNSS	Edit	Change
----------	-------	------	--------

Figure 2- 5 Edit TDM Trunk page

2.1.3.2.1 Editing a TDM Trunk Protocol

In contrast to a SIP trunk, each TDM Trunk also requires a trunk protocol. The selected protocol must be chosen to be compatible with the remote equipment connected to the trunk. The current protocol can be set or modified by selecting **Change**. Protocol configuration options are also available. All settings and options for the trunk protocol are specific to the user's installation. You should seek the advice of your service provider or switch maintenance team for advice on the protocol selection and settings to be used.

DPNSS

General settings

Impedence	120 Ohms (default) ▾
CRC enabled [?]	<input type="checkbox"/>
Master/Slave configuration	AX ▾

Basic features

Display direction [?]	Send and receive ▾
Allow incoming data calls [?]	<input checked="" type="checkbox"/>
Loop avoidance mapping [?]	<input type="radio"/> Disabled <input checked="" type="radio"/> Transparent <input type="radio"/> Transit
Global transit limit [?]	25
Insert loop avoidance in outgoing calls [?]	<input type="checkbox"/>
Do-not-disturb mapping [?]	<input checked="" type="checkbox"/>
Method for generating CLC [?]	<input type="radio"/> Use a fixed value <input checked="" type="radio"/> Map from the other call leg (default) <input type="radio"/> Map from the calling name
CLC when map is not possible [?]	CLC-DEC ▾
Override CLC when OLI restricted [?]	No Override ▾
Insert Bearer Service Selection (BSS) [?]	<input checked="" type="radio"/> Disabled <input type="radio"/> Preferred <input type="radio"/> Mandatory
Call Offer Enabled [?]	<input checked="" type="checkbox"/>
Call Transfer Enabled [?]	<input checked="" type="checkbox"/>

Call Diversion Supplementary Service Support

Call Diversion Enabled [?]	<input checked="" type="checkbox"/>
Automatic Diversion Validation [?]	<input type="checkbox"/>

Figure 2-6 Editing TDM Trunk Protocol

2.1.4 Endpoints

This page lists the IP endpoints that are configured in the system. Calls can be routed to and from groups of Endpoints as well as groups of trunk. Figure 2-7 shows the default list of endpoints.

Editing: My configuration

General	Trunks	Endpoints	Groups	Routes	Clocking	SIP	Codecs	Test
Default SIP Endpoint	Default endpoint to match incoming SIP calls that don't match any other endpoint							
Proxy	A SIP proxy							
ApplianX IP Gateway self	Certain supplementary services can result in the ApplianX IP Gateway being asked to call itself. This endpoint matches those calls and allows them to be routed correctly.							
Add a new endpoint								

[Save Configuration](#) [Cancel Changes](#)

Figure 2- 7 Endpoints

The default SIP endpoint is any endpoint that has not been explicitly set up. Thus if a call is received from an unknown SIP endpoint it can be routed. Note that this endpoint is only active if the **Allow calls from unknown endpoints** option is enabled on the **Routes** tab. The Proxy entry will have been set up in the wizard if that option had been chosen. This can be setup to set up inter working with Proxies or Soft PBX's. There are options to delete or edit endpoints on the write. There is also the option to add further endpoints. Clicking **Add a new endpoint** will take you to the screen shown in figure 2.8.

Editing: My configuration

[Apply](#) [Cancel](#)

> General

Name [?]

Description [?]

Routing group [?]

> Endpoint Options

Endpoint address [?]

Endpoint port [?]

Monitor this endpoint [?]

Trust this endpoint [?]

Update after transfer [?]

Figure 2- 8 Adding a new endpoint

Here the **Name** field is a unique name used to identify the endpoint. The **Description** field is a description to associate with the said endpoint. **Routing group** is the routing group that the endpoint will belong to. The **IP Address** and **Port** are self explanatory. **Monitor this endpoint** will result in the gateway periodically sending an OPTIONS message to the endpoint. If the endpoint does not get a reply then it will consider this endpoint as down and then endpoint will not be routed to. **Trust this endpoint** instructs the gateway to pass CLI information to the endpoint even if the CLI is passed with the presentation restricted flag set. The **Update after transfer** option controls whether the ApplanX should inform this endpoint of the new connected number if the other leg of the call has been transferred.

2.1.5 Groups

This page lists all the defined groups. A group is collection of Trunks or endpoints that are grouped together for the purpose of routing.

To change an existing Group click **Edit**. Click **Add a new group** to create a new Group. To delete an existing Group click **Delete**.

Editing: Copy of My configuration			
General Trunks Endpoints Groups Routes Clocking SIP Codecs Test			
Name▲	Description		
Default Incoming SIP group	Group for incoming SIP calls	Edit	Delete
Proxy group	Group containing the SIP proxy	Edit	Delete
TDM trunks	Default group for TDM trunks	Edit	Delete

Add a new group

Figure 2- 9 Groups

2.1.5.1 Adding or Editing a Group

Each Group requires a name distinct from all other Groups. Changing the name of a Group causes all references to the Group to also change. A free format description for the Group can be entered. The trunks/endpoints assigned to this Group are listed. The association of a Trunk with a Group is specified on the individual Trunk/Endpoint page. Finally, as shown in figure 2-10 there is an option to select the method by which the next trunk/endpoint is chosen. The options are round robin or first in the list.

