



MACMON NAC WHITE PAPER

Integration between macmon NAC
and WithSecure Business Suite Premium



Inhalt

1 About with Secure:	2
2 Sample use cases.....	3
2.1 macmon NAC checks the status of various security components of the WithSecure Endpoint security agents	3
2.2 macmon NAC reacts to threats.....	3
3 Configuration of WithSecure Business Suite Premium.....	4
3.1 Creating an API URL.....	5
4 Configuration of macmon NAC.....	8
4.1 macmon NAC reacts to threats.....	12
Contacting WithSecure.....	15
Contact.....	15

Version: 2.0

1 About with Secure:

WithSecure™ is your dependable partner for cyber security. IT service providers, MSSPs and countless companies as well as major financial institutions, manufacturers and thousands of the most advanced communication and technology providers worldwide trust us whenever it comes to results-based cyber security to protect and facilitate their business.

Our AI-controlled protection secures end points and cloud collaboration, our intelligent detection and reaction functions are supported by experts who identify risks to business by proactively searching for threats and repelling active attacks. Our consultants work with companies and technology providers to boost their resilience through evidence-based security consulting. With more than 30 years of experience in developing technologies to meet company objectives, we have built our portfolio with flexible business models to ensure we can grow alongside our partners.

2 Sample use cases

2.1 macmon NAC checks the status of various security components of the WithSecure Endpoint security agents

In recent years, there has been an increase in reports of viruses and ransomware attacks that can put the productivity of an entire company in jeopardy within seconds. These threats often infiltrate the company network from the web or through e-mails and can be triggered with just one ill-considered click. **WithSecure** and **macmon secure** work in a close and efficient partnership to ensure any infected endpoint device does not become the starting point for an infection that would spread to the whole company network.

The sophisticated **WithSecure Business Suite Premium** engine provides a range of components for effective local security at endpoint devices. Thanks to the communication between the **agents** and the **WithSecure Policy Manager**, all statuses are made available centrally. **macmon NAC** retrieves this information through the **Policy Manager REST API**, letting you ensure that endpoint devices that do not meet security requirements are automatically handled according to company policy, for instance, isolated from the network immediately or moved to a quarantine network.

macmon NAC also continuously monitors whether the virus signatures of all your corporate devices are up to date and summarizes this information in a format that is easy to read: Your company's requirements are met if the virus signatures on the endpoint device being checked are up to date. However, if an endpoint's virus signatures are older than your company policies allow, **macmon NAC** moves it to a separate network segment for updating if desired, and the administrator is notified accordingly. Either way, the solution lets administrators quickly identify whether virus signatures are up to date in company networks of any size.

2.2 macmon NAC reacts to threats

If the **WithSecure client** finds malware on an endpoint device, there may be only a few seconds to neutralize the threat. The information about the discovery of the malware is sent to the **WithSecure Policy Manager** connected to **macmon NAC** immediately.

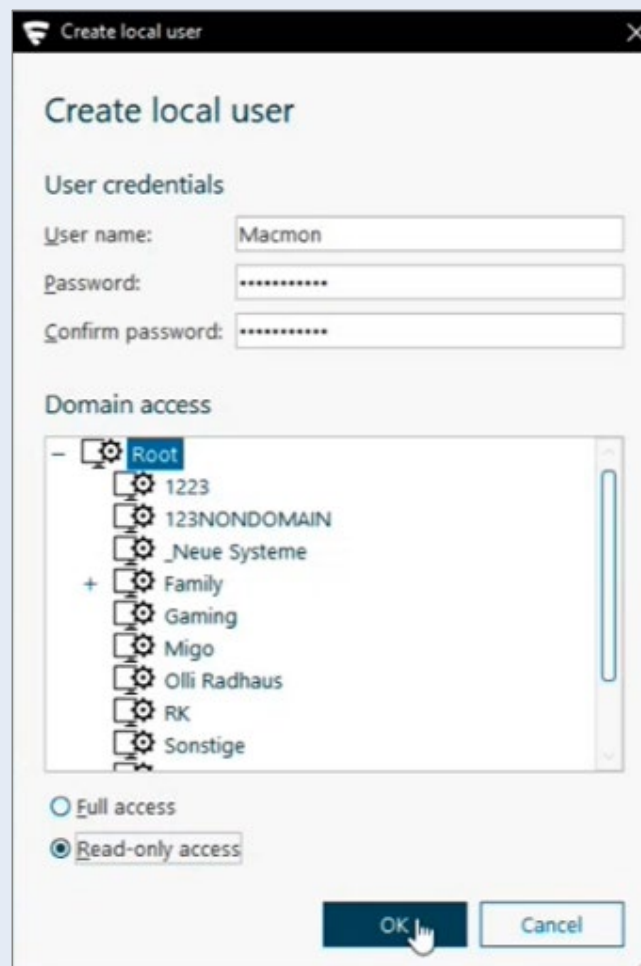
The notification not only indicates that a threat was found, but also whether the **WithSecure client** was able to resolve it. Two scenarios that may be assessed differently by **macmon NAC**: On the one hand, a threat or an unusual cluster of threats that were found and could be resolved in a short period of time. On the other, ransomware (in the form of a encrypting trojan, for example) that initially cannot be removed by the **WithSecure client**, because it needs to be cleaned using a special tool that is available separately, or because write protection is enabled. In both cases, the **WithSecure policy manager** immediately notifies **macmon NAC** of what the NAC solution is evaluating. The affected endpoint is moved to a special network segment for treatment and the responsible administrator is notified.

3 Configuration of WithSecure Business Suite Premium

We generally recommend using [dedicated users](#) for direct connections between systems. This would help prevent any misuse on the one hand and [ensure a clear assignment of information to users in any logs](#) on the other. With that in mind, the first thing to do is create a separate user for connecting to **macmon NAC** in the **WithSecure Policy Manager**.

To do so, proceed as follows:

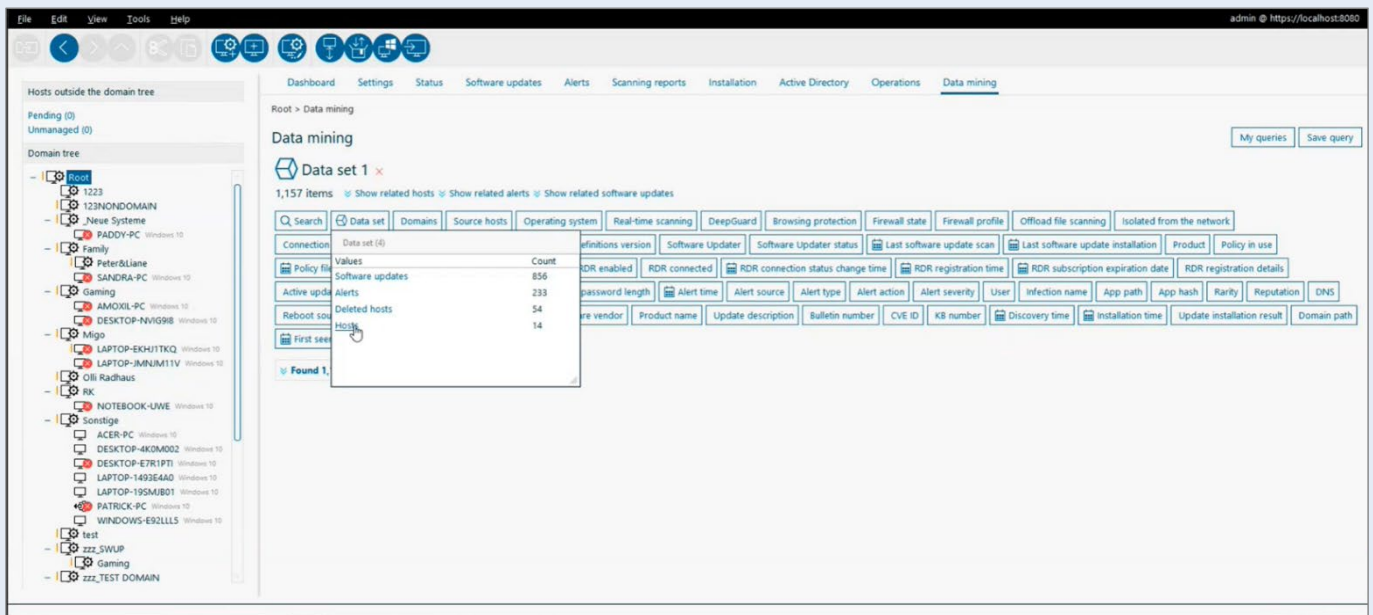
1. Open the Policy Manager user administration by choosing [Tools – Users...](#)
2. Choose [Create local user](#).
3. Enter a [user name](#) and [password](#).
4. Under "[Domain access](#)", select the highest level (unless changed: [Root](#)).
5. Limit access by selecting "[Read-only access](#)".
6. Choose **OK** to create the user.



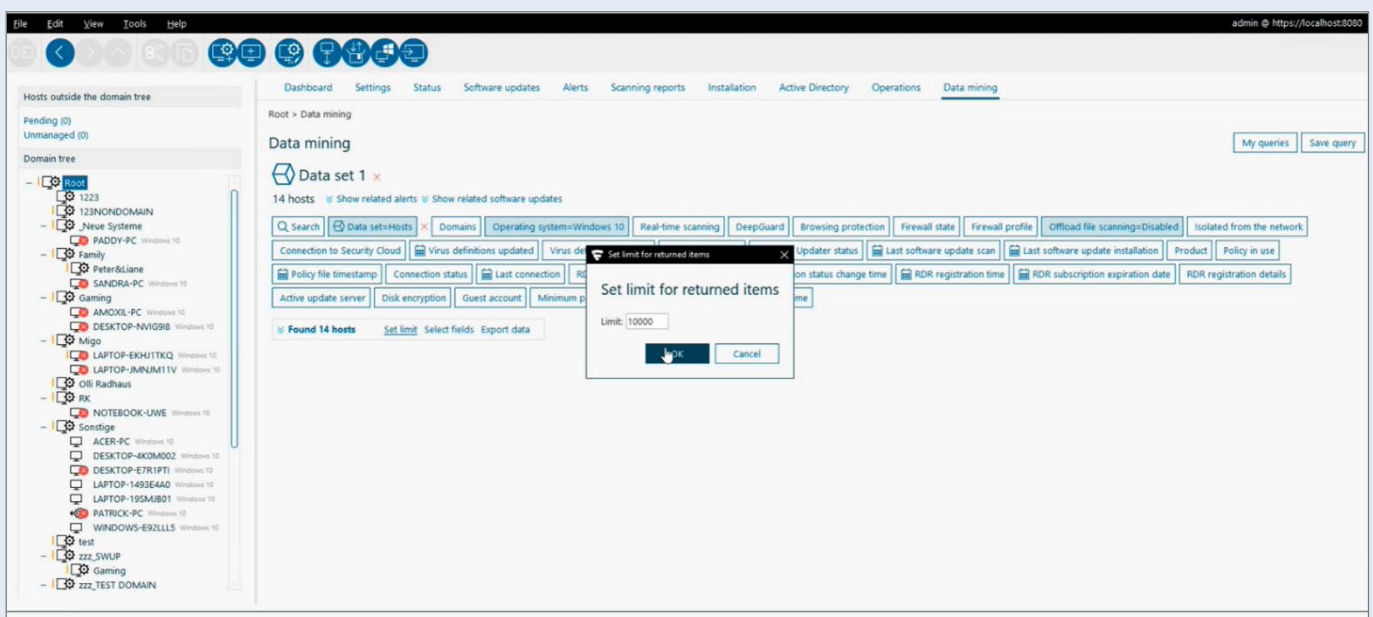
3.1 Creating an API URL

The **WithSecure Policy Manager REST API** provides an elegant way to create custom URLs that explicitly deliver your required content with no need for complex filters in the query. The URLs can be created through the GUI; the process is described in more detail below:

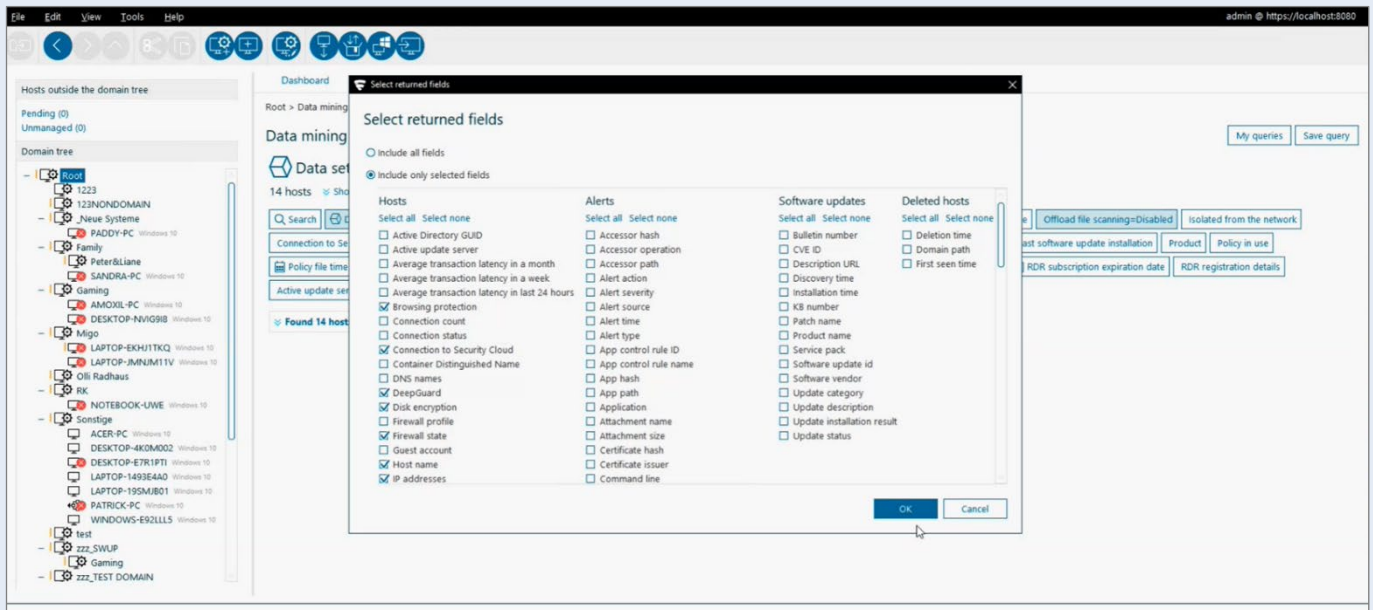
1. Navigate through the tabs at the top of the window and go to „*Data mining*“, here, select „*Data set*“ and then „*Hosts*“ as shown in the screenshot.



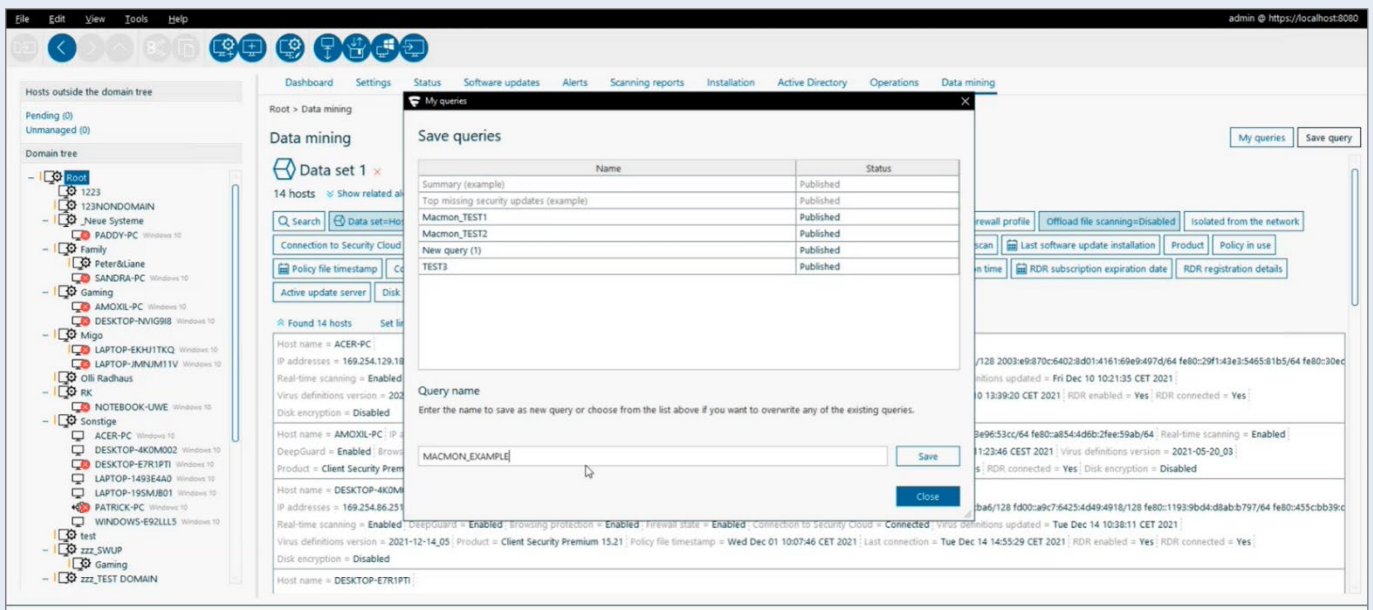
2. Click „*Set limit*“ and define a value of a sufficient size to see the details of all your endpoint devices at once – ideally with a buffer for more.



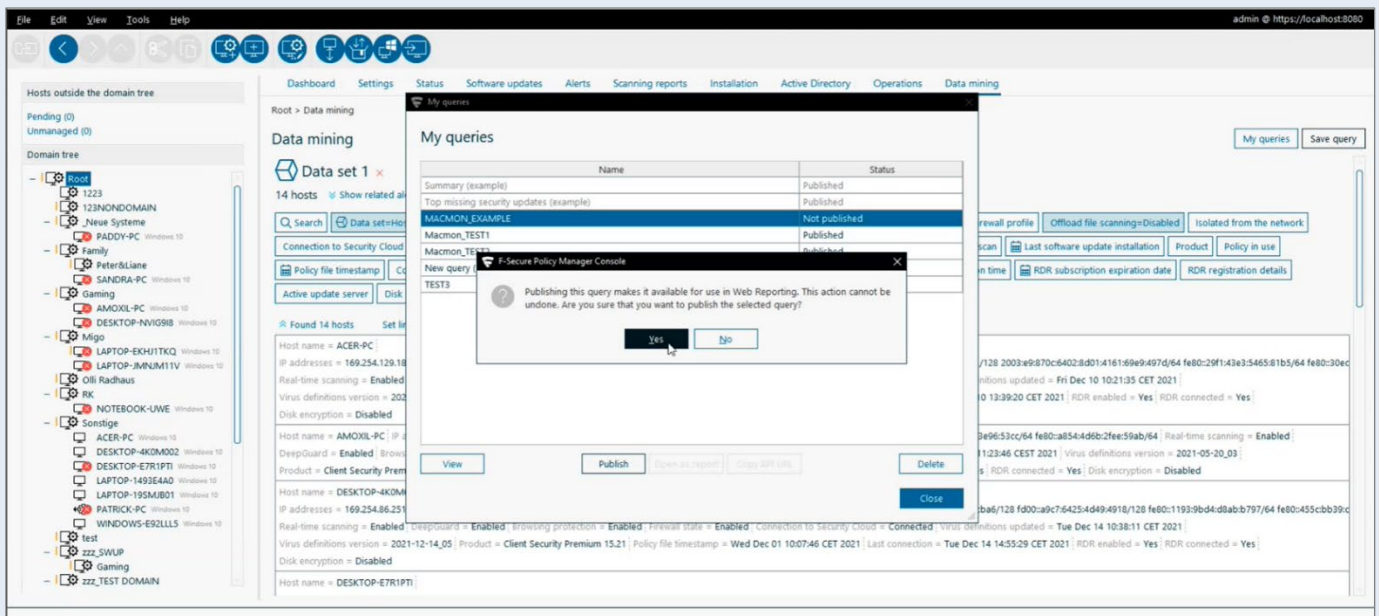
- Next, click „*Select fields*“ and select the components to be queried in the dialog box shown in the screenshot here. We recommend selecting all the values below so you can decide how to process the data in the **macmon NAC** GUI later. With that in mind, select the checkmarks for „*Browsing protection, 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*“.



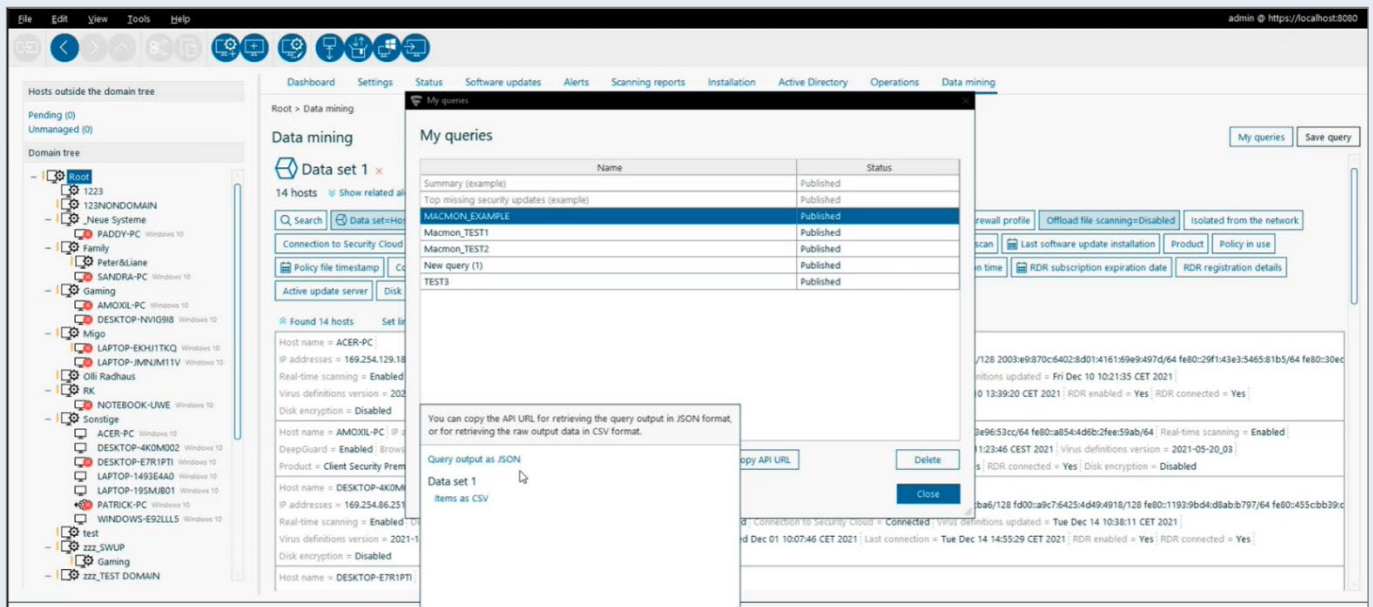
- Next, click „*Save query*“ in the top right corner of the GUI and enter a name of your choice for the data selection.



- Highlight the selection you just created and click „*Publish*“ and then „*Yes*“, to confirm that the selection is allowed to be used in web reporting.

