save IT first GmbH

Dokumentation Sophos Steuerung

Für die Steinhaus GmbH

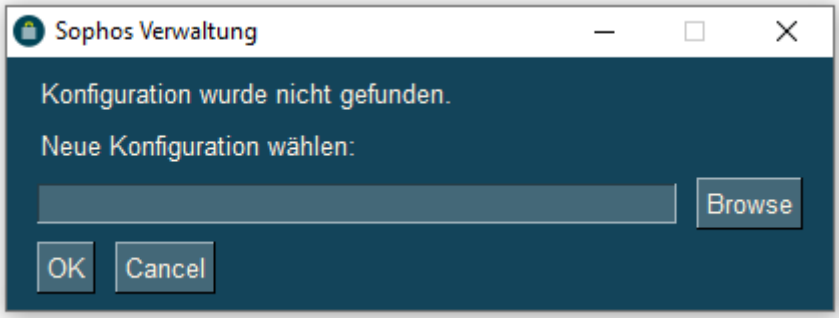
Julian Gundacker
12.1.2021

Inhalt

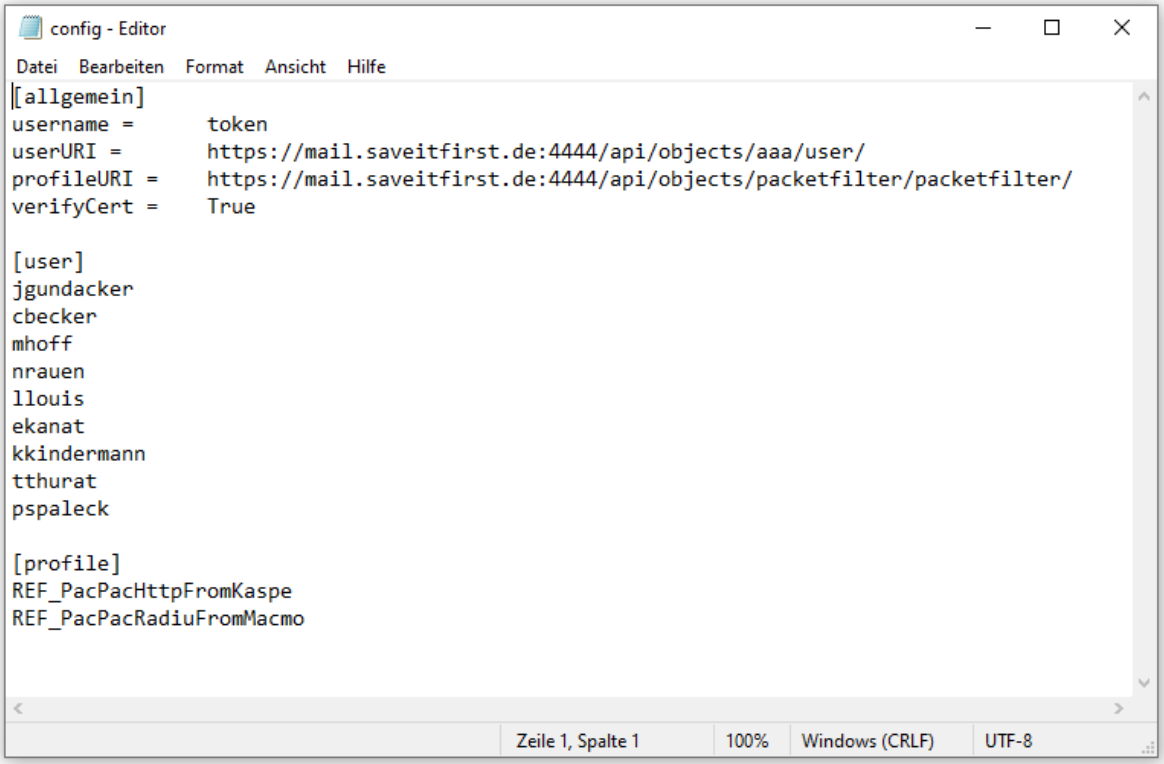
SAVE IT FIRST

Ersteinrichtung

Beim Initialaufruf wird der Speicherort der Konfigurationsdatei abgefragt.



