F-Secure

macmon
nac smartly simple

MACMON NAC WHITE PAPER

Integration with macmon NAC and F-Secure Business Suite Premium

Contents

Version: 1.2_en

Introduction

Nobody has better visibility into real-life cyber attacks than F-Secure. We're closing the gap between detection and response, utilizing the unmatched threat intelligence of hundreds of our industry's best technical consultants, millions of devices running our award-winning software, and ceaseless innovations in artificial intelligence. Top banks, airlines, and enterprises trust our commitment to beating the world's most potent threats. Together with our network of the top channel partners and over 200 service providers, we're on a mission to make sure everyone has the enterprise-grade cyber security we all need. Founded in 1988, F-Secure is listed on the NASDAQ OMX Helsinki Ltd.

Use Cases

In the last few years there are a lot of reports regarding viruses and ransomware, that potentially jeopardize the productivity of any company within seconds. Often, these threats make their way into companies via the web or emails where they are triggered accidentally. To prevent an infected endpoint from becoming the root of an infection of the entire corporate network, F-Secure Business Suite Premium and macmon NAC team up in a close and high-performing integration.

macmon NAC verifies the validity of signatures of F-Secure Business Suite Premium

The sophisticated engine of F-Secure Business Suite Premium is most effective, when it relies on up-to-date virus definitions. Those are made available by the central F-Secure Policy Manager of Business Suite Premium to connected F-Secure clients that are installed on corporate devices. macmon NAC monitors permanently if the virus definitions are up-to-date and provides a great overview of this information. When the virus definitions on an endpoint are up-to-date, it complies with the corporate policies. When they are older than the corporate policies suggest, macmon NAC moves this endpoint to another network segment and notifies the administrator if configured that way. In any case administrators get a quick overview of the current virus definitions' status on any corporate network.

macmon NAC reacts to threats

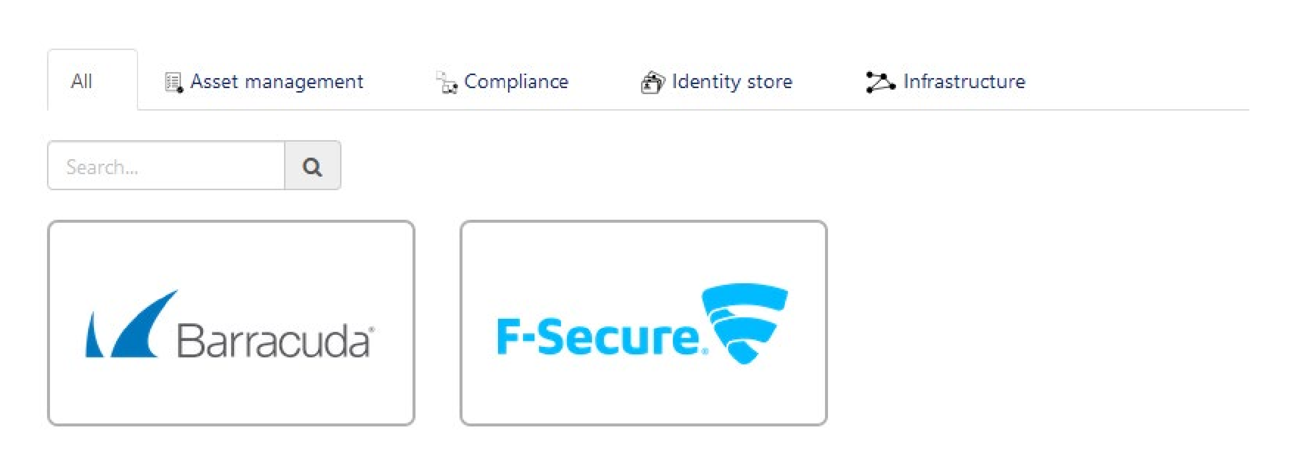
If the F-Secure Client detects a malicious software on an endpoint, the threat must be neutralized within seconds. The information on the finding is instantly passed on to the F-Secure Policy Manager that is connected to macmon NAC.

This information includes not only that a threat has been found but whether it was resolved by the F-Secure Client. These two cases can be handled differently by macmon NAC: On the one hand there might be a threat or an unusually high number of threats that are detected and resolved in a short period of time. On the other hand there might be ransomware, for example a crypto trojan, that cannot be removed by the F-Secure Client right away because either it must be removed with a special tool or a write lock is in place. F-Secure Policy Manager notifies macmon NAC in both cases which is processed instantly by the latter. Then, the infected endpoint is moved to a special network segment for the remediation process and the administrator in charge is notified.

Configuration of macmon NAC

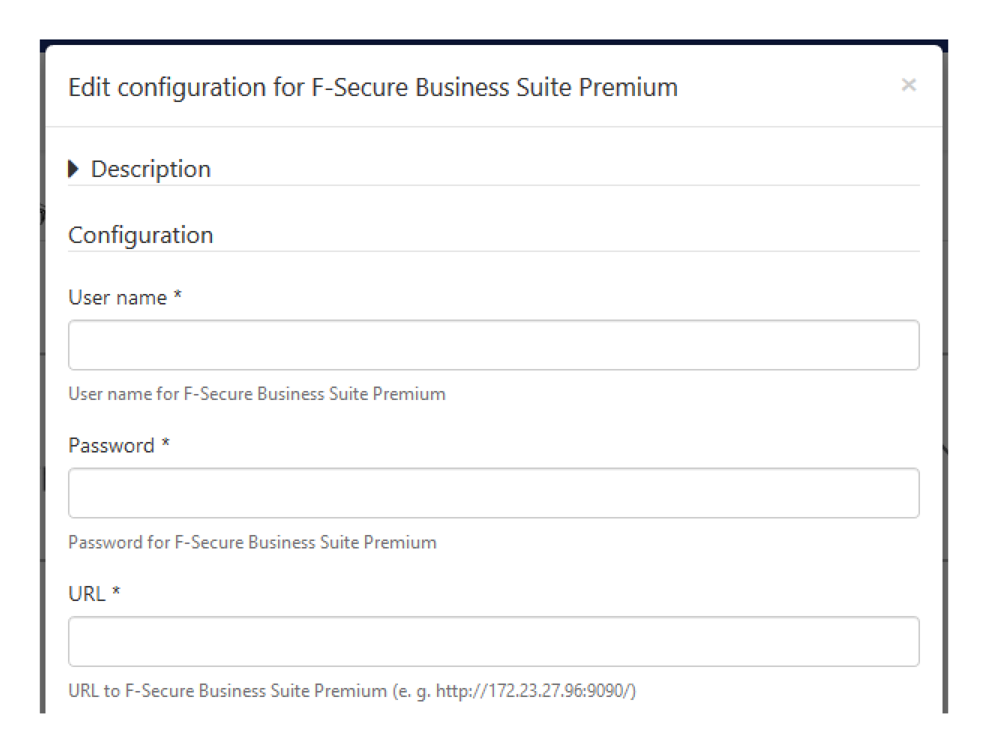
Configuration of the F-Secure Business Suite Premium integration

The configuration is done via the web GUI. Please tap on *Settings* and *Third party integrations*, then on *Compliance*.



If the border of the F-Secure tile appears gray the integration is not yet activated. Please tap on the tile for the configuration dialog to be shown.

1. Enter the *User name*, the *password* and the *URL*, that is needed to access *F-Secure Business Suite Premium*.



Edit configuration for F-Secure Business Suite Premium

Configuration

User name *

User name for F-Secure Business Suite Premium

Password *

Password for F-Secure Business Suite Premium

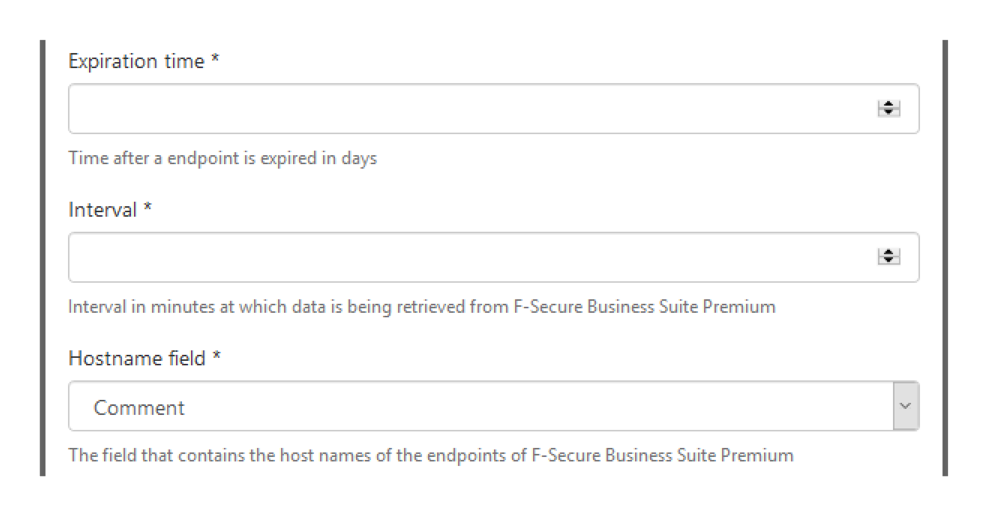
URL *

URL to F-Secure Business Suite Premium (e. g. http://172.23.27.96:9090/)

2. In the next section, enter the *expiration time* in days. An endpoint is considered expired, when it hasn't updated its virus definitions within this time.

3. In *Interval* you enter the interval in minutes at which data is being retrieved from *F-Secure Business Suite Premium*.
4. The *hostname field* specifies the field in macmon NAC that should hold the hostname in the endpoint entry. This hostname must match the name and format of the hostname used in the *F-Secure Business Suite Premium* web report. The field selected here must already contain the hostname.

   Example: In the web report, the hostname of any endpoint is *cspr-1*, and the same name must be entered in the selected field *Comment* of the corresponding endpoint entry, so that the endpoint can be mapped correctly.



Expiration time *

Time after a endpoint is expired in days

Interval *

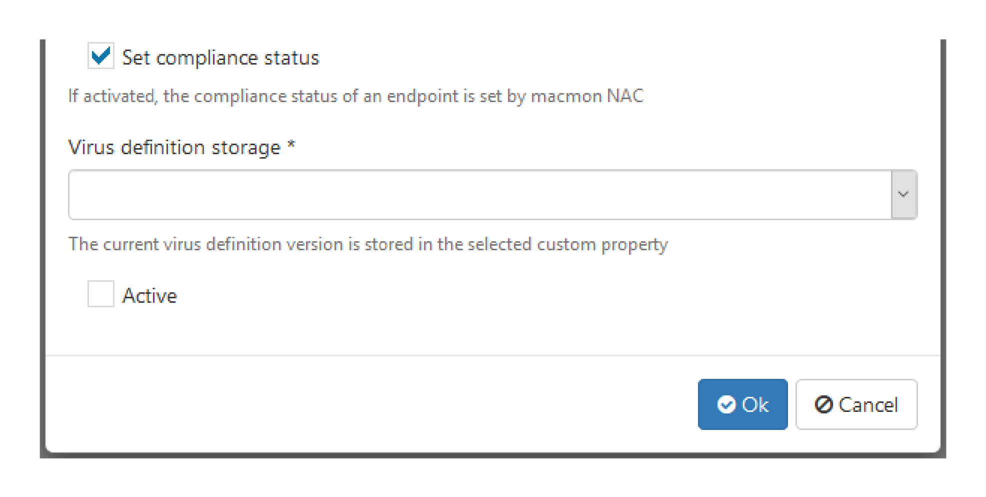
Interval in minutes at which data is being retrieved from F-Secure Business Suite Premium

Hostname field *

Comment

The field that contains the host names of the endpoints of F-Secure Business Suite Premium

5. Tick the box of Set compliance status to make macmon NAC set an endpoint to non-compliant if its virus definitions are expired and trigger the pre-configured reaction in this case. If an endpoint's virus definitions are up-to-date, macmon NAC will set it to compliant.
6. In *Virus definition version field*, you select the field in *macmon NAC* that keeps record of latest virus definition version of an endpoint. You can select any user-defined property you have set up in *Settings > User-defined property* before.
7. Activate the integration by ticking the box *Active* and confirm by tapping *Ok*.



☑ Set compliance status

If activated, the compliance status of an endpoint is set by macmon NAC

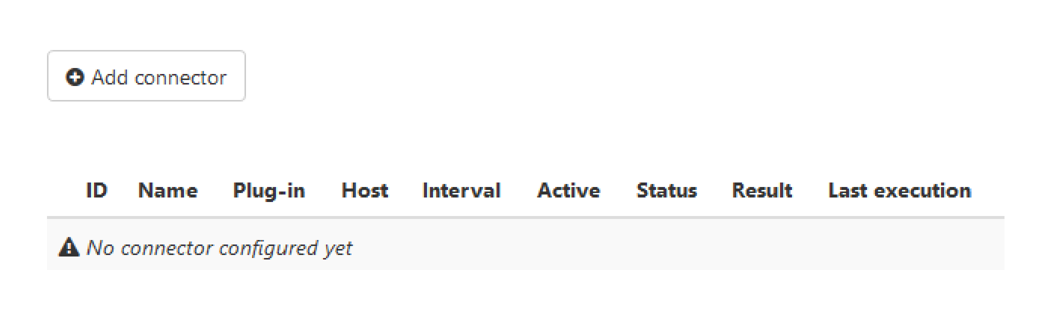
Virus definition storage *

The current virus definition version is stored in the selected custom property

☐ Active

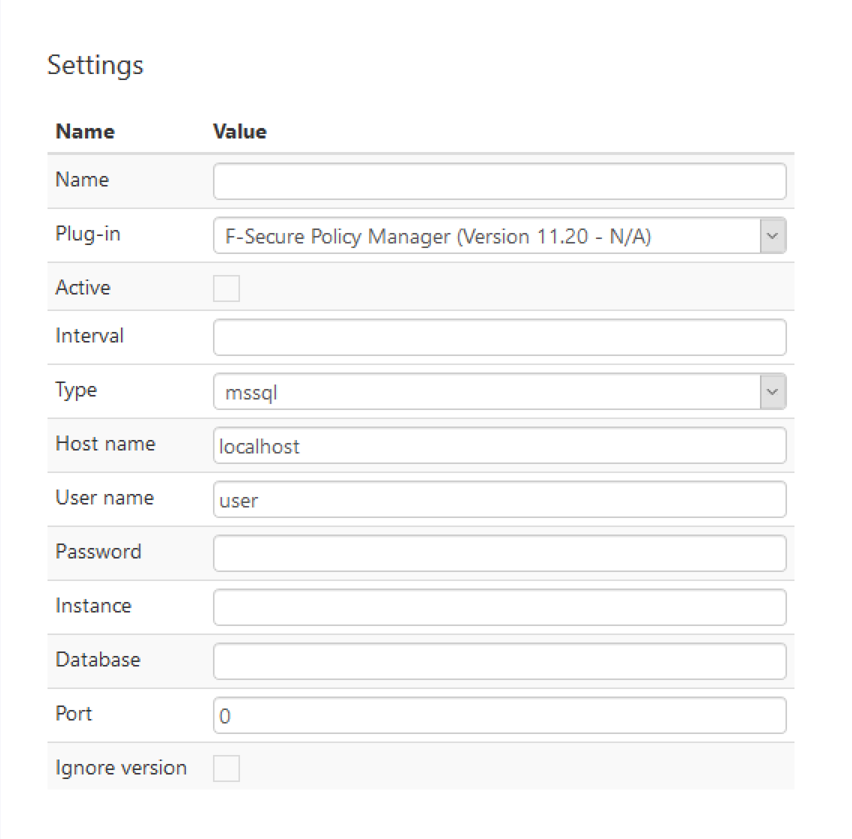
macmon NAC reacts to threats

The configuration is also done via web GUI. Tap on *Compliance* and *Antivirus connector*.



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

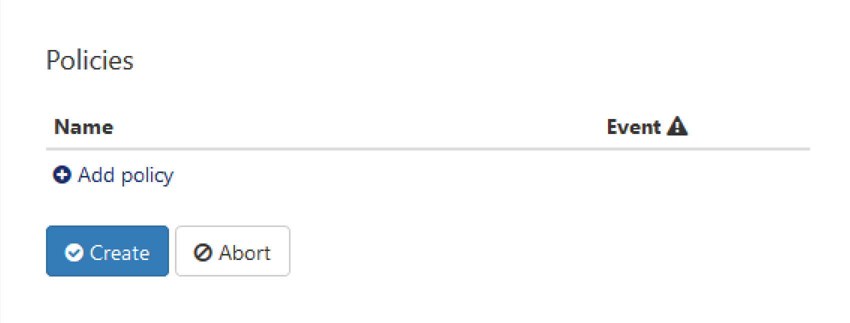
1. Then tap on *Add connector*.
2. In the *Settings* section, enter all necessary access credentials to access the database of *F-Secure Policy Manager*.



Settings

Name	Value
Name	
Plug-in	F-Secure Policy Manager (Version 11.20 - N/A)
Active	□
Interval	
Type	mssql
Host name	localhost
User name	user
Password	
Instance	
Database	
Port	0
Ignore version	□

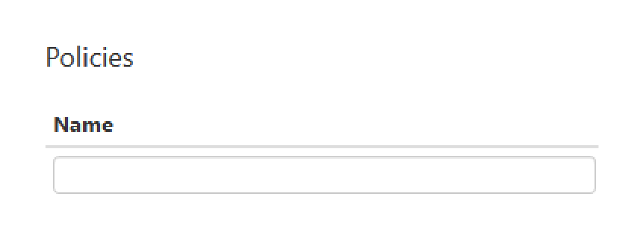
3. In the *Policies* section, tap on *Add policy*.



Policies

Name	Event ⚠
⊕ Add policy	

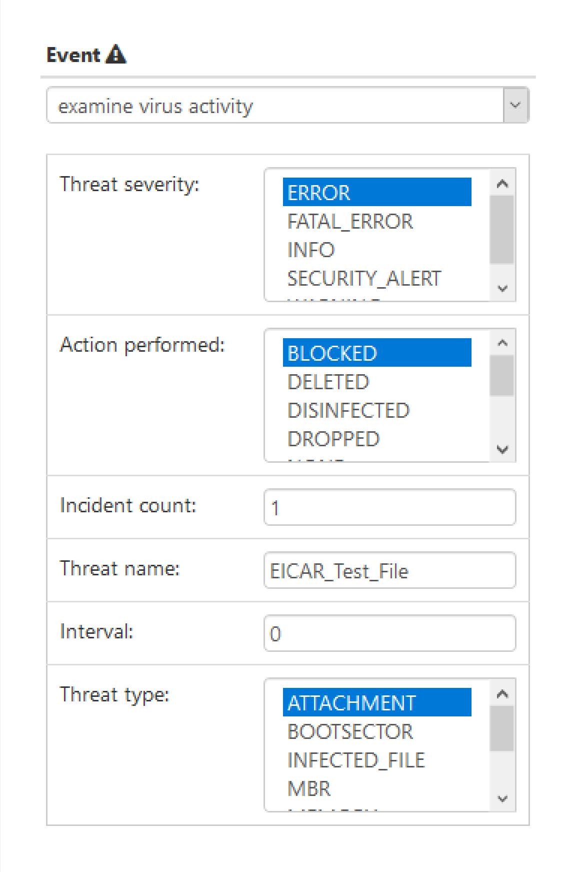
4. Choose a name for the policy.



Policies

Name

5. Configure the event as required in your corporate network. Please consult chapter *7.4.3 Plug-ins* of the macmon manual.

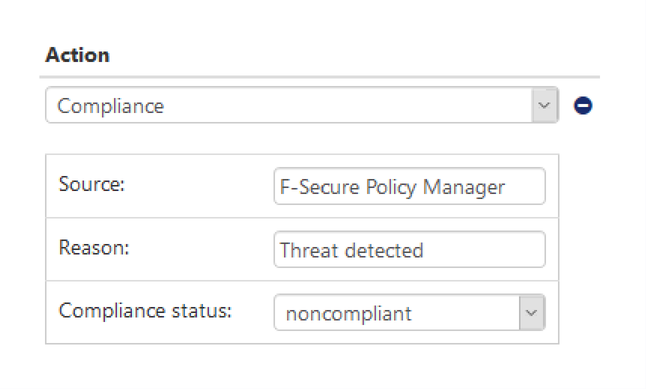


Event ⚠

examine virus activity

Threat severity:	ERROR FATAL_ERROR INFO SECURITY_ALERT
Action performed:	BLOCKED DELETED DISINFECTED DROPPED
Incident count:	1
Threat name:	EICAR_Test_File
Interval:	0
Threat type:	ATTACHMENT BOOTSECTOR INFECTED_FILE MBR

6. Select your desired action, e. g. compliance. Choose arbitrary names for the fields *Source* and *Reason*.



Action

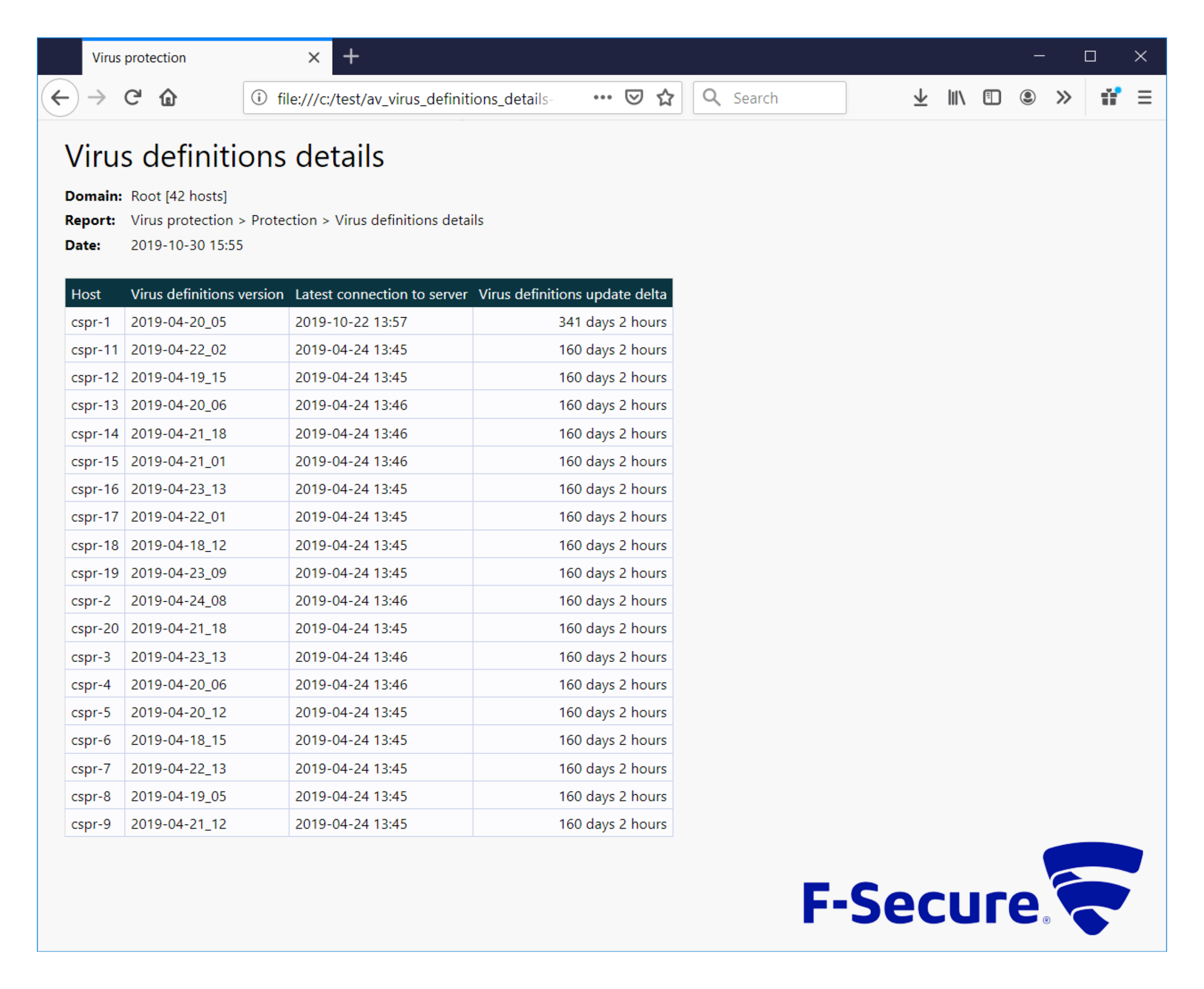
Compliance

Source:	F-Secure Policy Manager
Reason:	Threat detected
Compliance status:	noncompliant

7. Finish the configuration with a tap on *Create*.

Configuration of F-Secure Business Suite Premium

A configuration is not necessary. Data will be extracted from the web report and processed automatically by macmon NAC (see screenshot below).



