



MACMON NAC WHITEPAPER

Integration zwischen macmon NAC
und WithSecure Business Suite Premium



Inhalt

1	Über WithSecure:	2
2	Anwendungsfälle.....	3
2.1	macmon NAC prüft den Status diverser Sicherheitskomponenten der WithSecure Endpoint Security Agenten.....	3
2.2	macmon NAC reagiert auf Bedrohungen.....	3
3	Konfiguration von WithSecure Business Suite Premium.....	4
3.1	Erstellen einer API-URL.....	5
4	Konfiguration von macmon NAC	8
4.1	macmon NAC reagiert auf Bedrohungen.....	12
5	Kontakt bei WithSecure	15
	Kontakt.....	15

Version: 2.0

Über WithSecure:

WithSecure™ ist der zuverlässige Partner für Cybersicherheit. IT-Dienstleister, MSSPs und Unternehmen sowie die größten Finanzinstitute, Hersteller und Tausende der weltweit fortschrittlichsten Kommunikations- und Technologieanbieter vertrauen uns, wenn es um ergebnisorientierte Cybersicherheit geht, die ihren Betrieb schützt und ermöglicht.

Unser KI-gesteuerter Schutz sichert Endpunkte und Cloud-Zusammenarbeit, und unsere intelligenten Erkennungs- und Reaktionsfunktionen werden von Experten unterstützt, die Geschäftsrisiken identifizieren, indem sie proaktiv nach Bedrohungen suchen und aktive Angriffe abwehren. Unsere Berater arbeiten mit Unternehmen und Technologieanbietern zusammen, um durch evidenzbasierte Sicherheitsberatung die Widerstandsfähigkeit zu erhöhen. Mit mehr als 30 Jahren Erfahrung in der Entwicklung von Technologien, die den Unternehmenszielen entsprechen, haben wir unser Portfolio so aufgebaut, dass wir mit unseren Partnern durch flexible Geschäftsmodelle wachsen können.

1 Anwendungsfälle

1.1 macmon NAC prüft den Status diverser Sicherheitskomponenten der WithSecure Endpoint Security Agenten

In den letzten Jahren häufen sich die Meldungen zu Viren und Ransomware, die in Sekundenschnelle die Produktivität eines Unternehmens gefährden können. Häufig gelangen diese Bedrohungen über das Web oder via E-Mail in ein Unternehmen und können durch einen unbedachten Klick ausgelöst werden. Damit ein befallenes Endgerät nicht zum Ausgangspunkt einer Infizierung des ganzen Unternehmensnetzwerks wird, arbeiten **WithSecure** und **macmon secure** in einem engen und leistungsstarken Verbund.

Die ausgefeilte Engine von **WithSecure Business Suite Premium** bietet eine Reihe von Komponenten, um lokal auf den Endgeräten für effektive Sicherheit zu sorgen. Durch die Kommunikation zwischen den **Agenten** und dem **Policy Manager** von **WithSecure** sind sämtliche Status zentral verfügbar. **macmon NAC** fragt diese Details über die **REST API** des **Policy Managers** ab und bietet damit die Möglichkeit sicherzustellen, dass Endgeräte, die nicht den Sicherheitsvorgaben entsprechen, automatisch entsprechend der Firmenrichtlinie zu behandeln sind und zum Beispiel direkt vom Netzwerk zu trennen oder in ein Quarantänenetz verschoben werden.

macmon NAC überwacht zudem permanent, ob die Virensignaturen aller Unternehmensgeräte aktuell sind und fasst diese Information leicht ablesbar zusammen: Wenn die Virensignaturen auf einem Endgerät aktuell sind, entspricht es den Unternehmensvorgaben. Sind die Virensignaturen eines Endgeräts jedoch älter als durch die Unternehmensrichtlinien vorgegeben, so wird es von **macmon NAC** auf Wunsch zur Aktualisierung in ein eigenes Netzwerksegment verschoben und der Administrator darüber in Kenntnis gesetzt. In jedem Fall gewinnt ein Administrator einen schnellen Überblick über die Aktualität der Virensignaturen in Unternehmensnetzwerken jeder Größe.

1.2 macmon NAC reagiert auf Bedrohungen

Findet der **WithSecure Client** auf einem Endgerät eine Schadsoftware, so dürfen nur wenige Sekunden vergehen, um die Bedrohung zu neutralisieren. Die Information darüber wird sofort an den **WithSecure Policy Manager** übermittelt, der mit **macmon NAC** verbunden ist.

