White Paper

CodeMeter® in Virtual Environments

Rüdiger Kügler, Professional Services | Security Expert, WIBU-SYSTEMS AG

www.wibu.com

Content

Author:
Rüdiger Kügler first encountered software development in 1988, working in FORTRAN, C, and Assembler as part of his physics degree course. After obtaining his degree, he worked with Macromedia Director and Delphi in a series of multimedia projects. He was one of the pioneering developers who used Java applets for website banner adverts. Beginning in 1995, he was active as a project leader in multimedia and security projects for banks, online retailers, and software developers.

Since 2003, Rüdiger Kügler has been working with Wibu-Systems as a security expert and leader of the professional services team. His core competences include the protection of software against reverse engineering and the integration of licensing in the internal processes of software vendors.

Introduction

IT professionals everywhere enjoy the many advantages offered by virtual machines and terminal servers and are getting more out of less hardware and allowing easy recovery if things go wrong. As software publishers and vendors, you might have more mixed feelings about virtual machines. On the one hand, virtual machines give you an easy means of testing your software in a freely definable environment. On the other, virtual machines and terminal servers create major new challenges for licensing your products – at a time when licensing and protection against piracy have become indispensable for the success of your software.

CodeMeter offers you a powerful tool for safe and reliable licensing on both virtual machines and terminal servers. This whitepaper introduces you to different use cases that showcase the capabilities of CodeMeter.

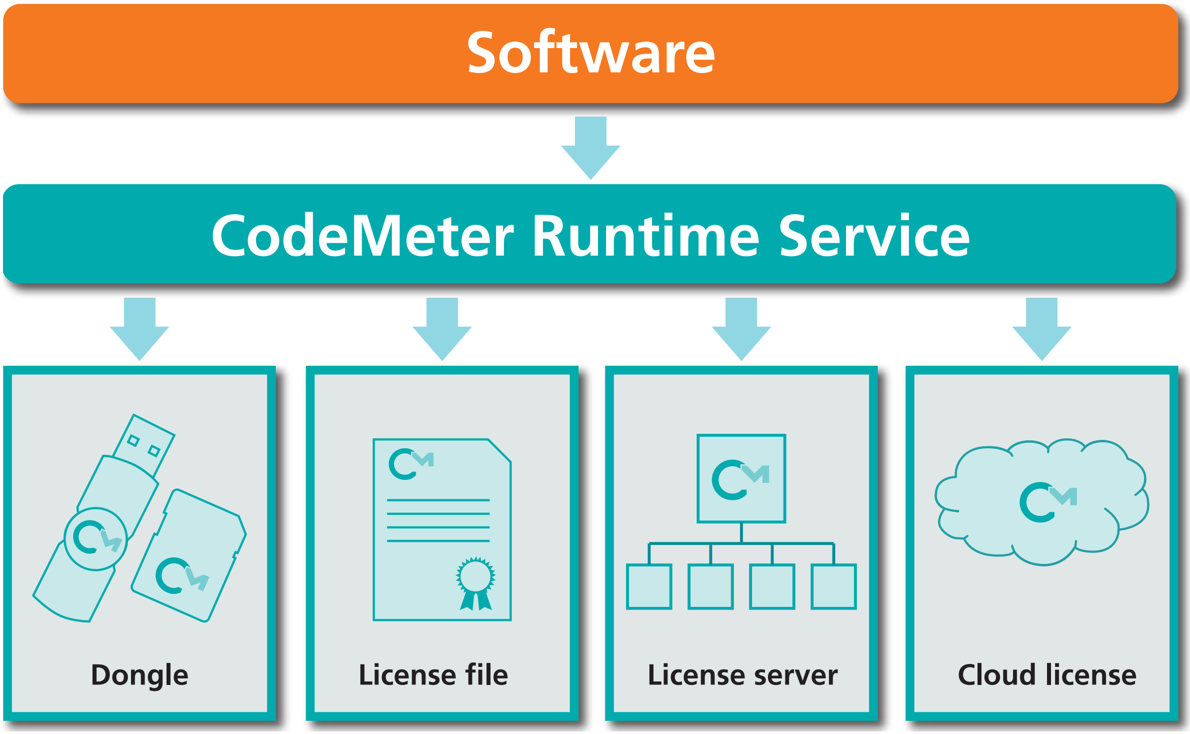


Image 1: CodeMeter overview

CodeMeter allows you to choose the following license containers for every individual client:

- Dongles (CmDongle: saves all licenses on secure external hardware)
- Soft licenses (CmActLicense: hardware-bound, encrypted license files)
- License servers (LAN, or WAN)
- Cloud license (CmCloud: stores all licenses on a server in the cloud)

The Threats and Challenges of Virtual Machines

A virtual machine is hardware simulated on a (host or master) computer. This virtual hardware runs a complete (guest or child) operating system, while severely restricting its ability to interact with the real environment around it. All guest systems and the host share the same real-life hardware, but without immediate access being given to the guest systems. They see a simulated – virtual – machine.

