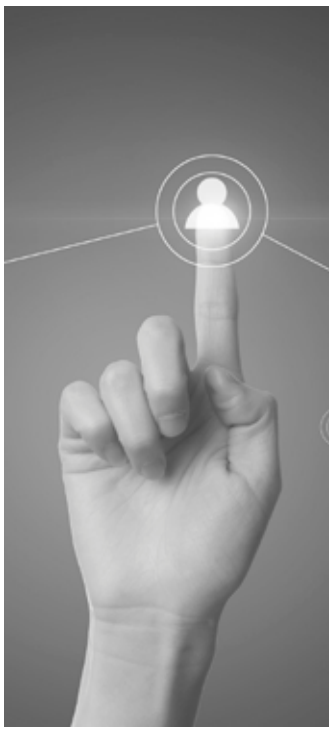
LimRAD Auth Platform

Policy Manager

New Generation Radius (AAA)



Policy Manager Radius server responds to industry standards without using open source code, with a completely new architecture and coding that conforms to industrial standards, by obtaining high performance with low hardware resources in standard or hardware manufacturers attributes in networks such as wired, wireless, VPN, APN. is a new generation Radius Server.

With its Multi Threading architecture, Radius can speed up the verification time by responding to low hardware resources by interpreting the requests coming to the server faster.

With advanced interpreter, requests from the user device are transmitted via the access device to the LimRAD Auth Platform - Policy Manager module in Radius standard.

Authentication is done from MS AD, LDAP, PostgreSQL, MySQL, MSSQL, JSON-API, Oracle or internal local user identity databases for authorization checks at the time of connecting devices to the corporate network. After authentication, policy manager provides authorization info with "Role", "Downloadable-ACL", "VLAN", and / or manufacturer-specific data on the type it can support the access device.

By separating according to the types of packages coming from user devices, corporate devices and users' own devices (BYOD) can be separated from each other, access to corporate resources can only be made from corporate devices.

Organizational Units located in the corporate data source in MS-AD and LDAP structures that can be easily integrated can be stored on the system temporarily and the rules can be written according to these data. In addition, different network authorizations can be made to users and / or devices using Security Groups, which are assigned to users on AD, LDAP.
Performs authentication and authorization process in wired and wireless networks.

It has one of the few original source codes in the world. It is produced using new technologies. No open source code was used. Performs authentication, access control and control of corporate customers' network access.

Key Features

- Redundant Virtual Appliance architecture
- Multiple roles and service rule architecture
- Multiple hardware manufacturer support
- Advanced reporting features
- Consolidated Log feature, forwarding log to external syslog servers

- Multiple database support as authentication sources.

MS Active Directory	PostgreSQL
LDAP	MySQL
Oracle	JSON-API
MSSQL	

- Supported virtualization platforms: VMware vSphere Hypervisor (ESX / ESXi), Microsoft Hyper-V, CentOS KVM and Amazon AWS

General Features

- Delivered as Hyper-V, CentOS KVM and Amazon AWS virtual image, can be installed quickly. Related settings are made on the web interface by giving the IP address with the quick setup wizard over the console.

- 802.1x, Captive Portal, MAC address authentication features

- Consolidated advanced recording feature is provided through the web interface

- All system records, authentication records and account information records can also be transmitted to external servers separately

- Can access user verification by accessing multiple user databases simultaneously

- It has a high performance and high flexibility to meet the different demands of the institutions

- Designed to use low hardware resource and can work as a virtual server.

- Developed in accordance with international standards, has multi-manufacturer support

- There is no hardware dependency.

- It has full control over the devices with its agent structure.

- Provides high performance in simultaneous authentication with its specially consolidated multi-processing capability

- Can work with 3rd party identity sources, simultaneously integrated with multiple identity sources

- It can transmit authentication information to integrated with external systems like firewalls. (Network SSO)

- With dynamic authorization, it can process the information coming from access devices within the rules and make authorizations.

