



baramundi – macmon whitepaper

Integration zwischen
baramundi Management Suite und macmon NAC

INHALT

1	Einleitung	2
2	Anforderungen	3
	baramundi	3
	macmon	4
3	Szenarien	6
1.	Neuer Endpunkt –     	6
2.	Initialinstallationen –     	7
3.	End of Life –     	7
4.	NON-Compliant –     	8
4	Legende	10
5	Hilfe und Kontakt	11
	baramundi	11
	macmon	11

© 2022 baramundi software GmbH

Aussagen über Ausstattung und technische Funktionalitäten sind unverbindlich und dienen nur der Information.
Änderungen vorbehalten. DocID: BMSMM-2022-001-RN-20221012-DE

1 Einleitung

Dieses Whitepaper soll eine Hilfestellung geben, die baramundi Management Suite (bMS) Unified Endpoint Lösung und die macmon Network Access Control (NAC) Anwendung optimal aneinander anzubinden. So können Sie aus der bMS macmon NAC zentral ansprechen und steuern. Mit der bMS als führendes System müssen sie neue Geräte oder Verschiebungen nur noch an einer Stelle pflegen. Außerdem können Sie so Regeln hinterlegen, mit denen nicht regelkonforme Geräte von ihrer Network Access Control Solution automatisch in ein gesichertes Netzwerk verschoben werden.

2 Anforderungen

baramundi

Dieses Whitepaper setzt voraus, dass baramundi Management Suite (bMS) für die Erfassung der Unternehmensgeräte eine vollständige Synchronisierung mit dem Active Directory durchgeführt hat oder diese manuell erfasst wurden. Diese Geräte werden entweder einer logischen Gruppierung oder über Filter einer dynamischen Gruppierung zugeordnet. Eine dynamische Gruppierung kann beispielsweise angelegt werden, indem die Endgeräte im Bestand nach Merkmalen wie dem aktuellen Patch Level gefiltert werden.

In den folgenden Fällen ist es sinnvoll, die Namensgebung der Gruppen in den beiden Systemen bMS und macmon NAC zu synchronisieren.

Auf Seiten des baramundi Servers bedarf es darüber hinaus folgendes.

Version

Mindestens einer baramundi Management Server 2020 R2 Installation

Lizenz

Das Modul Deploy muss lizenziert sein um Skripte entweder clientseitig oder serverseitig ausführen zu lassen.

Konfiguration

Bei Ausführung der Skripte serverseitig muss auf der Firewall des baramundi Servers der macmon Port 443 ausgehend geöffnet werden.

Dateien

Die folgenden BDS-Dateien werden für die nachfolgenden Anwendungsfälle benötigt.

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

Diese können durch die baramundi Kachel unter „Drittanbieter-Integration“ in Ihrem macmon NAC Webinterface heruntergeladen werden.

Serverseitig auszuführende Scripts werden auf dem baramundi Server im Verzeichnis baramundi\Management Server\Shared\Scripts\ServerSide abgelegt.

macmon

Auf Seiten macmon NAC gibt es folgenden Anforderungen:

Version

Mindestens eine macmon 5.26 Installation

Lizenz

Für die Verwendung der in diesem Dokument genannten Schnittstellen ist mindestens das macmon Network Bundle erforderlich. Für die Verwendung der Compliance-Skripte ist das Premium Bundle notwendig, um auf Seiten macmons den Compliance Zustand anzupassen.

Konfiguration

Die Konfiguration setzt einen Benutzer voraus, der das Recht "Erstellen" bei der Berechtigung "Endgeräte verwalten" gesetzt hat (entsprechend der beschriebenen UseCases also am besten auf alle Gruppen).

In den Einstellungen unter Benutzeroberfläche gibt es die ‚Base URL‘. Dies ist die URL zur macmon Appliance und wird herangezogen, um in den baramundi Skripten die URL zur macmon API zu erstellen.

Proxy

Bitte beachten, sie dass es sich hierbei um eine URL und Webaufruf handelt. Somit können mögliche Proxy-Einstellungen des ausführenden Systems (baramundi Server) den Webaufruf umlenken oder blockieren.