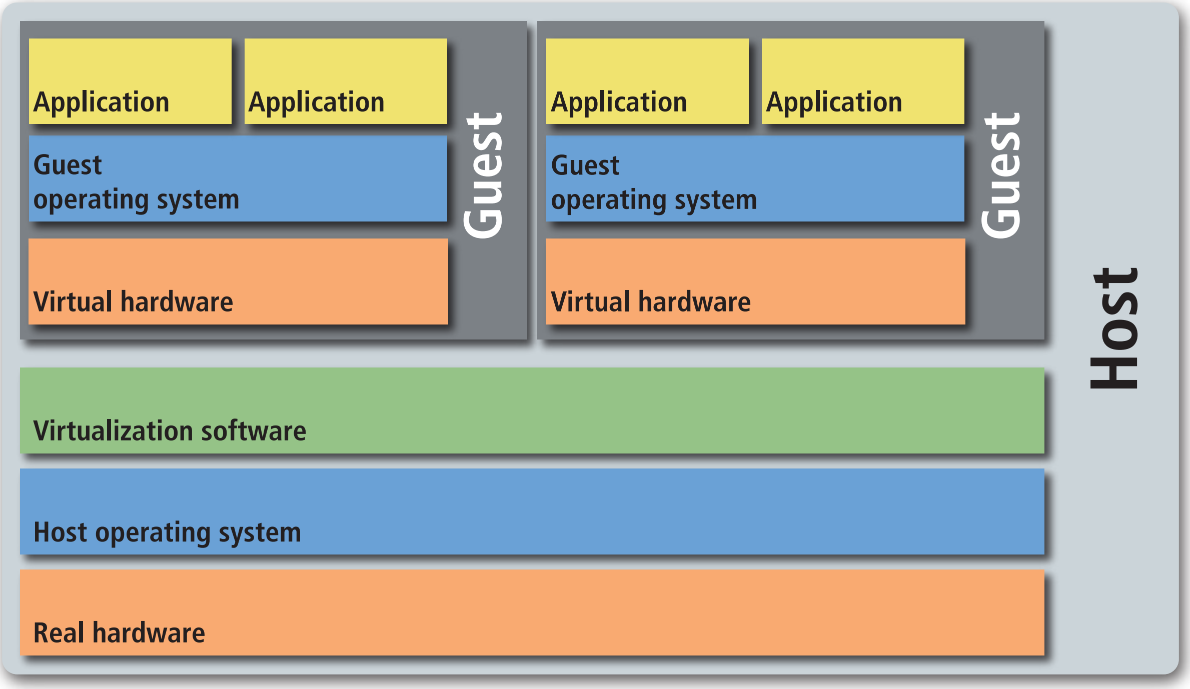


Image 2:
Architecture of a virtual machine

Virtual machines can be saved and recovered (returned to an earlier state) with considerable ease.

From a licensing point of view, virtual machines imply several new threats:

For dongle users:

- Illicit multiple use of a single license by using one dongle for several guest systems.

For pure soft licenses:

- Resetting time-limited or pay-per-use licenses by using a copy or snapshot.
- Duplicating machine-bound licenses by cloning the allocated machine in its entirety.

There are also unique challenges for the licit users of your software:

- The ability to connect dongles and virtual machines.
- High-availability license servers running on virtual machines.

Threats and Challenges of Terminal Servers

Terminal servers host the software installed on them. The applications are executed on the servers, and the users only have access to a client system that mirrors the server's display output on the user's hardware. Many users can use the same terminal server simultaneously, each being given a distinct session which operates independently from the other users' sessions. The client only provides mice, keyboards, or other peripherals.

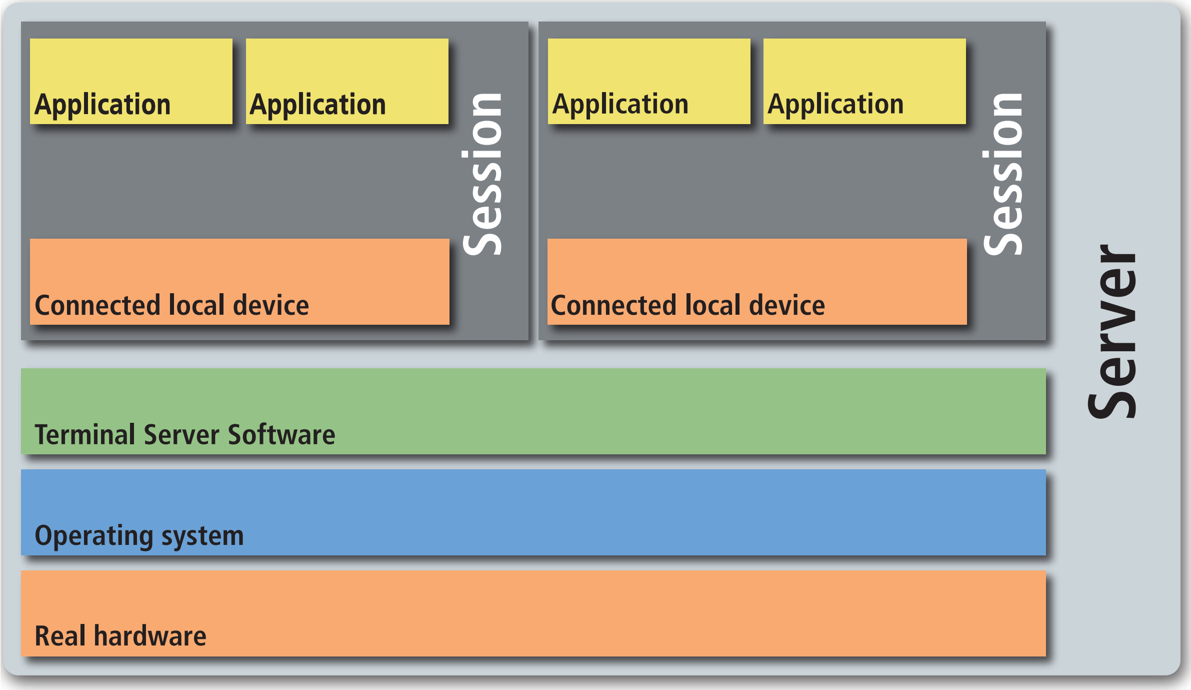


Image 3: Architecture of a terminal server

The following threats need to be considered:

- Illicit multiple use of single licenses in multiple simultaneous sessions on the terminal server.
- Use of a single-user license as a floating network license.

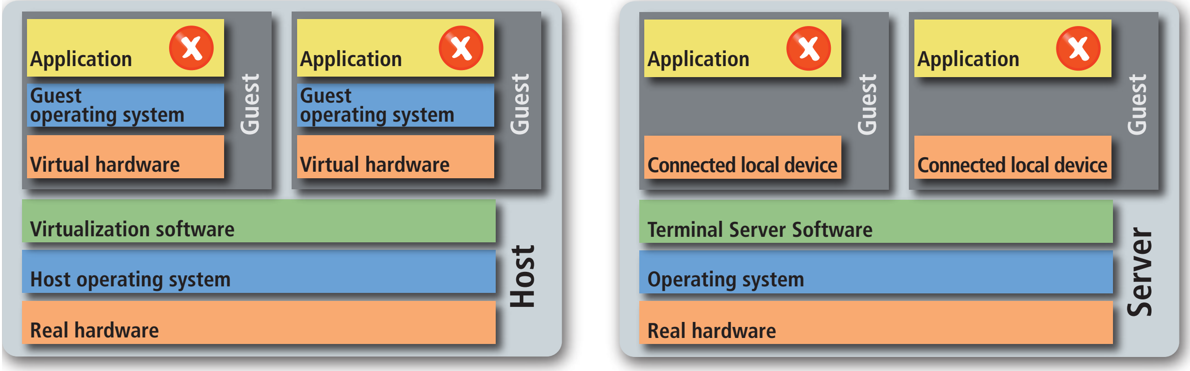
The following scenarios represent the specific challenges of terminal servers:

- How can I make a license available to defined users on the terminal server?
- How can a license kept on the client system be used on the terminal server?

