Support
signatures-support@infotech.de

Infotech
Gesellschaft für Informations- und Datentechnik mbH

Holthoffstr. 122a
45659 Recklinghausen

Telefon 02361-9130-0
Telefax 02361-9130-105
eMail info@infotech.de
Website www.infotech.de

InfoTech
Gesellschaft für Informations- und Datentechnik mbH

Stand: 10.07.2014

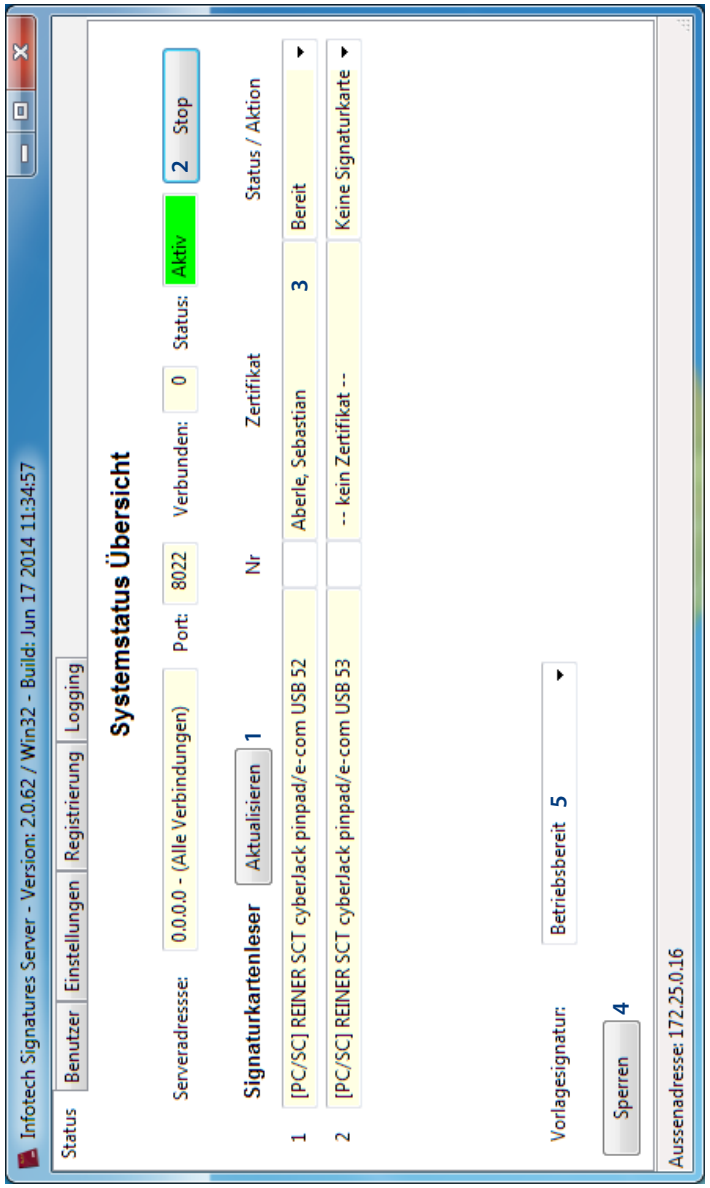
Windows

Signatures

Server - Hinweise zur Benutzung

Systemstatus

1 Suchen nach verbundenen Kartenlesern
2 Kontrolle des Netzwerkdienstes
· Start · Stop
3 Kontrolle der Kartendienste
· Sperren · Entsperren
· Beenden · Neustart
· Authentisieren
4 Sperren der Oberfläche
5 Kontrolle das Vorlagedienstes
· Sperren · Entsperren
· Neustart



Logging

Die angezeigten Informationen können zur Fehlerdiagnose und im Kontakt mit dem Signatures-Support bei Infotech genutzt werden. Es stehen Kontrollen zum Detailgrad des Loggings zur Verfügung.

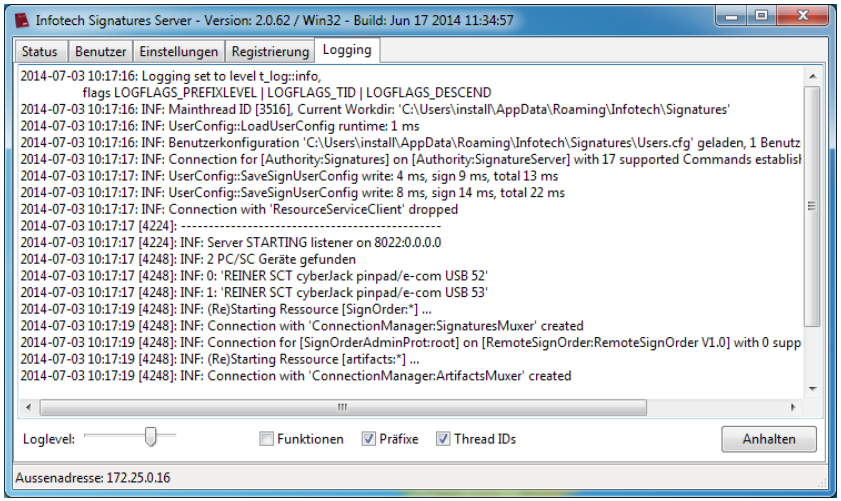


Abb.4

Registrierung

Es werden Informationen zur Registrierung des Servers angezeigt.