Zertifikat

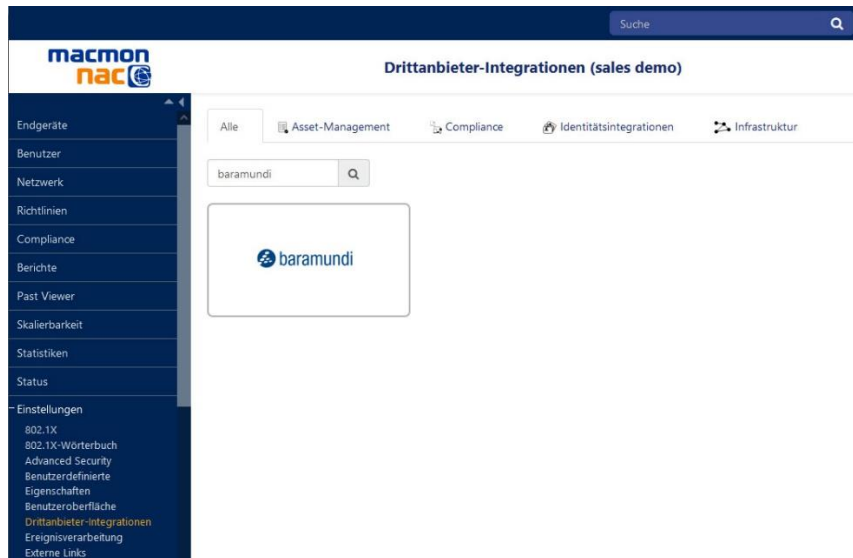
An der macmon appliance muss an Port 443 ein gültiges Zertifikat hinterlegt sein, um die per HTTPS gesicherte Kommunikation per Skript zu ermöglichen.

Beispielaufruf

Beispielaufufe der verwendeten macutil-API finden sie im macmon Handbuch im Kapitel „macutil unter Verwendung von https“

Drittanbieterkachel

Unter Einstellungen Drittanbieter-Integration kann durch die „baramundi Kachel“ die dazugehörige Konfiguration geöffnet und die erforderlichen baramundi Skripte heruntergeladen werden.



In der Konfigurationsseite müssen alle Pflichtfelder ausgefüllt sein, bevor die Informationen in Skriptdateien umgewandelt werden können. Nachdem die Felder befüllt sind, werden Hyperlinks zu den Dateien der Link-Liste generiert und können somit direkt aus der Kachel heruntergeladen werden.

Verwenden der Endgerätegruppe aus baramundi

Für die API Aufrufe, welche Endgeräte in der macmon Appliance anlegt oder bewegt, kann angegeben werden, dass die gleichnamige macmon Gruppe verwendet werden soll, welche das Endgerät bereits in baramundi (OUs) angehört. **Hinweis:** Wichtig hierbei ist, dass die Gruppen in macmon vorab existieren müssen, ansonsten werden die Endgeräte weder angelegt noch bewegt.

Konfiguration für baramundi Management Suite bearbeiten

▼ Beschreibung

Die baramundi Management Suite (BMS) kann zur Pflege von Endgeräten verwendet werden. Die Nutzung der hier verfügbaren Skripte sorgt für eine automatische Übertragung der Konfigurationen an macmon NAC, so dass diverse administrative Schritte nur in der BMS durchgeführt werden müssen. Die Use-Cases und die Verwendung in der BMS sind im Whitepaper genauer beschrieben. Mögliche Aktionen sind:

- Hinzufügen eines Endgerätes in macmon NAC
- Modifizieren der Gruppenzugehörigkeit eines Endgerätes in macmon NAC
- Verändern des Compliance Status eines Endgerätes in macmon NAC auf "NonCompliant"
- Verändern des Compliance Status eines Endgerätes in macmon NAC auf "Compliant"
- Löschen eines Endgerätes in macmon NAC

Das Ausfüllen der Felder innerhalb dieses Dialogs führt zur automatischen Modifikation der Skripte, so dass diese ohne weitere Änderungen im BMC verwendet werden können. Benutzername und Passwort werden hinterlegt und müssen einem Benutzer in macmon NAC mit entsprechenden Berechtigungen (Schreibend für die Endgerätegruppen) entsprechen. Wird das Feld "Spezifische Gruppe" leer gelassen, so wird beim Aufruf des Skripts die im BMC konfigurierte Endgerätegruppe des Endgerätes übernommen. Alternativ kann mittels der Auswahl einer konkreten Endgerätegruppe im Skript genau diese Gruppe hinterlegt werden, so dass bei der Nutzung des Skriptes alle Geräte genau der einen Gruppe in macmon NAC zugewiesen werden.