Past Solutions

One response to these challenges was equipping software with the means to identify virtual machines and terminal servers. When such an unwanted environment was identified, the software would cease to work with an error message to that effect.

Image 4: Outdated approaches



This solution can be considered unsuitable for today's world: it dries out an important revenue stream, as it cuts your business off from the entire virtual world. Every computer with remote desktop access is, by its nature, a terminal server and could therefore not operate your software. This is made worse by the effort required for integrating and maintaining the identification functionalities.

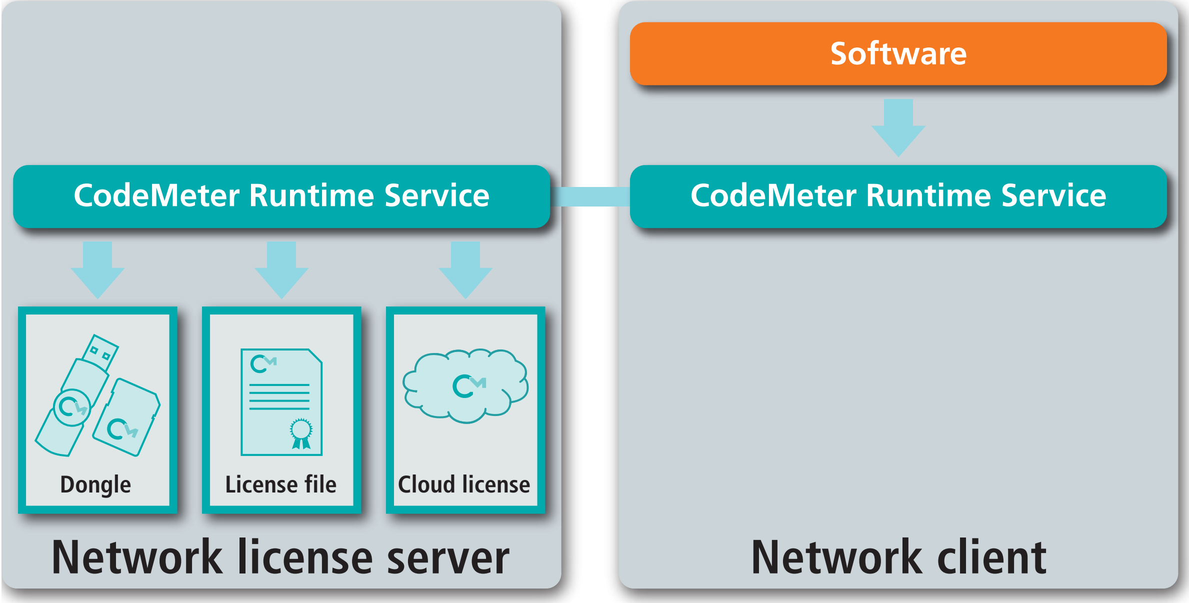
The solution revolved around the question of "where is the software running?" However, the question should instead be "where is the license?" This is the CodeMeter principle that offers you a generic, versatile, and automatically usable solution.

A Modern Solution: CodeMeter

The core element of the CodeMeter architecture is the CodeMeter Runtime Service (CodeMeter.exe). The CodeMeter Runtime Service is a service (Windows) or daemon (Linux and OS X) that you install on the user's machine alongside your software. The installation of the CodeMeter Runtime Service can happen as an invisible part of your software installation process. The CodeMeter Runtime Service is available for Windows, Linux, and OS X.

The CodeMeter Runtime Service organizes all connected CmDongles and all available CmActLicenses and provides the licenses for your software.

Image 5: CodeMeter in a network environment



The CodeMeter Runtime Service also acts as license server in the network. The user only installs the CodeMeter Runtime Service on a server in the network, configured as the license server for that network. The software then communicates with a local installation of the CodeMeter Runtime Service, which in turn communicates with the network server's CodeMeter Runtime Service that manages and allocates the available licenses.

Let Us Count That for You: License Quantity

Every license in the CodeMeter universe has a stated license quantity, defined by the software vendor when the license is created. The standard quantity is one.

When you integrate CodeMeter, you determine the manner of counting in your software. You can choose between "per access", "per machine," and "no count." All licenses, whether on a CmDongle, a local CmActLicense, or a license server, are treated completely alike.

Per access - UserLimit

Using the "per access" count, one license is flagged as used for each access (API command CmAccess2) to be released once the access ends (API command CmRelease). Each license can only be used for the number of times allowed by the license quantity value.

Per machine - StationShare

Using the "per machine" count, CodeMeter automatically records certain details about the software environment (session, IP address, process ID…) and transmits them to the CodeMeter Runtime Service. This information is then used to automatically identify each machine, each session on a terminal server, or each virtual machine as a separate entity. A license with a license quantity of three, for instance, can be used by two terminal servers and one virtual machine at the same time, but as often as needed in each of these sessions or the virtual machine.

Automatic Release

By using the process ID, CodeMeter Runtime Service detects whether the software is still active or not. Even if you forgot to include a function for releasing a license after use in your software, or in the unlikely case that your software crashes, the CodeMeter Runtime Service will detect this and automatically release the license.

Local License

A license quantity of zero has special meaning: it represents a local single-user license. It is counted as a license quantity of one, but the license, e.g. the CmDongle or the CmActLicense, has to be used on the same real or virtual machine. CodeMeter can automatically distinguish between a real terminal server and a remote desktop. Using a license with a license quantity of zero is not allowed in a session on a true terminal server, but is possible on local machines with a remote desktop.

