baramundi – macmon whitepaper

Integration between
baramundi Management Suite and macmon NAC

CONTENT

1 Introduction

This white paper is intended to aid in optimally connecting the baramundi Management Suite (bMS) Unified Endpoint solution and the macmon Network Access Control (NAC) application. This allows you to centrally address and control macmon NAC from the baramundi Management Suite (bMS). With bMS as the leading system, you only have to maintain new devices or transfers in one place. In addition, you can define rules that automatically move non-compliant devices from your network access control solution to a secure network.

2 Requirements

baramundi Management Suite

This whitepaper assumes that baramundi Management Suite (bMS) is fully synchronized with Active Directory through the automatic or manual capture of network devices. These devices are either assigned to a logical group or to a universal dynamic group (UDG) via filters. For example, a UDG can be created by filtering inventoried endpoints by characteristics such as the current patch level. For the use case scenarios described in this white paper, we recommend synchronizing the naming of groups in both the bMS and macmon NAC systems.

bMS requirements are:

Version

At least one baramundi Management Server 2020 R2 or later.

License

The Deploy module must be licensed to run scripts either client side or server side.

Configuration

When executing the scripts on the server side, the outgoing macmon port 443 must be opened in the baramundi server firewall.

Files

The following baramundi Deploy Scripts (bDS) files are required for the use case scenarios described below:

- macmon-macadd.bds
- macmon-maccompliant.bds
- macmon-macmod.bds
- macmon-macnoncompliant.bds
- macmon-macremove.bds

These can be downloaded through the baramundi tile under "Third-party integration" in your macmon NAC web interface. Scripts to be executed server-side are stored on the baramundi server in the baramundi\Management Server\Shares\Scripts\ServerSide directory.

macmon NAC

macmon NAC requirements are:

Version

macmon NAC 5.26 or later

License

To use the interfaces mentioned in this document, at least the macmon Network Bundle is required. To use the compliance scripts, the Premium Bundle is required to adjust the compliance state on macmon's side.
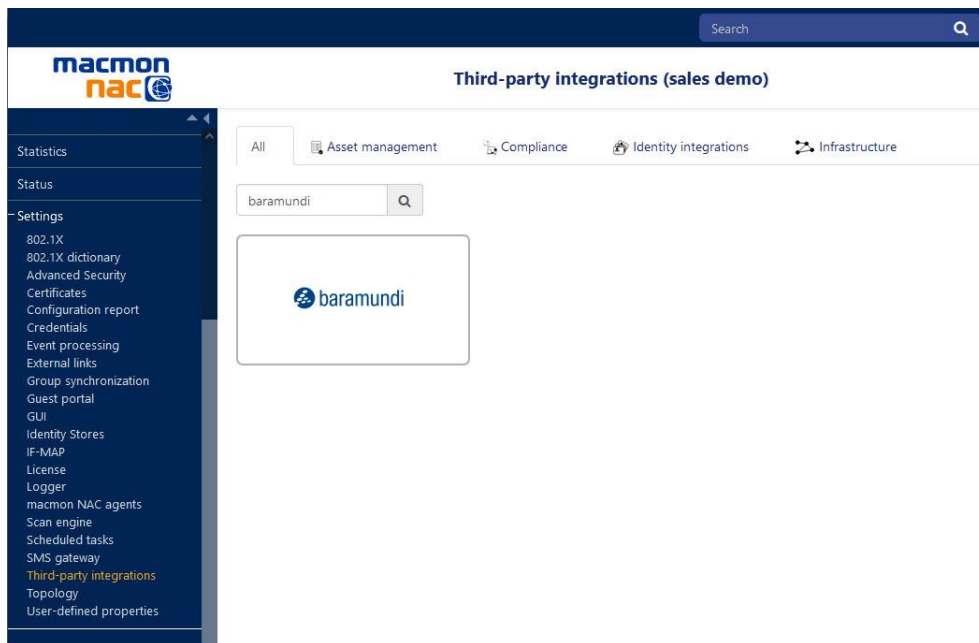
Configuration

The configuration requires a user who has set the "Create" right for the "Manage endpoints" authorization (i.e., preferably to all groups for the use cases described below).
In the settings under User Interface, there is the 'Base URL'. This is the URL to the macmon appliance and is used to create the URL to the macmon API in the baramundi scripts.

