F-Secure

macmon
nac intelligent einfach

MACMON NAC WHITEPAPER

Integration zwischen macmon NAC und F-Secure Business Suite Premium

Inhaltsverzeichnis

Version: 1.1_de

Einleitung

Niemand hat einen besseren Einblick in echte Cyber-Angriffe als F-Secure.
Das finnische IT-Sicherheitsunternehmen berät lückenlos von der frühzeitigen Erkennung von Bedrohungsszenarien bis zur adäquaten Reaktion. Mittlerweile werden die preisgekrönten Cybersecurity-Lösungen von F-Secure auf Millionen von Geräten genutzt. Führende Banken, Fluggesellschaften und Unternehmen vertrauen auf F-Secures Engagement bei der Bekämpfung der gefährlichsten Bedrohungen dieser Welt. Aus dieser Erfahrung und mithilfe innovativer KI-Lösungen entwickeln und realisieren die Security-Berater von F-Secure unübertroffene Sicherheitskonzepte und arbeiten zusammen mit einem Netzwerk aus Top-Channel-Partnern und über 200 Service-Anbietern an ihrer Mission: Die umfassende IT-Sicherheit für jeden Nutzer. F-Secure wurde 1988 gegründet und ist an der NASDAQ OMX Helsinki Ltd gelistet.

Anwendungsfälle

macmon NAC prüft Aktualität von Signaturen von F-Secure Business Suite Premium

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 F-Secure Business Suite Premium und macmon NAC in einem engen und leistungsstarken Verbund.

Die ausgefeilte Engine von F-Secure Business Suite Premium ist am effektivsten, wenn sie auf aktuelle Virensignaturen zurückgreifen kann. Diese werden vom zentralen F-Secure Policy Manager der Business Suite Premium bereitgestellt und von angeschlossenen F-Secure Clients, die auf den Unternehmensgeräten installiert sind, heruntergeladen. macmon NAC überwacht 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 beliebigen 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.

macmon NAC reagiert auf Bedrohungen

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

Dabei wird nicht nur übermittelt, dass eine Bedrohung gefunden wurde, sondern auch, ob sie vom F-Secure Client bereinigt werden konnte. Zwei Fälle, die von macmon 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 Kryptotrojaners, die zunächst nicht über den F-Secure Client entfernt werden kann, weil sie über ein separat erhältliches Spezialtool bereinigt werden muss oder ein Schreibschutz aktiv ist. F-Secure 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.

