Your PDF Guides

You can read the recommendations in the user guide, the technical guide or the installation guide for SIEMENS GIGASET 504. You'll find the answers to all your questions on the SIEMENS GIGASET 504 in the user manual (information, specifications, safety advice, size, accessories, etc.). Detailed instructions for use are in the User's Guide.

User manual SIEMENS GIGASET 504
User guide SIEMENS GIGASET 504
Operating instructions SIEMENS GIGASET 504
Instructions for use SIEMENS GIGASET 504
Instruction manual SIEMENS GIGASET 504

SIEMENS

Gigaset 504 AGU

Gigaset

For network security, wireless transmission can be encrypted using the WPA/WPA2 standard or 64/128-bit WEP.

Your device allows several users to access the Internet simultaneously. A single user account can be shared if your Internet service provider permits this. If you want to surf the Internet, watch IPTV and make calls using the Internet at the lowest possible cost, the Gigaset devices are a convenient and simple solution. The devices have an extensive range of functions but remain simple to use. They can be configured and operational within a few minutes. 4 The product series Gigaset 501/504 Do your part for the environment (ECO) Thanks to a switch-mode power supply unit, all of our broadband products offer significantly reduced power consumption - for more energyefficient use, which helps make a cleaner environment for everyone. You can turn the WLAN off completely when you're not using it. It's our goal to ensure a sustainable economic process by using an environmentally friendly production and management system - which makes it easy for us to meet the strict ISO 14001 standards for international environmental management. Features and applications The router Gigaset 504 AGU's wide range of features makes it ideal for a large number of applications. Depending on your device, some of the features may differ from the description in this instruction manual.

u Internet access The router supports shared Internet access for up to 252 users via the integrated ADSL /ADSL2+ modem. This means several users in your network can surf the Internet at the same time, all using the same Internet account. u Setting up a local area network The router offers the following possibilities: Depending on the device up to four devices connected via Ethernet ports with a transmission speed of 10 or 100 Mbps (with automatic recognition).

You're reading an excerpt. Click here to read official SIEMENS GIGASET 504 user guide

http://yourpdfguides.com/dref/3955640

Up to 252 mobile terminals connected via a radio interface with a transmission speed of up to 54 Mbps. It complies with IEEE 802. 11g standard and can work with all products that satisfy Standard IEEE 802.11b or 802.11g. Using the router Gigaset 504 AGU makes it easy to set up a network at home or in small offices. For example, users can exchange data or share resources in the network, such as a file server or printer.

The router Gigaset 504 AGU supports DHCP for dynamic IP configuration of the local area network, and DNS for domain name mapping. An introduction into the various options of establishing a local network can be found in the appendix in section "Local area networks with Gigaset products" on page 66. u Security functions The router Gigaset 504 AGU offers comprehensive security features: Firewall protection against unauthorised access from the Internet All PCs in the local area network use the Public IP address of the router to establish Internet connections, making them 'invisible' to other Internet users. The router only allows access from the Internet if it has been requested from the local area network. Thanks to the firewall, the router also offers comprehensive protection against attacks from computer hackers. 5 The product series Gigaset 501/504 Service filtering and URL blocking The router can filter Internet access, allowing you to determine which PCs may access which Internet services. You can also deactivate access to certain Internet domains and sites (URL blocking). Access control and encryption for the local area network You can use various encryption methods and authentication methods (WEP, WPA/ WPA2-PSK, WPA/WPA2, MAC access control) to prevent unauthorised access to your wireless LAN or to make data illegible to ung the device fulfilled. u To access the Internet you require a DSL port (splitter), the access data for your Internet service provider. For experienced users The default settings for the router Gigaset 504 AGU are: IP address: 192.

168.254.254 Subnet mask: 255.255.255.0 WLAN: Off SSID: AlShamil Radio channel: 1 or automatic System password: admin Trademarks Gigaset Communications GmbH is a trademark licensee of Siemens AG. Microsoft, Windows 98/SE, Windows ME, Windows 2000, Windows XP, Windows Vista and Internet Explorer are registered trademarks of the Microsoft Corporation. Mozilla Firefox is a registered trademark of the Mozilla Organisation. 11 Installing the device Installing the device Overview of the installation steps 1. First install an Ethernet network card in the PCs you want to connect to the router Gigaset 504 AGU.

The installation is described in the user guides for these products. 2. Then make the necessary connections (PCs, splitter) on the router Gigaset 504 AGU and activate the device (page 15). 3. Then configure the router Gigaset 504 AGU to activate the device's Internet access (refer to the section entitled "Internet" on page 23).

To do this you will need the access data for your Internet service provider. 4. If you wish to use other functions of the router Gigaset 504 AGU, for example the comprehensive security features, use the Advanced Settings (page 22). Note: Before the PCs can communicate with the router and with each other in a local network, you may have to change your network settings (see page 17). Configure these network settings on one PC first so that it can establish a connection to the router.

You can then use this PC to configure the device. To find out how to do this, refer to the document entitled "Configuring the local area network" on the CD-ROM. Setting up the router Gigaset 504 AGU The router can be set up in any suitable location in the home or office. You do not need any special wiring. However, you should comply with the following guidelines: u Operate the router only indoors within a temperature range of 0 to +40 °C. Do not u u u u u u position the router near sources of heat. Do not cover the ventilation slots. High temperatures can damage the device. A mains socket for 220/230 V~ and a connection socket for the splitter or LAN must be available in the place where you set up the router. Do not position the device in the immediate vicinity of stereo equipment, TV sets, microwave ovens or the like.