Third Party Tile

Under Settings, Third-party integration, the associated configuration can be opened through the "baramundi tile" and the required baramundi scripts can be downloaded.

In the configuration page, the displayed fields are mandatory fields to be passed to the script files. After filling out the fields, the files of the link list become hyperlinks and can be downloaded directly from the tile.

Using the end device group from baramundi
For the API calls that create or move end devices in the macmon appliance, you can specify use of the macmon group with the same name as the baramundi group in which the device(s) belong. It is important to remember that the macmon groups must already exist, otherwise the devices will neither be created nor moved.

3 Scenarios

1. New Endpoint -

Use Case

A new device that is added to baramundi should be automatically transferred to macmon.

How-To

1. As mentioned in the requirements, put **macmon-macadd.bds** under baramundi\Management Server\Shares\Scripts\ServerSide.
2. Create a new job, which includes the step "Execute server-side action" and calls the **macmon-macadd.bds** script.
3. Job assignment:

    i.   <u>Windows</u>

Under job properties in the "Automatic assignment" tab, define a criterion for all endpoints.

Example: <Primary MAC is not empty>.
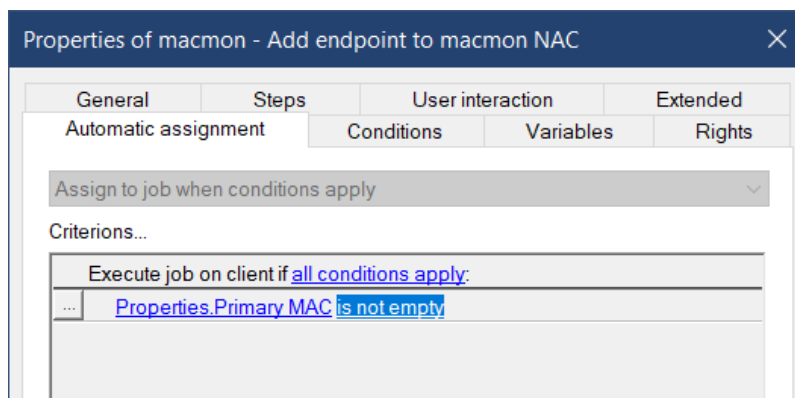
    ii.   <u>Mobile Devices</u>

    In the job properties, check "Assign to new devices".

By accepting this setting, this job is automatically assigned to all Windows endpoints for which the MAC address field in the database is filled. The scheduler then assigns this job once to all applicable endpoints and executes the server-side action to create the endpoint on the macmon NAC. If another Windows endpoint is created in the future, this job is automatically assigned to it for creation in macmon. The job also is automatically assigned to newly created mobile devices.

2. Initial Installations -

Use Case

A known Windows or mobile device was put into operation in the bMS and is subsequently moved in macmon to a group and production VLAN.

How-To

1. As mentioned in the requirements, put **macmon-macadd.bds** under baramundi\Management Server\Shares\Scripts\ServerSide.
2. Add a new job step at the end of the complete installation job or initial configuration, which calls the "Execute server-side action" step with the **macmon-macmod.bds** script.

   Note: When downloading scripts through the baramundi tile in the macmon WebUI, there is an option to define a macmon target group.

3. End of Life -

Use Case

A known device is deleted in the bMS and should be deleted in macmon as well.

How-To

1. As mentioned in the requirements, put **macmon-macadd.bds** under baramundi\Management Server\Shares\Scripts\ServerSide.
2. Add a new job step at the end of the device remote wipe or wipe disk job (or similar), which calls the "Execute server-side action" step with the **macmon-macremove.bds** script.

4. NON-Compliant -

Use Case

If an endpoint becomes NON-compliant, the information is transferred to macmon (a big advantage is that client administrators make the decision, not network administrators).

How-To

1. As mentioned in the requirements, put **macmon-macadd.bds** under baramundi\Management Server\Shares\Scripts\ServerSide.
2. Create a new job for <u>Windows endpoints or for mobile endpoints</u>, which includes the step "Execute server-side action" and calls the **macmon-macnoncompliant.bds** script.