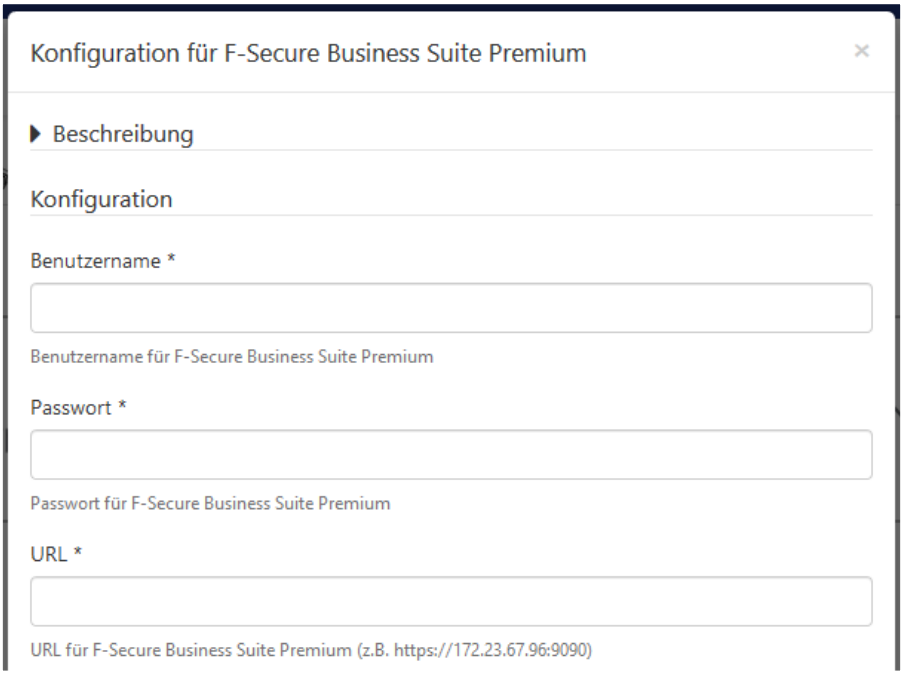
Konfiguration von macmon NAC

macmon NAC prüft Aktualität von Signaturen von F-Secure Business Suite Premium

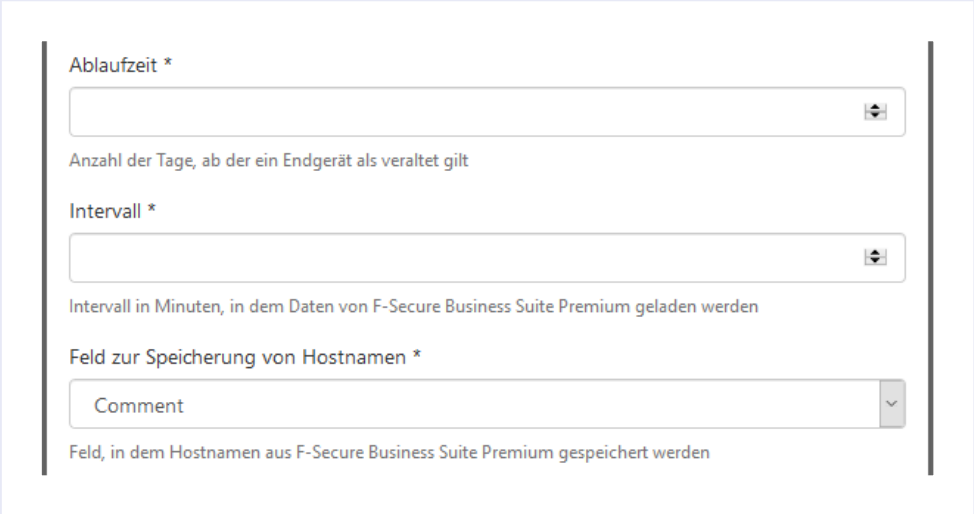
Die Konfiguration wird über das Web-GUI durchgeführt. Tippen Sie auf *Einstellungen* und *Drittanbieter-Integrationen*, dann auf *Compliance*.

Wenn der Rahmen der F-Secure-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 drei Teile aufgeteilt.

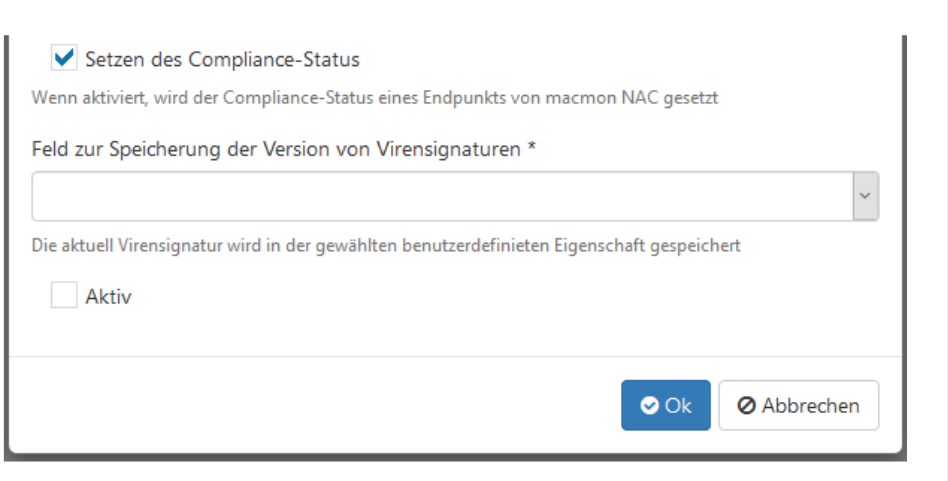
1. Geben Sie zunächst den *Benutzernamen*, das *Passwort* und die *URL* ein, unter der Ihre Installation von *F-Secure Business Suite Premium* erreichbar ist. Benutzen Sie hier gegebenenfalls einen Benutzer mit eingeschränkten Rechten, wie im Abschnitt *Konfiguration eines lokalen Benutzers* des nachfolgenden Kapitels beschrieben.