This may cause interference. Position the router so that it is as near to the centre of your wireless network as possible. The general rule is: The higher you place the antenna, the better the performance. Make sure that the place where you position the router offers optimum reception throughout the house, apartment or office. Make sure the router cannot fall down, as this could damage the antenna. Position the router on a non-slip surface. Do not place the router on any furniture surface that could be affected by the heat from the device. Lay the cables so that nobody can trip over them. You should not cover the cables with anything. 12 Installing the device Please remember: Network connections (LAN) via cables and telephone lines may only be set up with the router within enclosed rooms.

Connecting to the splitter data port You can operate the router in two different operating modes in order to set up an Internet connection: with an integrated ADSL modem with an external modem, such as a VDSL or cable modem Using the integrated ADSL modem ì Connect the ADSL port (grey) on the router to the ADSL socket on the splitter. To do this, use the DSL cable supplied (grey). Splitter ADSL cable (grey) 13 Installing the device Using an external modem In this case the LAN1 port is used as WAN port. The integrated ADSL modem is then deactivated. ì Connect the LAN1 port on the router with an external modem.

To do this, use the ì Then connect this modem to the relevant communications port (e.g. splitter). cable supplied with your modem or any Ethernet straight cable having an RJ45 connector on both sides. Modem Ethernet cable To put the LAN port into operation for a WAN connection you have to change the Connection type of the Internet connection to Ethernet (see page 23).

14 Installing the device Wired connection to the PC You can connect wired or wireless PCs to your router to create a local area network (LAN). First connect just one PC to the router via cable. You can then carry out the general configuration. Wireless connection is possible after completing the installation of the router and switching on the WLAN function via the configuration program. You will find information about this topic in the chapter "Configuring wireless connections" on page 39. ì Connect one of the LAN ports (LAN1 LAN4, yellow) on the router to the Ethernet network card in your PC. To do this, use the LAN cable supplied (CAT5, yellow). LAN cable (yellow) ì Alternatively you can also connect a PC via the USB port (blue).

15 Installing the device Connecting to the mains power supply Please remember: Only use the mains adapter supplied with the device (9 V DC, 1 A). ì Connect the mains adapter cable to the POWER socket on the router.

ì Plug the mains adapter into a mains socket. ì Switch on the device. The router is now switched on and ready for operation. Checking the operating state Your router Gigaset 504 AGU is now ready for use. The LED displays on the front panel of the router provide information about the operating state (see page 8). When the device is ready for use, the LEDs light up as follows: u The Power LED on the front lights up. u The ADSL LED flashes to indicate that the DSL connection is being synchronised. Once this process is complete, the ADSL LED lights up permanently. u The LAN LEDs light up if a device is connected to the corresponding LAN port. u The USB LED lights up if a device is connected to the USB port.

If this is not the case, refer to the section entitled Troubleshooting on (page 62). Making the basic settings You can now make the basic settings for Internet access using the user interface of the router (page 18). 16 Installing the device Network configuration of the PCs In order to communicate via the router Gigaset 504 AGU, the network configuration may have to be set up on the connected PCs. This usually takes place automatically provided you have not made any changes to the standard settings for the network configuration and you use one of the following operating systems: u Windows Vista u Windows XP u Windows 2000 With Windows 98/SE, you have to carry out the network configuration. The description of the network configuration can be found on the CD-ROM.

17 The user interface The user interface You have connected a PC to the router Gigaset 504 AGU and possibly made the settings in the local area network. You can now configure the router using this PC from the user interface of the router. As Internet browser we recommend Microsoft Internet Explorer V 6.0 or higher, or Mozilla Firefox V 1.0 or higher.

Note: To start the configuration environment, you may need to deactivate the HTTP proxy for your browser. If you use Window Vista or Windows XP Service Pack 2, you will need to configure the popup blocker. You will find additional information on these two points on "Deactivating HTTP proxy and configuring a pop-up blocker" on page 72. If you use a firewall, it must allow connection to the router. For details, refer to the user guide for your firewall. If necessary, deactivate the firewall before you configure your router. You can re-activate the firewall afterwards. Starting the user interface To access the user interface of the router Gigaset 504 AGU: ì Start your Internet browser. ì Enter the IP address of the router in the browser's address field: http://192.168.

254.254 The login screen appears: For your security, the configuration program is protected with a password. The default password generally required is admin. This may differ depending on the provider settings. If necessary, check the details on the device label. 18 The user interface ì Enter the password. ì Click Login. Note: For security reasons you should change this password at a later stage (page 50). A page with security information will appear. If you carry out all the general and security settings using the user interface, your device and network will be fully protected.

If not, the next time you log on you will be informed of security gaps in the configuration program. ì Click OK. The start screen is displayed. The start screen The start screen is the starting point for all configuration and administration procedures. Start screen functions You can start the following actions on the start screen: u Select the language for the user interface (page 20).

u When you have configured an Internet connection for the first time, you can view the selected connection service and the status of the Internet connection, choose a different connection service and set up or close an Internet connection (page 20). The start screen shows the status and also the Connect or Disconnect button. u Open the Status menu to obtain status information about the router (page 56). u Open the Advanced Settings menu for additional configuration options (page 22). You can call up the Advanced Settings menu and Status information at any time and on any user interface screen using the tabs at the upper margin of the user interface.