Editing: Copy of Copy of My configuration

Apply Cancel

General settings

Routing Group Name

Routing Group Description

Endpoint selection method

Endpoints assigned to this Routing Group

Endpoint Name	Endpoint Description	Endpoint Type	
Trunk 2		TDM	▼ ↓ ×
Trunk 3		TDM	▲ ▲ ▼ ↓ ×
Trunk 4		TDM	▲ ▲ ▼ ↓ ×
Trunk 1		TDM	▲ ▲ ×

Add

Figure 2-10 Edit Group

2.1.6 Routes

This page allows modification of the routes assigned to a group. The drop down box at the top allows you to select the group that you wish to route from, see figure 2 – 11 Editing Routes.

Editing: My configuration

General Trunks Endpoints Groups Routes Clocking SIP Codecs Test

Routing Options

Use the same rules for all groups

Allow calls from unknown endpoints

Routing Rules

Name ?	DDI criteria ?	DDI man. ?	CLI criteria ?	CLI man. ?	Destination ?	
Route to proxy	9%	%	%	%	Proxy_group	

Add new rule

Figure 2-11 Editing Routes

By default there are no routes configured. The **Use the same rules for all groups** option is enabled and the **Allow calls from unknown endpoints** option is disabled.

When **Use the same rules for all groups** is enabled routing rules that route based on the destination and/or originating address are required. These rules are applied to all routing groups. This is the easiest method to use when configuring the ApplianX as it automatically deals with cases where the ApplianX is diverted or transferred to itself by a SIP endpoint.

When **Use the same rules for all groups** is disabled, each routing group has its own list of routing rules that are applied to incoming calls. When SIP supplementary features are in use (e.g. diversion or transfer) this can sometimes result in the gateway being asked to call itself. In a configuration where this is likely to happen you will need to set up additional routing rules that allow these calls to be routed to the correct destination.

The **Allow calls from unknown endpoints** option controls the ability of the gateway to route calls from endpoints that it doesn't know about. When this option is enabled, calls from unknown endpoints match the Default SIP Endpoint endpoint and are routed according to the rules assigned to the group that the Default SIP Endpoint is in.

Routes can be added using the **Add** button. The **DDI Criteria** and **CLI Criteria** fields define the pattern used to match the dialled destination address and originating address. The following characters are used to define the pattern:

- % matches any sequence of digits
- ? matches any single digit
- individual digits match themselves

For example, 81% will match any number beginning with 81, whereas 8??2 will match any 4 digit number beginning with an 8 and ending with a 2.

The DDI and CLI **Manipulation** fields define how the destination and originating addresses will be changed. The following characters are used to define the translation:

- ? uses the next character from the incoming string
- ! deletes the next character from the incoming string
- % uses the remainder of the incoming string (any further characters in the translation string will be ignored)
- \$ deletes the remainder of the incoming string
- Any other digit is copied to the outgoing string.

For example, if the incoming Destination number is 8120 and the destination address manipulation field is set to 123!% then the destination address used for the outgoing call will be 123120.

By selecting the edit icon on the right of any routes advanced options are available for that route. Figure 2-12 shows this.

Codecs

Defer codecs to the global setting

Transport

Defer transport to the global setting

TDM Options

Originating address screening [?]	Transparent <input type="text"/>
Originating address presentation [?]	Transparent <input type="text"/>
Originating address numbering plan [?]	Transparent <input type="text"/>
Originating address numbering type [?]	Transparent <input type="text"/>
Destination address numbering plan [?]	Transparent <input type="text"/>
Destination address numbering type [?]	Transparent <input type="text"/>

Manipulation

Default originating address [?]	<input type="text"/>
Originating URI parameters [?]	<input type="text"/>
Destination URI parameters [?]	<input type="text"/>

Echo Cancellation

Apply echo cancellation [?]	<input checked="" type="checkbox"/>
Apply automatic gain control [?]	<input type="checkbox"/>
Echo cancellation span [?]	0 <input type="text"/>
Use non-linear processing [?]	<input checked="" type="checkbox"/>
Generate background noise [?]	<input checked="" type="checkbox"/>
Non-linear processing limit (in dbM0) [?]	0 <input type="text"/>

Figure 2-12 Advanced Route Options

The Codecs option allows different codecs to be selected for a particular route. The transport option allows UDP or TCP to be the default for outgoing calls. By default both of these options will defer to the global settings that can be set in the SIP and Codecs sections of the gateway configuration pages.

Following these are a number of options to force the gateway to use particular values for screening, presentation, destination address plan and type and destination address plan and type.

2.1.7 Clocking

This page controls the source of the Gateway's telephony clock. A correctly configured clock is essential for proper operation of the Gateway.