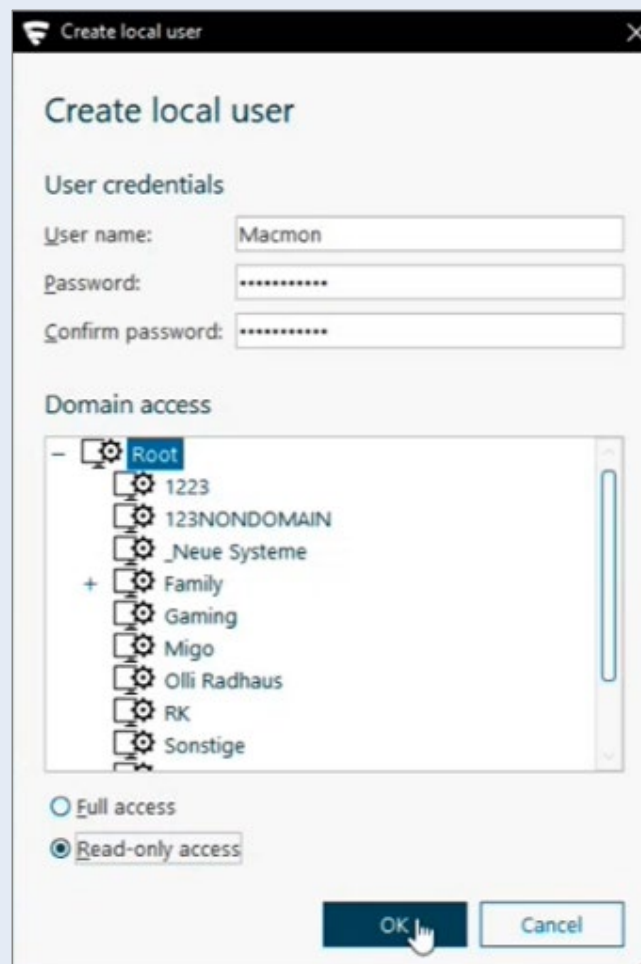
Dabei wird nicht nur übermittelt, dass eine Bedrohung gefunden wurde, sondern auch, ob sie vom **WithSecure Client** bereinigt werden konnte. Zwei Fälle, die von **macmon NAC** unterschiedlich bewertet werden können: Einerseits eine Bedrohung oder eine ungewöhnliche Häufung von Bedrohungen, die in einem kurzen Zeitraum gefunden und bereinigt werden können. Andererseits Ransomware, beispielsweise in Form eines Kryptotrojans, die zunächst nicht über den **WithSecure Client** entfernt werden kann, weil sie über ein separat erhältliches Spezialtool bereinigt werden muss oder ein Schreibschutz aktiv ist. Der **WithSecure Policy Manager** benachrichtigt **macmon NAC** in beiden Fällen, was umgehend von der NAC-Lösung ausgewertet wird. Das betroffene Endgerät wird in ein spezielles Netzwerksegment zur Heilung verschoben und der zuständige Administrator benachrichtigt.

2 Konfiguration von WithSecure Business Suite Premium

Grundsätzlich ist zu empfehlen für direkte Verbindungen zwischen Systemen **dedizierte Benutzer** zu verwenden, um zum einen den Missbrauch zu verhindern und zum anderen eine eindeutige Zuordnung in etwaigen Logs zu erreichen. Erstellen Sie daher als erstes im **WithSecure Policy Manager** einen eigenen Benutzer zur Kopplung mit **macmon NAC**.

Gehen Sie hierbei wie folgt vor:

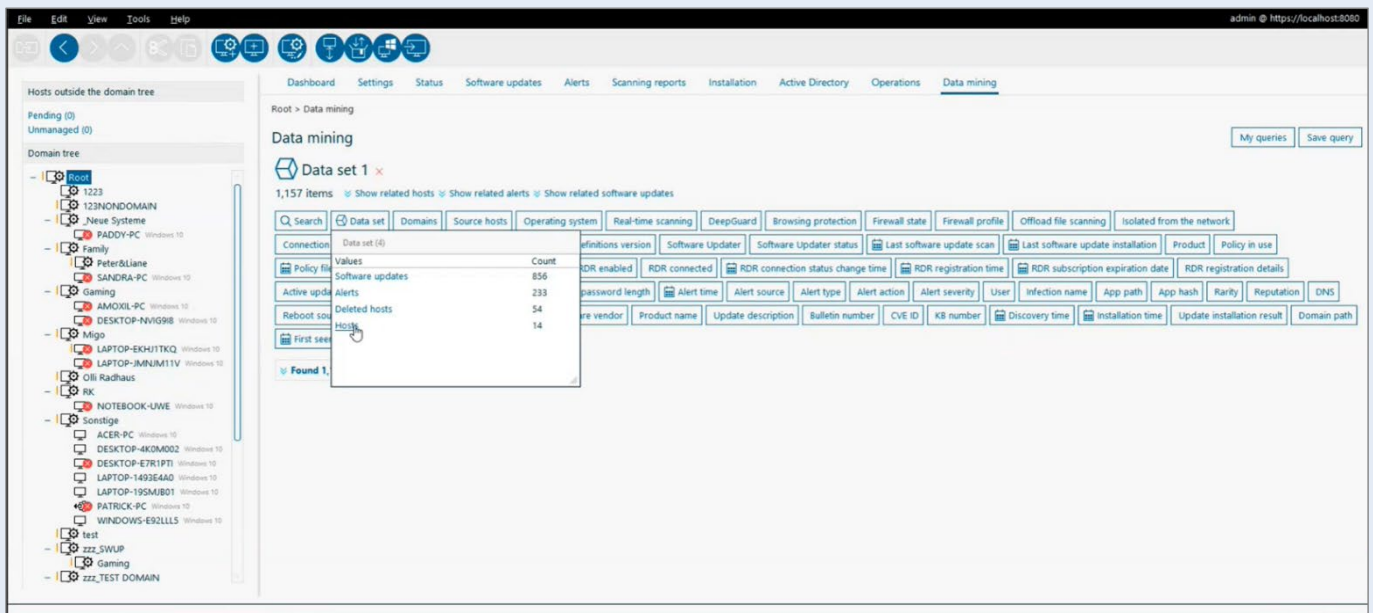
1. Öffnen Sie die Benutzerverwaltung von **Policy Manager** unter *Tools – Benutzer...*
2. Wählen Sie *Lokalen Benutzer erstellen*.
3. Vergeben Sie einen **Benutzernamen** und **Passwort**.
4. Wählen Sie unter „*Zugriffsmodus*“ die oberste Ebene (sofern nicht geändert: *Stamm*) aus.
5. Limitieren Sie den Zugriff durch Auswahl von „*Schreibgeschützter Zugriff*“.
6. Wählen Sie **OK**, um den Benutzer anzulegen.



