

# HiCrypt™

Einrichtung mit Floating Licence

**digitronic  
computersysteme gmbh**

Oberfrohaer Straße 62  
D-09117 Chemnitz  
Telefon: +49 (0) 371 81539-0  
Fax: +49 (0) 371 81539-900  
Internet: [www.digitronic.net](http://www.digitronic.net)  
E-Mail: [info@digitronic.net](mailto:info@digitronic.net)



© 2014 digitronic computersysteme gmbh

Dieses Dokument ist urheberrechtlich geschützt, und seine Verbreitung unterliegt den Lizenzen, die seine Verwendung, Vervielfältigung und Verbreitung einschränken. Kein Teil dieses Produkts oder Dokuments darf ohne vorherige schriftliche Genehmigung von digitronic in irgendeiner Art und Weise reproduziert werden.

Verfasser: digitronic  
Stand: 9. Mai 2014

# I N H A L T

## Inhaltsverzeichnis

---

<b>1</b>	<b>Einleitung .....</b>	<b>1</b>
<b>2</b>	<b>Einrichtung Lizenzserver .....</b>	<b>2</b>
<b>3</b>	<b>Einrichtung HiCrypt™ .....</b>	<b>4</b>
<b>3.1</b>	<b>Terminal Server .....</b>	<b>4</b>

# KAPITEL 1

## 1 Einleitung

---

Dieses Dokument beschreibt, wie bei der Einrichtung von HiCrypt™ unter Verwendung von Floating Lizenzen mit WIBU CodeMeter USB-Dongle vorzugehen ist.

Um die Lizenzen im Netzwerk zur Verfügung zu stellen, muss zunächst ein Lizenzserver eingerichtet werden, an dem dann der USB-Dongle angesteckt werden kann. Danach kann HiCrypt™ auf beliebigen Systemen im Netzwerk installiert werden.

# KAPITEL 2

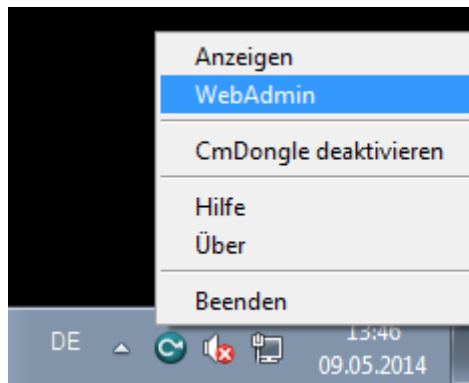
## 2 Einrichtung Lizenzserver

---

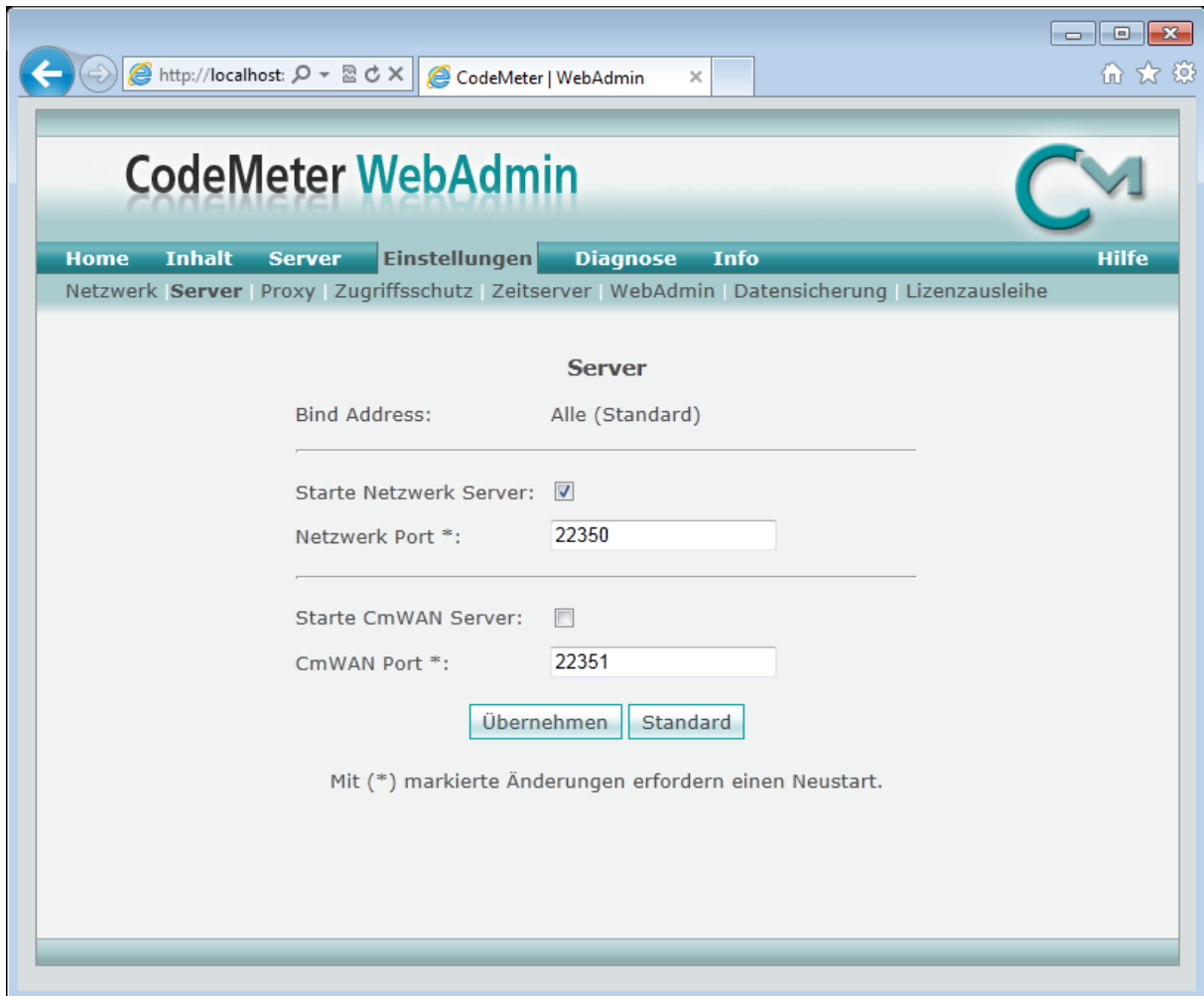
Auf dem System, welches als Lizenzserver dienen soll, muss die CodeMeter Runtime Umgebung installiert werden. Hierfür kann ein beliebiger Server oder Client-PC verwendet werden, solange dieser immer im Netzwerk erreichbar ist und über einen USB-Port verfügt.