The page displays two columns. The left-hand column shows the Available Clock Sources. These are all the TDM Trunks not currently selected as a possible clock source. The right-hand column shows Selected Clock Sources. These TDM Trunks are currently selected as possible clock sources.

To move an "Available" trunk to the "Selected" column, highlight it and then click the ">" button.

To move a "Selected" trunk to the "Available" column, highlight it and click the "<" button.

To move all "Available" trunks to the "Selected" column, click the ">>" button.

To move all "Selected" trunks to the "Available" column, click the "<<" button.

The Selected Clock Sources are listed in the order of application. This order can be changed by highlighting individual trunks and then selecting **Move Up** or **Move Down**.

There is an additional option to fallback to a locally generated clock source when no other clock source is available.

In operation, the first listed Selected Clock Source that is found to be functional will be used. If, at any time, this should be detected as failed, the Gateway will automatically switch to the next listed functional clock source.

By default all physical TDM trunks are pre-selected with **Fall back to local clock** also selected. This should only need to be changed if the local Gateway installation requires it.

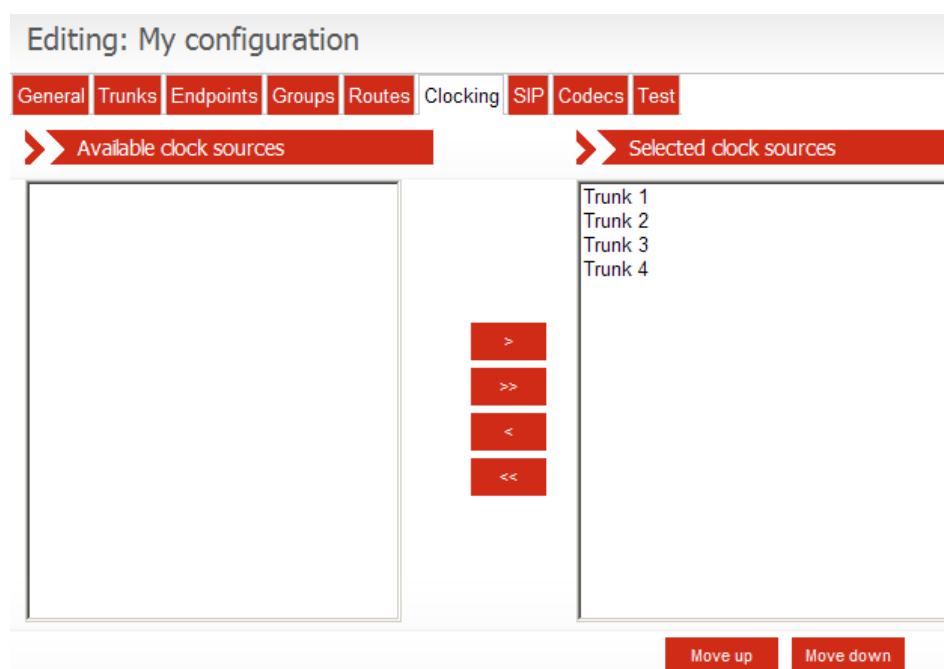


Figure 2-13 Clocking control page

2.1.8 SIP

This page configures SIP telephony settings.

SIP transport for outgoing calls can be either UDP or TCP as required for the user's network.

DTMF over IP send method: When the RFC2833 encoded RTP option is enabled DTMF tones will be encoded using the RFC2833 codec. When the option to use current codec is selected the tone will be sent in band. Other options are to send the tone in SIP Info messages as SIP Info dtmf or SIP Info dtmf-relay. For SIP Info DTMF type each DTMF tone is stripped from the audio stream and sent as a SIP INFO application/dtmf message. The body of each SIP INFO message indicates the dialled DTMF digit. For dtmf-relay type each DTMF tone is stripped from the audio stream and sent as a SIP INFO application/dtmf-relay message. The body of each SIP INFO message indicates the dialled DTMF digit and its duration.

Tone duration of regenerated DTMF: This option allow the specification of the duration of DTMF tones, regenerated in response to SIP INFO messages of application/dtmf mime type.

Interdigit duration of regenerated DTMF: This option allows the specification of the duration of silence in between DTMF tones, regenerated in response to SIP INFO messages.

Enable comfort noise: By default comfort noise generation is on. In some circumstances this can cause problems so this option is to turn it off.

Enable 183 provisional Responses: This option allows the sending of 183 provisional responses.

Enable Discontinuous Transmission (DTX): With this enabled the ApplianX will not send packets when there is silence.

Enable Packet Loss Concealment (PLC): With this set the ApplianX will attempt to conceal gaps in the audio.

Enable RTCP: This option is to enable the sending of RTCP packets.

Use 'sendonly' for Hold: The SDP attribute is set to "a=sendonly to indicate a hold.

Use 'inactive' for Hold: The SDP attribute is set to "a= inactive to indicate a hold.

Use 'recvonly' for Hold: The SDP attribute is set to "a= recvonly to indicate a hold.