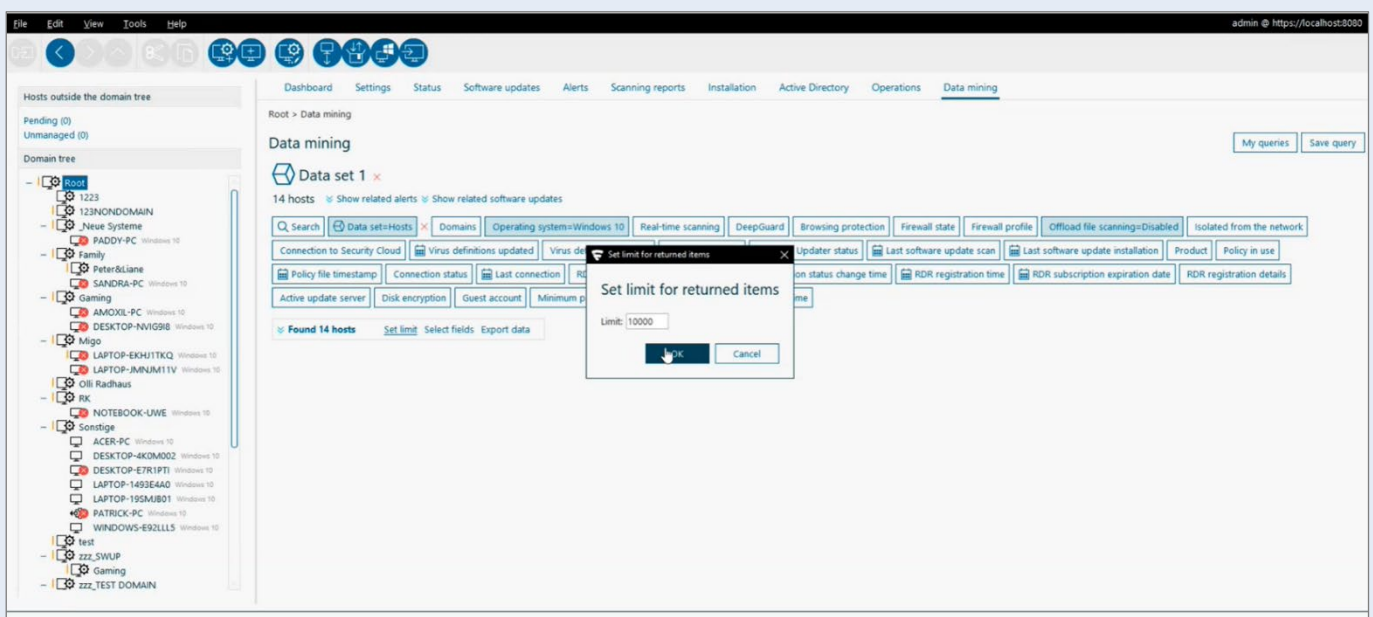
2.1 Erstellen einer API-URL

Die REST API des **WithSecure Policy Managers** bietet eine elegante Art, um **passgenaue URLs** zu erzeugen, welche explizit den gewünschten Content liefern, ohne dass bei der Abfrage komplexe Filter eingebaut werden müssen. Die **Erzeugung der URL ist über die GUI möglich** und wird im Folgenden genauer beschrieben:

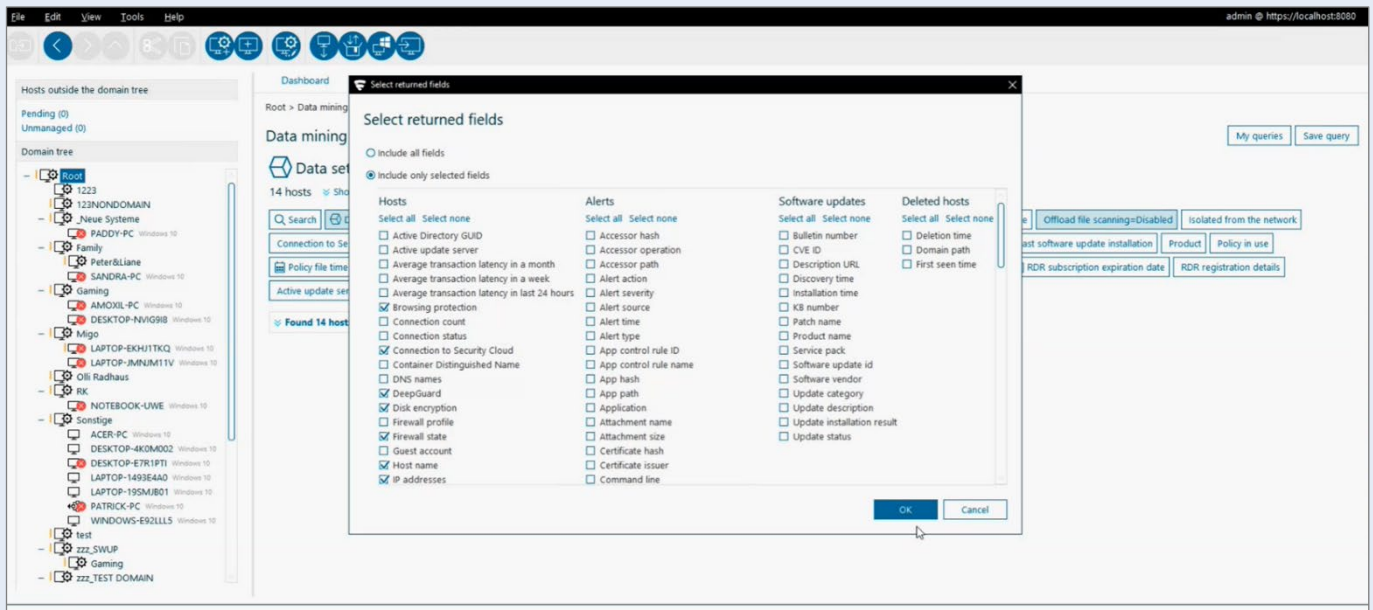
1. Navigieren Sie über die Tabs am oberen Fensterrand zu **„Data mining“**, wählen Sie wie hier im Screenshot **„Data set“** und dann **„Hosts“**.