Konfiguration

Benutzername *
admin

Benutzername des macmon-Benutzers

Passwort *

Passwort des macmon-Benutzers

Name der Endgerätegruppe
Verwenden der Endgerätegruppe aus baramundi

Die macmon-Endgerätegruppe, zu der Endgeräte hinzugefügt werden

Link-Liste

Bitte alle benötigten Felder oben ausfüllen, um den Link zum Herunterladen zu aktivieren

Endgerät zu macmon hinzufügen: macmon-macadd.bds
Endgerätegruppe in macmon ändern: macmon-macmod.bds
Endgerät in macmon löschen: macmon-macremove.bds
Compliance-Status auf "compliant" ändern: macmon-maccompliant.bds
Compliance-Status auf "non-compliant" ändern: macmon-macnoncompliant.bds

Anwenden Schließen

3 Szenarien

1. Neuer Endpunkt –

Use Case

Ein neues Endgerät, welches in baramundi aufgenommen wird soll danach automatisch an macmon übertragen werden.

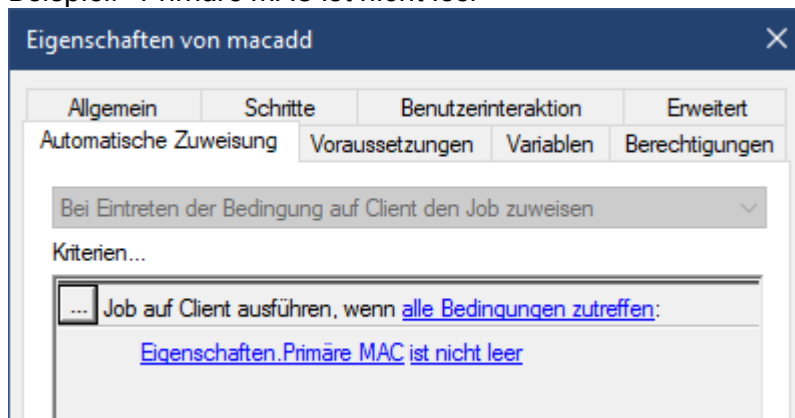
HowTo

1. Wie in den Voraussetzungen erwähnt das **macmon-macadd.bds** unter baramundi\Management Server\Shared\Scripts\ServerSide ablegen.
2. Neuen Job erstellen, welcher den Schritt „Serverseitige Aktion ausführen“ beinhaltet und das Skript **macmon-macadd.bds** aufruft.
3. Jobzuweisung

i. Windows

Unter den Eigenschaften dieses Jobs im Reiter „Automatische Zuordnung“ ein Kriterium für alle Endpoints hinterlegen.

Beispiel: <Primäre MAC ist nicht leer>



ii. Mobile Geräte

In den Jobeigenschaften den Haken „Neuen Geräten zuweisen“ setzen.

Durch ein Übernehmen dieser Einstellung wird dieser Job automatisch allen Windows Endpunkten zugewiesen, bei welchen in der Datenbank das Feld der MAC-Adresse gefüllt ist. Somit weist der Scheduler allen zutreffenden Endpunkten diesen Job einmalig zu und führt die Serverseitige Aktion aus um den Endpunkt auf der macmon NAC anzulegen. Wird in Zukunft nun ein weiterer Windows Endpunkt angelegt so wird auch diesem automatisch dieser Job zum Anlegen in macmon zugewiesen. Für mobile Geräte gilt nach dem Setzen des Hakens, dass der Job neu erstellten mobilen Geräten den Job automatisch zuweist.