For incoming SIP calls, the **SIP listening ports** can be changed if required from the default of 5060. In addition, by default, the SIP service will listen on both UDP and TCP ports for incoming calls. If either of these is not required, enter 0 (zero) to disable the port. NOTE: If both ports are set to 0 (zero), the Gateway will be unable to make or receive SIP calls.

General	Trunks	Endpoints	Groups	Routes	Clocking	SIP	Codecs	Test
SIP transport for outgoing calls								
Transport protocol	UDP							
Media options								
DTMF over IP send method ?	RFC2833 encoded RTP							
Tone duration of regenerated DTMF ?	250							
Interdigit duration of regenerated DTMF ?	250							
Enable comfort noise ?	<input checked="" type="checkbox"/>							
Enable 183 provisional responses	<input checked="" type="checkbox"/>							
Enable Discontinuous Transmission (DTX) ?	<input checked="" type="checkbox"/>							
Enable Packet Loss Concealment (PLC) ?	<input checked="" type="checkbox"/>							
Enable RTCP ?	<input type="checkbox"/>							
Use 'sendonly' for Hold	<input checked="" type="radio"/>							
Use 'inactive' for hold	<input type="radio"/>							
Use 'recvonly' for Hold	<input type="radio"/>							
SIP listening ports								
UDP listen port (0 to disable)	5060							
TCP listen port (0 to disable)	5060							
SIP features								
Endpoint monitoring timeout ?	120							
MWI_HEADING								
SIP_MWI_ACCEPT_METHOD	<input checked="" type="checkbox"/>							
SIP_MWI_SEND_METHOD	<input checked="" type="checkbox"/>							

Figure 2-14 SIP configuration page

2.1.9 Codecs

The Appliance Gateway can negotiate and exchange RTP audio with SIP devices using a range of codecs. This page allows the selection and prioritisation of these codecs.

The page displays two columns. The left-hand column shows the Available Codecs. These are all the codecs not currently selected. The right-hand column shows Configured Codecs. These codecs are currently selected.

To move an “Available” codec to the “Selected” column, highlight it and then click the “>” button.

To move a “Selected” codec to the “Available” column, highlight it and click the “<” button.

To move all “Available” codecs to the “Selected” column, click the “>>” button.

To move all “Selected” codecs to the “Available” column, click the “<<” button.

The Configured Codecs are listed in the order that they will be offered in a SIP INVITE SDP. This is also the order of preference when accepting a SIP INVITE. This order can be changed by highlighting individual codecs and then selecting **Move Up** or **Move Down**.

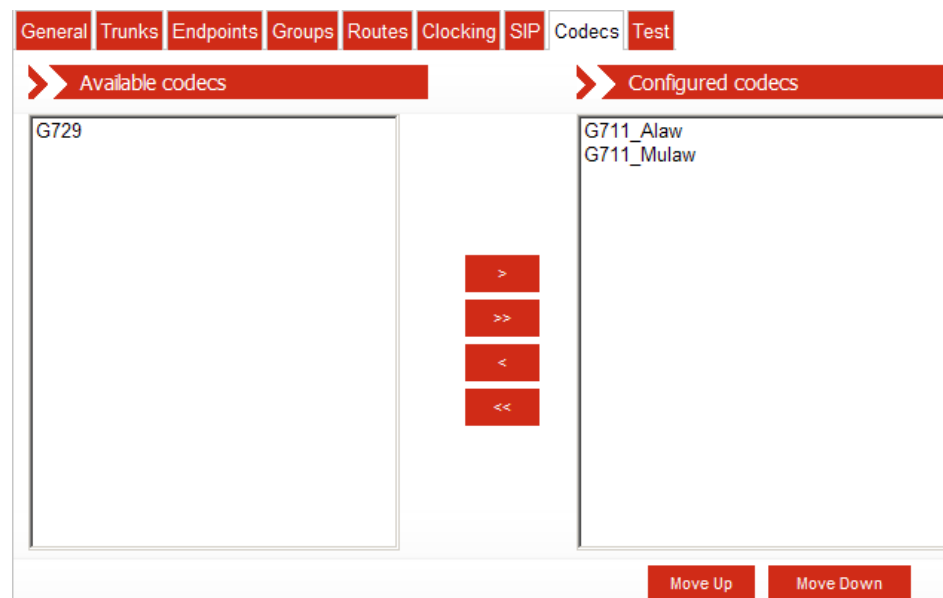


Figure 2-15 Codec configuration page

2.1.10 Test

Gateway configuration is quite complex. The Test page is provided to help the user validate the configuration without the need to place live calls.

The **Configuration Issues** section lists any detected inconsistencies that may be a problem e.g. Trunks that are not assigned to a group, or Groups without any routing rules.

The **Test Routing** section allows the user to enter destination and originating telephone numbers along with the incoming call trunk. Selecting **Test!** causes the routing rules for this configuration to be applied as if this were a real call. The different steps of the routing decisions made will be shown similar to that shown below.