Licenses on Network License Servers

The CodeMeter Runtime Service is installed on a server in the network and configured to act as a network license server. The CmDongle is hooked up to this machine, or the CmActLicense is activated and linked with the server by means of the specific traits of the server.

All available licenses on the license server are immediately available for use in virtual machines or on terminal servers. The license quantity allows the network license server to count the allowed number of physical or virtual machines or sessions on terminal servers.

As software publishers, you only need to provide a license with the right license quantity for your user.

CmDongle: One Dongle, One User

You can configure the CmDongle either as a Mass Storage Device (MSD) or as a Human Interface Device (HID). Since this process relies on a standard driver, the unit can be connected to a virtual machine in all current operating systems. Encrypted communication ensures full security when using a standard driver for either HID or MSD.

CmDongle limited to exclusive mode

If the user uses a USB device (such as a CmDongle) on a host with multiple guest systems, typical virtualization software will allow either exclusive or shared modes. In the exclusive mode, the USB device is only available to a single guest or the host system itself, whereas the shared mode allows several systems to access the same USB device.

The CodeMeter Runtime Service on a guest system detects and uses only CmDongles that have been connected exclusively to that guest system. Any shared CmDongles are automatically locked out. This makes the simultaneous use of a CmDongle on multiple guest systems impossible.

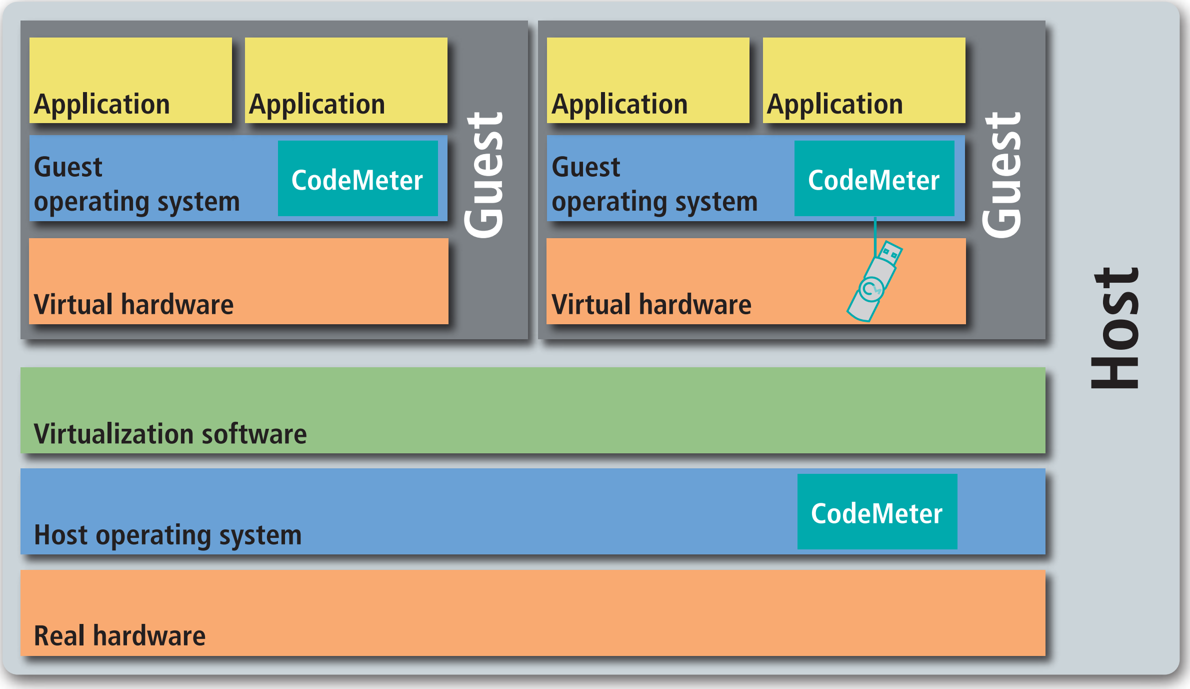


Image 6: The CmDongle runs exclusively in one single guest – The use of licenses is permitted.

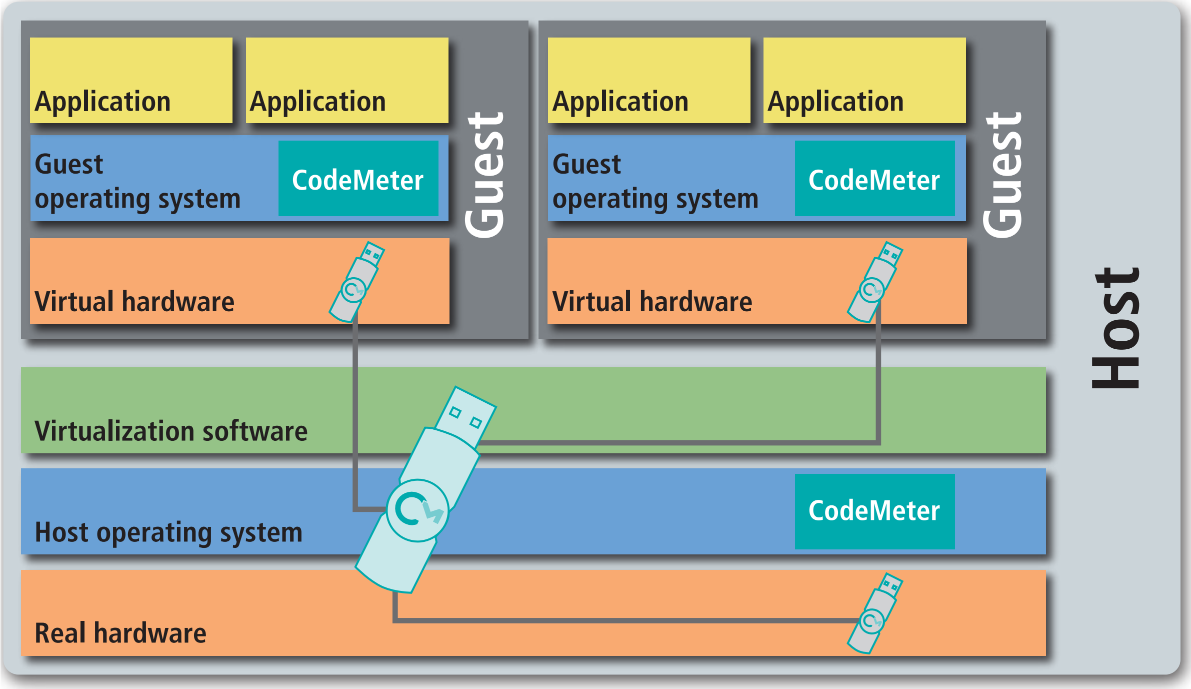


Image 7: A CmDongle in a shared environment – The use of licenses is not allowed.

No multiple use of CmDongles

What happens when CmDongles are passed through from guest system to guest system? Again, the CodeMeter Runtime Service and every CmDongle come equipped with automatic defenses against that. The CodeMeter Runtime Service can handle multiple CmDongles and CmActLicenses, but every single CmDongle is used exclusively by a single CodeMeter Runtime Service. This is achieved by setting a specific parameter when the CodeMeter Runtime Service and the CmDongle establish encrypted communication. If the CmDongle is then connected to a different CodeMeter Runtime Service, this parameter is broken. The license managed by the original CodeMeter Runtime Service is automatically released, and your software can respond accordingly.

Another mechanism ensures that the fast or automated reconnecting of CmDongles (either in terms of switching virtual machines or in a reverse USB hub) can be distinguished from normal operations and detected as the attack it is. In such cases, the CmDongle is automatically locked out for five minutes.

As software publisher, you can rest assured that CodeMeter does everything automatically for you.

CmDongle on a Host System

On host systems that use standard operating systems like Windows, Linux, or OS X, the user can install the CodeMeter Runtime Service on the host system itself, configured as a network license server. For this purpose, the CmDongle remains connected directly to the host system.

As long as the guest system has a TCP/IP connection with the host and the license has a license quantity of one or more, software on the guest system can behave like software on a client in the network and use one license on the host's network license server. That network license server automatically makes sure that the same license is not used more times than allowed by the defined license quantity. With a license quantity of one, the license can be used by only a single guest system at a time.

As software publisher, you provide the licenses with the license quantity of your choosing (typically, a quantity of one) for the user.

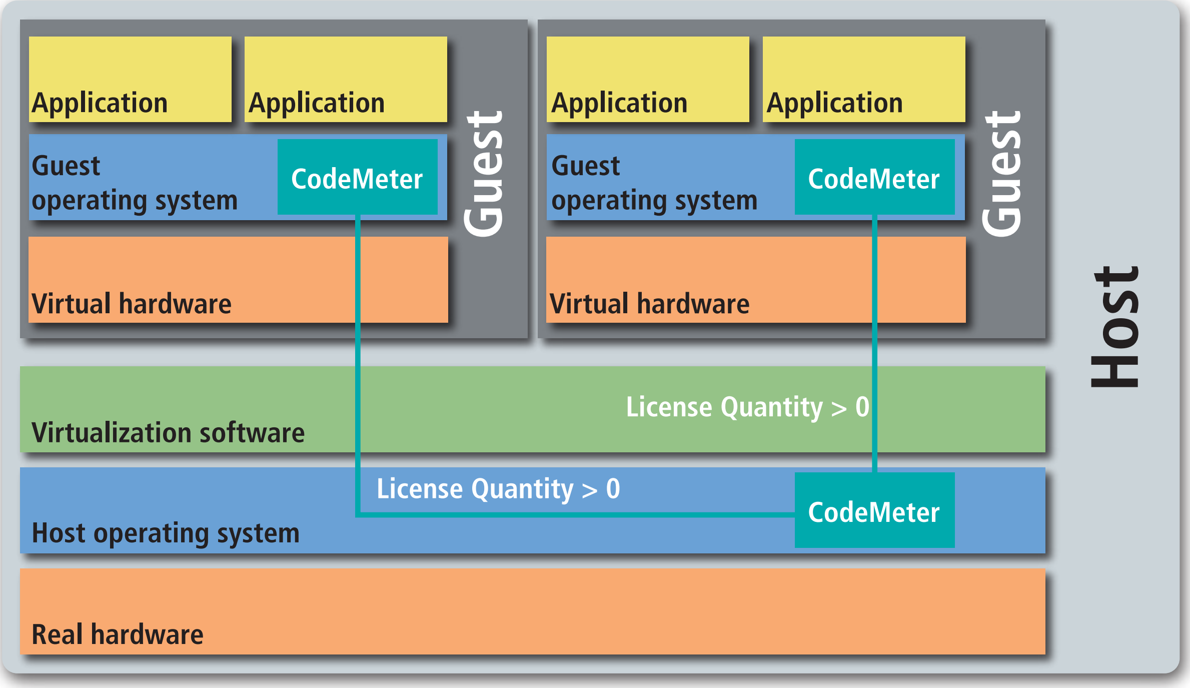


Image 8: License server on the host system

CmDongle on USB-over-Ethernet

A CmDongle can be used in a virtual environment by means of a USB-over-Ethernet device even if the virtual machine allows no direct feed-through of a USB connection.

The same rules apply as when feeding through a USB connection directly to the virtual machine. The CodeMeter Runtime Service allows any CmDongle to be used only for a single machine at a time. It detects when the CmDongle is disconnected and automatically releases the license for the software to respond. A CmDongle plugged to many devices in quick succession is considered an attack and leads to a 5-minute lockout of the unit.

Again, you as the software publisher can be safe in the knowledge that CodeMeter handles everything automatically for you.

CmActLicense on a Host System

A CmActLicense on a host system behaves similar to a CmDongle. The user installs the CodeMeter Runtime Service and configures it as a network license server on the host system.

In this case, the fingerprint of the CmActLicense's binding to that system is created by referencing the real hardware features of the host system. CodeMeter SmartBind® determines many different traits and features of the hardware, prioritizes them by their validity, and creates the fingerprint. The CmActLicense you produced is then bound to the host system and can be used only by that system or provided to other machines or guest systems by a network license server on the host system. By determining the license quantity, you decide whether the license can be used only locally on the host, or also as a network client on a guest system.

As software publisher, you also determine how tolerant the CmActLicense is when it comes to changes to the host system hardware by choosing between "loose," "medium," or "strict" settings.

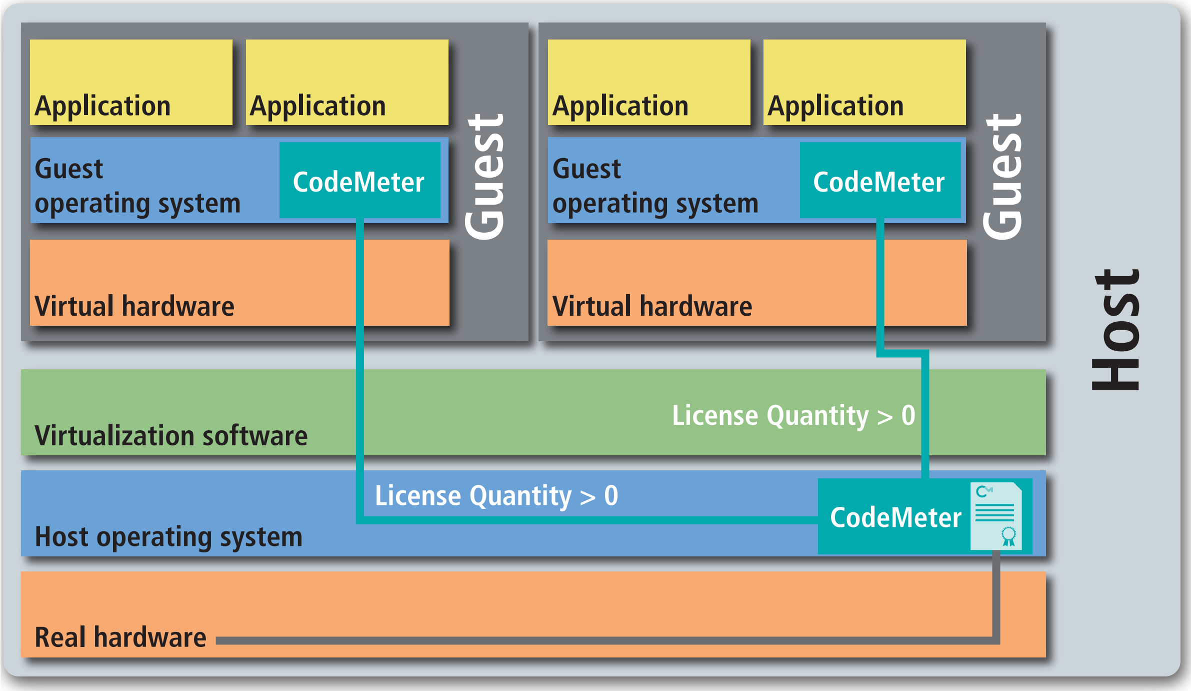


Image 9: CmActLicense bound to the host system

Users cannot use the same CmActLicense in each guest system as the host, even though they share the same hardware. CodeMeter automatically prevents the proliferation of licenses by users trying to use the same CmActLicense in a guest system on the same host.

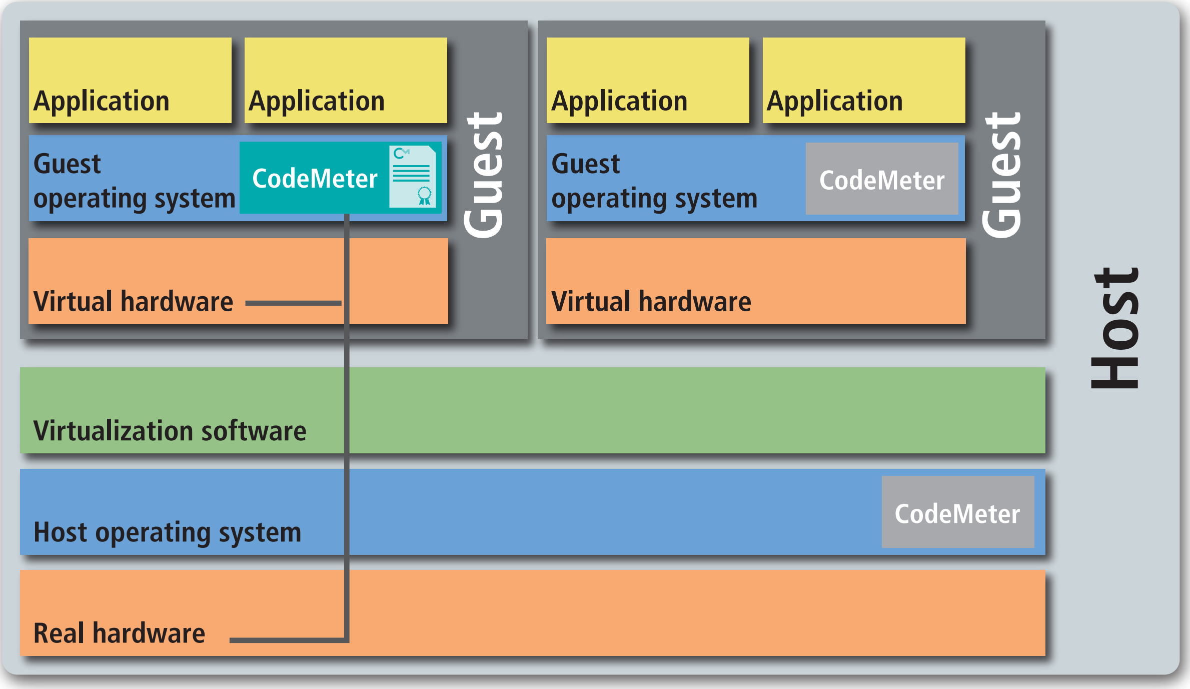
CmActLicense on a Guest System

A CmActLicense is capable of being activated on a guest system. As the software publisher, you decide whether you allow or prohibit this.

SmartBind – A custom recipe

The CodeMeter Runtime Service detects automatically whether it is on a guest system. When identifying and prioritizing the different hardware features, CodeMeter SmartBind uses a custom formula, chosen specifically for virtual environments, which gives much higher priority to features that relate to the underlying real hardware than to features that are only virtual. Features that change when moving to a different machine are also given such higher weighting.

Image 10: CmActLicense in a guest system



Protecting against cloned guest systems

CodeMeter SmartBind offers a CmActLicense maximum protection against the cloning of entire guest systems. When using the tolerance settings “medium” or “strict,” SmartBind automatically detects that the guest system has been copied to a different hardware and flags the CmActLicense as corrupt and unusable. Since the fingerprint is included as a cryptographic key in CodeMeter protection, the CmActLicense cannot simply be “repaired” by patching a query – without the correct hardware features; the CmActLicense cannot be used anymore.

Moving the guest system

If a guest system is moved within the same host system, the CmActLicense remains valid. This means that any changes in the configuration introduced by the user will not automatically mean a support incident for you as the software vendor. This represents no threat for your business, since a moved guest system can normally not be used multiple times on the same host system.

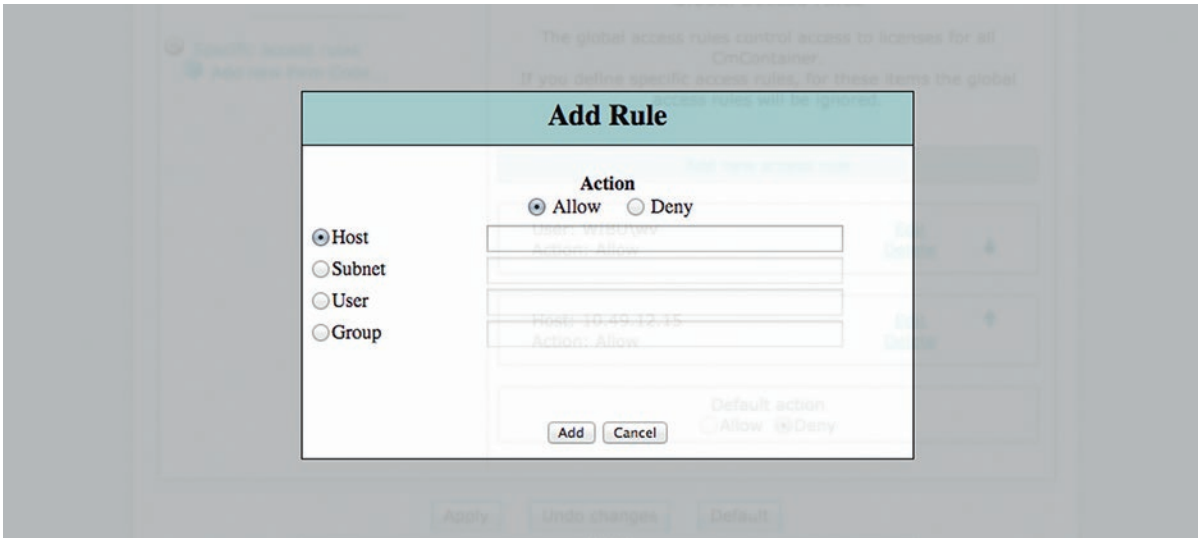
Moving a guest system to another host system has two different aspects to be considered. It is a potential threat, since the same guest system and, by implication, the same license would be present in duplicate form. At the same time, it constitutes the essence of a high availability solution. As the software publisher, it is up to you to decide on the configuration of CodeMeter. CodeMeter SmartBind set to “medium” or “strict” will detect any move to a different host system with better than 98% reliability. This is the best detection rate allowed by current technology.

By setting SmartBind to “loose” or using a weaker bind, such as a “random number” or “IP address,” you can determine that a license on a guest system can be taken to a different host system. This gives your clients the ability to establish a simple high availability solution.

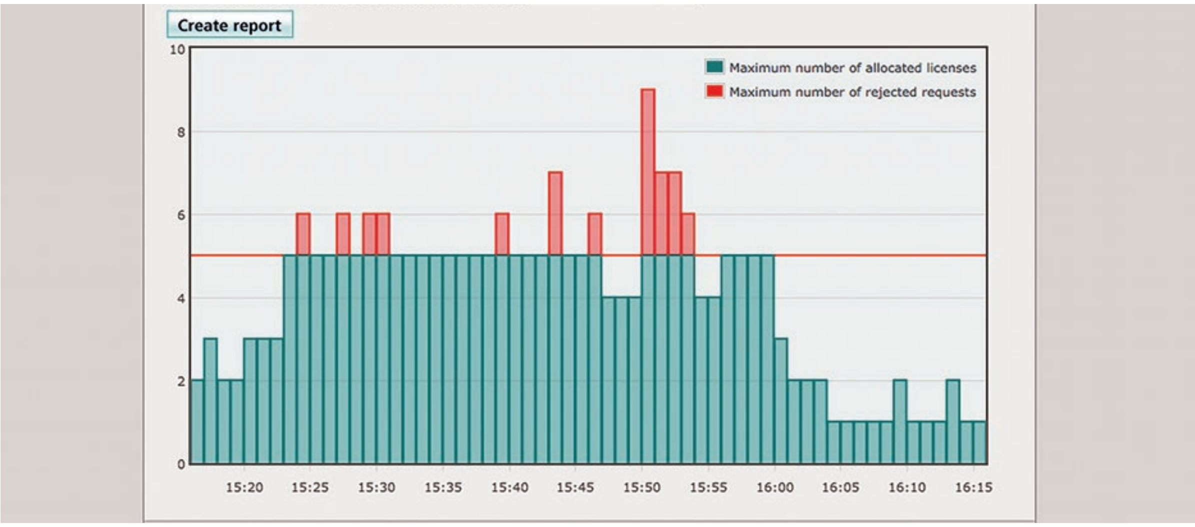
License Management for Users

CodeMeter allows the user of your software to reserve licenses for specific machines, users, or user groups in the active directory. By doing so, the user can make sure that only authorized personnel can access the available licenses. This can prevent unauthorized people from “hogging” licenses, especially when the protected software and the CodeMeter Runtime Service are both kept on a terminal server.

The user can allocate floating network licenses flexibly and directly to named staff members. For example, ten available licenses could include three licenses for the support team, four licenses for the development team, and a further three licenses for free use. The access can also be limited to specific machines, users, or groups. A defined maximum number states how many of these machines or people can use the licenses.



With the detailed information about usage times, the user can monitor how licenses are used and detect any bottlenecks or unused reserves in the available resources.