2. Initialinstallationen –

Use Case

Ein bekanntes Windows oder mobiles Endgerät wurde durch baramundi in Betrieb genommen und wird im Anschluss in macmon in eine produktive Gruppe und somit Produktions-VLAN verschoben.

How To

1. Wie in den Voraussetzungen erwähnt, das **macmon-macmod.bds** unter baramundi\Management Server\Shared\Scripts\ServerSide ablegen.
2. Einen neuen Jobschritt am Ende des Komplettinstallationsjobs oder der initialen Konfiguration hinzufügen, welcher den Schritt „Serverseitige Aktion ausführen“ mit dem Skript **macmon-macmod.bds** aufruft.

Hinweis: Beim Herunterladen der Skripte durch die baramundi Kachel in der macmon WebUI gibt es die Möglichkeit eine macmon Ziel-Gruppe zu definieren.

3. End of Life –

Use Case

Ein bekanntes Gerät wird in baramundi gelöscht und soll korrespondierend in macmon NAC ebenso als Endpunkt gelöscht werden.

How To

1. Wie in den Voraussetzungen erwähnt, das **macmon-macremove.bds** unter baramundi\Management Server\Shared\Scripts\ServerSide ablegen.
2. Einen neuen Jobschritt am Ende des Gerät Fernlöschens oder Wipe-Disk-Jobs (o.ä.) hinzufügen, welcher den Schritt „Serverseitige Aktion ausführen“ mit dem Skript **macmon-macremove.bds** aufruft.

4. NON-Compliant –

Use Case

Wird ein Endpunkt NON-Compliant, so wird die Information an macmon übertragen (Der große Vorteil ist, dass die Client-Administratoren die Entscheidung treffen und nicht die Netzwerk-Administratoren).

How To

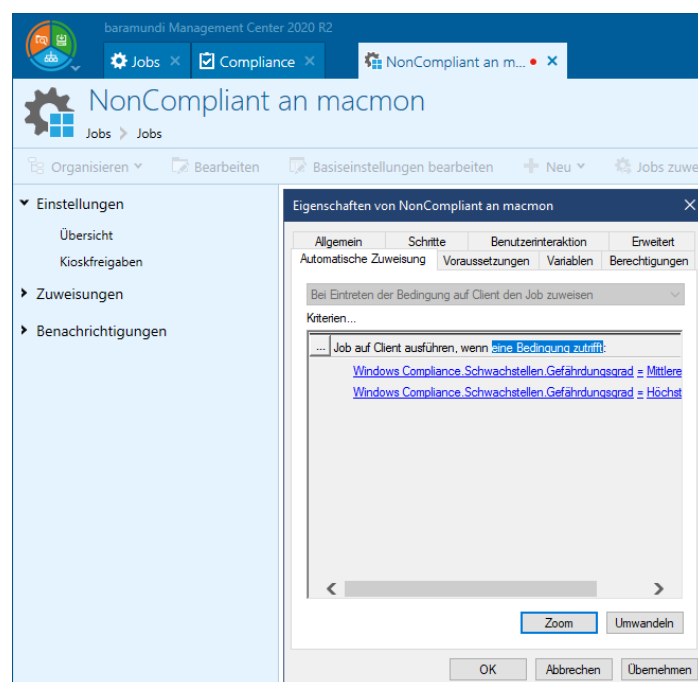
1. Wie in den Voraussetzungen erwähnt, das **macmon-macnoncompliant.bds** unter `baramundi\Management Server\Shared\Scripts\ServerSide` ablegen.
2. Neuen Job für Windows Endpunkte oder für mobile Endpunkte erstellen, welcher den Schritt „Serverseitige Aktion ausführen“ beinhaltet und das Skript **macmon-macnoncompliant.bds** aufruft.

Hinweis: Das hier beschriebene komplette Vorgehen bei Endpunkten, welche NON-Compliant sind, kann auch für Compliant Endpunkte angewandt werden. Hierzu das Skript **macmon-maccompliant.bds** heranziehen, sowie die Bedingungen (dynamische Gruppen) entsprechend anpassen.

3. Job Zuweisungen
 - i. Windows

Unter den Eigenschaften dieses Windows-Jobs im Reiter „Automatische Zuordnung“ ein Kriterium für die zutreffenden Endpunkte hinterlegen.