Difference Features

LimRAD Auth Platform developed from scratch without using any open source code projects

LimRAD can work in redundant architecture and is designed to ensure business continuity. All setup and management is provided from the web portal interface instead of complex command lines.

Since network and user traffic does not pass through it, it can authenticate from the central data. With different and dynamic levels of authority, multiple management roles can be provided on a single server, depending on the level of authority.

Each module has been implemented according to industry standards.

It has low hardware resource usage with its scalable multithreading architecture.

It can provide service from the smallest businesses to large scale enterprises, distributed telecommunication service providers

It does not allow disruption in your business continuity as it is located in the central authentication position.

It support full flexibility with creation of any number of device access rules and enforcement rules and their combinations.

With the information such as access device, time, device type, location, user name on which the access is made, users can be separated and authenticated accordingly. For example, request coming as *@company1.com can be directed to one authentication source, requests coming as *@company2.com can be directed to another one. It provides high flexibility with data regular expression matching infrastructure it uses.

With support of multiple hardware manufacturers, it eliminates your hardware brand dependencies. Can work with all industry standard manufacturers.

Up to 50,000 users can be simultaneously verified on a single virtual appliance with capacity to be increased while operating (*).

Protocol Features

- Radius AAA
- Radius CoA
- WMI
- SSH, Telnet
- SNMP
- Captive Portal (Hotspot) (**)
- EAP
- EAP MD5
- EAP GTC
- EAP PEAP
- EAP TLS (v1,0-v1,1-v1,2)
- EAP TTLS
- PAP
- MSCHAPv2, MSCHAP
- CHAP
- Windows Machine Authentication
- SMB v2/v3
- SYSLOG integration
- Certificate Authority (CA)
- Secure communication with HTTPS
- OTP Server
- SMS Gateway
- SMTP Relay

- If the necessary hardware resource and license are provided

** It is seperately licensed and the module starts working when the license is included in the system.

Supported User Information Databases

- Microsoft Active Directory
- LDAP
- Oracle
- PostgreSQL
- MSSQL
- MySQL
- Local DB
- Microsoft Azure Active Directory
- JSON API

RFC Standards

- RFC 2246
- RFC 2548
- RFC 2759
- RFC 2865
- RFC 2866
- RFC 2869
- RFC 2882
- RFC 3079
- RFC 3576
- RFC 3579
- RFC 3580
- RFC 3748
- RFC 4017
- RFC 4346
- RFC 4514
- RFC 4518
- RFC 4849
- RFC 5216
- RFC 5246
- RFC 5280
- RFC 5281
- RFC 7231

IP V6 Features

- Web and CLI based management.
- Authentication and authorization for IPv6
- Syslog, DNS, NTP, IPv6 integration

802.1x L2 AUTHENTICATION

LOCAL – GENERAL SPECIFIC NETWORKS

USER DEVICES

USER INFORMATION CORPORATE INFORMATION STORE

- MS, Active Directory
- MSSQL, MYSQL, PostgreSQL, Oracle
- LDAP
- Local

LimRAD AUTH PLATFORM

USER EVALUATION AND IMPLEMENTATION

- User access rule determination
- Establishing a service relationship
- Making user authentication
- Determining the suitability of the defined rules
- Applying the return rule set according to the appropriate rule control
- Transmission of relevant Radius Attributes to the Access Device (VLAN, Role)
- Keeping records and / or transmitting to related servers
- Keeping Account Information, keeping it associated with the user

ACCESS DEVICES

- Switch
- Wireless Access Point
- Wireless Controller
- APN server
- VPN Server
- Firewall
- Any device that supports Radius protocol

USER NETWORK ACCESS REQUEST TRANSLATED TO RADIUS STANDARD

LİMATEK SİSTEM TEKNOLOJİLERİ SANAYİ TİCARET A.Ş.
ODTU Technopolis Gallium Block No: BK12 06800 Çankaya/ANKARA
0312 287 76 73