Virus definitions details

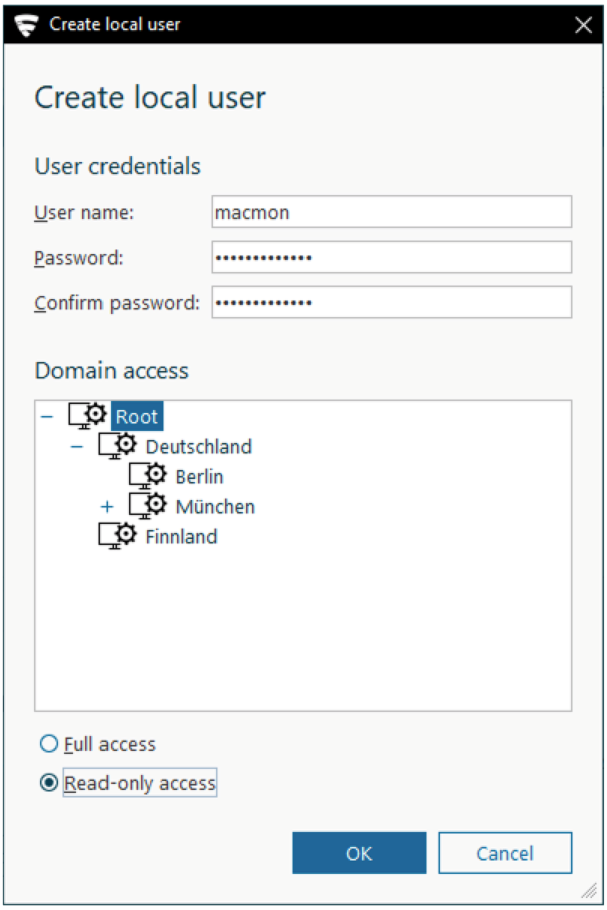
Domain: Root [42 hosts]
Report: Virus protection > Protection > Virus definitions details
Date: 2019-10-30 15:55

Host	Virus definitions version	Latest connection to server	Virus definitions update delta
cspr-1	2019-04-20_05	2019-10-22 13:57	341 days 2 hours
cspr-11	2019-04-22_02	2019-04-24 13:45	160 days 2 hours
cspr-12	2019-04-19_15	2019-04-24 13:45	160 days 2 hours
cspr-13	2019-04-20_06	2019-04-24 13:46	160 days 2 hours
cspr-14	2019-04-21_18	2019-04-24 13:46	160 days 2 hours
cspr-15	2019-04-21_01	2019-04-24 13:46	160 days 2 hours
cspr-16	2019-04-23_13	2019-04-24 13:45	160 days 2 hours
cspr-17	2019-04-22_01	2019-04-24 13:45	160 days 2 hours
cspr-18	2019-04-18_12	2019-04-24 13:45	160 days 2 hours
cspr-19	2019-04-23_09	2019-04-24 13:45	160 days 2 hours
cspr-2	2019-04-24_08	2019-04-24 13:46	160 days 2 hours
cspr-20	2019-04-21_18	2019-04-24 13:45	160 days 2 hours
cspr-3	2019-04-23_13	2019-04-24 13:46	160 days 2 hours
cspr-4	2019-04-20_06	2019-04-24 13:46	160 days 2 hours
cspr-5	2019-04-20_12	2019-04-24 13:45	160 days 2 hours
cspr-6	2019-04-18_15	2019-04-24 13:45	160 days 2 hours
cspr-7	2019-04-22_13	2019-04-24 13:45	160 days 2 hours
cspr-8	2019-04-19_05	2019-04-24 13:45	160 days 2 hours
cspr-9	2019-04-21_12	2019-04-24 13:45	160 days 2 hours

Configuration of a local user

Optionally, you can create an user that accesses this web report with read-only privileges:

1. Open the *Policy Manager Console* user administration in *Tools – Users...*
2. Select *Create local user*.
3. Assign an user name and password.
4. In *Domain access*, select the top level (by default, it is *Root*).
5. Limit access by selecting *read-only access*.
6. Press *OK*.



Create local user

User credentials

User name: macmon

Password: ••••••••••••••

Confirm password: ••••••••••••••

Domain access

- Root
  - Deutschland
    - Berlin
    - München
  - Finnland

○ Full access

● Read-only access

Contact at F-Secure

F-Secure branch office D/A/CH
F-Secure GmbH
Kistlerhofstr. 172c
81379 Munich
Germany

Email: vertrieb-de@f-secure.com | Website: www.f-secure.de | Phone: +49 89 787 467 0