Test Routing

This page provides a way to see how the Appliance IP Gateway will route calls without having to make a configuration live first.
Enter the destination and originating numbers as the Appliance IP Gateway will see it and select a trunk that the call is to be received on.

Destination address

Originating address

Trunk call arrives on

Test!

```
INCOMING CALL IS TDM
Matched rule: Route to proxy
Using endpoint: Proxy
  Destination address: sip:1234@192.168.9.91
  Originating address: sip:5678@10.202.205.244
  Numbering presentation: ALLOWED
  Numbering screening: NOT SCREENED
```

Figure 2-16 Test page

2.2. Backing up and Restoring Configurations

To save or restore configuration information select **Global Configuration** under the **System Configuration** section in the main menu. This will reveal further options. From here select **Backup and Restore**. This will bring up the backup and restore page as shown below in Figure 2-17.

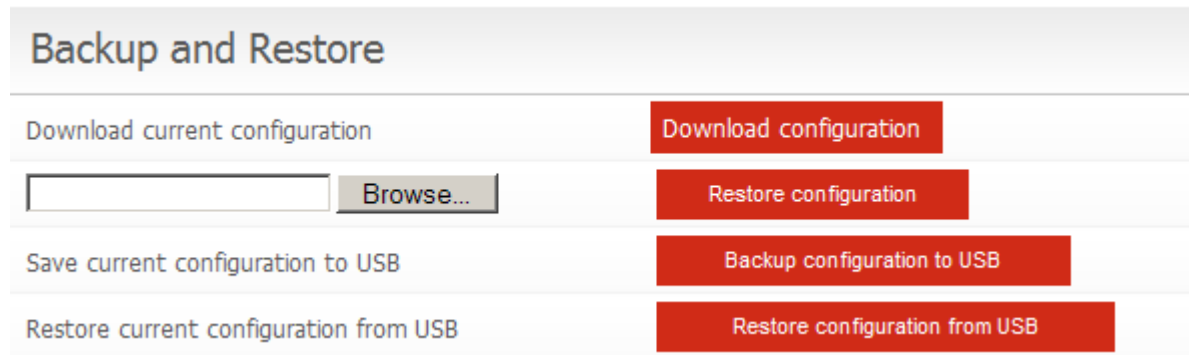


Figure 2-17 Backup and Restore

To make save a backup of a configuration on the PC that the web browser is on select the **Download configuration** button on the right. If using Internet Explorer on Windows then this will bring up a window similar to the one below shown in Figure 2-18. Selecting **Save** will bring up the Windows save menu so that you can select where the file is saved and what name is used.