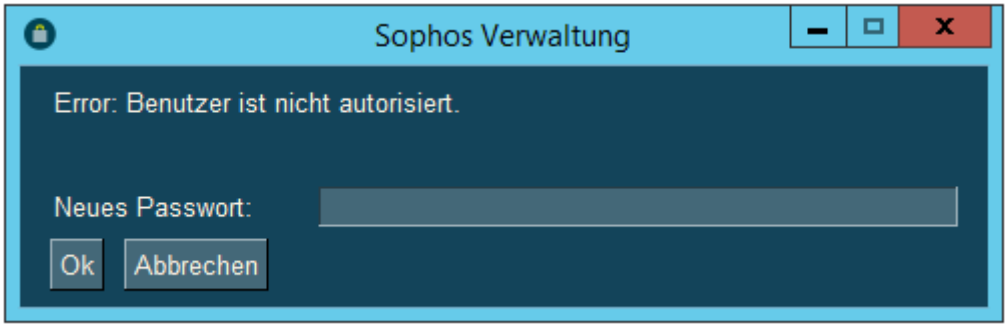
Es ist die config.ini auszuwählen. Folgend eine Beispielkonfiguration.



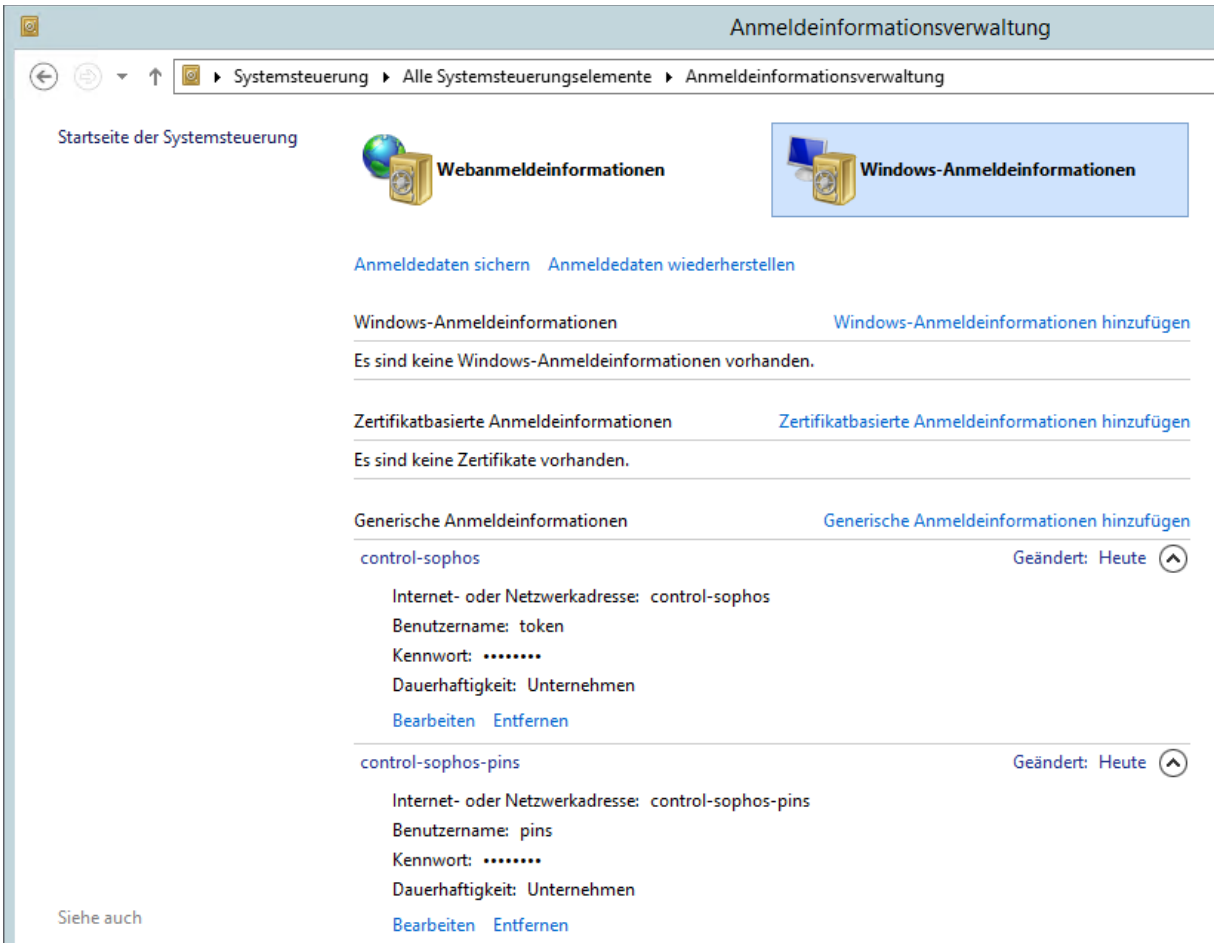
- username = Benutzer, welcher zur Abfrage an der Sophos UTM verwendet wird
- userURI = API-Benutzerverzeichnis-URL
- profileURI = API-Netzwerkprofil-URL
- verifyCert = Gibt an ob das Zertifikat der beiden URLs auf die Gültigkeit des Zertifikats geprüft werden.
- [user] = Liste aller Nutzernamen, welche abgefragt werden sollen.
- [profile] = Liste aller Profile, welche über die REF-ID abgefragt werden sollen.

Die Speicherung des Pfades zur Konfigurationsdatei wird unter *%userprofile%\appdata\local\sophos-control\location.config* abgespeichert.

Im Anschluss wird das Passwort des Benutzers, welcher in der Konfigurationsdatei angegeben wurde, abgefragt und geprüft.

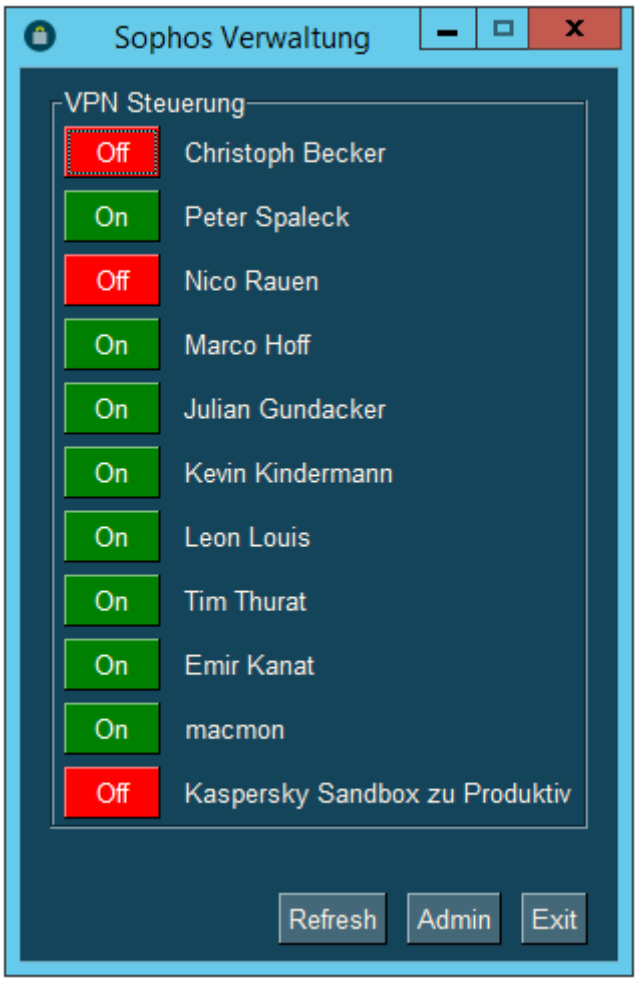


Das Passwort wird im Speicher für Windows-Anmeldeinformationen des Benutzers gespeichert.



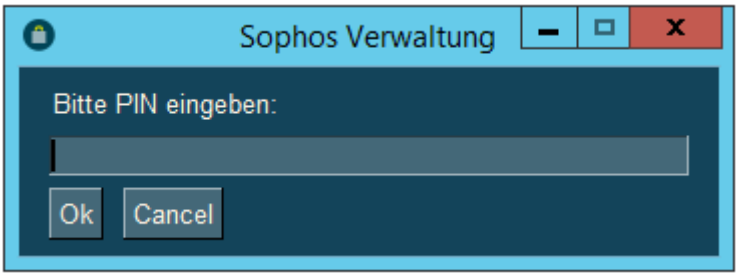
Folgend öffnet sich die Benutzeroberfläche

Benutzeroberfläche



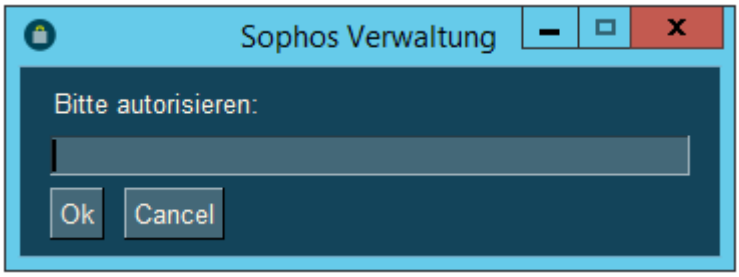
Der Benutzer erhält eine Übersicht aller Benutzer und Profile, welche abgefragt werden, sowie dessen Status. Bei den Benutzern wird der Anzeigename, bei den Profilen die Beschreibung ausgegeben.

Bei Klick auf einen Status kann er diesen nach erfolgreicher PIN-Eingabe ändern.

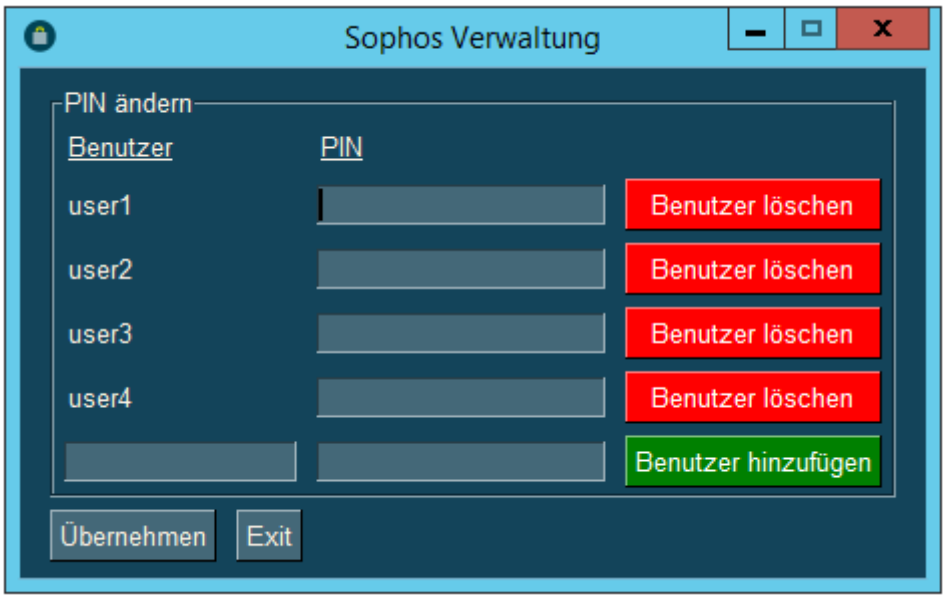


Die PINs werden auch im Speicher für Windows-Anmeldeinformationen abgespeichert.

Die PINs und die dazugehörigen Benutzer können über den Button „Admin“ geändert werden. Zur Authentifizierung wird hier wieder das Passwort des Nutzers, welcher die Sophos steuert, abgefragt.

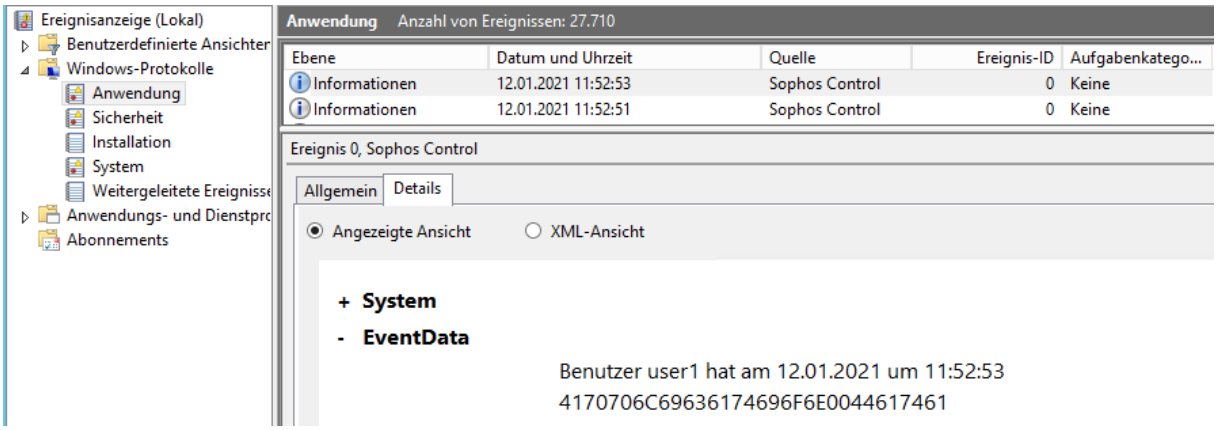


Nach erfolgreicher Authentifizierung erscheint die Benutzer und PIN-Verwaltung.



Hier Benutzer angelegt und gelöscht werden. Sowie neue PINs vergeben werden. Da die Loggingfunktion die Verknüpfung nur nach PIN / Passwort durchführt, kann ein PIN nicht doppelt vergeben werden.

Das Logging wird zum einen in der Windowsereignisanzeige, im Bereich Anwendung durchgeführt.



Zum anderen wird unter *%userprofile%\AppData\Local\sophos-control\sophos-control.txt* ein ausführlicheres Log geschrieben.

In der Oberfläche gibt es des Weiteren einen „Refresh“ Button. Dieser ermöglicht es erneut den Status aller Objekte abzufragen. Dies geschieht allerdings auch automatisch alle 30 Sekunden.