19 The user interface Selecting a language The user interface exists in various languages. The language modules available are located on the CD supplied. If you wish to change the preset language, proceed as follows: ì Insert the CD into the CD drive of your PC. ì Click Language at the top right of the start screen. ì Select the new language you require from the list. ì Click OK to load the desired language. ! Do not switch off the device during loading, as this could render your device inoperative. Once the procedure has been concluded, the start screen will be displayed again. Connecting to the Internet manually Once you have configured your Internet access (see page 25), you can establish a manual connection to the Internet on the start screen if you have selected Connect on demand or Connect manually as the Connection mode. To establish or end an Internet connection manually: ì Open the start screen of the router as described on page 18.

If you have already started the user interface, click the start screen tab at the top left of the window. If you have not yet started the user interface, do so now and log on. ì Click Connect to establish a connection to the Internet. ì Click Disconnect if you no longer require the connection. 20 The user interface Elements in the user interface The user interface screens contain the following elements: Help Click this tab top right on the screen to display explanations about the current user interface screen. Log Off button The Log Off button is always displayed on the right of the user interface. If you click Log Off, the session is ended and the login screen appears again. Buttons in the Advanced Settings menu OK Cancel Transfers the settings you have made to the router configuration. Deletes all the entries on a screen since the last time you clicked OK. Other buttons may be displayed depending on the function in question. These are explained in the relevant sections. 21 Configuring Advanced Settings Configuring Advanced Settings In the Advanced Settings menu, you can configure all the options for the router Gigaset 504 AGU. The following table contains the options available in this menu. Menu Internet Description This menu comprises all the setting options relating to the Internet. In particular, you can do the following: u Check and change the configuration for Internet access (page 25), Local Network Wireless Network Administration functions, for example access control from local PCs to the Internet or the blocking of certain Web sites (page 28), u Make the NAT settings required to provide your own services on the Internet (page 30), u Set up dynamic DNS for a fixed Internet address on the device (page 35), u Configure the Quality of Service (QoS) (page 36).

You can change the Private IP address of the router here and make settings on the DHCP server (page 37). You can configure the options for wireless communication (SSID and encryption) here and restrict access to the router (page 39). You can make or change various system settings here, for example change the password (page 50), set the time (page 49) or activate remote management (page 51). In addition, you can also back up the data on the router or update the firmware (page 52). u Configure the firewall, i.

e. a number of security and special 22 Configuring Advanced Settings Internet If you have configured the router Gigaset 504 AGU using the Gigaset Installer, you have also configured the WAN connection (Internet access). You can check or change these settings in the Internet menu. This menu also offers you a wide range of possibilities for setting up security settings and limiting access to the Internet as well as for providing your own services on the Internet. You can carry out the following via the Internet menu: Internet Activate/deactivate the Internet connection, set up additional connection services and edit the virtual connection parameters (see page 23), Check and edit the configuration of the Internet connection (see page 25), Protect the network against unauthorised external access (see page 28), Provide your own services on the Internet (NAT, see page 30), Set up dynamic DNS (page 35), Quality of service: You can define the settings and quality for data transfer (see page 36) Internet Connection Firewall Address Translation (NAT) Dynamic DNS Qos Internet selection You can activate or deactivate the Internet connection for the router on this screen. You can choose the connection type and set up and edit a number of connection services. ì In the Advanced Settings menu, select: Internet. ì Select the appropriate option to activate or deactivate the Internet function of the router. 23 Configuring Advanced Settings ì Choose the desired Connection type for your Internet connection: Choose the ADSL if you are using the integrated ADSL modem of the router. Choose Ethernet if you are setting up the connection to the Internet via an Ethernet network connection (e.

g. if you are using an external modem with an Ethernet connection). If you change the connection type, you must also modify your Internet access settings accordingly (page 25). ì If you have selected Ethernet, click OK to save and apply the changes. ì If you have selected ADSL, you can now set up multiple connection services. Configure multiple connection services Your Internet service provider can permit you to set up a number of Connection services. You can set up these services here. ì Select the appropriate option to activate or deactivate Configure multiple connection services. If you have already configured an Internet connection, this is shown as Connection service selected to edit. This is then also displayed on other pages of the Internet menu. ì Make the following settings: Enter the VPI / VCI values for each connection service that you have received from your Internet service provider. Enter a description to identify the respective connection service. Click Add to create a new entry. Click Delete to delete an entry. ì Click OK to save and apply the changes.

24 Configuring Advanced Settings Internet Connection You can set up or change the configuration of your Internet connection on this screen. All the settings you make here must coincide with the features your Internet service provider makes available to you. False information can lead to problems with your Internet connection. ì If you want to configure or modify settings for the Internet connection, select from the Advanced Settings menu: Internet Internet Connection. Connection type ADSL All settings apply for the displayed connection service that you selected for editing on the Advanced Settings Internet (page 23) screen.

If you only set up one connection service, no selection is displayed. ì Enter the account data you have been given by your service provider: Protocol, User name, Password. ì Enter a Host name for your router ì Choose if your router should be used As Default Gateway for this Internet connection. ì Apply the default settings for the parameters MTU, Line mode, Encapsulation, QoS class and VPI / VCI unless your service provider has provided you with other data. Note: Please ensure that you enter all the details from your provider correctly, otherwise the configuration may fail and you will not be able to connect to the Internet. 25 Configuring Advanced Settings Connection type Ethernet ì Enter the account data you have been given by your service provider: User name, Password. ì Enter a Host name for your router ì Apply the default setting for the parameter MTU, unless your service provider has provided you with other data. Note: Please ensure that you enter all the details from your provider correctly, otherwise the configuration may fail and you will not be able to connect to the Internet. ì Specify how Internet sessions are to be established via Connection mode: Select Always on if the connection is to exist at all times when the router is turned on. Note: If you are on a time-based tariff, this option can result in high connection charges.