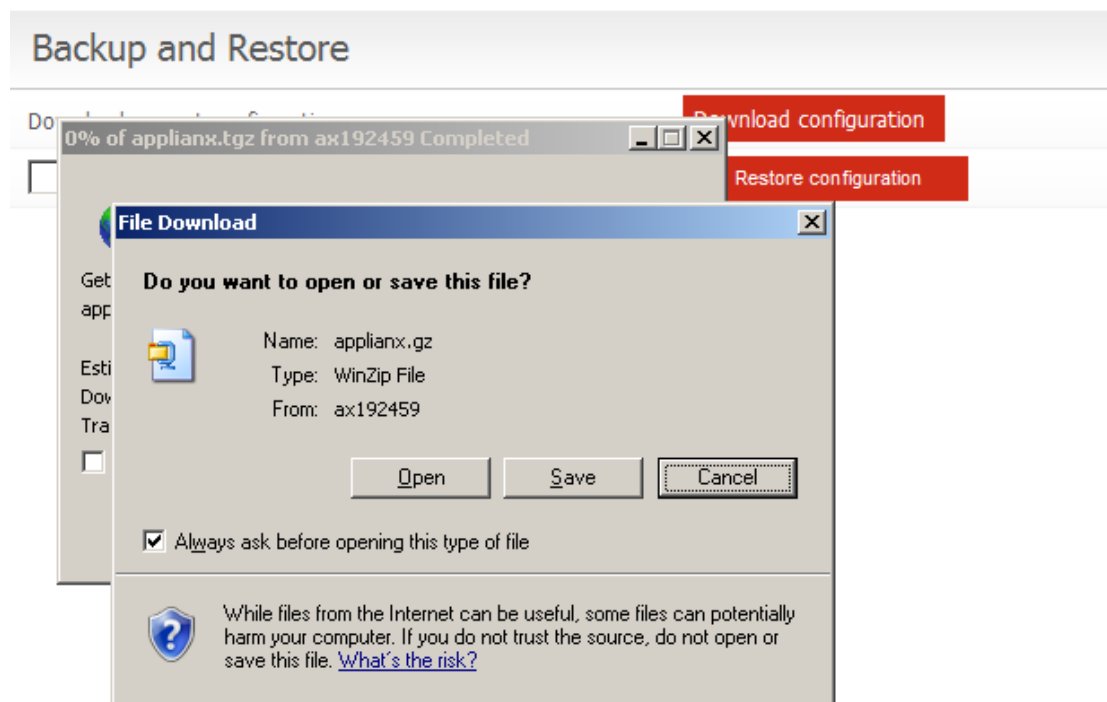


Figure 2-18 Saving the File

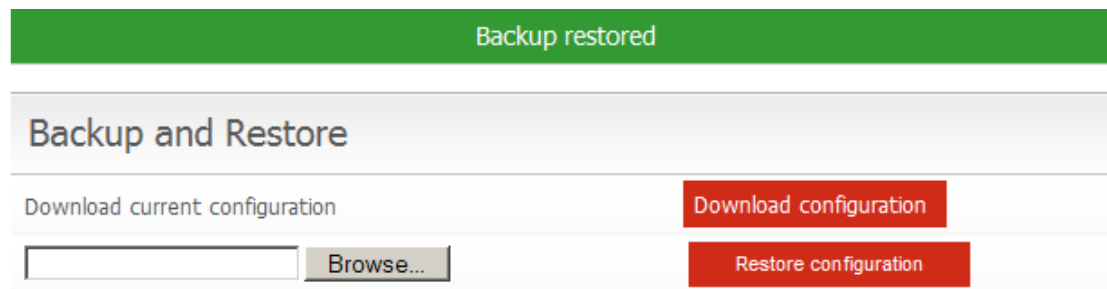
To restore a previously saved configuration then either enter the path and filename in the box provided or select browse to locate and select the backup file. Once the required back up has been selected select **Restore configuration**.



The screenshot shows a web interface titled "Backup and Restore". It has a header bar with the title. Below the header, there are two rows of controls. The first row contains the text "Download current configuration" on the left and a red button labeled "Download configuration" on the right. The second row contains a text input field with the value "C:\applianx.gz" on the left, a "Browse..." button next to it, and a red button labeled "Restore configuration" on the right.

Figure 2-19 Restore configuration

If this is successful then you will see the message as shown below



The screenshot shows a success message "Backup restored" in a green banner at the top. Below the banner is the same "Backup and Restore" interface as in Figure 2-19, but the text input field is now empty.

Figure 2-20 Backup restored

In addition back ups can be saved and retrieved to and from a USB flash memory device that is placed in the USB slot in the front of the ApplianX. If a non-bootable USB device is placed in the USB slot of the ApplianX when it is booted and it has a previously saved configuration on it then the ApplianX will come into service with that configuration.

3.0 Additional Information

3.1 Routing Overview

The routing of telephone calls forms the core function of the Gateway and is the most complex area to configure. A caller dials a number that causes a call to arrive at the gateway. The Gateway applies user-defined rules to the dialled number in order to identify the target user and how they can be contacted. The Gateway then makes an outbound call to this target user and connects the two calls together. This whole process is termed call routing.

Some definitions:

- Trunk – a physical connection capable of carrying many calls
- Group – a user defined logical group of trunks or endpoints
- Telephone number – a sequence of digits associated with a physical telephone, e.g. 01234567890
- SIP user address – a sequence of characters in SIP URL format associated with a SIP client user, e.g. johnsmith@hiscompany.com
- Originating Address – the telephone number or SIP address of the caller
- Destination Address – the telephone number or SIP address of the callee
- Route – a set of information that specifies :
 - a pattern to match against a call destination address
 - a rule that allows changes to the originating address
 - a rule that allows changes to the destination address
 - the type of routing to perform (to a Trunk Group or a User)
 - a trunk group on which to make outgoing calls

Some important things to know:

- Each Group must have at least one rule associated with it
- Each Group will generally require different rules to correctly process incoming calls
- Each Group can only contain Trunks of one type, either SIP or TDM

4.0 Diagnostics

4.1 Remote Logging

On the main menu on the left of the screen, as seen through the ApplianX web interface, you will see a Diagnostics section. Selecting Remote Logging takes you to the following, Figure 4-0.

Remote Logging

Enable remote logging [?]

Host to receive logs [?]

Logging port [?]

Log sources

Log Type	Status	
Call activity trace	stopped	<input type="button" value="Start"/>
SIP protocol trace	stopped	<input type="button" value="Start"/>
Switch trace	stopped	<input type="button" value="Start"/>
TING trace	stopped	<input type="button" value="Start"/>
Trunk 1 protocol trace	stopped	<input type="button" value="Start"/>
Trunk 2 protocol trace	stopped	<input type="button" value="Start"/>
Trunk 3 protocol trace	stopped	<input type="button" value="Start"/>
Trunk 4 protocol trace	stopped	<input type="button" value="Start"/>

Figure 4-0 Remote Logging

There are no facilities for storing Logging information on the ApplianX. However the ApplianX supports the use of Syslog and can send information using the syslog protocol to a client that can receive the said information. The majority of Linux distributions will include a syslog daemon and it will most likely be running by default. For Windows there are freeware implementations available. Also the ApplianX Trace Tool can receive and decode the protocol messages. The trace available through the remote logging is currently targeted at the ApplianX development engineers and support staff. Check the ApplianX web site www.applianx.com for announcements with respect to the addition of self help tools.