2. Geben Sie im nächsten Abschnitt die *Ablaufzeit* in Tagen ein. Ein Endgerät gilt als veraltet, wenn es nicht innerhalb dieser Zeit eine Aktualisierung seiner Virussignaturen erhalten hat.
3. Im Feld *Intervall* geben Sie das Intervall in Minuten an, in dem macmon NAC neue Daten von *F-Secure Business Suite Premium* lädt.
4. Das *Hostnamen-Feld* gibt das Feld in *macmon NAC* an, das im Endgeräte-Eintrag den Hostnamen vorhalten soll. Dieser Hostname muss mit der Bezeichnung und dem Format von dem im Web-Bericht von *F-Secure Business Suite Premium* verwendeten Hostnamen übereinstimmen. Das hier ausgewählte Feld muss bereits den Hostnamen enthalten.
   Beispiel: Im Web-Bericht lautet der Hostname eines beliebigen Endgeräts *cspr-1*. Exakt diese Bezeichnung muss nun auch in beispielsweise dem ausgewählten Feld *Kommentar* des zugehörigen Endgeräte-Eintrags hinterlegt sein, damit das Endgerät korrekt zugeordnet werden kann.



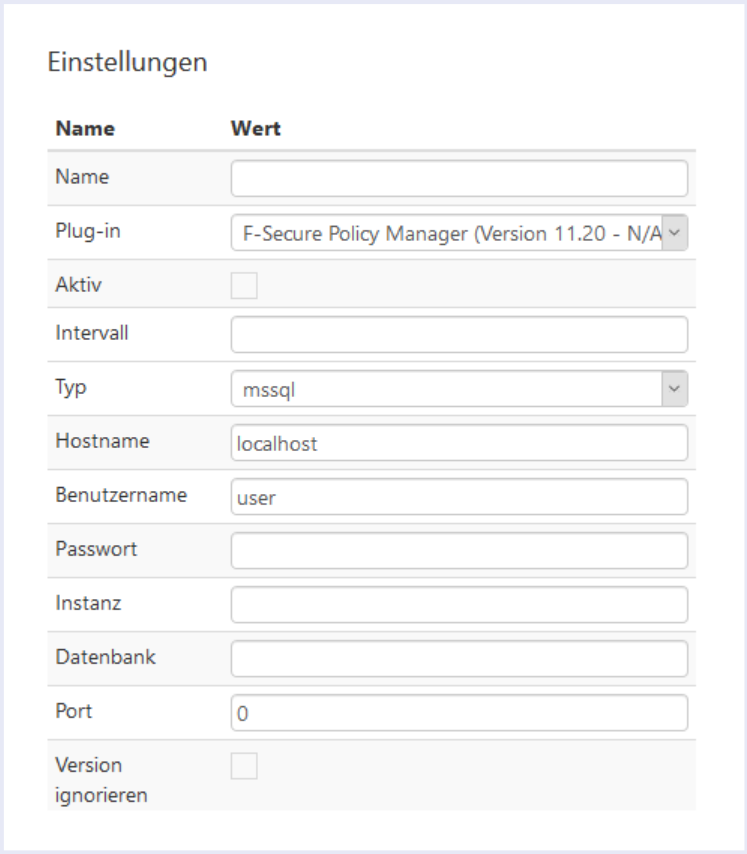
5. Setzen Sie den Haken der Checkbox *Compliance-Status*, wenn macmon NAC ein Endgerät, dessen Virensignaturen veraltet sind, als non-compliant markieren soll. In der Folge wird die Reaktion ausgeführt, die für den Status *non_compliant* konfiguriert wurde. Erhält ein Endgerät eine Aktualisierung seiner Virensignaturen, so wird es von macmon NAC als *compliant* markiert.
6. In *Feld für die Version von Virensignaturen* wählen Sie das Feld aus, in der pro Gerät die aktuelle Version der Virussignaturen gespeichert werden soll. Zur Auswahl stehen benutzerdefinierte Eigenschaften, die Sie in *Einstellungen* > *Benutzerdefinierte Eigenschaften* selbst anlegen können.
7. Aktivieren Sie die Integration durch Setzen des Hakens der Checkbox *Aktiv* und schließen Sie die Konfiguration durch Drücken von *Ok* ab.



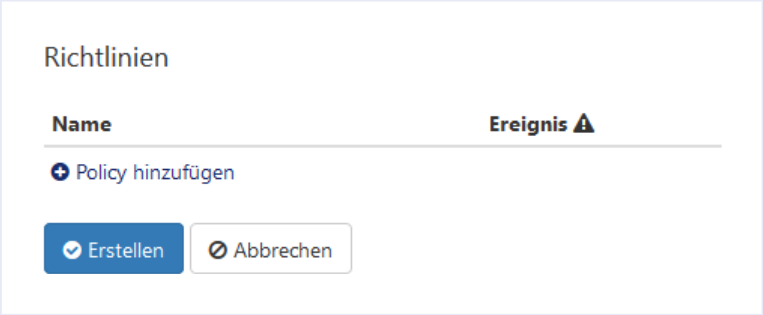
macmon NAC reagiert auf Bedrohungen

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

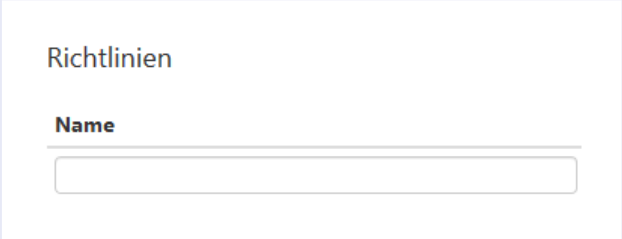
1. Klicken Sie danach auf Konnektor hinzufügen.
2. Geben Sie im Bereich *Einstellungen* alle notwendigen Zugangsdaten ein, um auf die Datenbank von *F-Secure Policy Manager* zugreifen zu können.



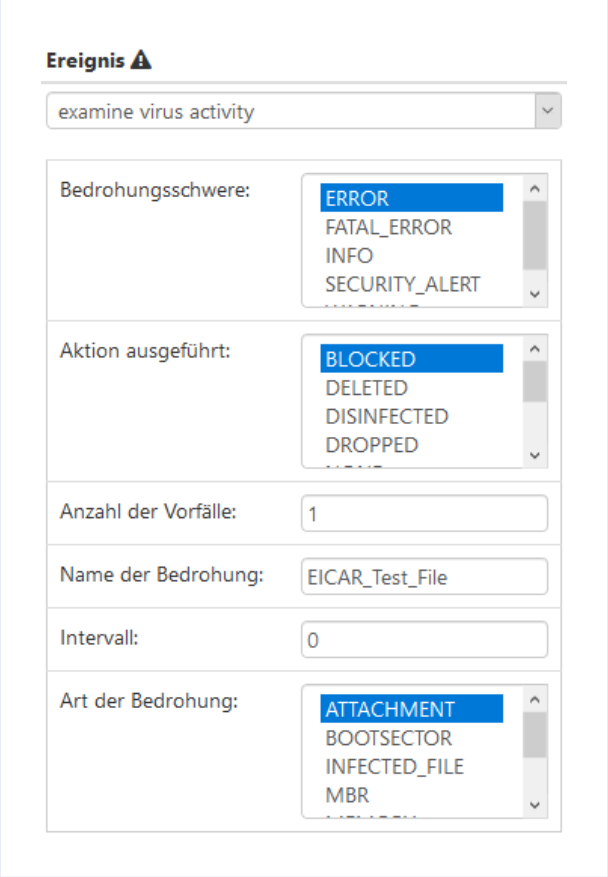
3. Klicken Sie danach im Bereich *Richtlinien* auf Policy hinzufügen.