Die aktuellste Version ist unter der URL <http://www.wibu.com/de/anwendersoftware.html> zu finden.

Nach der Installation der CodeMeter Runtime ist das Icon des CodeMeter Control Centers im Systray zu finden. Über einen Rechtsklick auf das Icon muss nun der WebAdmin gestartet werden, wie in der folgenden Abbildung zu sehen.



Im WebAdmin ist unter Einstellungen|Server der Haken bei „Starte Netzwerk Server“ zu setzen und mit Übernehmen zu bestätigen.



Jetzt werden die, für die Verwendung im Netzwerk freigegebenen Lizenzen, aller an diesem System angeschlossenen CodeMeter-Dongle im Netzwerk bereitgestellt.

Sie können jetzt den mitgelieferten USB-Dongle am Lizenzserver anschließen.

# KAPITEL 3

## 3 Einrichtung HiCrypt™

---

Zur Installation führen Sie das Setup HiCrypt.msi aus.

Sollte sich der Lizenzserver nicht im gleichen Subnetz befinden, dann muss über den Parameter HICRYPT\_LICENSE\_SERVER die IP-Adresse des Lizenzservers übergeben werden. Der Aufruf würde dann also wie folgt lauten:

```
msiexec /i HiCrypt.msi HICRYPT_LICENSE_SERVER=aaa.bbb.ccc.ddd
```

### 3.1 Terminal Server

Um die Lizenzanzahl nicht zu überschreiten, sollten auf einem Terminalserver zwei Parameter in der Registry gesetzt werden. Diese sind in den FAQs unter <http://hicrypt.com/faq.html> beschrieben. Hier ein Auszug mit den beiden betreffenden Parametern.

#### Wie kann ich diejenigen Anwender festlegen, die HiCrypt™ verwenden dürfen?

Grundsätzlich startet HiCrypt™ automatisch für jeden Anwender nach der Benutzeranmeldung. Dies gilt für alle Anwender eines Computers gleichermaßen.

Arbeiten mehrere Anwender mit dem gleichen Computer und kommt gar ein Terminal-Server zum Einsatz, so kann die Benutzergruppe, die HiCrypt™ verwenden darf, eingeschränkt werden. Hierfür wird ein Wert in der Windows-Registrierung verwendet, in dem die Benutzergruppen angegeben werden, denen die Verwendung von HiCrypt™ gestattet ist.

Führen Sie die nachfolgenden Schritte aus, um den Beispielgruppen "HiCrypt-Anwender" und "HiCrypt-Manager" die Verwendung von HiCrypt™ zu gestatten (für diesen Vorgang benötigen Sie administrative Berechtigungen für den Computer).

- Starten Sie die Windows-Registrierung.
- Legen Sie in dem Schlüssel **HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\HiCryptSvc\Parameters** einen "Wert der mehrteiligen Zeichenfolge" mit dem Namen **AllowedUserGroups** an.
- Tragen Sie darin die beiden Gruppen "HiCrypt-Anwender" und "HiCrypt-Manager" in jeweils eine eigene Zeile ein. Verwenden Sie hierzu das Format für Down Level-Logon-Namen (DOMAIN\GroupName) oder das UPN-Format (GroupName@DNSDomainName.com). Bei lokalen Gruppen ist der Gruppenname ausreichend.
- Starten Sie anschließend den Computer neu, um die vorgenommenen Änderungen zu übernehmen.

## Wie kann ich verhindern, dass HiCrypt™ bei Anwendern gestartet wird, denen die Verwendung nicht gestattet ist?

Wenn Sie die Anwender, die HiCrypt™ verwenden dürfen, eingeschränkt haben, können Sie mit Hilfe eines weiteren Wertes in der Windows-Registrierung verhindern, dass HiCrypt™ für alle übrigen Anwender gestartet wird.

Führen Sie die nachfolgenden Schritte aus, um dies zu erreichen (für diesen Vorgang benötigen Sie administrative Berechtigungen für den Computer).

- Starten Sie die Windows-Registrierung.
- Legen Sie in dem Schlüssel **HKEY\_LOCAL\_MACHINE\Software\digitronic\HiCrypt** (32bit) oder in dem Schlüssel **HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\digitronic\HiCrypt** (64bit) einen "DWORD-Wert (32-Bit)" mit dem Namen **SilentQuitIfUserIsNotInAllowedGroups** an.
- Setzen Sie dessen Wert auf **1**, um den Start von HiCrypt™ bei Anwendern zu verhindern, denen die Verwendung von HiCrypt™ nicht gestattet ist.
- Starten Sie anschließend den Computer neu, um die vorgenommenen Änderungen zu übernehmen.