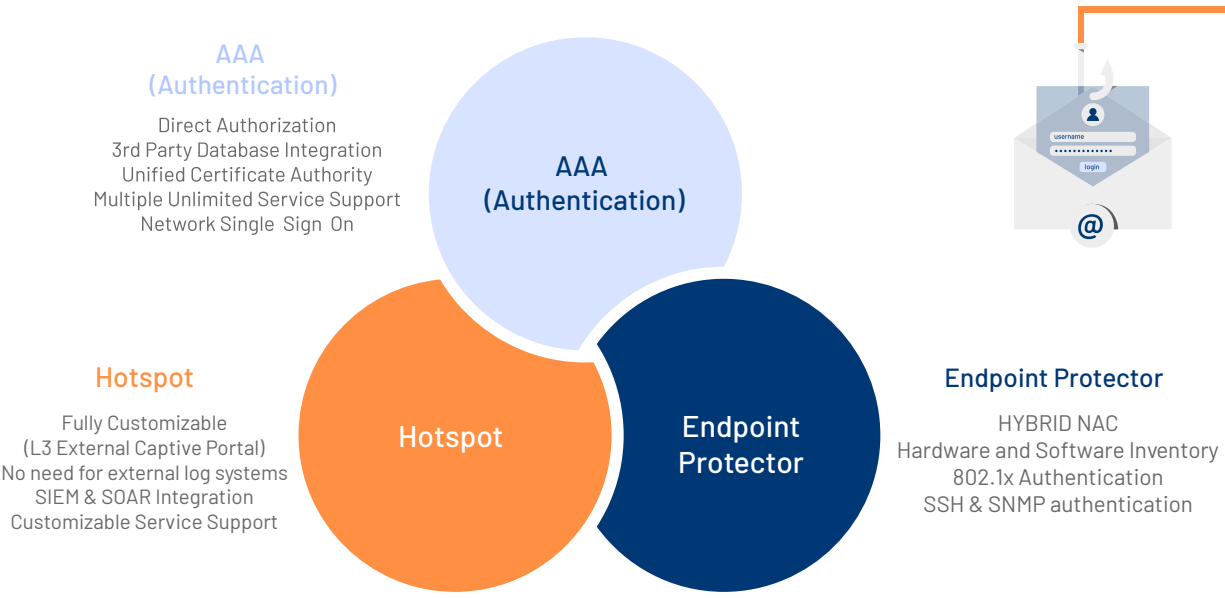
S3M Security
Easy Way to Connect

S3M SECURITY
NETWORK ACCESS CONTROL

S3M Security Network Access Control is a network security solution installed on a single virtual server and running in a modular architecture.

The solution includes the AAA Authentication module with authentication, authorization, accounting and CoA features for wired and wireless network, the Hotspot module that provides a fully customizable L3 External Captive Portal that performs guest identity registration and verification on wired and wireless networks and the Endpoint Protector which provides protection and control according to corporate policies in network access.



These 3 modules helps to regulate and enforce access policies to network resources based on user identity, device type, and security posture. Authentication AAA module can detect and block unauthorized access attempts, mitigate security threats, and ensure compliance with organizational security policies. Endpoint Protector's features can also can control the network access of IoT and devices without an operating system and can detect anomalies. Overall, the solution helps to protect corporate data against external and internal threats and to provide controlled and secure sharing of corporate networks with guests.

Key Features

Group-based unified network access control

Management and monitoring with a single interface, valid for all modules

Integration with external log servers

Exportable report templates (in Excel, CSV, PDF formats)

Dynamic authorization

Support for multiple authentication and authorization sources (internal, Active Directory, LDAP, SQL, JSON)

Isolated local and guest user databases

BYOD authorization with built-in certificate server

Comprehensive, customizable interface

Bi-directional API support and data exchange

Key Differences

Centrally controlled platform

Suitable for use in closed networks

Vendor agnostic working principle: can work with all products that meet IEEE standards

Vendor specific working principle: can work with the vendors as if it is their own product, not causing any conflicts.

Allows viewing Accounting charts from a single dashboard

With its scalable architecture, it can be easily used in all small / mid / large enterprises, all organizations

Supports active-passive redundancy architecture

With the built-in certificate manager, certificates can be generated and used on the system, and there is an advanced CCT (Client Connectivity Tool) that allows users to upload their own certificates.

Available in any language with installable language packs

Available as virtual appliance, can run on VMware ESX/ESXi, Microsoft Hyper-V, Proxmox VM platform, Amazon AWS and Google Cloud

Update can be performed via the system interface, console connection is not mandatory

Offers Hybrid NAC technology, agent and agentless architectures can be used together and take advantage of both

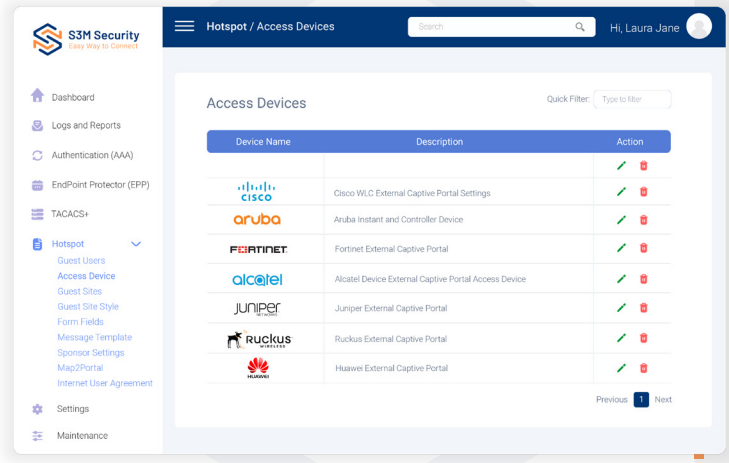
Supports Network Single-Sign-On

AAA AUTHENTICATION MODULE

- With the AAA Authentication module, the solution provides 802.1x implementation in international standards for APN, VPN, wired or wireless network security.
- Supports authentication by MAC address.
- Performs authentication of IoT devices and non-OS devices. Also performs 802.1x verification with information such as IMEI, IMSI, CID coming over APN networks.
- Users are divided into groups according to their connection parameters and methods.
- Authenticated user devices have group actions and access rights according to the groups they are assigned from (Dynamic Authorization).
- Authorization and group information obtained from many different identity sources such as Active Directory, SQL, Oracle are used in dynamic authorization.
- Integrates with Active Directory if used as a system authentication source.
- Users are registered regardless of their network permissions. These registration records are reported in detail and can be examined. After the incoming request and verification, group actions can be followed.

TLS/TTLS Protocols for Secure Network Access

- Supports EAP, TLS/TTLS protocols for network access. The certificate server required for the protocols is provided as built-in. If requested, the certificates are signed by the corporate certificate server.
- It supports users to create their own certificates with their credentials and install them on devices.
- Radius requests can be forwarded to external proxy servers, so it supports network services such as "eduroam".
- Provides integration with Network Single-Sign-On Checkpoint, Paloalto, Fortinet and Sophos. User data is sent to the firewall with Network SSO. The information of authorized users can be transferred to other authentication sources.
- With the SSO feature, JSON API integration can be provided to protect the identity source.



HOTSPOT MODULE

- Simplifies workflow processes for guest network access. Instead of network administrators creating separate accounts for each guest, it allows guests to register and verify themselves in the system.
- It works as a fully customizable L3 External Captive Portal.
- The Dynamic Authorization features available in the AAA Authentication module also apply here. Network SSO feature is also active in this module.
- Supports SMS, Email and Sponsor structures. These features can be used separately or in combination.
- In guest network access, device and user information of the users who come to register to the portal are collected. This information can be forwarded to an external server if desired. Authentication can be performed by integrating with various databases (card door access system, personnel tracking system, etc.)
- Does not require any external recording system. If use is required, it is integrated with SIEM/SOAR.
- Fully customizable service support is provided.