Terminal Server Client

Individual use cases need the license to be stored on the terminal server client. In such cases, the CodeMeter Runtime Service is installed on the client and configured as a network server.

The protected software on the terminal server is given the IP address and name of the client and establishes a link with the license server stored on it. By controlling access to the client, the user can make sure that the license is indeed used only by himself. On the terminal server's side, this setup requires only a direct TCP/IP connection to the client via port 22350.

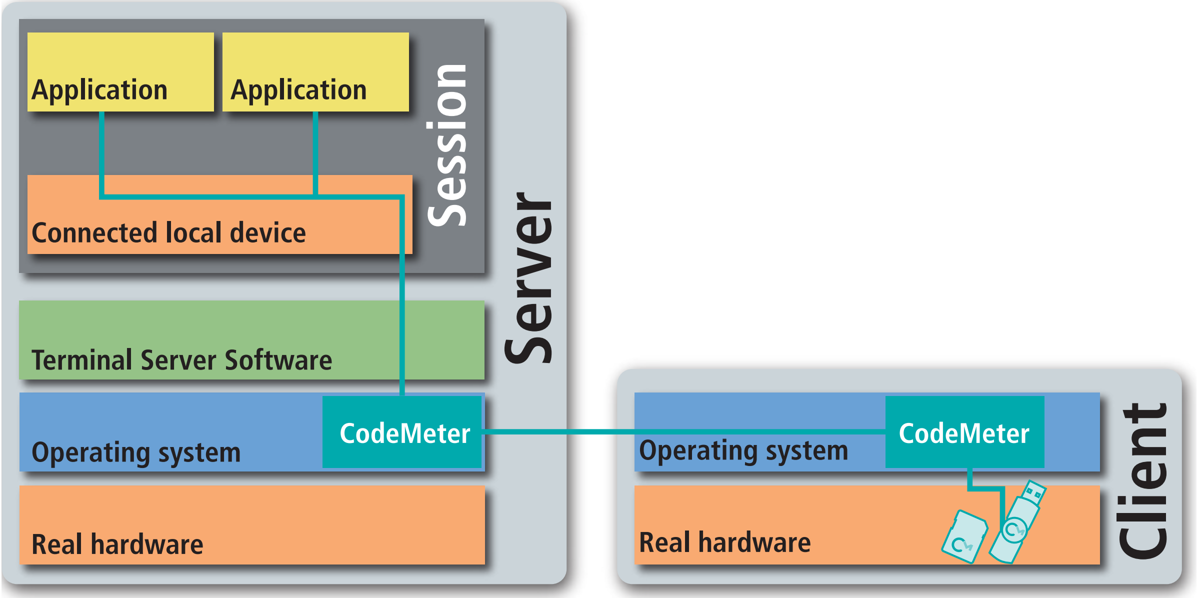


Image 11: CmDongle on a client with high availability and security

High Availability and Security

High availability in a non-trusted environment requires a networked license server with 2-of-3 redundancy.

Your user receives three identical and related network license servers from you. Your software links up with all three servers. Two servers have to be available at any one time, with the right licenses on all available servers. This ensures that your software will remain available even if one server is lost.

You can equip the three network license servers either with a CmDongle or a CmActLicense or with a combination of both. When using a CmActLicense, you can define whether the network license server is allowed to run on a real system or a virtual machine and how much tolerance CmActLicense should allow when changed or moved.

Conclusions

CodeMeter is fully equipped for use in virtual environments and on terminal servers and offers a ready-for-use solution for any realistic use case.

- CodeMeter is a single solution for real and virtual systems.
- CodeMeter offers top protection against the abuse of license.
- CodeMeter is easily integrated in your software.
- CodeMeter counts the use of your licenses as you require.
- CodeMeter can be customized flexibly to match your unique needs.

CodeMeter gives you full control over your business and makes your licensing models for virtual environments as versatile and secure as licenses for real hardware.

Headquarters

WIBU-SYSTEMS AG
Rueppurrer Str. 52-54,
76137 Karlsruhe, Germany
Telephone: +49 721 93172-0
Fax :+49 721 93172-22
sales@wibu.com | www.wibu.com

WIBU-SYSTEMS Branch Offices

WIBU-SYSTEMS (Shanghai) Co., Ltd.
Shanghai: +86 21 556 617 90
Beijing: +86 10 829 615 60
info@wibu.com.cn

WIBU-SYSTEMS NV/SA
Belgium | Luxembourg
+32 3 400 03 14
sales@wibu.be

WIBU-SYSTEMS sarl
France
+33 1 73 03 04 91
sales@wibu.fr

WIBU-SYSTEMS USA, Inc.
USA: +1 800 6 Go Wibu
+1 425 775 6900
sales@wibu.us

WIBU-SYSTEMS LTD
United Kingdom | Ireland
+44 20 314 747 27
sales@wibu.co.uk

WIBU-SYSTEMS BV
Netherlands
+31 74 750 14 95
sales@wibu-systems.nl

WIBU-SYSTEMS IBERIA
Spain | Portugal
+ 34 91 414 8768
sales@wibu.es

5062-005-01/20140910

WIBU-SYSTEMS AG (WIBU®), a privately held company founded by engineers Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative technology leader in the global software licensing market.

In its mission to deliver unique, most secure and highly flexible technologies to software publishers and industrial manufacturers, Wibu-Systems has developed a comprehensive, award-winning suite of hardware- and software-based solutions incorporating internationally patented processes dedicated to the integrity protection of digital assets and intellectual property. Wibu-Systems' product portfolio addresses a wide variety of application delivery models, including PCs, mobile, embedded automation, cloud computing, SaaS, and virtualized architectures.

Through its motto "Perfection in Protection, Licensing and Security", Wibu-Systems is standing up for ethically produced software and reinforces its dedication to eradicate software counterfeiting, reverse-engineering, code tampering, as well as device and smart factory sabotage, espionage and cyber-attacks.

Headquartered in Karlsruhe, Germany, Wibu-Systems holds subsidiaries in Seattle, USA, as well as in Shanghai and Beijing, China; the company also has sales offices in Belgium, France, the Netherlands, Portugal, Spain, the United Kingdom and a capillary world distribution network.

SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU
SYSTEMS