



Gavika Information Technologies Pvt. Ltd.

#66/2, First Cross, Bhuvaneshwari Nagar, Banashankari Third Stage,
Kathriguppe, Bengaluru, Karnataka 560085, India
Web: <http://www.gavika.com> * E-mail: info@gavika.com

Gavika RADIUS

December 2019.

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current Gavika product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from Gavika and its affiliates, suppliers or licensors. Gavika products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of Gavika to its customers are controlled by Gavika agreements, and this document is not part of, nor does it modify, any agreement between Gavika and its customers.

© 2019 Gavika Information Technologies Pvt. Ltd., Bangalore. All rights reserved.

The problem:

The organization has a wired or a wireless network or both on-premises. The organization has a need to protect its network from unauthorized use. The organization needs to be able to monitor its network usage by devices and people.

In a typical small-office or home network, the secret password to access the WiFi network is shared between all the employees. Often, the password is shared with guests too. The secret is seldom changed. This practice or a lack of security policy implementation poses numerous risks to the organization such as:

- vulnerable to malware and VIRUS
- unauthorized use of WiFi network by unknown people
- data, intellectual property and identity theft
- ransom-ware attack



Gavika Information Technologies Pvt. Ltd.

#66/2, First Cross, Bhuvaneshwari Nagar, Banashankari Third Stage,
Kathriguppe, Bengaluru, Karnataka 560085, India
Web: <http://www.gavika.com> * E-mail: info@gavika.com

- network performance issues
- Internet access availability issues
- Internet over usage
- and exposure to many more attack vectors

The Solution

Implement a AAA system to gain visibility into network usage, prevent unauthorized use of the network and be able to audit network access.

How?

Gavika RADIUS is a software solution that implements AAA.

What is AAA?

AAA stands for authentication, authorization and accounting. They are a family of network protocols when put together, enables robust network security.

Gavika RADIUS allows you to implement AAA to secure your wired and wireless networks.

What is RADIUS?

Remote Authentication Dial-In User Service (RADIUS) is a networking protocol to implement a centralized AAA solution.

With Gavika RADIUS, you can build your own RADIUS server. Gavika RADIUS provides a web interface to administer AAA. At its core, Gavika RADIUS is a software application used by network administrators to install and monitor a RADIUS server along with a few related components.

What is NAS?

A **network access server (NAS)** is a component in a networking device that has a RADIUS client. Typically, NAS functionality is built into mid-range and



Gavika Information Technologies Pvt. Ltd.

#66/2, First Cross, Bhuvaneshwari Nagar, Banashankari Third Stage,
Kathriguppe, Bengaluru, Karnataka 560085, India
Web: <http://www.gavika.com> * E-mail: info@gavika.com

higher-end WiFi access points.

What is needed to implement AAA?

- An existing wired or wireless network.
- A NAS(Typically present in a WiFi access point).
- A virtual machine or a dedicated computer server hardware (could be a desktop computer in smaller networks)
- Working Linux OS on the server. (At the moment only CentOS 7 is supported)

How to go about installing Gavika RADIUS?

Buy a software license from Gavika. Logon to your account on www.gavika.com and find instructions to download and install the software from your account section on gavika.com.

If your organization does not want to perform the installation yourselves, you can buy support and maintenance contracts from Gavika or its authorized partners. The authorized person from Gavika or its partner organization will perform the installation at your site.

What can I do with Gavika RADIUS?

You can perform a number of things to secure your network. In most common implementations, network administrators perform these actions:

- Create a user account for each person that needs access to the network. Every user will have their own password. Password sharing is discouraged.
- Associate the MAC address of the user's devices to their user accounts. Thereafter, a user will be able to access the network only from their designated devices.
- Monitor and review the reports provided by Gavika RADIUS to see access patterns and network usage.
- Implement network usage timing-restrictions. Create user groups and associate users to groups. For the designated group, set allowed timings to access the network. For example, people who work in the day shift do



Gavika Information Technologies Pvt. Ltd.

#66/2, First Cross, Bhuvaneshwari Nagar, Banashankari Third Stage,
Kathriguppe, Bengaluru, Karnataka 560085, India
Web: <http://www.gavika.com> * E-mail: info@gavika.com

not need access to the network during the night. For such a situation, set Weekdays 08:00 to 20:00 hours as the allowed time for the group “day shift users”.

- Audit the network access. Gavika RADIUS provides anomaly reports for your convenience.

Do I need a RADIUS solution?

If you have a network and if you need to secure it, RADIUS is often a good choice.

Does Gavika RADIUS provide hotspot feature?

Yes. Gavika RADIUS has a complementary hostpost/guest management application called GGP. GGP stands for GRADIUS Guest Portal. GGP allows self-registration of guest users. Administrators set policies for guest management such as how long the guest has to be allowed to access the network. When the guests register and verify their mobile numbers, GGP allows them to access the network and Internet.

Does Gavika RADIUS provide a self-service user-portal?

Yes. Gavika RADIUS has a complementary user-portal called GUP. GUP stands for GRADIUS User Portal. From the GUP, RADIUS users can perform a number of self-service actions such as changing their passwords, viewing their network usage, etc.

Does the solution scale?

Yes. You can implement Gavika RADIUS in a all-in-a-box or complex topologies. Gavika RADIUS is capable of configuring high-availability for the database, web interface and the targeted RADIUS servers. In addition to that, Gavika RADIUS can consume third-party or customer managed services such as a databases.

Do you offer a disaster recover solution?

Yes. Gavika RADIUS has built-in features to generate and store backups to your designated targets. We also offer ability to recover from backups programmatically.



Gavika Information Technologies Pvt. Ltd.

#66/2, First Cross, Bhuvaneshwari Nagar, Banashankari Third Stage,
Kathriguppe, Bengaluru, Karnataka 560085, India
Web: <http://www.gavika.com> * E-mail: info@gavika.com

What if my needs are not met by standard installations?

Gavika RADIUS is modular by design. Custom modules are available on request. It is also possible to develop new pluggable modules and attach them to a running installation.

We also provide consulting and customization services. Get in touch with us to discuss your specific use-case.

References

- AAA - [https://en.wikipedia.org/wiki/AAA_\(computer_security\)](https://en.wikipedia.org/wiki/AAA_(computer_security))
- RADIUS - <https://en.wikipedia.org/wiki/RADIUS>
- CentOS - <https://www.centos.org/>
- NAS - https://en.wikipedia.org/wiki/Network_access_server