

Garderos Configuration Server

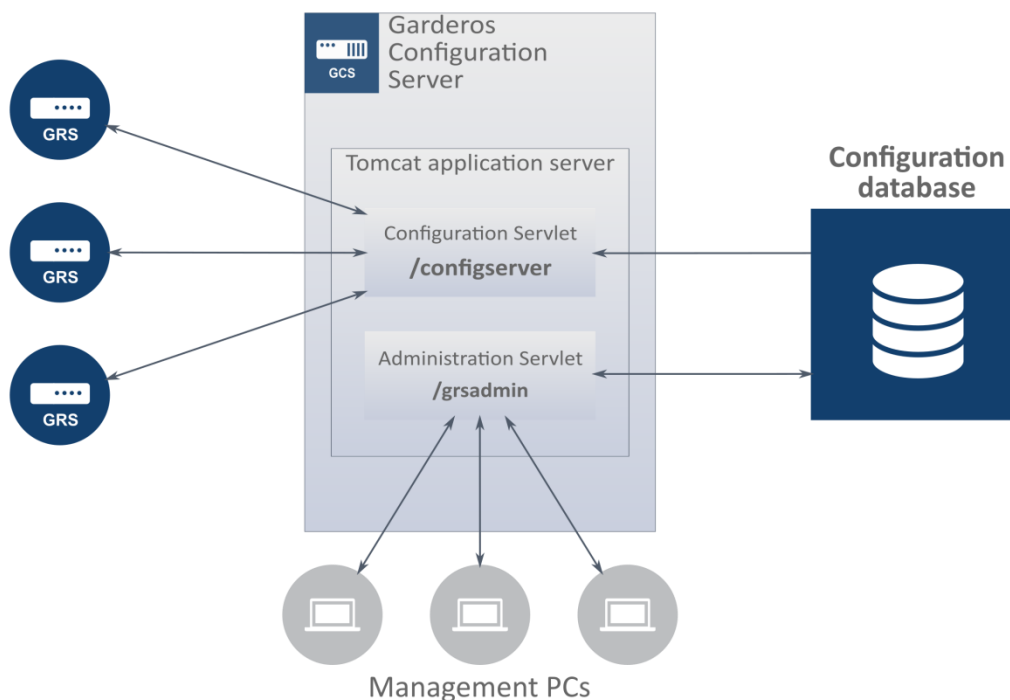
Garderos routers use an HTTP-API for auto-configuration. Centrally stored configuration files can be downloaded and the router will check for updates of the configuration file within a configurable period of time.

The Garderos Configuration Server supports your mass roll out in an easy and efficient way. When operating a network with many routers, most configuration parameters like the addresses of NTP servers, SNMP servers and which interfaces to activate will be the same on all devices, while a few parameters, like the IP addresses on the router's LAN interfaces and maybe IPsec tunnel policies depend on the router's location. The Garderos Configuration Server dynamically creates configuration files from templates, replacing macros by values taken from a configuration database.

The Garderos Configuration Server consists of 2 components, which can be run in Tomcat Java Application Servers:

- The Configuration Servlet creates the configuration files for the Garderos routers
- The Administration Servlet is a simple management interface used to manipulate the routers in the Configuration Server's database.

While the Configuration Server is implemented as platform independent Java Servlets, the typical setup is a Linux server (e.g. RedHat Enterprise or Ubuntu Server) with Tomcat application server.



The servlets are implemented in a modular way and can both run on the same application server or on different servers.

Configuration Servlet

The routers requesting a configuration file send a unique identifier (usually their name) and a hash of their secret to the Configuration Servlet. The Configuration Servlet will look up the identifier in the database and check the router's secret. If a matching router configuration is found and the secret is valid, the Configuration Servlet picks the correct template and fills the macros with the corresponding values from the database.



While the database is delivered with a default database schema, the schema can be enhanced and any required value can be stored in the database for later use in the configuration templates.

Apart from the router name as standard identifier, the routers can also be identified by serial number, MAC address and public IP (future: IMSI of the inserted SIM card; 3G-Routers only).

Administration Servlet

In many cases routers and router locations are already managed by an existing inventory management system. In this case the Garderos Configuration Server is operated without the Administration Servlet and integrated with an existing database.

In a so called greenfield scenario the Administration Servlet allows to add, change and remove router configurations from the Garderos Configuration Server's database from a web based GUI, requiring almost no integration effort.