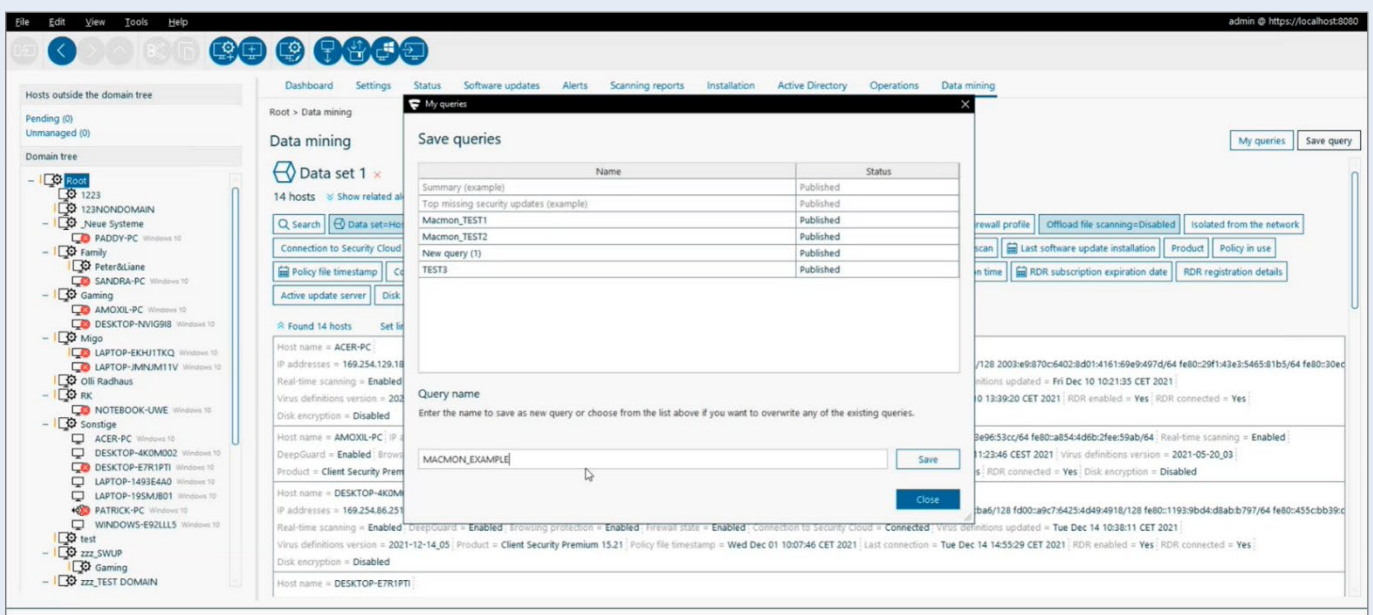
2. Klicken Sie auf **„Set limit“** und definieren Sie einen Wert der ausreichend groß ist, um die Details zu all Ihren Endgeräten auf einmal zu bekommen – optimaler Weise mit einem Puffer nach oben.



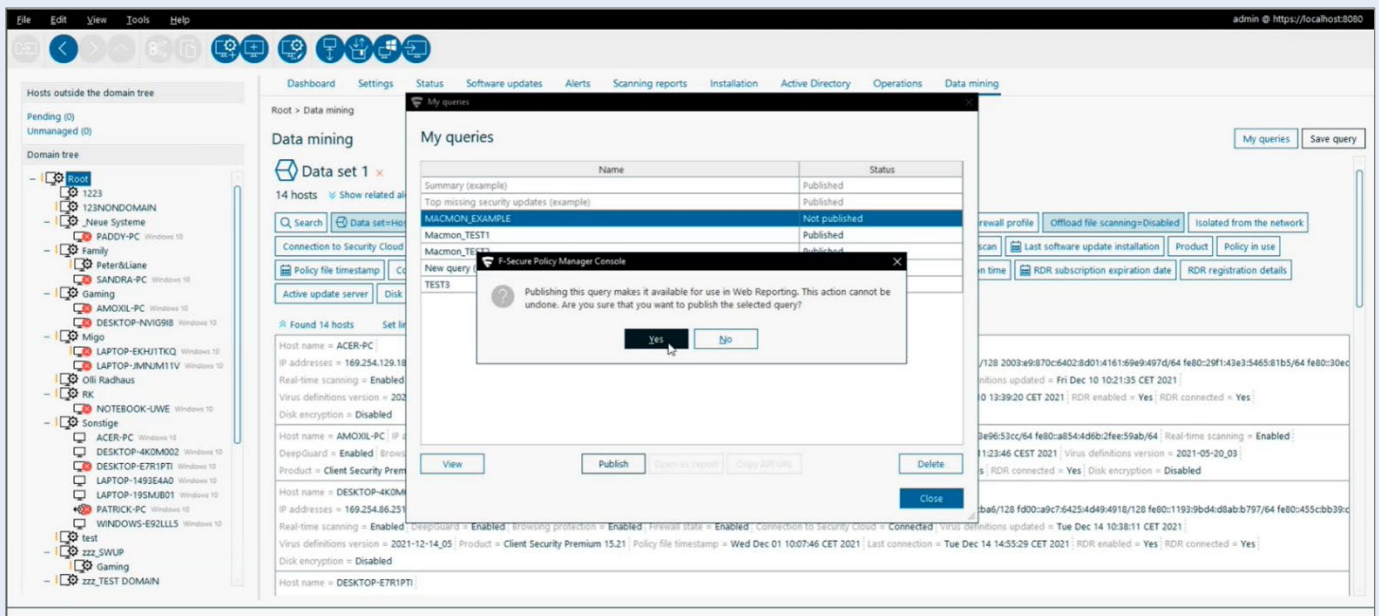
3. Klicken Sie als nächstes auf „*Select fields*“ und wählen Sie in dem hier im Screenshot sichtbaren Dialog die Komponenten aus, die abgefragt werden sollen. Es empfiehlt sich dabei alle folgenden Werte zu selektieren, um später in der **macmon NAC GUI** zu entscheiden, wie mit den Daten verfahren werden soll. Setzen Sie daher die Haken für „*Browsing protection, Connection to Security Cloud, DeepGuard, Disk encryption, Firewall state, Host name, IP addresses, Last connection, Policy file timestamp, Product, RDR connected, RDR enabled, Real-time scanning, Virus definitions updated, Virus definitions version*“.



