# MACMON 802.1X

macmon
nac smartly simple

## 802.1X – "Out of the Box"

**The Institute of Electrical and Electronics Engineers (IEEE) is a global association that has committees for standardising technology, hardware and software. The standard 802.1X has already been revised and revamped several times and represents a well-developed recommendation for the secure authentication of devices in networks. macmon supports this standard and aids its introduction and operation.**

## Capabilities of IEEE 802.1X

The issues of guaranteeing unique authentication in both wireless and wired networks is well known. For procedures that are relatively easy to implement from a technical point of view, such as checking the MAC addresses, it is often argued that properties are too easy to falsify. For this reason, in the fundamental technology, macmon already uses more properties than just the MAC address for identification and this enables it to check system footprints (IP address, operating system, IP ports) – to falsify all of these at once demands an extremely high level of criminal energy.

### Key facts

- ✓ Using an open standard combined with best practice
- ✓ Possibilty of hybrid operation - with and without 802.1X
- ✓ Locating endpoints by communicating with the switches and access points
- ✓ Linking with AD/LDAP and other identity stores
- ✓ Dynamic & automatic setting of rules
- ✓ Easy to implement and operate
- ✓ Grouporiented configuration instead of complex setting of rules
- ✓ Establishing and implementing of concepts for different security levels and areas

Yet the standard 802.1X can also go one step further than this. A RADIUS server is included for the authentication, which decides whether or not to grant access. Various properties can be used as proof or a means of authentication – for example, the MAC address, username/password or certificate. Since access to the network is granted by the switch only after successful confirmation by the RADIUS server, there are no unused or non-secure ports, as recommended by the BSI.

When granting access, additional rules can also be provided, which are then implemented by the switch. If the switch is technically capable of doing this (Layer3), a specific VLAN, defined ACLs or almost any other attributes can be assigned.

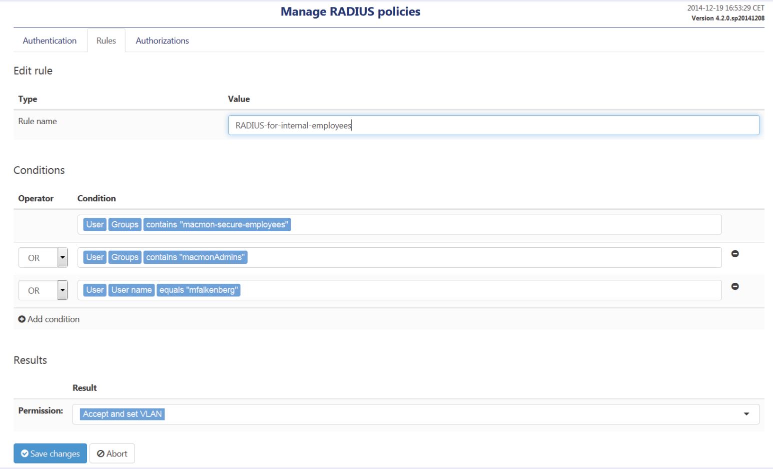
## Implementing IEEE 802.1X

The launch of such powerful and sophisticated access protection requires careful planning. It makes sense to use the standard because more and more components, such as the different end devices but also the switches, comply with the requirements. It should be noted, however, that the use of 802.1X is not secure per se, but that various options are available here for establishing the identity of the end device, which in turn allows you to apply different levels of security.

If only the MAC address is used as identification, it is very easy to falsify it, which brings into question the increased security provided by launching IEE 802.1X. With macmon Network Access Control, the MAC address can be used for authentication, while the above-mentioned footprint is also used in order to shut "intruders" with falsified MAC addresses out of the network. In this way, end devices that cannot provide high-quality identification can also be integrated as securely as possible.

The highest level of security when combined with 802.1X is achieved if certificates are used for the authentication. However, for the certificates that are used, an appropriate infrastructure must also be created in order to use this PKI (Public Key Infrastructure) to manage the certificates and to monitor their validity.

Opting for the medium level of security is therefore often a very good compromise between the highest goal and the work required to achieve that goal. However, a username and password are already extremely high-quality methods of identification, meaning that, depending on the field of application, there is no objection to using these. Of course, not every device can be provided with its own username and password quickly and easily.



Manage RADIUS policies

2014-12-19 16:53:29 CET
Version 4.2.0.sp20141208

Edit rule

| Type | Value |
|---|---|
| Rule name | RADIUS-for-internal-employees |

Conditions

| Operator | Condition |
|---|---|
| | User Groups contains "macmon-secure-employees" |
| OR | User Groups contains "macmonAdmins" |
| OR | User User name equals "mfalkenberg" |

Results

| | Result |
|---|---|
| Permission: | Accept and set VLAN |

macmon therefore offers different variants in order to use existing means and reduce the effort this entails. This means that, with the active directory connection, the accounts of all of the devices that are already contained in the directory service (and, if required, the users) can be used for the authentication. Individual devices that are not included can be provided with separate access data, and groups of special systems, e.g. VoIP telephones, can be provided with joint access data.

In this case, however, it is essential for this enhanced option to also be intelligently and easily implemented by macmon. This means that almost any identity sources, such as AD, LDAP or databases, can be linked together in real time to check identities while the set of rules is automatically created in the background. Simply assigning groups, such as from the active directory to the macmon device groups, makes configuration significantly simpler. macmon uses the group configurations as a basis to automatically create the required RADIUS rules and also, thanks to the managed rule editor, always provides the option to define any exceptions. However, this is precisely the difference – you only define the exceptions...

With macmon, you simplify the implementation of 802.1X many times over and, at the same time, also cover the areas of your network that are not yet compatible with 802.1X. Step-by-step implementation and mixed operation are also possible without any further problems.

The use of your existing infrastructure and your existing company identities, the intuitive and self-generating set of rules together with macmon's device-related and group oriented approach, as well as a range of further simplifications, all means that a security standard that is actually complex can be successfully implemented as easily and quickly as possible. macmon does things differently – give us a try!

How the devices in your network are authenticated and authorised by macmon depends entirely on the circumstances and capabilities of your infrastructure. macmon is even able to automatically activate and deactivate the 802.1X mode at the switch. This means that it is no longer necessary to rigidly define the network areas in which you would or would not like to use 802.1X – macmon automatically configures your switches based on the group configuration.

From the MAC address combined with other system information, to the industry standard IEEE 802.1X with its various forms (MAC address bypass, username/password, AD/LDAP or certificate), all of the capabilities are included in the macmon network bundle.

For even higher safety requirements, we can offer the macmon TP module (authenticated by the TPM chip) separately.

## Contact

macmon secure GmbH
Alte Jakobstrasse 79-80 | 10179 Berlin | Germany
Phone: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu