

Installationshinweise zur Netzwerkinstallation von SandStat

Allgemeine Hinweise

Vor allen Arbeiten am Computer, vor allem vor Software-Updates und Installationen, empfehlen wir einen System-Wiederherstellungspunkt zu setzen.

Nachfolgend wird die Einrichtung des Netzwerk-Keys

- I) innerhalb eines lokalen Netzwerks, sowie
- II) mit Zugriff aus der Ferne über VPN

erläutert.

Dabei kann der Netzwerk-Key an einen beliebigen Computer im Netzwerk angeschlossen werden. Es muss sich dabei nicht um den Domänen- oder File-Server handeln.

1) Verwendung des Netzwer-Keys innerhalb eines lokalen Netzwerks

a) Update/Neuinstallation von SandStat auf dem/den Clientrechner/n

Zur Nutzung des Netzwerk-Keys ist ein Update auf die SandStat-Version 4.9.xx erforderlich. Hierzu ist die Installations-Datei „sandstat4.9.x_setup.exe“ auf der CD bzw. in der von uns zur Verfügung gestellten zip-Datei zu auszuführen.

Bitte beachten Sie, dass die Installationsroutine erst nach einem kurzen Moment startet. Nach Abschluss der SandStat-Installation wird der Datenbank-Treiber installiert – diesen Prozess bitte nicht abbrechen.

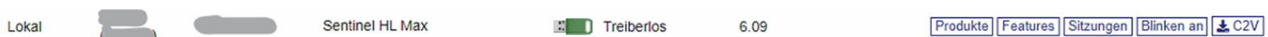
Eine zusätzliche Installation eines Dongle-Treibers etc. ist am Client-Rechner bei der Nutzung innerhalb eines lokalen Netzwerks nicht (mehr) erforderlich.

b) Einrichten des Netzwerk-Keys

Auf dem Rechner, an dem der Netzwerk-Key angeschlossen ist, ist der Netzwerk-Treiber zu installieren. Bitte starten Sie hierzu die Datei „HASPUserSetup.exe“ im Unterverzeichnis „\Treiber\Dongle“ der CD-ROM bzw. der zip-Datei.

Nach erfolgreicher Installation des Netzwerk-Treibers kann im Internet-Explorer mit dem Befehl: <http://localhost:1947/> das Programm „Sentinel Admin Control Center“ gestartet und die Dongle-Informationen angezeigt werden.

Bitte wählen Sie unter „Sentinel Keys“ den entsprechenden SandStat-Key aus (unter „Produkte“ / „Products“ steht die Bezeichnung „SandStat4.9.xx“):



Bei den „Features“ werden die freigeschalteten Programmteile angezeigt inkl. der Anzahl der zeitgleich möglichen Instanzen (Spalte „Gleichzeitigkeit“ / „Concurrency“). Dies entspricht der Anzahl der Lizenzen, die für diesen Netzwerk-Key erworben wurden.

Unter „Sitzungen“ / „Sessions“ können Sie erkennen, wieviel Nutzer gerade mit SandStat mit Zugriff auf den Netzwerk-Key arbeiten.

Ist die maximale Anzahl erreicht und ein weiterer Rechner startet SandStat, kommt es zu der Meldung „Too many current users (H0038)“.

II) Zugriff über VPN

a) Vorbereitung Clientrechner

Analog zu Punkt I a) ist auf dem Clientrechner die SandStat-Version 4.9.xx erforderlich.

Zusätzlich muss in diesem Falle der Dongle-Treiber auf dem Client-Rechner installiert sein. Bitte starten Sie hierzu die Datei „HASPUserSetup.exe“ im Unterverzeichnis „\Treiber\Dongle“ der CD-ROM bzw. der zip-Datei.

Nun muss die Verknüpfung zur IP bzw. zum Hostname des Servers eingetragen werden. Hierzu geben Sie bitte im Internet-Browser der Befehl <http://localhost:1947/> ein:

localhost:1947/int_ACC_help_index.html

Sentinel Admin Control Center

Admin Control Center Help

Welcome to the Admin Control Center. This application enables you to manage access to software licenses and Features, to control detachable licenses, to control sessions, and to diagnose problems.

Note: You can select the language in which Admin Control Center is displayed from the bottom of the Options pane.

> The Admin Control Center enables you to monitor the following:

- All the Sentinel protection keys that are currently available on the network server, including their identity, type, and location
- The number of users currently logged in to a protection key, and the maximum number of users allowed to be simultaneously logged into that specific key
- The Features to which each protection key allows access, and any restrictions that apply to the Feature
- The users who are currently logged into a specific protection key, including detailed login information

Note: SL UserMode keys are only displayed for the local (Windows) machine. SL UserMode keys are not displayed when the configuration parameter **Do Not Load hasplmv.exe** is selected.

> You can perform actions, such as:

- Detaching a license from the network and attaching it to your machine or a different recipient machine
- Cancelling a detachable license prematurely
- Installing an update to a license on a key that is visible in Admin Control Center

> You can implement and manage cloud licensing.

> You can make basic configuration changes, including:

- Setting the display refresh time
- Configuring access permissions from a client machine to a remote server, and configuring a server to allow it to be remotely accessed
- Defining values for Products with detachable licenses

> The Diagnostics page enables you to view system information related to the current Sentinel License Manager, and to generate reports.

Related Topics

- Security Considerations
- Cloud Licensing
- Detaching Licenses - Overview
- Sentinel Keys
- Products
- Features
- Sessions
- Update/Attach
- Access Log
- Configuration
- Diagnostics

Bitte gehen Sie auf die Auswahl „Configuration“ und dann zum Reiter „Access to Remote License Manager“. Da bitte die IP oder der Hostname des Servers eintragen (lassen). Diese Info bekommen Sie von Ihrem für die IT-zuständigen Kollegen bzw. IT-Dienstleister.

The screenshot shows the Sentinel Admin Control Center interface. The main header is 'Sentinel Admin Control Center'. Below it, the page title is 'Configuration Host Name: af-len-2021'. The left sidebar contains a navigation menu with the following items: Sentinel Keys, Products, Features, Sessions, Update/Attach, Access Log, Configuration (highlighted), and Diagnostics. The main content area has four tabs: Basic Settings, Users, Access to Remote License Managers (selected), and Access from Remote Clients. Under the 'Access to Remote License Managers' tab, there are three settings: 'Allow Access to Remote Licenses' (checked), 'Broadcast Search for Remote Licenses' (checked), and 'Remote License Search Parameters' (with an empty text input field). A note states: 'You may experience a delay of a few minutes before your changes take effect.' At the bottom of the configuration area, there are three buttons: 'Submit', 'Cancel', and 'Set Defaults'.

b) Vorbereitung VPN

Die Kommunikation erfolgt über Port 1947. Daher muss diesen Port im VPN-Netz freigeschaltet werden.