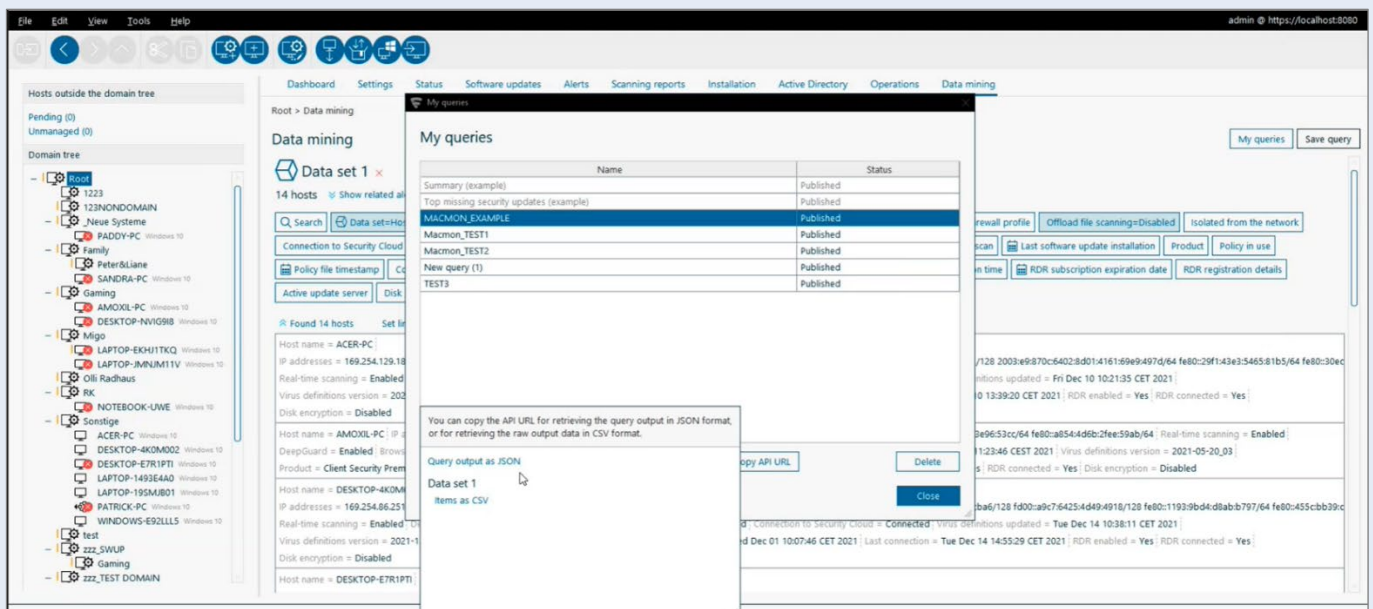
4. Klicken Sie als nächstes oben rechts in der GUI auf „*Save query*“ und vergeben Sie einen beliebigen Namen für die Datenselektion.



- Wählen Sie die gerade erstellte Selektion und klicken Sie auf „Publish“ und dann auf „Yes“, um zu bestätigen, dass die Selektion im Webreporting verwendet werden darf.

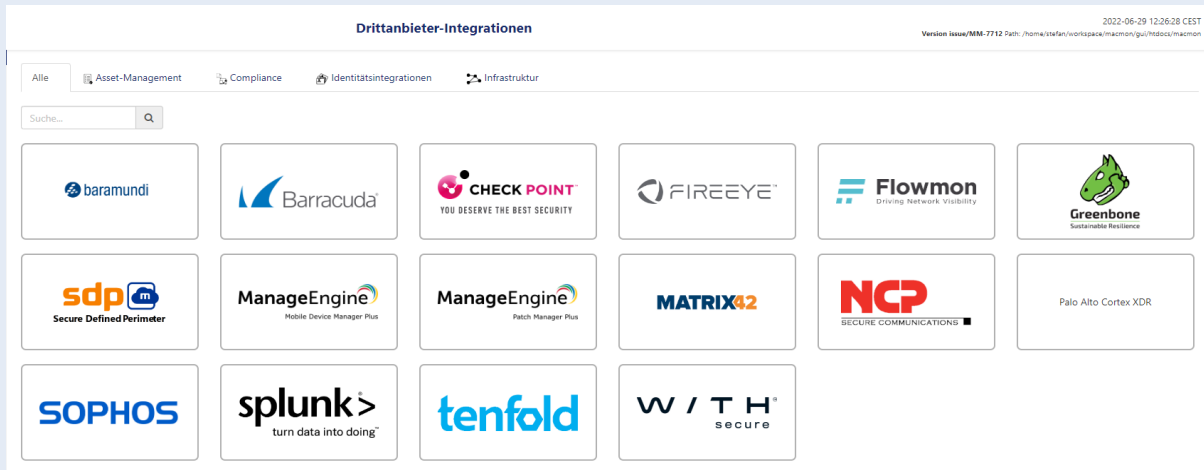


- Klicken Sie nun als letzten Schritt auf „Copy API URL“ und wählen dann wie hier im Screenshot ersichtlich „Query output as JSON“.



3 Konfiguration von macmon NAC

Die Konfiguration wird über das **Web-GUI** durchgeführt. Tippen Sie auf „**Einstellungen**“ und „**Drittanbieter-Integrationen**“, dann auf „**Compliance**“.



Wenn der **Rahmen der WithSecure-Kachel grau** ist, ist die Integration **noch nicht aktiviert**. Bitte tippen Sie auf die Kachel, um den Konfigurationsdialog aufzurufen.

Zur besseren Übersichtlichkeit ist der Dialog hier in mehrere Abschnitte aufgeteilt.