 Select Connect on demand if applications such as an Internet browser or an email program are to connect to the Internet automatically. In the Idle time before disconnect field, enter a period after which the Internet connection is to end automatically if no data is transmitted (the default setting is 3 minutes). This time setting only applies to the Connect on demand and Connect manually options. Select Connect manually if you always want to establish and end the Internet connection manually. If you are on a time-based tariff this will save you high connection charges. Setting the Connection mode ì Click OK to apply the settings. 26 Configuring Advanced Settings Using UPnP (Universal Plug and Play) PCs with UPnP (Universal Plug & Play) can offer their own network services and automatically use services offered in the network. Note: The operating system Windows ME, Windows XP or Windows Vista must run on the PC. Check, if the UPnP function has been installed on the PCs operating system. Maybe you have to install the UPnP components retroactively.
Please consult the documentation of your operating system. As soon as you have installed UPnP on a PC operating system and activated it on the router, applications on this PC (e.g. Microsoft Messenger) can communicate via the Internet without you needing to expressly authorise it. In this case, the router automatically implements Port forwarding, thereby facilitating communication via the Internet.

The task bar on the PC on which UPnP is installed contains an icon for the router. Click this icon to open the user interface. On Windows XP system, this icon is also shown under network connections. ì In the Advanced Settings menu, select: Internet Internet Connection. ì Click UPnP.

Note: When the UPnP function is active, system applications can assign and use Ports on a PC. This poses a security risk. ì Click OK to apply the settings. 27 Configuring Advanced Settings Firewall The firewall functions of the router Gigaset 504 AGU include various security functions for the local network. You can do the following: u Enable or disable the router firewall. u Block access by individual PCs to selected services or Web sites. The firewall functions for the router are activated and configured in the factory. If you want to deactivate the firewall, carry out the following steps: ì In the Advanced Settings menu, select: Internet Firewall. ì Click the required option. ì Click OK to apply the settings.

Setting up access control to the Internet The Access Control function allows you to control access to various services for one or more PCs. You can permit or block access to URLs and services at certain times. ì In the Advanced Settings menu, select: Internet Firewall Access Control. 28 Configuring Advanced Settings ì Activate the Access Control function by selecting On. You have the following setting options for Access Control: URL Filter With the URL Filter you can block or allow access to certain Web sites or Internet domains. When you have entered the relevant URLs, you can create access rules which use the URL Filter for selected clients in your network. ì Select the Filtering mode: ì ì ì ì Allow URLs in list (block all others) or Block URLs in list (allow all others) Enter the relevant URL in the field. Click Add to create a new entry. Click Delete to delete an entry. Click OK to apply the settings.

Access Rules You can limit access to the Internet for all clients, or only for certain clients in the network, thereby allowing or blocking access to services. ì Click Add to create an access rule. ì Select the Access rule type from the list: Apply to all clients: The rule applies to all PCs in the network. Specify IP address range: You select the PCs to which the rule is to apply by entering an IP address range. Specify IP address or Specify MAC address: The rule applies to a PC you have selected via the IP address or MAC address.

ì Enter a name for the access rule in the Comment field. ì Define the Access level. Choose one of the following options: Deny access to internet Allow web browsing Allow web browsing with URL filter If you have set up URL filters on the Access Control screen (page 29), you can activate them here. 29 Configuring Advanced Settings Custom You can specify your own service filter here. Specifying an own service filter The services in the list are blocked for Internet access.

The specified service filter applies to all clients. To create a service filter, proceed as follows: ì Select the services that are to be blocked. Select predefined services from the Predefined applications list. The most popular Internet services are offered. Or Specify your own services manually. Select the Protocol and enter the appropriate port number or port range in the Port start and Port end fields. To define one single port enter the same number in both fields. Entering a Comment that is displayed will help you to identify different services. Enable the Filter checkbox to use the respective service for the service filter. Click Add to create a new entry with the entered data or for the selected, predefined application.

ì ì Click Delete to delete an entry. ì When you have completed all the settings in this screen, click OK to apply them. Setting up the NAT function The router Gigaset 504 AGU comes equipped with the NAT (Network Address Translation) function. With address mapping, several users in the local network can access the Internet via one or more public IP addresses. All the local IP addresses are assigned to the router's public IP address by default. One of the characteristics of NAT is that data from the Internet is not allowed into the local network unless it has been explicitly requested by one of the PCs in the network. Most Internet applications can run behind the NAT firewall without any problems. For example, if you request Internet pages or send and receive e-mails, the request for data from the Internet comes from a PC in the local network, and so the router allows the data through. The router opens precisely one port for the application. A port in this context is an internal PC address, via which the data is exchanged between the Internet and a client on a PC in the local network.