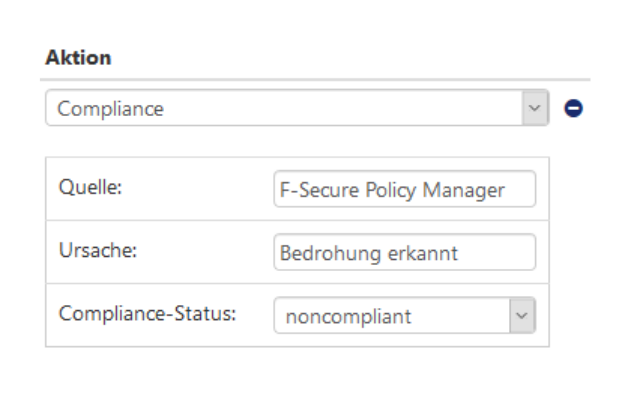
4. Vergeben Sie einen Namen für die Policy.



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.



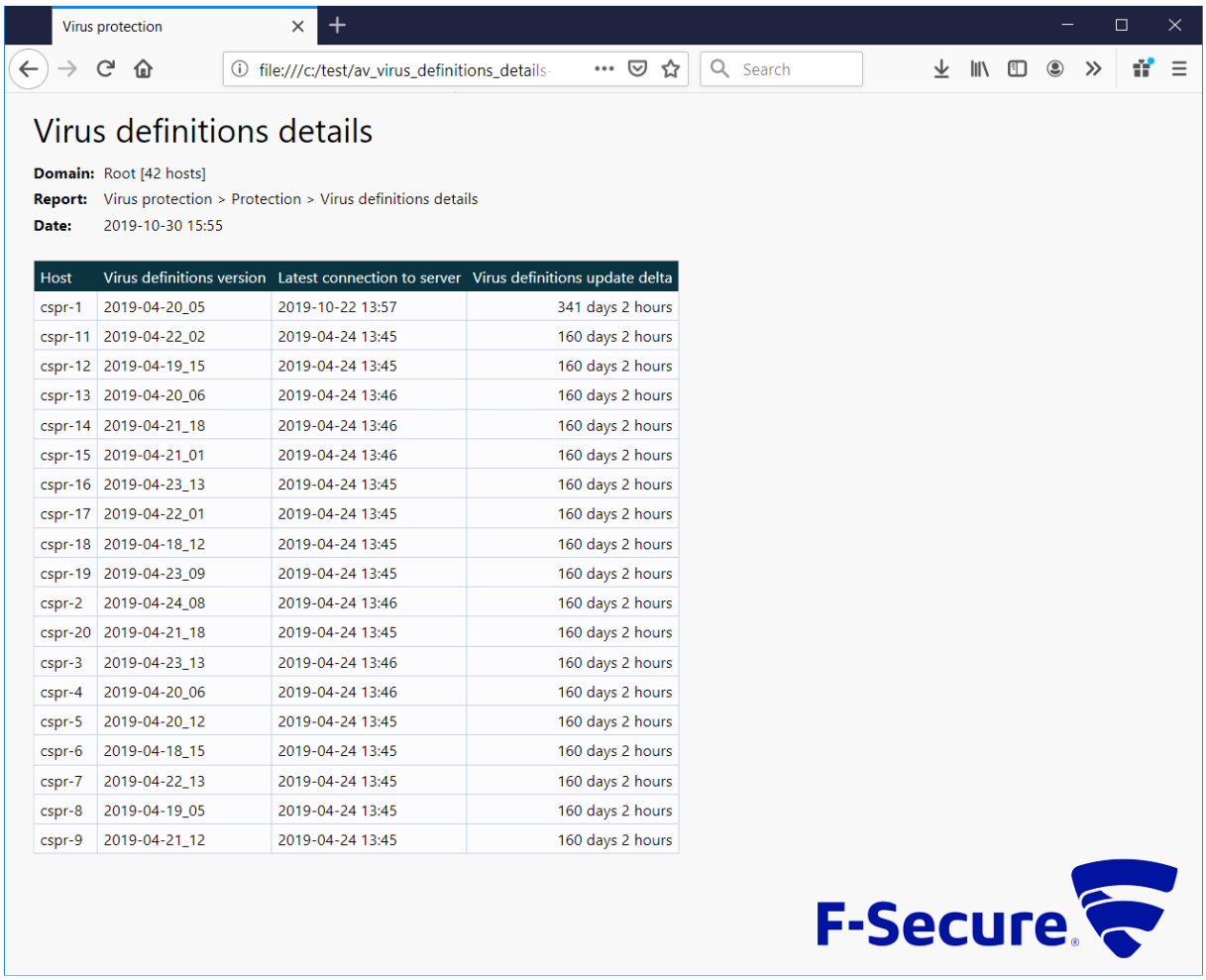
6. Wählen Sie eine gewünschte Aktion, beispielsweise Compliance. Sie können beliebige Namen für die Felder Quelle und Ursache wählen.



