



UNITED SECURITY PROVIDERS

PROTECTING WHAT MATTERS.

USP NETWORK AUTHENTICATION SYSTEM™



STRENGTH FROM WITHIN.

For corporate networks, the interface to the public network is always secured as a first priority. However, internal connections are often neglected or considered safe as long as they are on the company's own premises, leaving the back door wide open to harmful software and unauthorised users. The USP Network Authentication System™ (NAS) bars this door in an efficient, uncomplicated manner.

Risks in internal connections arise for instance when guests connect their computer to the network in meeting rooms. Worms or viruses can be unintentionally transmitted in this way. Employees who have been on field assignments can also accidentally bring malware into the company when their computers have been in contact with other networks but have received no security updates. In extreme cases, even industrial espionage may be involved.

Of course, preventing mobility, wireless technologies or exchange with third parties is not an option. The NAS offers an immediate, simple remedy that enables safe communication with your partners and visitors, without putting a strain on your network. Furthermore, using the NAS brings you a step closer to the international standard IEEE 802.1x, which will be introduced everywhere in a few years' time.



UNITED SECURITY PROVIDERS

PROTECTING WHAT MATTERS.

A QUICK, HANDY SOLUTION.

Rapid integration

The USP Network Authentication System™ supports all devices and network infrastructures, regardless of manufacturer. The system can be quickly and cheaply integrated into anything from small to worldwide networks, either on a company-owned server or as an appliance in your system landscape. This improves your network protection with immediate and substantial effect.



Complete verification

The NAS runs checks on all devices that are in use. Depending on your needs, devices with no virus protection or those that fall below a set security standard have either limited or no access to your IT resources. You are free to choose the criteria. Additionally, each connected participant is registered, thus improving security and deterring criminal intent.

Inventory overview

The solution can be connected to a centrally run inventory database. It contains information on all devices that are currently connected to the network or have been connected since the NAS was set up. The high data quality ensures a complete overview of your corporate network at all times, ready to be analysed depending on your criteria. Such an overview is also very useful for support functions, for implementing a central purchasing policy and for corporate governance in the area of security.

CLEAR, BINDING RULES FOR SECURITY.

Authentication of all devices

The USP Network Authentication System™ screens all devices without exception that attempt to connect to the corporate network and checks them against your security policy. This check is based on certificates or the hardware address. A network scan detects all devices that are in permanent operation and do not or rarely require authentication. As a result, unknown or high-risk devices are identified and transferred to a quarantine area where they are dealt with.

Freely configurable rules

The NAS has a set of rules that you can easily define to suit your needs. This allows you to assign a defined status to all device ports or device groups: alarm, block, isolate or always open. Devices that do not meet your rules are then, for instance, automatically blocked or transferred to a guest network or quarantine area. The decision on access rights can also be made manually. The set of rules permits detailed configuration and offers you the protection you need, whilst still remaining flexible to everyday business eventualities.



UNITED SECURITY PROVIDERS

PROTECTING WHAT MATTERS.



Verification that clients are up to date

The USP Network Authentication System™ supports the IFTNCCS-SOH Statement of Health protocol. It checks that virus protection and the operating system are fully up to date, so you are aware whether the device automatically receives operating system updates. Depending on this assessment, the device is granted full, limited or no access.

Managed service

The NAS can be purchased either as a package at an affordable licence price or as a remote managed service. This provides you with high security at low, calculable costs. What's more, the strain is taken off your IT employees, as all operational tasks are taken care of by experts. In addition, our managed service also offers periodic reports and the latest product features, while a service level agreement means you can enjoy professional support up to 24 hours a day, seven days a week.

UNITED SECURITY PROVIDERS – PROTECTING WHAT MATTERS.

United Security Providers is a group of leading specialists in information security who have joined forces to close the gaps in network and application security. As the Swiss market leader in this sector with more than 80 highly qualified specialists, we now also handle this task on an increasingly international level.

Our efforts are centred on providing maximum security for your business processes in terms of both confidentiality and availability. Solutions from United Security Providers effectively protect your existing IT infrastructure, whilst also providing opportunities to simplify it. This gives you the freedom to align your processes with changing client needs and market requirements where necessary, thus strengthening your competitive position.

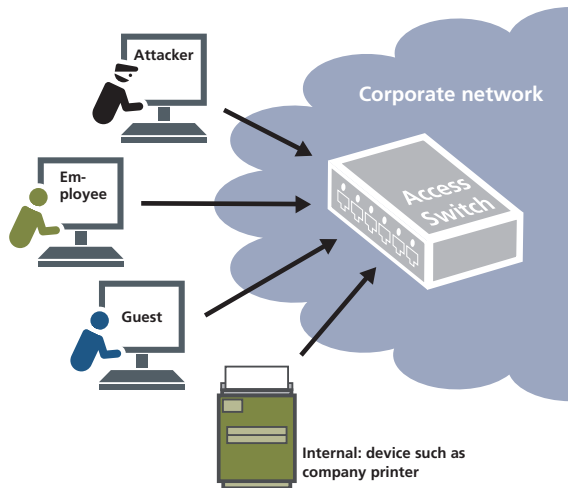
Since 1994, a growing number of clients have been placing their trust in United Security Providers. Our clients include renowned Swiss financial service providers, administrative organisations, multinational corporations and transport and logistics companies, all of whom demand first-class products and services. And that's just what we offer – 24 hours a day, seven days a week – by operating mission-critical network and security infrastructures at more than 200 locations across the globe.