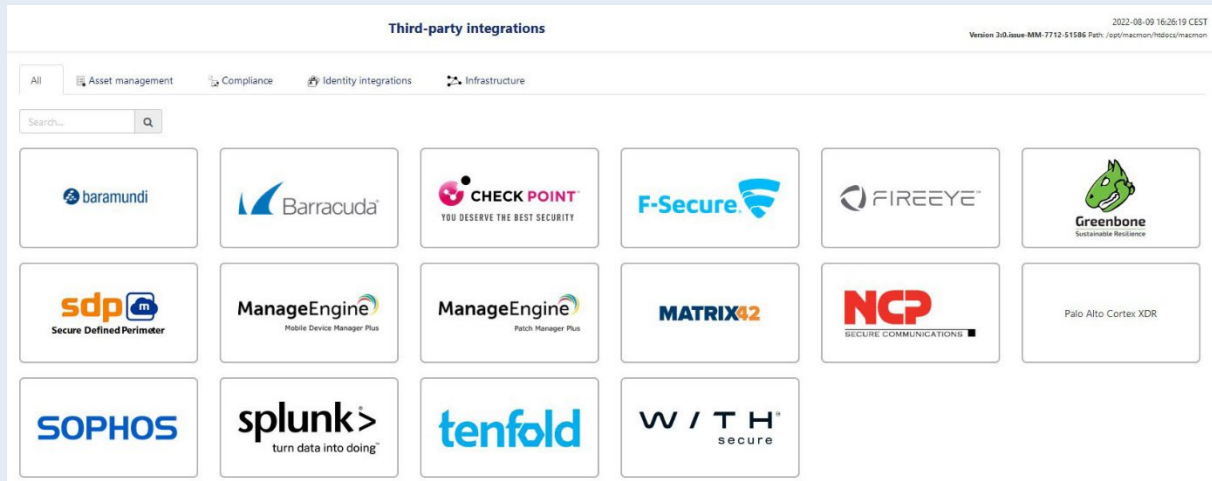


- In the last step, click „*Copy API URL*“ and then choose „*Query output as JSON*“ as shown in the screenshot here.



4 Configuration of macmon NAC

The configuration is carried out through the [Web-GUI](#). Tap „*Settings*“ und „*Third-party integrations*“, then tap „*Compliance*“.



If the **frame of the WithSecure** tile is gray, the integration **has not been enabled yet**. Please tap the tile to open the configuration dialog box.

The dialog is divided into multiple sections here to allow greater clarity.

1. First, enter the API URL created in the [WithSecure Policy Manager](#) in the relevant field and add a „*User name*“ and „*Password*“ for accessing the API.

If your [WithSecure Policy Manager installation](#) is not provided with a verifiable certificate, you can disable the check in the dialog box here by removing the checkmark (not recommended).

Edit configuration for WithSecure Policy Manager

▼ Description

The integration between macmon NAC and WithSecure here explicitly refers to a connection to WithSecure Policy Manager. Please follow the descriptions of the whitepaper provided here to create the report in the GUI of WithSecure Policy Manager and copy the corresponding API URL. By storing the URL and the read-authorized credentials here in the configuration dialog, you establish the basis for retrieving and processing the security information about your endpoints. In the following, you can define for each security function/property whether the status should be checked at all, whether it should be included in an overall assessment, or whether it is a "must" criterion, the non-fulfilment of which will result in the affected endpoint being treated as "non-compliant" in macmon. At the end of the configuration dialog, you can also define that a certain number of negative statuses will cause an endpoint to become "Almost-Non-Compliant" or "Non-Compliant". If none of the limits is reached, the endpoint is set to "compliant".

Identifier: [WITHSECURE_POLICY_MANAGER]

Configuration

URL *

The report URL generated by the WithSecure Policy Manager

User name *

User name for WithSecure Policy Manager

Password *

Password for WithSecure Policy Manager

☒ SSL certificate verification

This defines if the SSL certificate of WithSecure Policy Manager needs to be verified.

- The selection fields in the dropdown that now appears each refer to individual components of the **WithSecure Endpoint Security agents**. Here you can choose whether you want the status of the relevant components to be checked at all, whether it should be checked in order to use the result in an overall status at the end or whether a negative check result for a specific component should even result in the status **"Non-Compliant"** in **macmon NAC**.

Status check for the WithSecure Real-Time Scanner *

no check

Checks or ignores the WithSecure Real-Time Scanner being active.

Status check for the WithSecure Deep-Guard *

no check

Checks or ignores the WithSecure Deep-Guard being active.

Status check for the WithSecure Harddisc Encryption *

no check

Checks or ignores the WithSecure Harddisc Encryption being active.

Status check for the WithSecure Rapid Detection & Response *

no check

Checks or ignores the WithSecure Rapid Detection & Response being active.

Status check for the WithSecure Object Reputation Service Protocol *

no check

Checks or ignores the WithSecure Object Reputation Service Protocol being active.

Status check for the WithSecure Browsing Protection *

no check

Checks or ignores the WithSecure Browsing Protection being active.

Status check for the WithSecure Desktop-Firewall *

no check

Checks or ignores the WithSecure Desktop-Firewall being active.

3. In addition to the components, you can also now query the [age of virus signatures](#) and the [date of the last connection between the agent and Policy Manager](#), and then apply this information according to your security requirements. To use one or both checks, [leave the applicable checkbox deactivated](#) and choose the number of days.

In this case, reaching the number of days in the *"Warning"* field means that the negative status is included in the overall status at the end, while reaching the number of days in the *"Maximum"* field results in an immediate *"Non-Compliant"* status for the relevant endpoint.

☐ No check of the age of WithSecure virus signatures

There will be no check of the virus signatures age if the checkbox is active. If the age of the virus signatures is checked, the limit of the below configuration for "warning" results in a negative or positive status of this criteria while the limit of the below configuration for "maximum" results directly in a "non-compliant" status of the related endpoint.