Communicating via a port is subject to the rules of a particular protocol (TCP or UDP). If an external application tries to send a call to a PC in the local network, the router will block it. There is no open port via which the data could enter the local network. Some applications, such as games on the Internet, require several links, i.e.

several ports so that the players can communicate with each other. In addition, these applications must also be permitted to send requests from other users on the Internet to users in the local network. These applications cannot be run if Network Address Translation (NAT) has been activated. 30 Configuring Advanced Settings Using port forwarding (the forwarding of requests to particular ports) the router is forced to send requests from the Internet for a certain service, for example a game, to the appropriate port(s) on the PC on which the game is running. When the router is supplied, the NAT function (Network Address Translation) is activated, i.

e. all IP addresses of PCs in the local network are converted to the router's public IP address when accessing the Internet. 31 Configuring Advanced Settings You can use the NAT settings to configure the router to carry out the following tasks: u Set up the router as a virtual server by configuring Port Forwarding (page 32), u Open the firewall for a selected PC (page 34). Note: For the functions described below, the IP addresses of the PCs must remain unchanged. If the IP addresses of the PCs are assigned via the DHCP server of the router, you must select Never expires (page 38) as the setting in the Local Network menu entry for the Lease time or assign static IP addresses for the PCs. By default the NAT function is activated. You should only deactivate the NAT function if you want to configure you own firewall in you local network. ì In the Advanced Settings menu, select: Internet Address Translation (NAT) ì Select the required option.

Port Forwarding If you configure Port Forwarding, the router Gigaset 504 AGU outwardly assumes the role of the server. It receives requests from remote users under its public IP address and automatically redirects them to local PCs.

The private IP addresses of the servers on the local network remain protected. Internet services are addressed via defined port numbers. The router needs a mapping table of the port numbers to redirect the service requests to the servers that actually provide the service. Port Forwarding has been configured for this purpose. 32 Configuring Advanced Settings ì In the Advanced Settings menu, select: Internet Address Translation (NAT) Port Forwarding ì ì ì ì Select the required application from the Predefined Applications list. Select the checkbox in the Enabled column to activate the entry. Click the Add button. The data for the required service is entered on the screen. Click the Delete button to delete an entry. If the application you require is not in the list, you must manually enter the relevant data on the screen: ì Select the protocol for the service you are providing from the Protocol list.

ì Under Public port, enter the port number(s) of the service you are providing. You can use   a single port number, several port numbers separated by commas, port blocks consisting of two port numbers separated by a dash, or any combination of these (for example 80,90-140,180). ì In the Local port field, enter the internal port number to which service requests are to be forwarded. You can only specify one port number here. ì Enter the IP address of the PC that provides the service in the Local IP address field.

Example: The Web server has been configured to react to requests on port 8080. However, the requests from Web sites enter the Web server via port 80 (standard value). If you add the PC to the forwarding table and define port 80 as the public port and port 8080 as an internal port, all requests from the Internet are diverted to the service with the port number 80 on the Web server of the PC you have defined with port 8080. ì ì ì ì ì Comment: Enter a description that makes it easy to identify different entries. Select the checkbox in the Enabled column to activate the entry.
Click the Add button to add a new entry. Click the Delete button to delete an entry. Click OK to apply the settings. 33 Configuring Advanced Settings Opening the firewall for a selected PC (Exposed Host) You can set up a client in your local network to be a so-called "exposed host" (DMZ). Your device will then forward all incoming data traffic from the Internet to this client. You can then, for example, operate your own Web server on one of the clients in your local network and make it accessible to Internet users. As the exposed host, the local client is directly visible to the Internet and therefore particularly vulnerable to attacks (e.g. hacker attacks). Only activate this function if it is absolutely necessary (e.

g. to operate a Web server) and other functions (e.g. port forwarding) are not adequate. In this case you should take appropriate measures for the clients concerned. Note: Only one PC per public IP address can be set up as an Exposed Host (see also Port Forwarding on page 32). ì In the Advanced Settings menu, select: Internet Address Translation (NAT) Exposed Host ì ì ì ì Enter the Local IP Address of the PC that is to be enabled as an Exposed Host. Enter a name for the PC in the Comment field. Activate Enabled by ticking the check box. Click the Add button to add the entry to the list.
You can add more than one PC to the list, but you can only activate one of them. ì Click the Delete button to delete the entry from the list. ì Apply the settings by clicking OK. 34 Configuring Advanced Settings Dynamic DNS Any service you provide on the Internet can be accessed via a Domain name. Your router's Public IP address is assigned to this domain name.
If your Internet service provider assigns the IP address for your local network's WAN connection dynamically, the IP address of the router can change. The assignment to the domain name will no longer be valid and your service will no longer be available. In this case you must ensure that the assignment of the IP address to the domain name is updated regularly. This task is performed by the dynamic DNS service (DynDNS). You can use the DynDNS service to assign the router Gigaset 504 AGU an individual fixed domain name on the Internet even if it does not have a static IP address.
Various Internet service providers offer a free DynDNS service. If you use the service of a DynDNS provider, your service can be reached on the Internet as a subdomain of one of the DynDNS service domains. One possible service is DynDNS.org (http://www.DynDNS.org). If you have activated the device's DynDNS function, it will monitor its public IP address. When this changes, the device will open a connection to DynDNS.org and update its IP address there. Note: You must have an account with the service you have chosen (e.

g. DynDNS.org) before you can use the DynDNS function. Follow the instructions on the provider's Web site. Then enter the user data when configuring the router. ì In the Advanced Settings menu, select: Internet Dynamic DNS ì Activate the Dynamic DNS function. ì Select a provider from the Service provider list. ì Enter Domain name, User name and Password. You will have received all the necessary information when you registered with your Service provider. ì Click OK to apply the settings.
35 Configuring Advanced Settings Qos (Quality of Service) Many communication and multimedia applications require high speed and large bandwidths to transfer data between the local network and the Internet. However, for many applications there is often only one Internet connection available with limited capacity. Qos (Quality of Service) divides this capacity between the different applications and provides undelayed, continuous data transfer where data packets with higher priority are given transmission preference. The QoS configuration dialogue enables you to optimise the transmission behaviour for certain applications. For example IPTV is your favourite application and so you want to ensure that no other application will disturb the transmission of IPTV data.
ì In the Advanced Settings menu, select: Internet Qos. All settings apply for the displayed connection service which you selected for processing in the Advanced Settings Internet screen (page 23). ì Select the option Differentiated services, i.e. the prioritisation of certain services for the data transfer between your network and the Internet.
For each Priority is specified which data packets are to be given priority of transfer.