1. Fügen Sie zunächst die im **WithSecure PolicyManager** erzeugte **API-URL** in das entsprechende Feld ein und ergänzen Sie „**Benutzername und Passwort**“ für den Zugriff auf die API. Sollte Ihre **WithSecure PolicyManager Installation** nicht mit einem verifizierbaren Zertifikat versehen sein, so können Sie hier im Dialog mit der Entfernung des Hakens die Prüfung deaktivieren (nicht empfohlen).

Konfiguration für WithSecure Policy Manager bearbeiten ×

▼ Beschreibung

Die Integration zwischen macmon NAC und WithSecure bezieht sich hier explizit auf eine Verbindung zum WithSecure Policy Manager. Bitte folgen Sie den Beschreibungen des hier bereitgestellten Whitepapers, um in der GUI des WithSecure Policy Manager den Bericht zu erstellen und die zugehörige API-URL zu kopieren. Mit der Hinterlegung der URL sowie den lesberechtigten Zugangsdaten hier im Konfigurationsdialog stellen Sie die Grundlage zum Abrufen und Verarbeiten der Sicherheitsinformationen zu Ihren Endgeräten her. Im Folgenden können Sie je Sicherheitsfunktion / -eigenschaft definieren, ob der Status überhaupt geprüft werden soll, in eine Gesamtbewertung einfließen soll, oder bereits für sich genommen ein „Muss-Kriterium“ darstellt, dessen Nichterfüllung dazu führt, dass das betroffene Endgerät in macmon als „Non-Compliant“ behandelt wird. Am Ende des Konfigurationsdialoges können Sie zudem definieren, dass eine bestimmte Menge an negativen Status dazu führt, dass ein Endgerät „Almost-Non-Compliant“ oder „Non-Compliant“ wird.

Identifikator: [WITHSECURE_POLICY_MANAGER]

Konfiguration

URL *

Die URL zum Bericht, erstellt von WithSecure Policy Manager

Benutzername *

Benutzername für WithSecure Policy Manager

Passwort *

Passwort für WithSecure Policy Manager

SSL-Zertifikatsprüfung

Diese Option legt fest, ob das SSL-Zertifikat von WithSecure Policy Manager überprüft werden soll.

2. Die nun folgenden Dropdown Auswahlfelder beziehen sich jeweils auf einzelne Komponenten des **WithSecure Endpoint Security Agenten**. Dabei können Sie auswählen, ob der Status der jeweiligen Komponenten überhaupt geprüft werden soll, ob er geprüft werden soll, um das Ergebnis am Ende in einem Gesamtstatus zu verwenden oder ob ein negatives Prüfungsergebnis einer bestimmten Komponente sogar schon allein zu dem Status „Non-Compliant“ in **macmon NAC** führen soll.

Prüfung des Status von WithSecure Real-Time Scanner *

Nicht prüfen ▼

Prüft oder ignoriert, ob WithSecure Real-Time Scanner aktiv ist

Prüfung des Status von WithSecure Deep-Guard *

Nicht prüfen ▼

Prüft oder ignoriert, ob WithSecure Deep-Guard aktiv ist

Prüfung des Status von WithSecure Harddisc Encryption *

Nicht prüfen ▼

Prüft oder ignoriert, ob WithSecure Harddisc Encryption aktiv ist

Prüfung des Status von WithSecure Rapid Detection & Response *

Nicht prüfen ▼

Prüft oder ignoriert, ob WithSecure Rapid Detection & Response aktiv ist

Prüfung des Status von WithSecure Object Reputation Service Protocol *

Nicht prüfen ▼

Prüft oder ignoriert, ob WithSecure Object Reputation Service Protocol aktiv ist

Prüfung des Status von WithSecure Browsing Protection *

Nicht prüfen ▼

Prüft oder ignoriert, ob WithSecure Browsing Protection aktiv ist

Prüfung des Status von WithSecure Desktop-Firewall *

Nicht prüfen ▼

Prüft oder ignoriert, ob WithSecure Desktop-Firewall aktiv ist

3. Ergänzend zu den Komponenten können nun noch das [Alter der Virensignaturen](#) sowie das [Datum der letzten Verbindung zwischen Agent und PolicyManager](#) abgefragt und je nach Ihren Sicherheitsanforderungen verwendet werden. Um eine oder beide Prüfungen zu verwenden, lassen Sie die jeweilige [Checkbox deaktiviert](#) und wählen Sie die Anzahl an Tagen. Dabei sorgt das Erreichen der Anzahl an Tagen im Feld „*Warnen*“ dafür, dass der negative Status am Ende in den Gesamtstatus einfließt, während das Erreichen der Anzahl an Tagen im Feld „*Maximal*“ zu einem sofortigen „*Non-Compliant*“ Status des entsprechenden Endgerätes führt.

Keine Prüfung des Alters der WithSecure Virussignatures

Wenn die Checkbox aktiv ist, erfolgt keine Prüfung, wann das Endgerät das letzte Mal mit %s %s verbunden war. Wenn das Alter der letzten Verbindung geprüft wird, führt das Limit der Konfiguration für "Warnung" zu einem negativen oder positivem Status des Kriteriums, während das Limit der unteren Konfiguration für "Maximum" direkt zum Endgeräte-Status "Non-Compliant" führt.

Warnen, wenn mehr als X Tage (WithSecure Virussignatures)

Prüft das Alter der WithSecure Virensignatures, ob sie älter als der angegebene Wert. Wird ignoriert, wenn "Alter nicht überprüfen von WithSecure Virussignatures" aktiv ist.

Maximales Alter in Tagen (WithSecure Virussignatures)

Prüft das Alter der WithSecure Virensignatures, ob sie älter als der angegebene Wert. Wird ignoriert, wenn "Alter nicht überprüfen von WithSecure Virussignatures" aktiv ist.

Kein Prüfung, wann das Endgerät das letzte Mal mit WithSecure Policy Manager verbunden war.