Warn if more than X days (WithSecure virus signatures)

5

Checks the age of WithSecure virus signatures if it is older than the given value. Will be ignored if "No check of the age of WithSecure virus signatures" is active.

Maximum age in days (WithSecure virus signatures)

10

Checks the age of WithSecure virus signatures if it is older than the given value. Will be ignored if "No check of the age of WithSecure virus signatures" is active.

☐ No check of the last time the endpoint was connected to WithSecure Policy Manager

If the checkbox is active there is no check of the last time the endpoint was connected to WithSecure Policy Manager. If the age of the last connection is checked, the limit of the below configuration for "warning" results in a negative or positive status of this criteria while the limit of the below configuration for "maximum" results directly in a "non-compliant" status of the related endpoint.

Warn if more than X days (WithSecure Policy Manager)

5

Checks the age of the last connection to WithSecure Policy Manager. Will be ignored if "No check of the last time the endpoint was connected to WithSecure Policy Manager" is active.

Maximum age in days (WithSecure Policy Manager)

10

Checks the age of the last connection to WithSecure Policy Manager. Will be ignored if "No check of the last time the endpoint was connected to WithSecure Policy Manager" is active.

In the last section of the dialog box, you can now use the checks configured earlier for the [definition of the overall status](#). In the first field shown here, you can define a [number of negative checks](#) that, when reached, changes the status of the relevant endpoint to ["Almost Non-Compliant"](#). This does not result in an automatic reaction; however, the status can then be used in the overview and/or in the [macmon NAC policies](#).

4. In turn, reaching the number of days based on your configuration in the second field immediately results in the ["Non-Compliant"](#) status for the endpoint, together with the standard reactions for endpoints with this status that have already been configured in [macmon NAC](#).
5. The ["Set status 'Compliant'"](#) checkbox now lets you choose whether to set the status ["Compliant"](#) for all endpoints for which the status ["Almost Non-Compliant"](#) or ["Non-Compliant"](#) was not found. That provides for a good overall summary in [macmon NAC](#), because not only negative statuses are transferred. Even more importantly, however, it also results in an [automatic "cure"](#), because devices that did not meet the requirements previously and that may have been isolated from the network are also [marked as "Compliant" again](#), and therefore returned to the network, if a repeated scan results in positive values.
6. In the ["Interval" field](#), enter the interval in minutes in which [macmon NAC](#) is to load new data from [WithSecure Business Suite Premium](#).
Note: If this feature is used, the execution time in larger environments can increase significantly, as the status of all end devices included in the report are now updated.
7. Finally, you have the option of entering [the time that the virus signatures were last updated](#) on the endpoints in a [user-defined property](#). The property is created automatically in this case and can be used for further actions in both the policies and the reporting.
Note: Due to the amount of data in the report and the complexity of the evaluation, the interval should not be too small in large environments. A value of 10 minutes or higher is recommended.
8. Set the mark for the ["Active"](#) checkbox to activate the integration and press ["Apply"](#) to close the configuration.

Number of negative checks for overall status "Almost-Non-Compliant". *

Number of negative statuses of the checks above, which will result to the overall status "Almost-Non-Compliant"

Number of negative checks for overall status "Non-Compliant". *

Number of negative statuses of the checks above, which will result to the overall status "Non-Compliant"

☐ Set status "Compliant"

The "Compliant" status is set for all endpoints for which the limit for "Almost-Non-Compliant" is not reached and no check leads directly to the "Non-Compliant" status.

Interval *

Interval in minutes (range: 1-59) at which data is being retrieved from WithSecure Policy Manager.

☐ Save the virus signatures timestamp per endpoint.

Creates a user-defined property "Date of the WithSecure virus signatures" to store the information per endpoint. The property is removed when deactivating the checkbox.

☐ Active

Link list

Please fill in all required blanks above to activate the download links below

The whitepaper to the WithSecure Policy Manager integration: [whitepaper.pdf](#)

4.1 macmon NAC reacts to threats

This configuration is also carried out using the web GUI. Tap *"Compliance"* and *"Antivirus connector"*.

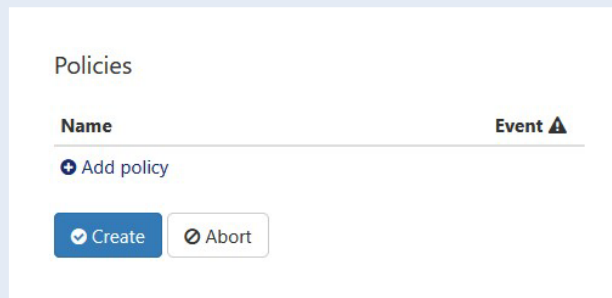
ID	Name	Plug-in	Host	Interval	Active	Status	Result	Last execution
⚠ No connector configured yet								

1. Then, click *"Add connector"*.
2. In the *"Settings"* area, add all the credentials required to access the **WithSecure** Policy Manager database.