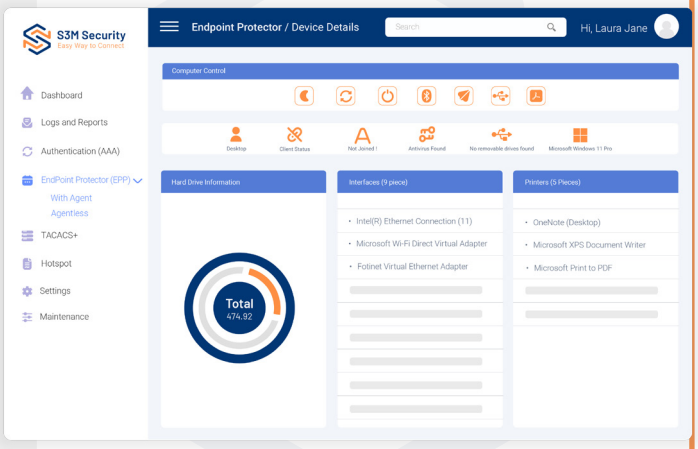
Corporate Vendor Support

Can be integrated with all corporate vendors

If there is an unknown vendor by the solution, integration can be done again by using the vendor's manual documents.

ENDPOINT PROTECTOR MODULE

- With built-in hardware and software inventory collection system, hardware changes can be monitored and reported by system administrators.
- The resource usage of the devices is observed and thus unnecessary investments that may be made are prevented.
- It eliminates security vulnerabilities that may occur by running licensed and unlicensed software installed on devices or just being present on the device. Devices that do not comply with the specified policies are automatically redirected to quarantine networks or network access on the device is terminated.

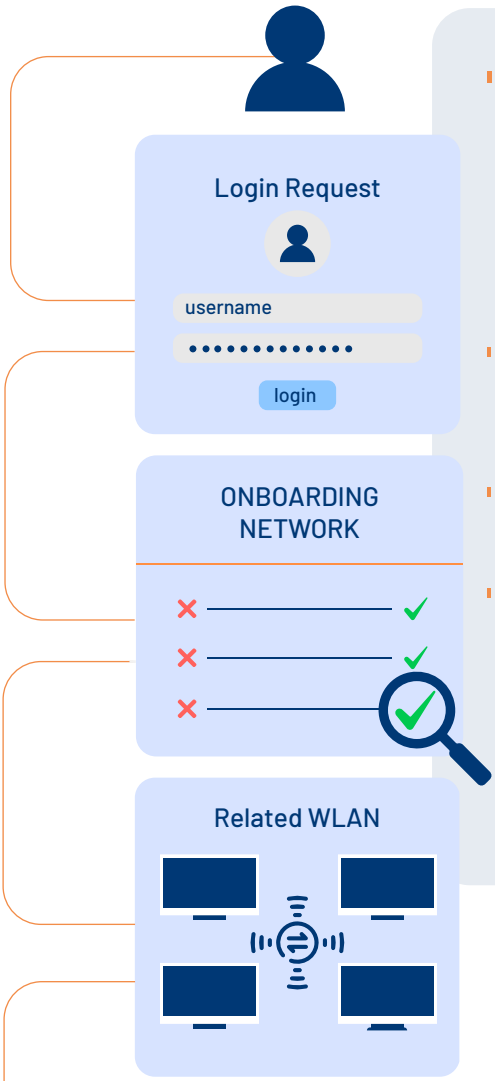


S3M Securtiy
Hybrid NAC

- We offer the Hybrid NAC capability, which allows agent and agentless architecture to work together, with the S3M Security Network Access Control solution.
- Agent-based architecture working with 802.1x protocol can work seamlessly with agentless architecture working with SNMP and SSH.
- The agent architecture runs as a service on devices. It reports activity such as hardware changes, external hardware add-ons, and hardware inventory is set up along with software and application inventory. There are scenarios available to administrators by default.
- In the agentless architecture, connections are established with the switches with SSH and SNMP. It consists of a parametric structure. Commands can be written by users as well as default rulesets can be used. Rule sets that are unpredictable by product developers can also be created by users.