Our carefully selected business partners help you to choose and integrate the perfect solution for you, meaning that United Security Providers is always at hand – wherever you are in the world.

USP NETWORK AUTHENTICATION SYSTEM™

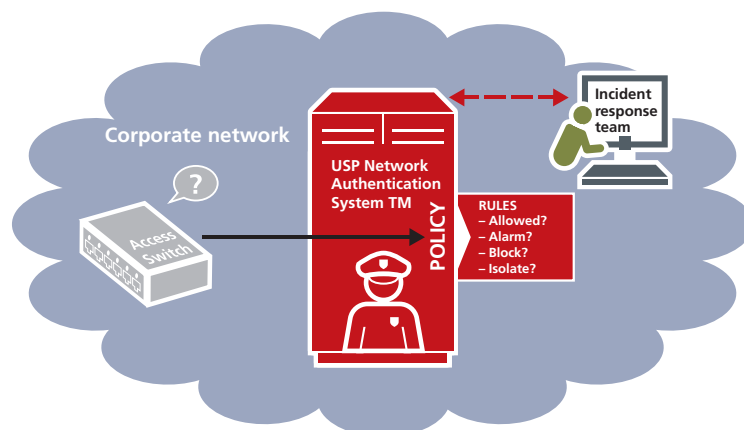
HOW IT WORKS.

1



Various devices attempt to connect to the internal network.

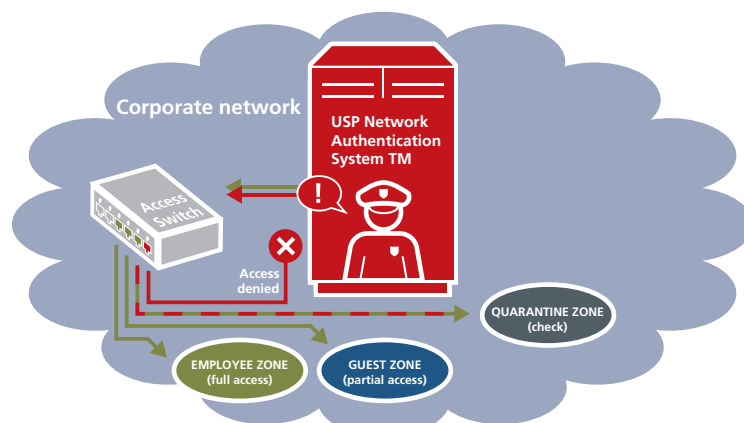
2



The access switch notifies the NAS that a new device has been connected to the network. The NAS uses the defined security policy and the inventory database as a basis to check whether

the device is authorised and establishes which rule must be applied. Guest devices can be granted temporary network access via the helpdesk.

3



The NAS sends the information (access allowed/denied and allocation to the corresponding zone) to the switch, which then implements the command.

USP NETWORK AUTHENTICATION SYSTEM™

TECHNICAL INFORMATION.

Communication with the network infrastructure

- SNMP v1, v2c or v3 (standard: SNMP v2c)
- SNMP traps
- SNMP MIB-II (IP-MIB, IF-MIB, Bridge MIB)
- SNMP Q Bridge MIB or vendor-specific MIBs for VLAN information
- IEEE 802.1x
- IEEE 802.1Q VLAN
- Dynamic VLAN assignment
- DNS zone transfer (RFC 1995)

IEEE 802.1x support

- IEEE 802.1x RADIUS (RFC 3580)
- EAP (RFC 3748, RFC 2716)
- RADIUS proxy support

User interface

- HTTPS, SSLv3/TLS (RFC 4346)
- Web GUI with role-based authorisation model
- Predefined roles: helpdesk, support, admin, reporting

Management interface

- Management Web GUI (HTTPS)
- SSHv2
- Central configuration management integrated in Web GUI

Performance and availability

- Copy of data held at separate geographical locations
- Multi-threaded architecture, good scalability with use of multicore CPUs

- Central system easily capable of monitoring several thousand switches/routers and several tens of thousands of terminals: maximum size only determined by the hardware used and the latency in the network

Logging and alerting

- Recording of all important events in the log (log files and log tables in the database).
- Forwarding of log messages and alerts using Syslog or SNMP trap
- Event scripting with actions that can be defined as required (e.g. sending e-mails/SMS messages or opening a trouble ticket in a ticketing system)

Interfaces for data exchange

- Import interface with support for several independent source systems
- JDBC, ODBC, SQL, XML
- Import of flat files (CSV files) via SFTP

Reporting

- Reporting engine integrated in the Web GUI
- Output format: HTML, PDF or text files
- Option to connect up reporting tools such as Business Objects, Crystal Reports, etc.

Platforms and operating systems

- Java™ platform, standard edition, version 5 (or higher)
- Servlet 2.4/JSP 2.0 Web container (e.g. Tomcat 5.x)
- Linux, UNIX or Windows servers

United Security Providers
Bahnhofstrasse 4
P.O. Box
3073 Gümligen
Switzerland

Phone +41 31 959 02 02
Fax +41 31 959 02 59
www.united-security-providers.ch

United Security Providers
Förrlibuckstrasse 220
P.O. Box
8031 Zurich
Switzerland

Phone +41 44 496 61 11
Fax +41 44 496 61 99
www.united-security-providers.ch



UNITED SECURITY PROVIDERS
PROTECTING WHAT MATTERS.