4.1 Diagnostic Log

This page gives a high level record of actions carried out by the gateway. It will also show any errors that the gateway encountered while coming into service. This information should be passed to your support contact if you think that there is a problem with the gateway.

Diagnostic Log

```
2009-03-23 14:32:55 Info System booted
2009-03-23 14:32:55 Info Waiting for hardware detection
2009-03-23 14:33:07 Info Loading configuration My configuration
2009-03-23 14:33:07 Info Clock source is now: Local
2009-03-23 14:33:07 Info Starting protocol firmware download
2009-03-23 14:33:08 Info Firmware download to trunk Trunk 1 succeeded (firmware=dpnss.pmx)
2009-03-23 14:33:10 Info Firmware download to trunk Trunk 2 succeeded (firmware=dpnss.pmx)
2009-03-23 14:33:11 Info Firmware download to trunk Trunk 3 succeeded (firmware=dpnss.pmx)
2009-03-23 14:33:13 Info Firmware download to trunk Trunk 4 succeeded (firmware=dpnss.pmx)
2009-03-23 14:33:13 Info Firmware download complete
2009-03-23 14:33:13 Info Configuration My configuration loaded
2009-03-23 14:33:13 Info System Starting
2009-03-23 14:33:13 Info System Started
```

Figure 4-1 Diagnostic Log

In the above example the system boots and then waits for internal hardware detection to complete. Configuration loading commences and then the Protocol firmware is downloaded to the TDM trunks.

5.0 Troubleshooting

5.1 Logging into the remote interface

5.1.1 I can't get access to the ApplianX Gateway Web Interface

- Try using the ApplianX Search Tool on a Windows PC to detect the ApplianX and to obtain its IP address.
- Try checking the cabling and then try to log in again. The PC and the ApplianX administration port must be on the same network.
- If you are using an old distribution of Linux then try updating to a current distribution.
- On a Windows XP PC are you using Microsoft Explorer Version 6 or 7? If not try using one of these browsers. Note that version 7 is preferred.
- Try connecting the network port of your PC directly to the ApplianX administration port.
- Try accessing the web interface from an up to date Linux or MAC OS X PC using axnnnnnn.local address if you have one available.
 - Did this work? If so you may have DNS/DHCP network issues. Move to using static IP addresses
- Try setting the IP of the box to static IP addresses using a USB flash memory stick as described in section 1.9.2.

5.1.2 I log on but the overview screen has errors at the top

- Wait a couple of minutes and then refresh the screen. The web interface can start before the gateway, which means that until the gateway has started, the interface will report that it cannot talk to the gateway engine.

5.1.3 I get a warning saying that the gateway can has not connected to the hardware.

- This is normal when the unit has started or been rebooted or has had its IP settings changed. The elements that make up the gateway are just starting and establishing their communication paths.

5.2 Making Calls through the Gateway

5.2.1 I can't make a call from the TDM side of the Gateway to an IP client.

- Check the Call Status Page by selecting "Calls" under the Status section on the menu on the left of the Administration web interface. Now make the call in from the TDM side of the gateway. If you check the Call Activity at the bottom of the screen check that the Call was received by the gateway. In this case you can see that the Gateway did indeed receive the call but could not route it. You will need to check your routing rules so that the Gateway has the information it needs to route the calls. See section 2 of this User Guide.

Call Activity

Time	Location	Numbers	Message
2007-09-03 17:21:51.054	Trunk 1 Ts: 1	From: 666 To: 888	Released (request_terminated, raw cause=0x10)
2007-09-03 17:21:50.950	Trunk 1 Ts: 1	From: 666 To: 888	Call released (LC_NORMAL, raw cause=16)
2007-09-03 17:21:45.799	Trunk 1 Ts: 1	From: 666 To: 888	Unroutable cal
2007-09-03 17:21:45.798	Trunk 1 Ts: 1	From: 666 To: 888	Incoming call detected

- If there are no calls present then check the Status of the Trunk. This is done by selecting **Trunk Status** from the **Status** section of the menu. If the Trunk is good then the Layer 1 should be showing zero for Slips Errors, Bipolar Violations and Frame Alignment Errors. If there are errors on these then please check the cabling. Ensure that you have configured the correct protocol for the TDM trunks. Also check the options that have been chosen for the protocol and ensure that these are in line with the TDM lines that you are connecting to the ApplianX Gateway.

Layer 1 Information

Slip errors	0
Bipolar violations	0
Frame Alignment errors	0

- If there are no Layer 1 Errors then check the Layer 2. If this isn't showing "green" for the bearer channels on the trunk then there is a layer 2 problem. Check that you have the correct protocol loaded for the TDM trunks that you are connecting to the Gateway. Check with your service provider or PBX maintenance team for set up information for the protocol.

Layer 2 Information



5.3 Configuring the Gateway

5.3.1 I have made changes to the configuration but they don't seem to have any effect.

- The Gateway does not allow you to edit a configuration that is in use. For this reason you can copy a configuration and edit this. Before these changes can take effect you must select that the gateway use this edited configuration. This is done by selecting the "Use" button by the side of the edited configuration on Edit Configurations page.