Wenn die Checkbox aktiv ist, erfolgt keine Prüfung, wann das Endgerät das letzte Mal mit WithSecure Policy Manager verbunden war. Wenn das Alter der letzten Verbindung geprüft wird, führt das Limit der Konfiguration für "Warnung" zu einem negativen oder positivem Status des Kriteriums, während das Limit der unteren Konfiguration für "Maximum" direkt zum Endgeräte-Status "Non-Compliant" führt.

Warnen, wenn mehr als X Tage (WithSecure Policy Manager)

Prüft das Alter der letzten Verbindung zu WithSecure Policy Manager. Wird ignoriert, wenn "Alter nicht überprüfen von WithSecure Policy Manager" aktiv ist.

Maximales Alter in Tagen (WithSecure Policy Manager)

Prüft das Alter der letzten Verbindung zu WithSecure Policy Manager. Wird ignoriert, wenn "Alter nicht überprüfen von WithSecure Policy Manager" aktiv ist.

Im letzten Teil des Dialogs können nun abschließend die zuvor konfigurierten Prüfungen zur [Definition eines Gesamtzustands](#) verwendet werden. Dabei kann im ersten hier abgebildeten Feld eine [Anzahl an negativen Prüfungen](#) definiert werden, bei dessen Erreichen der Status des entsprechenden Endgerätes auf „[Almost-Non-Compliant](#)“ geändert werden. Dies hat keine automatische Reaktion zur Folge, jedoch kann der Status zum einen in der Übersicht und zum anderen im Regelwerk von **macmon NAC** verwendet werden.

4. Das Erreichen der Anzahl an Tagen entsprechend Ihrer Konfiguration im zweiten Feld führt wiederum direkt zum Status „[Non-Compliant](#)“ des Endgerätes mit den bereits in **macmon NAC** konfigurierten [Standardreaktionen für Endgeräte mit diesem Status](#).
5. Mit der Checkbox „[Status „Compliant“ setzen](#)“ haben Sie nun noch die Möglichkeit zu entscheiden, ob für alle Endgeräte, bei denen nicht die Status „[Almost-Non-Compliant](#)“ oder „[Non-Compliant](#)“ ermittelt wurden, den Status „[Compliant](#)“ zu setzen. Das erlaubt eine gute Gesamtübersicht in **macmon NAC**, da nicht nur negative Status übertragen werden. Noch viel wichtiger führt es aber auch zu einer [automatischen „Heilung“](#), da Geräte, die vorher nicht den Vorgaben entsprachen und eventuell vom Netzwerk isoliert wurden, durch positive Werte bei einem erneuten Scan auch [wieder als „Compliant“ markiert](#) und damit zurück ins Netzwerk geführt werden.
6. In dem Feld „[Intervall](#)“ geben Sie das Intervall in Minuten an, in dem **macmon NAC** neue Daten von **WithSecure Business Suite Premium** lädt.
Hinweis: Wenn diese Funktion genutzt wird, kann sich die Ausführungszeit in größeren Umgebungen deutlich verlängern, da nun der Status aller Endgeräte, die im Report enthalten sind, aktualisiert werden.
7. Zuletzt haben Sie noch die Möglichkeit den [Zeitpunkt des letzten Updates der Virensignaturen](#) auf den Endgeräten in einer [benutzerdefinierten Eigenschaft](#) eintragen zu lassen. Die Eigenschaft wird in diesem Fall automatisch erstellt und kann für weitere Aktionen im Regelwerk, wie aber auch im Reporting verwendet werden.
Hinweis: Aufgrund der Datenmenge des Reports und Komplexität der Auswertung, sollte das Intervall in großen Umgebungen nicht zu klein gewählt werden. Empfohlen wird ein Wert von 10 Minuten oder höher.
8. Aktivieren Sie die Integration durch Setzen des Hakens der Checkbox „[Aktiv](#)“ und schließen Sie die Konfiguration durch Drücken von „[Anwenden](#)“ ab.

Anzahl negativer Prüfungen insgesamt für den Status "Almost-Non-Compliant". *

Die Anzahl negativer Status der obigen Prüfungen, die insgesamt zum Status "Almost-Non-Compliant" führen.

Anzahl negativer Prüfungen insgesamt für den Status "Non-Compliant". *

Die Anzahl negativer Status der obigen Prüfungen, die insgesamt zum Status "Non-Compliant" führen.

Status "Compliant" setzen

Der Status "Compliant" wird für alle Endgeräte gesetzt, bei denen das Limit für "Almost-Non-Compliant" nicht erreicht ist und auch keine Prüfung direkt zum Status "Non-Compliant" führt.

Intervall *

Intervall in Minuten (Bereich: 1-59), in dem Daten von WithSecure Policy Manager abgefragt werden.

Speichern des Zeitpunkts der Virussignaturen pro Endgerät.

Erstellt eine benutzerdefinierte Eigenschaft "Datum der WithSecure Virensignaturen", um diese Information pro Endgerät zu speichern. Bei Deaktivieren der Checkbox wird die Eigenschaft wieder entfernt.

Aktiv

Link-Liste

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

Das Whitepaper zur WithSecure Policy Manager-Integration: [whitepaper.pdf](#)

3.1 macmon NAC reagiert auf Bedrohungen

Die Konfiguration wird ebenfalls über das **Web-GUI** durchgeführt. Tippen Sie auf „*Compliance*“ und „*Antivirus-Konnektor*“.