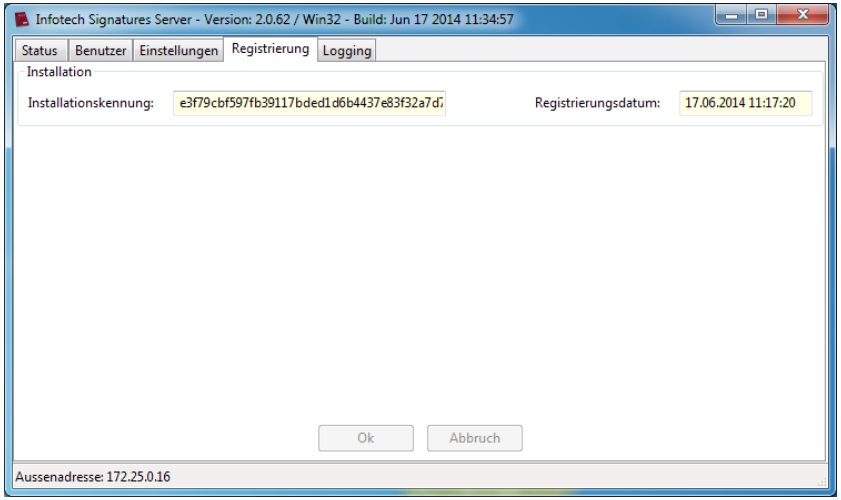


Abb.3

Nach Abschluss der Beta-Phase kann die Zusatzoption „Automatische Umläufe“ bei Bedarf kostenpflichtig zugebucht werden (während der Testphase steht die Option kostenfrei zur Verfügung).
Ein bei der Buchung erhaltener Lizenzschlüssel kann dann auf dieser Seite eingetragen und zur Freigabe angefragt werden. Die Prüfung der Freigabe kann einige Zeit dauern, die Aktivierung erfolgt dann automatisch im Hintergrund.
Soll eine aktivierte Lizenz auf einen anderen Server übertragen werden muss sie zuvor auf dem bisherigen Server freigegeben werden.

Beim Erststart des Servers erfolgt automatisch eine anonyme Registrierung bei Infotech. Während der Laufzeit prüft der Server die Registrierung periodisch.
Der Host „ca.infotech.de“ muss dazu auf TCP-Port 25050 dauerhaft erreichbar sein.

Die Übersicht über den Systemstatus zeigt den Zustand sämtlicher Serverkomponenten an und gestattet die Kontrolle der einzelnen Module über die Aktionsfelder.

Während der Laufzeit neu ans System angeschlossene Kartenlesegeräte werden nach Klick auf *Aktualisieren* zur Nutzung in der darunter dargestellten Liste freigegeben. Neu eingelegte Signaturkarten werden in der Regel automatisch erkannt. Der Vorgang kann durch die Aktion *Neustart* am entspr. Kartenleser forciert werden. *Authentisieren* startet nachträglich die PIN-Eingabe, falls diese nicht direkt beim Einlegen einer Karte durchgeführt wurde.

Die Sperre der Benutzeroberfläche kann z.B. bei gemeinsam genutzten Servermaschinen genutzt werden. Beim Entsperren wird ein ggf. gesetztes Kennwort (vgl. Abschnitt *Einstellungen*) abgefragt.

Benutzer

Benutzer können jederzeit neu angelegt oder gelöscht werden. Nach Änderungen an einem Benutzer müssen diese durch Klick auf *Ok* oder *Abbrechen* bestätigt oder verworfen werden, bevor andere Objekte angewählt werden können.

Ein Benutzer kann über die Checkbox *Neu anfordern* gezwungen werden sein Kennwort bei der nächsten Verbindung zu ändern. Ebenso kann das Kennwort über *Neu zuweisen* zurückgesetzt werden. Das dabei automatisch erzeugte Kennwort muss nach einmaliger Verwendung durch den Benutzer ebenfalls wieder geändert werden.

Zur automatischen Freigabe von Gerätezertifikaten kann automatisch eine jeweils einmalig gültige Freigabe-TAN generiert werden.