In addition, PHBs (Per Hop Behaviours) are used to decide whether data packets are to be forwarded immediately and ahead of all others (EF, Expedited Forwarding), guaranteed and without data loss (AF, Assured Forwarding), or normally (BE, Best Effort). If your application already supports QoS, it determines the priority automatically. Your device recognises this when forwarding. It recognises certain Predefined applications and assigns each packet the relevant priority. You can also define what proportion of the bandwidth for your Internet connection is to be made available to a particular class as Allocated bandwidth. ì Select the Allocated bandwidth for Predefined applications. ì Click OK to save and apply your changes. 36 Configuring Advanced Settings LAN configuration You can use the LAN configuration to define an IP address for the router Gigaset 504 AGU and configure the DHCP server. ì In the Advanced Settings menu, select: Local Network.

Defining the private IP address for the router Gigaset 504 AGU On this screen you can change the device's IP address. The preset IP address is 192.168.254.254. This is the Private IP address of the router. This is the address under which the device can be reached in the local network. It can be freely assigned from the block of available addresses. The IP address under which the router can be reached from outside is assigned by the Internet service provider. The default Subnet mask for the local network administered by the router is 255.
255.255.0. ì If you want to assign a different IP address to the router, enter your chosen IP address in the boxes next to IP address. Please make sure to note which subnet mask is set when assigning the IP address.
The preset subnet mask defines that the first three parts of the IP address must be identical for all network components (including routers). We recommend that you use an address from a block that is reserved for private use. This address block is 192.168.1.
1 to 192.168.255.254. ì Adjust the Subnet mask if necessary. The Subnet mask specifies how many address parts of the IP address must be identical for all network components (including routers). 37 Configuring Advanced Settings Notes: New settings can only be made after the router has been rebooted. If necessary, reconfigure the IP address on your PC (including one that is statically assigned) so that it matches the new configuration. Configuring the DHCP server The router has a DHCP server for which the factory setting is active. Consequently, the IP addresses of the PCs are automatically assigned by the router.

Note: u If the DHCP server for the router is activated, you can configure the network setting on the PC so that the option Obtain an IP address automatically is set up. For further information, refer to the section entitled "Configuring the local area network" on the CD-ROM. u If you deactivate the DHCP server, you will have to assign a static IP address for the PCs that use the network settings. ì To activate the DHCP server, select On. ì If the DHCP server is active, you can define a Lease time. The least time indicates how long the client may use the allocated IP configuration. Note: If you select Never expires, the IP addresses are never changed. Activate this option if you want to make NAT or firewall settings using the IP addresses of the PCs; otherwise you have to assign static IP addresses to these PCs. ì Define the range of IP addresses the router should use to automatically assign IP addresses to the PCs. Define the First issued IP address and the Last issued IP address.
field. ì You can define the name of a domain (Windows workgroup) in the Domain name ì Apply the settings by clicking OK. Assigning static IP addresses to individual PCs Even if you have activated the DHCP server, you can still assign a static IP address to individual PCs (e.g. when setting up these PCs for NAT functions).
ì ì ì ì ì Enter the MAC address of the PC to which you want to assign a static IP address. Enter the IP address you wish to assign to the PC. Click Add to add the entry to the list. Click Delete to delete the entry from the list. Apply the settings by clicking OK.
38 Configuring Advanced Settings Configuring wireless connections The WLAN function of your router Gigaset 504 AGU is deactivated on delivery. You can activate it on this page. If you have implemented wireless PC communication via the router, you should improve the security settings of your wireless network via the Advanced Settings Wireless Network menu. You can carry out the following functions: Wireless Network Activate the wireless module of the router and specify basic settings for your wireless network, for example SSID, Transmission mode or Sending power. Set up Encryption for wireless transmissions (page 41). Restrict access to the LAN of the router (page 45). Activate the repeater function (Wireless Distribution System, WDS) and define repeaters to increase the range of your WLAN (see page 46). Encryption Allowed Clients WDS Setting ì In the Advanced Settings menu, select: Wireless Network. ì Select On for the Wireless Network. Devices can only log in wirelessly if the WLAN module of the router is activated.

You can now make the settings for the wireless network. Channel All clients in the network use the set radio channel for wireless data transfer. You can choose between various channels, depending on your current location. ì Select Automatic so that the best channel for transmitting the data is used automatically. 39 Configuring Advanced Settings SSID For the wireless network components to be able to communicate with one another, you must use the same SSID (Service Set Identifier). The default SSID for the router is AIShamil. For security reasons you should change this SSID. ì Enter a character string of your choice. The SSID is case-sensitive. It can contain up to 32 characters.
Use a combination of letters, digits and special characters. Note: The connection to the wireless network adapters will be interrupted until you have entered the new SSID in them as well. SSID broadcast If this option is enabled, the router will send the SSID in all data transfers and the SSID of the router will be displayed on PCs that have a wireless network adapter. In this case, hackers could use the SSID to detect your network. If SSID broadcast is deactivated, the SSID of the router will not be displayed.
This increases protection against unauthorised access to your wireless network. Make a note of the SSID. You will need it to log on to the PC. ì Select Off to deactivate SSID broadcast. To protect your wireless network, you should also enable encryption of data transmissions (page 41).
Transmission mode The IEEE 802.11g standard permits data transfer up to 54 Mbit/s, and the IEEE 802.11b standard up to 11 Mbit/s.