<u>Note</u>: The complete procedure described here for endpoints that are NON-compliant can also be used for compliant endpoints. To do this, use the **macmon-maccompliant.bds** script and adapt the UDG criteria accordingly.
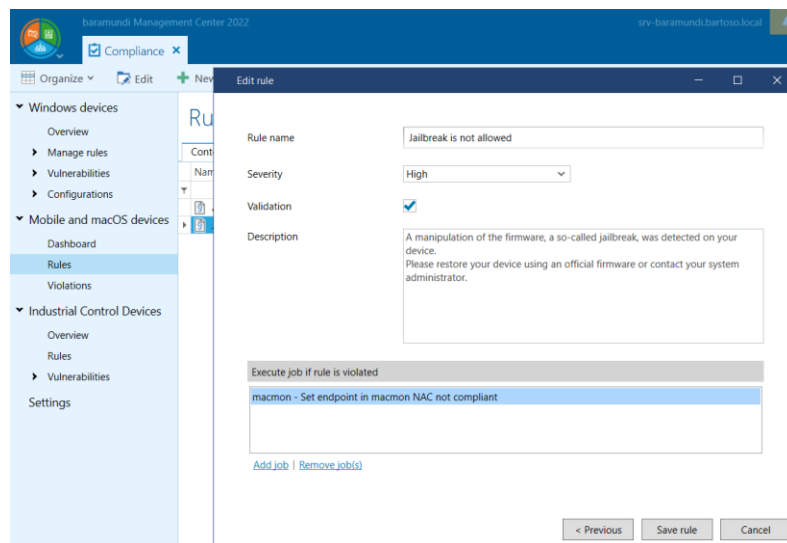
3. Job Allocation
   i.   <u>Windows</u>

Under job properties in the "Automatic assignment" tab, define a criterion for the applicable endpoints.

Example: <WindowsCompliance.Vulnerabilities.Threat Level = Medium>.

   ii. <u>Mobile Devices</u>

Under Compliance > Mobile devices, create a new rule that automatically assigns the job from step 2 if the rule was violated.

4 Map Key

Microsoft Windows

macOS

Android

Wear OS

Apple iOS / iPadOS

Windows Mobile

Network device (SNMP)

Industrial control unit

5 Help and Contact

baramundi customers

baramundi customers with questions about the bMS, job settings or bDS processing can contact baramundi support.

https://www.baramundi.com/en/support/

macmon customers

macmon customers with questions about macmon NAC, the macmon API or handling endpoints in macmon can contact macmon support.

https://www.macmon.eu/support/

About baramundi Software

baramundi software develops Unified Endpoint Management for the central administration of PCs, mobile devices and servers. It automates software distribution, simplifies patch management and creates transparency in the network. baramundi thereby makes a significant contribution to IT security and frees up resources.

www.baramundi.com

See how the baramundi Management Suite can benefit your company by registering for our free live webinar!

Experience how you can use the baramundi Management Suite to automatically manage and secure your PC clients, servers and mobile devices.

https://www.baramundi.com/en/it-training/

About macmon secure

Since 2003, the IT experts at macmon have been offering infrastructure manufacturer agnostic solutions that provide instant network transparency to protect heterogeneous networks from unauthorized access. macmon NAC can be implemented quickly and easily, with significant added value for your network security. macmon NAC also integrates seamlessly with other security solutions from international technology partners, such as endpoint security or firewalls. Graphical reports and topology diagrams provide customers with an immediate overview of their network. This makes macmon NAC a key building block for IT security, digitization and mobile office. With its **Z**ero **T**rust **N**etwork **A**ccess strategy, macmon secure extends its proven protection to all company resources in the cloud. It is the only provider of NAC and SDP with identity and access management that is both from Germany and hosted in Germany. macmon secure also offers its customers and partners a comprehensive training program and 24x7 support in English and German.

We are looking forward to meeting you!