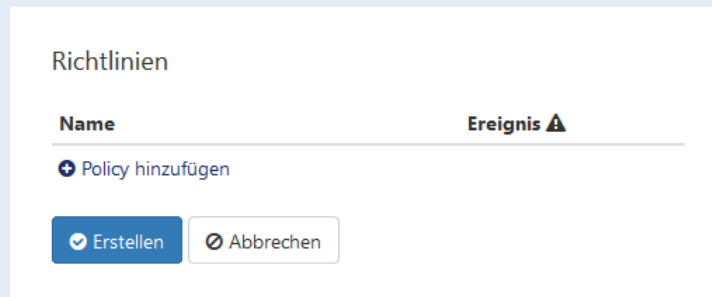
ID	Name	Plug-in	Host	Intervall	Aktiv	Status	Ergebnis	Letzte Ausführung
⚠️ <i>Kein Konnektor konfiguriert bisher</i>								

1. Klicken Sie danach auf „*Konnektor hinzufügen*“.
2. Geben Sie im Bereich „*Einstellungen*“ alle notwendigen Zugangsdaten ein, um auf die Datenbank von **WithSecure Policy Manager** zugreifen zu können.


Einstellungen

Name	Wert
Name	<input type="text"/>
Plug-in	F-Secure Policy Manager (Version 11.20 - N/A <input type="text"/>
Aktiv	<input type="checkbox"/>
Intervall	<input type="text"/>
Typ	mssql <input type="text"/>
Hostname	localhost
Benutzername	user
Passwort	<input type="text"/>
Instanz	<input type="text"/>
Datenbank	<input type="text"/>
Port	0
Version ignorieren	<input type="checkbox"/>

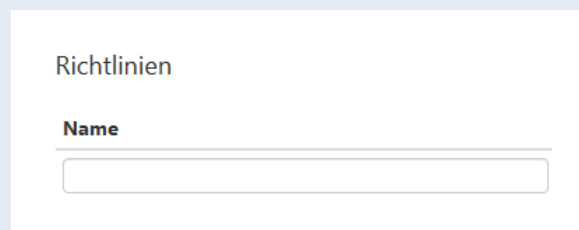
3. Klicken Sie danach im Bereich „*Richtlinien*“ auf „*Policy hinzufügen*“.



Richtlinien

Name	Ereignis 
+ Policy hinzufügen	

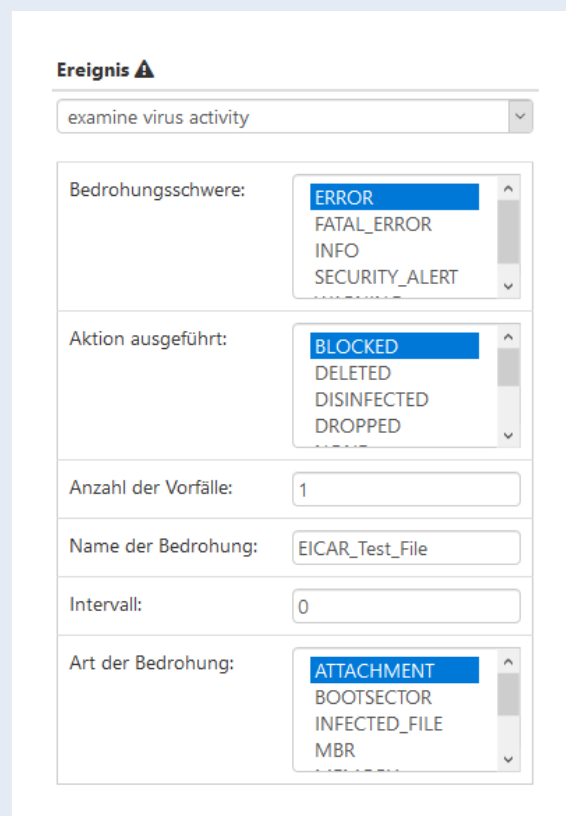
4. Vergeben Sie einen Namen für die Policy.




Richtlinien

Name

5. Konfigurieren Sie das Ereignis wie in Ihrem Unternehmensnetzwerk benötigt. Beachten Sie hierbei bitte auch das [Kapitel 7.4.3 „Plug-ins“](#) im **macmon-Handbuch**.



Ereignis 

examine virus activity

Bedrohungsschwere:

Aktion ausgeführt:

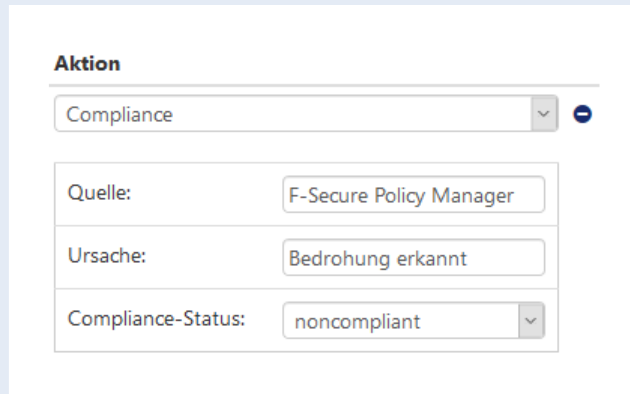
Anzahl der Vorfälle:

Name der Bedrohung:

Intervall:

Art der Bedrohung:

- Wählen Sie eine gewünschte Aktion, beispielsweise „*Compliance*“. Sie können beliebige Namen für die Felder „*Quelle*“ und „*Ursache*“ wählen.



The screenshot shows a configuration form titled "Aktion". It contains the following fields:

- A dropdown menu labeled "Aktion" with the value "Compliance" selected.
- A text input field labeled "Quelle:" with the value "F-Secure Policy Manager".
- A text input field labeled "Ursache:" with the value "Bedrohung erkannt".
- A dropdown menu labeled "Compliance-Status:" with the value "noncompliant" selected.

- Schließen Sie die Konfiguration mit einem Klick auf „*Erstellen*“ ab.

Kontakt bei WithSecure

WithSecure Niederlassung D/A/CH
WithSecure GmbH,
Kistlerhofstr. 172c
81379 München

E-Mail: vertrieb-de@withsecure.com

Website: www.withsecure.de

Telefon: +49 89 787 467 0

Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin
Tel.: +49 (0) 30 23 25 777 - 0 | nac@macmon.eu