Choose IEEE 802.11g only to ensure the best possible data transfer rates in your network. To operate clients with older wireless network adapters in your network, select IEEE 802.11b/g (mixed). ì Select the required transmission mode for your wireless network. ì Select the required sending power for your device. Sending power It is recommended that you select a sending power with a range to suit the spatial environment of your local network.

A much greater range makes it easier to eavesdrop on your wireless data transfer. ì Click OK to apply the settings. 40 Configuring Advanced Settings Setting encryption If you are sending data over radio channels, we recommend that you activate encryption (WEP or WPA) on the components in the wireless network. WPA offers greater security than WEP. You should therefore select WPA encryption if it is supported by all components in your wireless network. WPA-PSK is a more efficient method for protecting wireless networks. Dynamic keys, based on TKIP (Temporal Key Integration Protocol) offer increased security. The new WPA2-PSK standard is based on AES. ì In the Advanced Settings menu select: Wireless Network Encryption The following security mechanisms are currently available: u WPA2-PSK and WPA2-PSK/WPA-PSK (page 41) u WEP encryption (Wired Equivalent Privacy, page 42) Note: If you want to use the repeater function of your router (page 46) you can only use WEP encryption. WPA2-PSK and WPA-PSK/WPA2-PSK WPA with pre-shared key (WPA-PSK) WPA-PSK is a special WPA mode for private users and users in small companies without their own authentication server.
After a certain period of time (Rekey interval), encryption keys are automatically generated with the pre-shared key, automatically changed ("rekeying") and authenticated between the devices. The standard of encryption available to you depends on the components in the wireless network. Every PC (network adapter) that requires access to a WPA-protected wireless network must also support WPA. To find out whether and how you can use WPA on your PC, read your network adapter's user guide. If all components support WPA2, select WPA2-PSK.
If you are using network adapters that only support WPA, select WPA-PSK/ WPA2-PSK. Your device then automatically defines the best possible way to protect your data for each client. The entries described below are identical for both options. ì Select the required option in the Security field. ì Enter a key in the WPA shared key field (up to 32 characters) and confirm it by entering it again.
Use a combination of letters, digits and special characters. 41 Configuring Advanced Settings ì If you select the Display characters option, the WPA shared key will be displayed in readable characters. ì Click OK to apply the settings. WEP encryption If WPA is not supported by all components in your wireless network, we recommend that you activate WEP Encryption on the components. ì Choose the WEP option in the Security field. ì Select the Authentication type: Select Shared to require that each client log in to the network with a specified key. Select Open to permit data transfer within the wireless network without the need to enter a key. You can choose either the standard 64-bit key or the more robust 128-bit key. The keys are generated in hexadecimal or in ASCII format. You must use the same keys for encryption and decryption for the router and all your wireless network adapters.

ì Select the Key length: 64 bits or 128 bits. ì Select the Input type, i.e. whether the key is to be entered manually or generated automatically by means of a Passphrase. 42 Configuring Advanced Settings Manual key entry ì Select the Key type, Hex or ASCII. If you select Hex as the key type, you can use the characters 0 to 9 and A to F. With a 64-bit encryption depth, the key is 10 characters long. An example of a valid key: 1234567ABC With a 128-bit encryption depth, the key is 26 characters long. An example of a valid key: 234567ABC8912345DEF1234567 If you select ASCII as the key type, you can use the characters 0 to 9, A to Z, a to z plus the special characters in the ASCII character set. With a 64-bit encryption depth, the key is 5 characters long. An example of a valid key: GIGA1 With a 128-bit encryption depth, the key is 13 characters long. An example of a valid key: GIGASET_504AG ì Enter up to four keys in fields Key 1 to Key 4. ì If you select the Display characters option, the keys will be displayed in readable characters. ì Select one of the four keys as the Default key. Note: u It is very important that you make a note of the key(s) that have been entered.
You will need this information to configure the wireless network adapters properly. u When you have concluded the configuration, you must change the WEP encryp- tion in the wireless network adapters for the connected PCs in the same way as they will not otherwise be given access to the wireless network of the router. ì Click OK to apply the settings. Generating a key by means of a Passphrase ì Enter a Passphrase (up to 32 characters) and confirm it by entering it again. The key is generated automatically.
43 Configuring Advanced Settings ì If you select the Display characters option, the Passphrase will be displayed in readable characters. ì Click OK to apply the settings. Connecting PCs wirelessly A wireless connection is made using a wireless network adapter that must be installed in your PC. This can be an 802.11g or 802.11b-compatible wireless network adapter. A wireless network is defined by assigning an identical SSID to all the devices. ì You should therefore enter the SSID for the router in your network adapter configuration: The default SSID is AlShamil. adapter and enter the correct key. ì Choose the used encryption method in the configuration settings of your network If the correct SSID and encryption key has been entered in your PC's wireless network adapter, the wireless link will be established automatically.