7. Schließen Sie die Konfiguration mit einem Klick auf *Erstellen* ab.

Konfiguration von F-Secure Business Suite Premium

Eine Konfiguration ist nicht erforderlich. Die Daten werden aus dem Webreport extrahiert und von *macmon NAC* automatisiert verarbeitet (vgl. Screenshot unten).

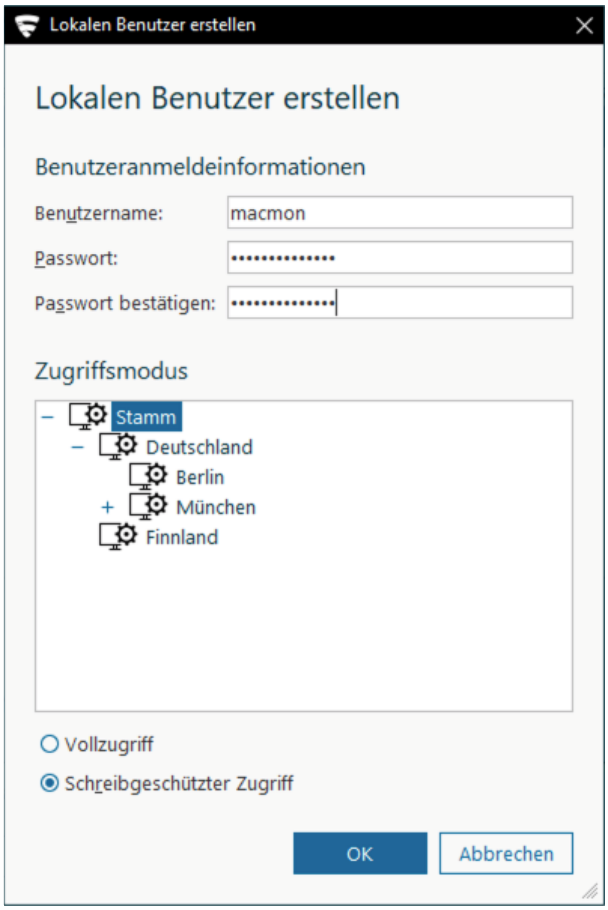


Host	Virus definitions version	Latest connection to server	Virus definitions update delta
cspr-1	2019-04-20_05	2019-10-22 13:57	341 days 2 hours
cspr-11	2019-04-22_02	2019-04-24 13:45	160 days 2 hours
cspr-12	2019-04-19_15	2019-04-24 13:45	160 days 2 hours
cspr-13	2019-04-20_06	2019-04-24 13:46	160 days 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

Konfiguration eines lokalen Benutzers

Optional kann ein Benutzer angelegt werden, der ausschließlich mit Leserechten auf den Webreport zugreift. 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.



Kontakt bei F-Secure

F-Secure Niederlassung D/A/CH
F-Secure GmbH,
Kistlerhofstr. 172c
81379 München

E-Mail: vertrieb-de@f-secure.com | Website: www.f-secure.de | Telefon: +49 89 787 467 0

Kontakt

macmon secure GmbH
Alte Jakobstraße 79-80 | 10179 Berlin
Tel.: +49 30 2325777-0 | nac@macmon.eu | www.macmon.eu