The screenshot shows the 'Modify router' page in the Garderos web interface. The page header includes the Garderos logo, language options (de | en), and user information (User: admin (Level 15)). The main content area features a 'Modify router' form with the following fields and descriptions:

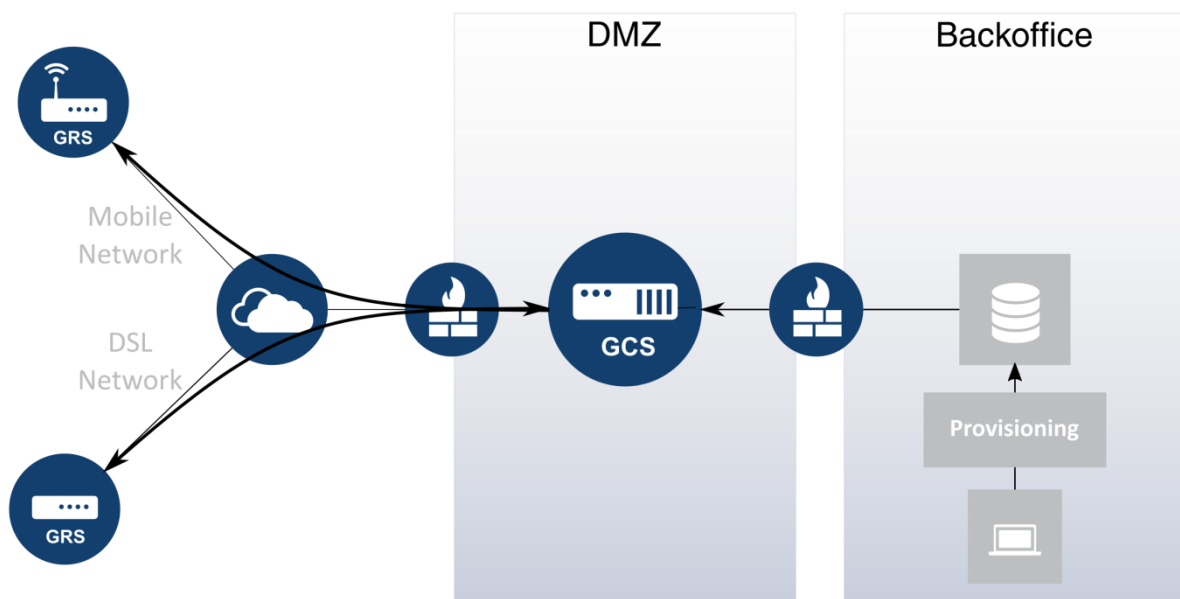
Routername	grs004	Unique name for identifying the router
Secret	garderos	Must match the "Shared Secret" in the GRS
Device type	r7728	Points to the template which the configuration is based on
Serial number	R77281120006	The serial number of the device
MAC		MAC address of the device
IMSI		Unique IMSI of the inserted SIM card
IP		Static WAN IP-address of the router
Client 1 IP	171.16.4.1/24	IP (with netmask) of client interface 1
Client 1 DHCP	171.16.4.5-171.16.4.10/24	DHCP Range for client interface 1
Hint		Optional. Any hint to the device, the customer...
Location		Optional. Address or other hint for the location

At the bottom of the form are buttons for 'save', 'copy & new', and 'delete'. The left sidebar contains navigation menus for 'Information', 'Router Management', 'File management', and 'User management'.

Integration and Configuration

Initial setup of the Garderos Configuration Server on an existing application server is fast and easy. Because not all customers for the Garderos Configuration Server already have an application server available, or do not want to run the Garderos Configuration Server on their existing machines, Garderos offers all services required to get the Garderos Configuration Server up and running:

- Requirement analysis
- Network planning
- Installation
- Configuration and setup of the initial configuration files
- Support



Typical network setup

Security Considerations

Configuration data of the routers should be well protected to prevent unauthorized access to your network. Security sensitive configuration data is encrypted inside the configuration file. State of the art security requires asynchronous encryption mechanisms to protect data exchanged via the Internet. The Garderos Configuration Server supports configuration file download by HTTPS with 2-way (client and server certificate) authentication and certificate revocation lists based on OCSP.

Like any other web based service, the Garderos Configuration Server should be protected by a firewall in addition to the mentioned security measures.

Garderos takes your security considerations into account while setting up a Configuration Server in your network.

Features

Environment	
Number of routers per server Configuration Servlet Administration Servlet	10,000 2,000 *)
Supported OS	CentOS 7, Ubuntu Server 16.4
Application server (depending on OS)	Apache Tomcat 7
Java Version	Java 8, OpenJDK 1.8
DBMS	MySQL
Minimum Space on HD	50GB
Minimum RAM	4GB
Software features	
Garderos router authentication by:	
<ul style="list-style-type: none"> - Hashed secret - User-Agent 	
HTTPS	
Client and server certificates	
OCSP	
Dynamic creation of configuration files	
Router recognition based on name, MAC, serial number, IP or IMSI	
Router authentication	
Supports multiple GRS versions	
Web based GUI	
Easily customizable administration pages	
Router monitoring:	
<ul style="list-style-type: none"> - View active routers - View dynamic router configuration files 	
Redundancy	
Integration with syslog	
Automatic role out of firmware updates	
Certificate file and script distribution	
Monitor thresholds announced by routers (customization)	

*) The number of supported routers depends on the functions used. Functions can be switched on and off in the servlet configuration and functions can be used for part of the routers only.