MACMON GUEST SERVICE

Opening up a network simply – and selectively!

Today, nearly everyone has at least one mobile device and expects to be able to access the Internet wherever and whenever they are, but it remains to be seen whether this is a blessing or a curse. However, mobile workers, service providers, suppliers and customers often require detailed access to certain resources in your company's network, which means that neither UMTS & LTE nor a completely separate guest network provide a sufficient solution.

The challenge

When using a Network Access Control solution, it is usually easy to allow new devices to access the network – you simply add these to the list of trusted devices. Without NAC, this step is, of course, redundant because there are no checks on who or what accesses the network.

The real challenge is therefore to design approval for the devices to be as convenient as possible and to perfectly integrate the processes into the company's existing processes. This is precisely where the "guest portal" from macmon comes in – even if the term "guest portal" no longer strictly reflects the numerous opportunities and usage scenarios.

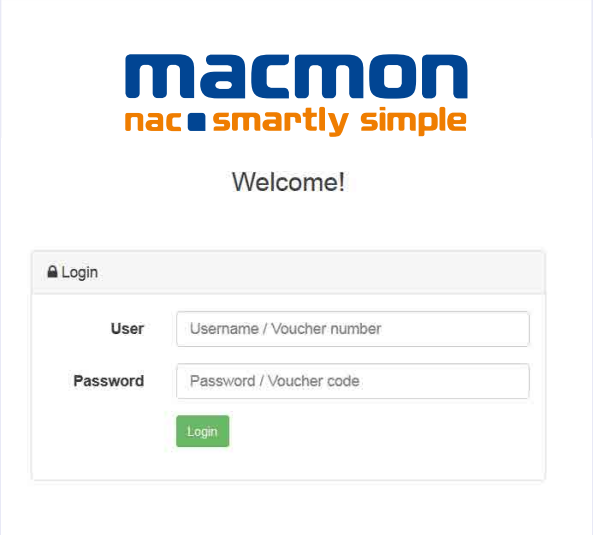
Key facts

- ✓ Independent of manufacturer and suitable for any environment
- ✓ Fast and easy to start up right across the company
- ✓ Can be used and operated in accordance with existing processes
- ✓ Reduces the IT department's workload thanks to delegating access rights
- ✓ Highly flexible access control for any situation
- ✓ Up-to-date and complete overview of all third-party devices
- ✓ Intelligent BYOD solution

Basic function

The fundamental requirement is as follows: To grant network access to third-party devices in a way that is flexible and meets requirements. And in a way that is optimal with regards to definable resources, that is revocable, has a time limit and can be traced.

A comprehensive Network Access Control solution is required to achieve this, as that is the only way in which all accesses can be monitored. Third-party systems can therefore be prevented from accessing the network without authorisation. The macmon network bundle includes all of the prerequisites for detecting third-party systems and blocking them from the network.



When using the macmon guest portal, you can not only disconnect third-party devices from the network, you can also specifically transfer them to a receiving network – for both LAN and WLAN, of course. In the receiving network they are guided via a captive portal to the macmon guest portal, in which they must register in order to access the network.

The log-on information that is required can be created and transferred in advance, prepared in the form of lists. This can then be kept at reception, for example, or if required, sent by e-mail or SMS after a successful self registration. The shared resources and the duration of the access can be defined when creating the access data, which means that every "visitor" can access precisely those resources that are approved for them.

From a technical point of view, SNMP and 802.1X technology can be used to implement this. However, in a wireless network in particular, 802.1X is strongly recommended. This is supported by almost all professional access points, meaning that the technical prerequisites are already fulfilled.

Dispersed environments

In the growing industry and the age of mergers and transfers, it is increasingly necessary to be able to offer several portals. Different locations and different companies in one location play an important role in this. The macmon guest portal is therefore capable of managing any number of entities centrally, to assign each of these their own layout and to guarantee any number of languages.

Simple administration

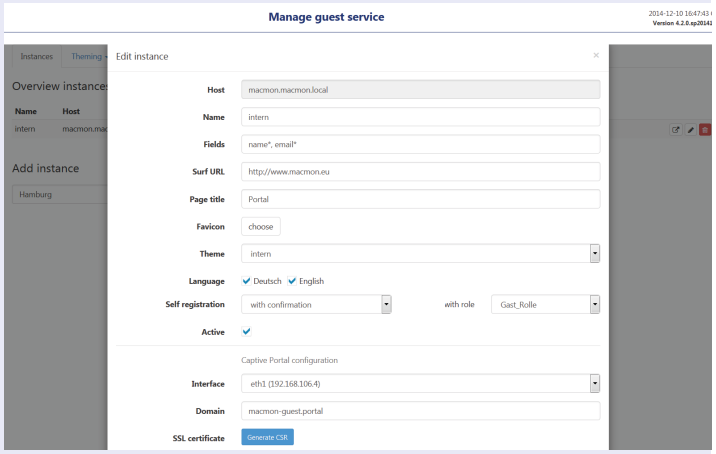
Having to manage an ever-increasing set of tools is making daily work more and more difficult. With the new macmon guest portal, particular importance is attached to simple administration. This means that the complete administration of all entities and settings can be carried out from one central location via an intuitive GUI that is integrated into macmon NAC. Settings, layout templates and languages can be copied so that you then only have to adjust them to match the important details. The layout is designed via an easy-to-use web editor and exceptions that may be required can be created quickly and intuitively.

Delegated access rights

The decision about whether or not a visitor should have access to the network is often not taken in the IT department at all. With the macmon guest portal, the rights to grant access are delegated to authorised employees (e.g. the head of the department). Without having to concern themselves with the administration of macmon NAC, they can create access data directly in the portal or confirm self-registered visitors.

A complete overview

It is extremely important to maintain a central and complete overview of everything – especially when entities are dispersed and access rights are delegated.



The configurable and graphic reporting by macmon therefore provides you with a continuous up-to-date overview of the access data that is created and used, the associated devices and the person granting access rights.

BYOD situations

Another requirement when checking network accesses is the intelligent handling of employees' devices. For this it is important to differentiate between whether the end devices being used are managed via a mobile device management solution or whether they belong to employees who accept no administrative agents on their p ersonal devices. In the first case, the devices can be easily detected by connecting the MDM system as an identity source to macmon and they can then be authorised for the defined network area. The second situation, however, is a bit trickier – though macmon is also the bestpossible choice for mapping it.

Employees who are authorised to do so can easily connect their personal devices to the network, where they will be connected to the guest portal. By entering their usual Windows username and password, a prompt gives them the opportunity to register the device and operate it in the company's network. To do this, they must accept the adaptable terms of service that are supplied by macmon, and they are then connected at the click of a mouse. Thanks to the registration, macmon can now guarantee access for as long as the access data is valid – meaning that if an employee leaves the company, their personal end devices are also automatically prevented from accessing the company network again. An overview of the devices that are brought along is also continuously guaranteed. The macmon guest service is a part of the macmon network bundle.

Contact

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