WLAN adapter 44 Configuring Advanced Settings Permitted clients On this screen you can specify the PCs that are to have wireless access to the router Gigaset 504 AGU and hence to your LAN and WLAN. The default setting for access control is deactivated. This means that all PCs that use the correct SSID can be logged in. Access control is based on the MAC addresss of the PC network adapters. ì In the In the Advanced Settings menu select: Wireless Network Allowed Clients. ì Activate access control by selecting On in the MAC address filter field. Entering PCs manually: fields. ì Enter the MAC Address and Device name of the required PCs in the appropriate ì Click Add to add the entry to the list. ì Click Delete to delete the entry from the list.

Note: Only following deletion is the entry transferred to the list of known MAC addresses.

ì Apply the settings by clicking OK. Selecting from the list of logged-in PCs ì Select the required PC from the Known wireless clients list. All PCs that were already entered manually on the router with the MAC address are displayed. ì Click Add to add the selected PC to the list. ì Click OK to apply the settings. 45 Configuring Advanced Settings Note: If you activate MAC access control, you must at least add the PC on which you are configuring the router to the list. Otherwise, you will have no access to the user interface and will receive an appropriate error message. If you have inadvertently denied all PCs access to the router, you have two options: u You can completely reset the router (page 10). u You can connect a PC to the router using one of the LAN connections. As MAC access control only affects PCs that are connected wirelessly, you can use this PC to change the configuration.

Repeater function (WDS) WDS (Wireless Distribution System) allows you to extend the range of your wireless network using a repeater. A repeater located at the outer range of a wireless network ensures that data is forwarded between WLAN clients in this wireless network and clients within its own wireless range. Repeaters and access points thereby form a common wireless network within which all clients can be moved about freely. Clients automatically set up a connection to the next access point / repeater (roaming). For security purposes you must determine which access points / repeaters are to form a common wireless network. If you want to use a repeater in your wireless network you must activate the Wireless Distribution System (WDS) function. Note: WDS can only be used with WEP encryption or without encryption. If you use WPA-PSK encryption (default) you have to change the encryption of your wireless network. For information refer to the section "Setting encryption" on page 41. ì In the In the Advanced Settings menu select: Wireless Network WDS Setting ì To activate WDS select the On option next to Wireless distribution system.

The environment is scanned for wireless networks in rage. If the search has been completed successfully the networks are displayed. 46 Configuring Advanced Settings All repeaters/access points in range are displayed with the following information: SSID Mac address Channel The Signal strength of the connection to the repeater, if one exists, is shown as a percentage. You can use this data to determine the best possible location for your repeater. You can register a maximum of three repeaters to extend your WLAN. You can enter additional repeaters manually. ì Click the Add button to register a repeater in your wireless network. ì Click the Delete button to remove a repeater from your wireless network. Note: The registered but currently unavailable repeaters are shown only by their MAC addresses. ì Click Refresh to update the display.

ì Click OK to apply the settings. 47 Configuring Advanced Settings Note: u WDS can only be used with WEP encryption or without encryption. You may have to change the encryption of your wireless network, if applicable. u The encryption settings on the repeater have to correspond to the settings on your router. u The router and the repeaters must use the same channel.

Further information can be found in the user manual for the repeater. 48 Administration Administration The user interface of the router Gigaset 504 AGU includes several helpful functions for administration. Regional Options System Password System Management Save & Restore Enables regional settings (page 49). Changes the system password (page 50). Configures system management (page 51).

Backs up and, if necessary, restores configuration data (page 52) or reset the router to the factory settings (page 53). Reboots the device (page 53). Updates firmware (page 54). Configures settings for the system log (page 55). Reboot Firmware Upgrade System Log Regional Options For operating your router Gigaset 504 AGU, you can select the location, time zone and format for entering the time and date, and you can also configure a time server for the Internet time (system time). ì In the Advanced Settings menu, select: Administration Regional Options. ì Select the country you are currently in from the list. You can set the time so that it automatically switches to summer time or the Time zone, as required. ì Select the required option or choose the Time zone for your location. ì Select the required format for entering the date and time from the Date format and Time format lists.

49 Administration Internet Time The System time of the device is automatically synchronised with the time server on the Internet. The time of the Last synchronization with time server is displayed for your information. ì If you would like to use your own time server, activate the On option next to the Use custom time servers field. ì Enter the Internet address of the time server in the Preferred time server or Alternate time server fields. ì Click OK to apply the settings. System Password You can assign a System Password to the user interface of the router Gigaset 504 AGU and specify the period after which a session is to be automatically ended if no further entry is made. ì In the Advanced Settings menu, select: Administration System Password. After installation, the user interface of the router is protected by the System Password admin. To prevent unauthorised changes being made to the configuration, you should set a new System Password from time to time. ì Enter the old System Password in the Current password field.

ì Enter a new System Password in the New password field and repeat it in the Confirm new password field. The System Password may contain up to 20 characters. The System Password is case sensitive. Avoid proper names and all too obvious words. Use a combination of letters, digits and special characters. Note If you forget your System Password, you have to reset the router Gigaset 504 AGU (page 10). This returns all your settings to the factory configuration. This means the system password is changed back to admin. 50 Administration Idle time before log off: ì Enter the number of minutes after which the configuration program is to be ended if no further entry is made. The default is 10 minutes.

If you enter 0, the program will never be ended automatically. ì Click OK to apply the settings. System management Your router Gigaset 504 AGU offers you the option of using remote management in addition to the configuration program that you access via a PC in your local network. ì In the Advanced Settings menu, select: Administration System Management.