Beispiel: `<WindowsCompliance.Schwachstellen.Gefährdungsgrad = Mittel>`



ii. Mobile Geräte

Unter Compliance > Mobile Geräte eine neue Regel erstellen, welche automatisiert den Job aus Schritt 2 zuweist, sofern die Regel verletzt wurde.

The screenshot displays the 'Regeln' (Rules) configuration page in the Baramundi Management Center. The left sidebar shows the navigation tree with 'Mobile und macOS-Geräte' expanded. The main area shows a table of rules, with 'Jailbreak is not allowed' selected. The details for this rule are shown in a modal window titled 'Regel bearbeiten'.

Name	Schweregrad	Regeltyp	App-Paketname	Geändert	Erstellt
Jailbreak is not allowed	Hoch	Jailbreak		Vor 13 Monaten	Vor 13 Monaten

Regel bearbeiten

Regelname: Jailbreak is not allowed

Schweregrad: Hoch

Prüfung: ☒

Beschreibung: A manipulation of the firmware, a so-called jailbreak, was detected on your device. Please restore your device using an official firmware or contact your system administrator.

Jobausführung bei Verstoß

macmonnoncompliant

[Job hinzufügen](#) | [Job\(s\) entfernen](#)

< Zurück Regel speichern Abbrechen

4 Legende

-  Microsoft Windows
-  macOS
-  Android
-  Wear OS
-  Apple iOS / iPadOS
-  Windows Mobile
-  Netzwerkgerät (SNMP)
-  Industrielles Steuergerät

5 Hilfe und Kontakt

baramundi

Bei Fragen rund um baramundi, die Jobeinstellungen oder der BDS Bearbeitungen wenden Sie sich als baramundi Bestandskunde bitte an Ihren baramundi Support.

<https://www.baramundi.com/de-de/support/>

macmon

Bei Fragen rund um macmon, dem Aufruf der macmon API oder der Handhabung der Endpunkte in macmon wenden Sie sich als Bestandskunde macmon bitte an Ihren macmon Support.

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

Über die baramundi software GmbH

baramundi software entwickelt Unified Endpoint Management zur zentralen Verwaltung von PCs, Mobilgeräten und Servern. Sie automatisiert Softwareverteilung, vereinfacht Patchmanagement und schafft Transparenz im Netzwerk. baramundi trägt so maßgeblich zur IT-Sicherheit bei und setzt Ressourcen frei.

www.baramundi.com

Sie möchten sich die baramundi Management Suite ansehen? Melden Sie sich zum Live Webinar an!

Erleben Sie im kostenfreien Webinar, wie Sie mit der baramundi Management Suite Ihre PC-Clients, Server und Mobilgeräte automatisiert verwalten und absichern.

<https://www.baramundi.com/de-de/schulungen-webinare/>

Über macmon secure

Die erfahrenen IT-Experten bieten seit 2003 herstellerunabhängige Lösungen, die heterogene Netzwerke dank sofortiger Netzwerktransparenz vor unberechtigten Zugriffen schützen. macmon NAC wird schnell und einfach implementiert, mit erheblichem Mehrwert für die Netzwerksicherheit. Dabei integriert sich macmon NAC sinnvoll mit weiteren Sicherheitslösungen internationaler Technologiepartner, wie Endpoint Security oder Firewall. Kunden erhalten sofortige Netzwerkübersicht mit grafischen Reports und Topologiedarstellung. Somit ist macmon NAC ein zentraler Baustein bei den Themenfeldern IT-Security, Digitalisierung und Mobile Office.

macmon secure dehnt mit seiner **Zero-Trust-Network-Access**-Strategie seinen bewährten Schutz auf sämtliche Unternehmensressourcen in der Cloud aus, und ist der einzige Anbieter von NAC plus SDP mit Identity and Access Management aus Deutschland, gehostet in Deutschland. Außerdem bietet macmon secure seinen Kunden und Partnern ein umfassendes Schulungsprogramm und deutschsprachigen 24x7-Support.

Wir freuen uns, Sie
kennenzulernen!

Kontaktieren Sie uns!



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