Die Nutzungszeiten des Dienstes können pro Benutzer eingeschränkt werden, z.B. zur zeitweisen Aktivierung einer Urlaubsvertretung oder zur Einschränkung auf die Laufzeit eines Projektes. Dazu Start- und/oder Enddatum festlegen und die entspr. Checkboxen aktivieren.

Über den Knoten *Signaturzertifikate* (1) können neue Zertifikate nach Auswahl des gewünschten Kartenlesers von der eingelegten Signaturkarte ausgelesen und einem Benutzer zugeordnet werden.

Auf dem Knoten *Gerätezertifikate* (2) werden von den Clients ohne Angabe einer korrekten Freigabe-TAN eingegangene Zertifikatsanforderungen angezeigt und können manuell gestattet oder verweigert werden.

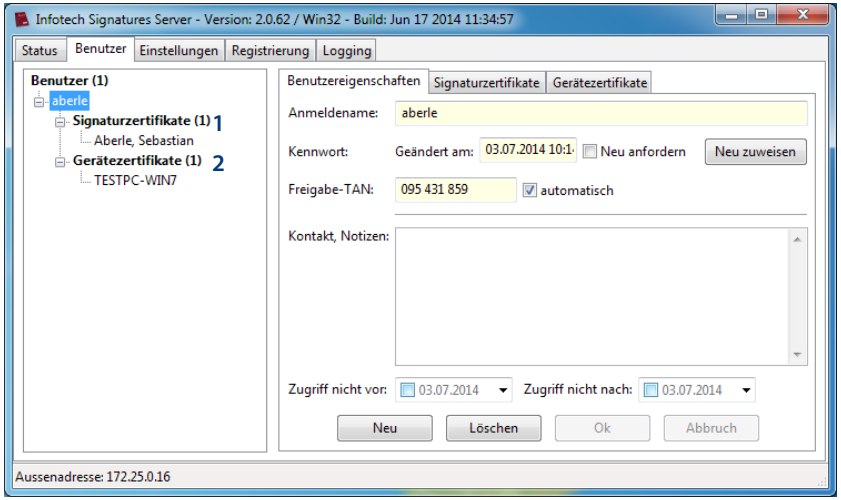


Abb.1

Einstellungen

Bei der Durchführung von OCSP-Prüfungen kann ein HTTP-Proxy (ohne Authentisierung) verwendet werden, dessen Adresse hier eingetragen wird.

Die Erreichbarkeit des Serverdienstes kann auf ein einzelnes Netzwerk-Interface der Servermaschine beschränkt werden, ebenso ist der TCP-Port frei wählbar. Voreingestellt sind alle verfügbaren Interfaces auf Port 8022.

Die Anzahl der fehlgeschlagenen Login-Versuche am Signaturdienst sowie die darauf folgende automatische Sperrzeit ist standardmäßig auf 3 Fehlversuche gefolgt von 10 Sekunden Sperre eingestellt. Diese Maßnahme verhindert, dass ein Benutzerkennwort durch einfaches Ausprobieren ermittelt werden kann.

Es kann ein Kennwort vergeben werden, welches die Serverkonfiguration schützt und beim Start des Servers sowie nach dem Entsperren der Benutzeroberfläche (vgl. Abschnitt *Systemstatus*) abgefragt wird.

! *ACHTUNG: Das Kennwort kann bei Verlust nicht zurückgesetzt oder wiederhergestellt werden! Wird es vergessen kann der Server nur komplett neu eingerichtet werden.*

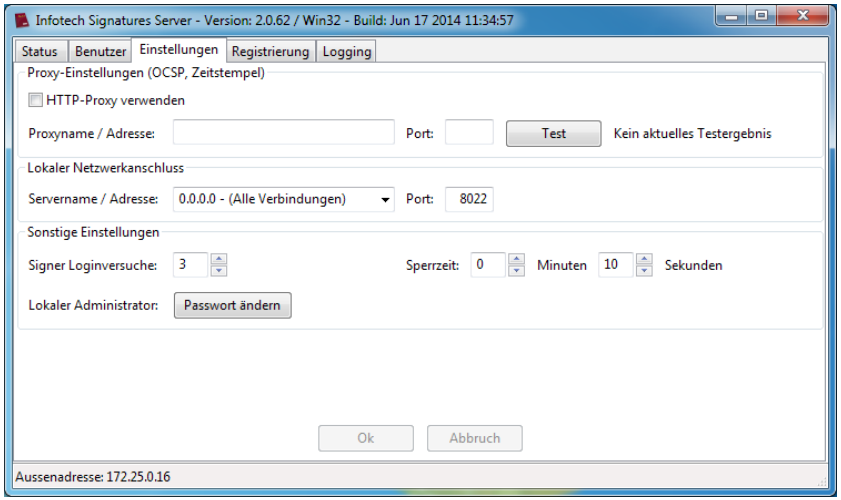


Abb.2