Settings

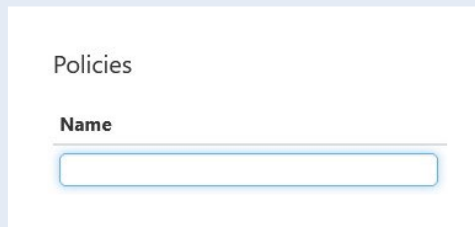
Name	Value
Name	<input type="text"/>
Plug-in	F-Secure Policy Manager (Version 11.20 - N/A) ▼
Active	<input type="checkbox"/>
Interval	<input type="text"/>
Type	mssql ▼
Host name	localhost
User name	user
Password	<input type="password"/>
Instance	<input type="text"/>
Database	<input type="text"/>
Port	0
Ignore version	<input type="checkbox"/>

- Then, click *"Add policy"* in the *"Policies"* area.



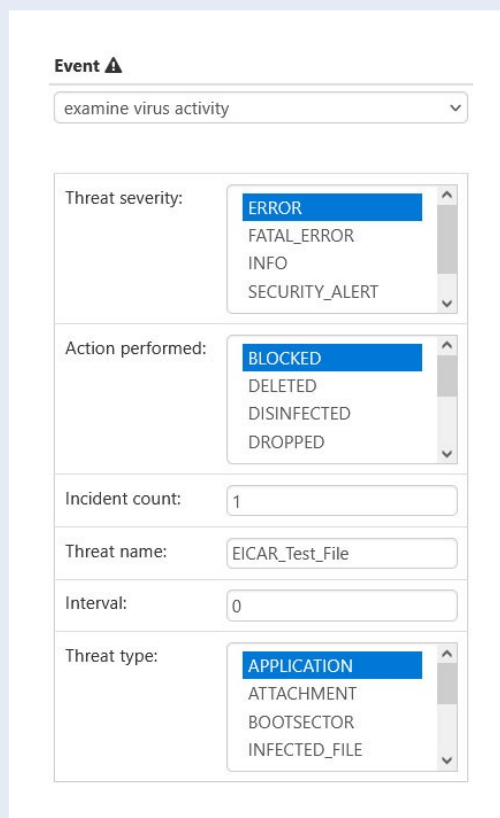
The screenshot shows a 'Policies' management interface. At the top, there's a header 'Policies'. Below it, there are two columns: 'Name' and 'Event' with a warning icon. A '+ Add policy' button is located below the 'Name' column. At the bottom, there are two buttons: 'Create' (with a checkmark icon) and 'Abort' (with a cancel icon).

- Enter a [name for the policy](#).



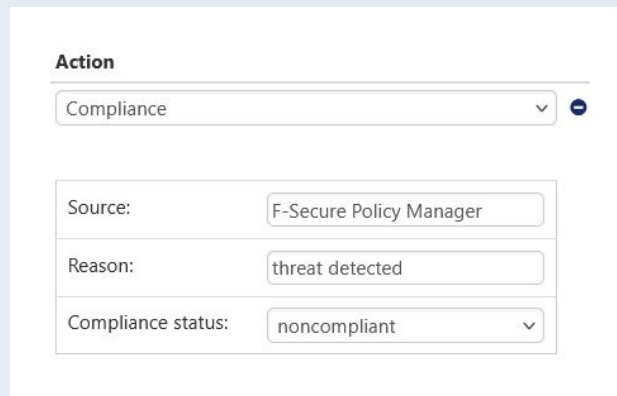
The screenshot shows a 'Policies' management interface. Below the 'Name' header, there is a text input field for entering the policy name.

- Configure the result as required in your company network. For more information, please see [chapter 7.4.3 "Plug-ins"](#) in the [macmon manual](#).



The screenshot shows an 'Event' configuration interface. At the top, there's a header 'Event' with a warning icon. Below it, there's a dropdown menu for 'examine virus activity'. The main configuration area is divided into several sections: 'Threat severity' with a dropdown menu showing 'ERROR', 'FATAL_ERROR', 'INFO', and 'SECURITY_ALERT'; 'Action performed' with a dropdown menu showing 'BLOCKED', 'DELETED', 'DISINFECTED', and 'DROPPED'; 'Incident count' with a text input field containing '1'; 'Threat name' with a text input field containing 'EICAR_Test_File'; 'Interval' with a text input field containing '0'; and 'Threat type' with a dropdown menu showing 'APPLICATION', 'ATTACHMENT', 'BOOTSECTOR', and 'INFECTED_FILE'.

6. Select a desired action (for example, "*Compliance*"). You can enter a name of your choice for the "*Source*" and "*Cause*" fields.



The screenshot shows a web form titled "Action". It contains three input fields: "Source" with the value "F-Secure Policy Manager", "Reason" with the value "threat detected", and "Compliance status" with a dropdown menu showing "noncompliant".

7. Click "*Create*" to complete the configuration.

Contacting WithSecure

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

E-Mail: vertrieb-de@withsecure.com
Website: www.withsecure.com/en/home
Phone: +49 89 787 467 0

Contact

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