- In agentless architecture, Linux and Mac machines are connected via SSH, a special tunnel is used for Windows.
- Agentless architecture allows sending Powershell and CMI commands remotely. It works in architectural layers.

- IP and location information is kept in the agent architecture. Keeping this information supports the continuation of the agent architecture even if the user goes out of the network.



- There is an improved identification structure in the agentless environment. This structure leaves the user in an onboard state when they request a login to the network. Basic controls are performed during this onboarding situation. After the controls, users are sent to the relevant VLAN according to their type.
- Domain structure is essential for using agentless architecture. There must be a domain structure to get the user information.
- The agentless architecture works almost as fast as the agent-based architecture, that is, the 802.1x protocol.
- This hybrid working structure S3M Security offers, specifically responds to basic customer demands. Provides the insights such as applications running on the devices, remote device shutdown, bluetooth on and off, domain membership query, antivirus status of the device, operating system update, etc.

Agentless NAC allows for quick deployment and ease of management, while agent-based NAC provides more advanced security features such as visibility and control.

By combining these two approaches, organizations can achieve a more comprehensive and flexible NAC solution that is tailored to their specific needs and for organizations that prefer to use these two architectures separately, we have made these two architectures almost equally superior.

Technical Features

Virtual Appliance

The solution is offered as a virtual appliance. Supported on the following virtualization platforms.

- VMware (ESX/ESXi)
- Microsoft Hyper-V
- CentOS KVM
- Amazon AWS
- Proxmox VE

Supported Identity Resources

- SQL (MySQL, PostgreSQL, ORACLE,MsSQL)
- Microsoft Azure Active Directory
- Microsoft Active Directory
- LDAP (Geric)
- Local SQL DB
- JSON
- Kerberos
- RADIUS (Proxy Target)

Supported Identity Resources

- Web-based management system (http, https)
- Log transmission to external server
- Internal database (separate for Guest and Local users)
- External database connection
- Active Directory integration support
- Interactive monitoring screen resource management
- Service monitoring and intervention feature
- Language pack support in all languages

RFC Standards

2246	2407	2408	2409
2548	2616	2759	2866
2869	2882	3079	3576
3579	3580	3748	3779
4017	4137	4301	4302
4308	4346	4514	4518
4809	4849	5176	5216
5246	5280	5281	5282
5424	6614	6818	6960
7030	7170	7296	7815

Protocol Support

- RADIUS
- RADIUS Dynamic Authorization
  RadSec (TLS encoded RADIUS)
  EAP-FAST(EAP-MSCHAPv2, EAP-GTC,EAP-TLS)
  PEAP(EAP-MSCHAPv2,EAP-GTC, EAP- TLS)
- EAP-TLS / TTLS, PEAP
- PAP, CHAP, MSCHAPv1, MSCHAPv2, EAP-MD5 WPA3
- Windows Machine Authentication
- Online Certificate Status Protocol(OCSP)
  EPP Protocol (TCP 4382)

IPv6 Support

RADIUS
Web-based and CLI-based management
Authentication & accounting server with IPv6 address
IPv6 proxy
IPv6 Syslog, DNS, NTP
IPv6 Virtual IP (Redundancy)

Hardware Requirement

	up to 2500 Device	up to 2500 to 5000 Device	up to 5000 to 15000 Device	up to 15000 to 25000 Device	up to 25000 to 50000 Device
vCPU	2vCPU	2vCPU	4vCPU	6vCPU	8vCPU
Memory	4GB	6GB	8GB	12GB	16GB
Storage	200 GB	200GB	200GB	300GB	400GB
I/O Read/Write	400-550 MB/s	400-550 MB/s	400-550 MB/s	500-650 MB/s	650-2000 MB/s
NIC	1 x 1GbE	1 x 1GbE	1 x 10GbE	1 x 10GbE	1 x 10GbE