5.3.1 I used the wizard to create an initial configuration but I have an error saying that there is no active configuration.

Required Actions

Error No active configuration (Please apply an available configuration (See 'Edit Configurations' page), or use the 'Setup Wizard' to create a new configuration)

- On completion of the Wizard a skeleton configuration is created. This configuration though is not automatically activated. On completion of the Wizard you will be directed to the Edit Configurations screen. Here the Skeleton created in the Wizard will be shown under the Available configurations section. Select **USE** to activate that configuration.

Available configurations			
Name	Description	Last updated	
Copy of My configuration		2007-09-20 14:37:53	Edit Delete Copy Use

6.0 Glossary

ApplianX – is a product brand of Aculab and has been developed in order to provide robust and reliable systems for the fast execution of Internet-based communication strategies, with rapid deployment and integration into existing infrastructures.

CAS – Channel Associated Signalling. This is a type of signalling associated with telephony where some dedicated bits in the transmitted stream are directly used to signal information about a particular voice channel. “T1 Robbed-Bit” is well known example of a CAS protocol used in United States.

E1 – 2.048 Mbit full duplex Communication Interface. Used in most countries outside of the United States, Canada and Japan.

HTTP - Hypertext Transfer Protocol. Used on the ApplianX to send information to and from Web Browsers

ISDN – Integrated Services Digital Network. Used within the ApplianX and this document to describe the family of protocol that have there origins in the ITU's Q931 and Q921 specifications. ETS300 102 in Europe and National ISDN 2 (NI2) are typical examples of ISDN protocols.

LAYER 1 – Known as the physical layer in the OSI (Open Systems Interconnection) 7 layer model. Responsible only for getting raw bits from one node to another. It has some alarm and error transmitting capabilities. Basically Layer1 accepts requests from Layer 2.

LAYER 2 – Known as the data link layer in the OSI (Open Systems Interconnection) 7 layer model. This transfers data between two nodes on the same network. It usually has error detection and possibly correction. Within this document and the ApplianX user screens we refer to Layer 2 for TDM protocols. For ISDN protocols this is based upon the ITU (International Telecommunications Union) Q921 standard.

LINUX – A Unix like operating system that is supported and distributed by many organisations. Well know distributions include RedHat, Fedora, Suse, Debian and Ubuntu to mention just a few.

MAC OS X – The Unix based operating system used on Apple (Apple Incorporated formerly Apple Computers Incorporated) PC's.

PBX – Private Branch eXchange. This is a local switch that traditional terminates POTS (Plain Old TelephoneS) and route calls between users and into other switches on TDM networks (and more recently IP networks).

SIP – Session Initiation Protocol. A signalling protocol that has been defined by a number of IETF (Internet Engineering Task Force) that can be used for, among other things, setting up and controlling IP voice communications. The ApplianX IP gateway uses this for the setting up of IP telephony calls.

SNMP – Simple Network Management Protocol. This can be set up on the ApplianX so that SNMP software (not supplied) can be used to monitor elements of the

ApplianX status remotely. This requires use of the MIB (Management Information Base) that can be found on the ApplianX web site <http://www.applianx.com>.

T1 – 1.544 Mbit full duplex Communication Interface. Used mostly in the United States, Canada and Japan.

TDM – Time Division Multiplexed. Used in this documents to reference the ISDN and CAS Trunks. Also know as the T1 or E1 interfaces on the ApplianX

Timeslot – A dedicated slot on the TDM interface used for carrying digitised voice and data information. Typically an E1 interface will have 30 of these and T1 23 or 24.

TRUNKS – Either an E1 or T1 interface. A wired connection that carries a collection of voice channels and signalling channels. Sometimes the ApplianX will refer to “SIP Trunks”. This is a virtual concept that all IP Telephony traffic is a “Trunk”. This is for the benefit of writing routing tables and rules.

URI – Uniform Resource Identifier. Within the context of the ApplianX this is used for identifying the addresses of SIP User Agents (IP Phones). It is used in the wider networking world and is not SIP specific.

USB – Universal Serial Bus. Used with the ApplianX for inserting external memory devices for the configuring of IP settings and saving and restoring of configurations.

User Agent –Used within this document to indicate a SIP Telephone although it does have meaning in other contexts such as the World Wide Web.

Web Interface – This is the User Interface on the ApplianX that has been designed to work with a web browser (not supplied) to allow administrators to configure, monitor and maintain the ApplianX. Examples of web browsers are Microsoft Internet Explorer (ie6/ie7), Safari, Firefox and Opera to name just a few.

Windows – Within this document Windows is used a collective term for a number of operating systems developed by Microsoft Corporation. Namely Windows XP, 2003 Server and Vista. (Previous versions such as 3.1, 95, 2000 and ME have not been tested against the ApplianX)

ZEROCONF – This is a set of techniques that automatically creates a usable network without DHCP and DNS servers or manual configuration. This is used in the ApplianX when the unit is set to DHCP and no DHCP server can be found on the network.