Get in touch!
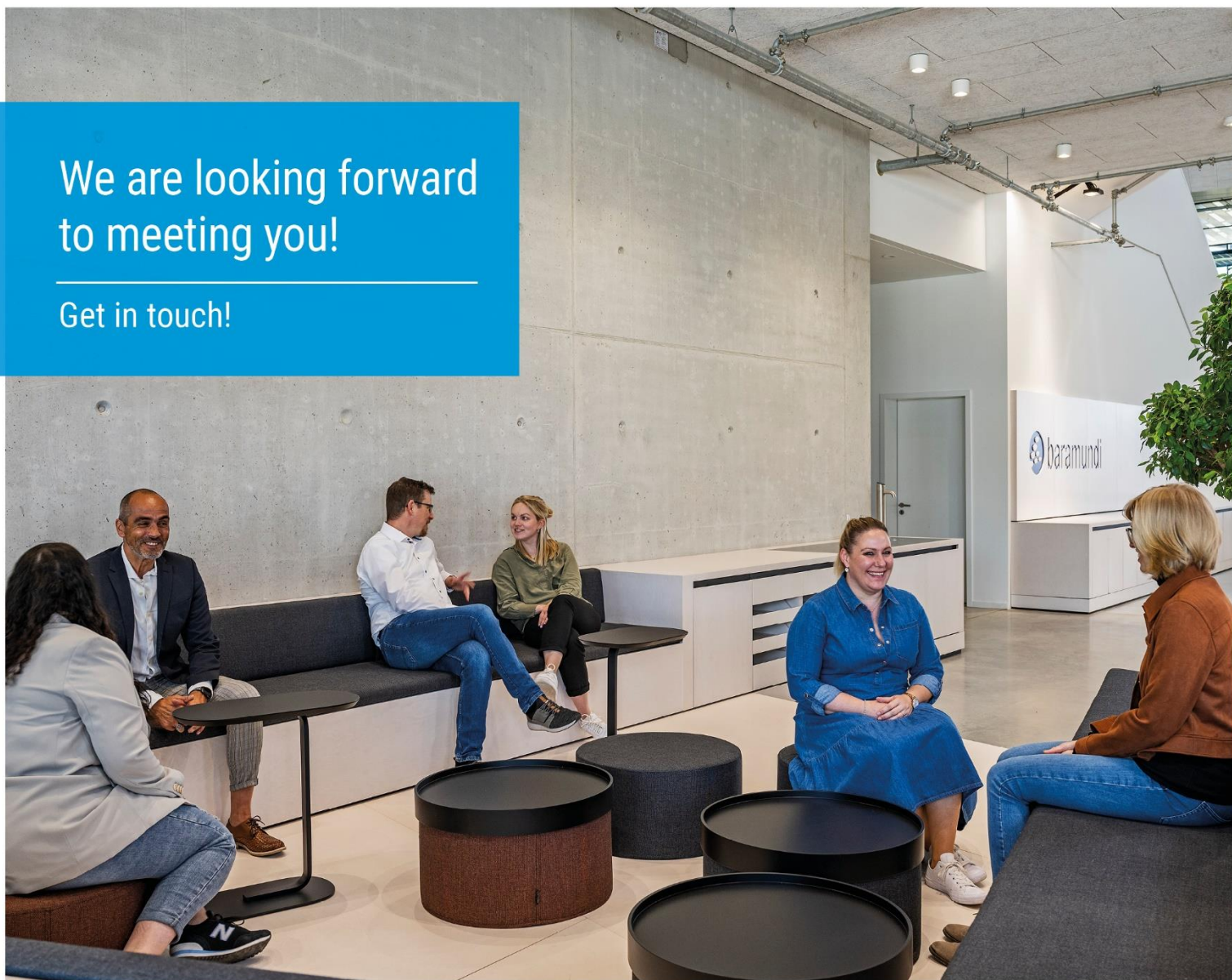
baramundi software GmbH
Forschungsallee 3
86159 Augsburg, Germany

🇩🇪 +49 821 5 67 08 - 380
request@baramundi.com
www.baramundi.com

🇬🇧 +44 2071 93 28 77
request@baramundi.com
www.baramundi.com

🇵🇱 +48 735 91 44 54
request@baramundi.com
www.baramundi.com

🌐 +49 821 5 67 08 - 390
request@baramundi.com
www.baramundi.com

🇦🇹 +43 1 71 72 85 45
request@baramundi.com
www.baramundi.com

🇮🇹 +39 340 8861886
request@baramundi.com
www.baramundi.com

🇨🇭 +41 77 280 49 79
request@baramundi.com
www.baramundi.com

baramundi software USA, Inc.
30 Speen St, Suite 401
Framingham, MA 01701, USA

🇺🇸 +1 508-861-7561
requestUSA@baramundi.com
www.baramundi.com