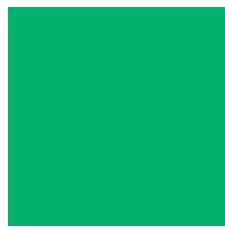


€MBEDDED 4 MAGAZINE



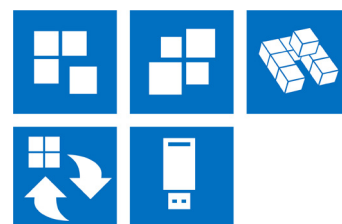
Windows 10 IoT

10

Enterprise Core



Elbacom
Embedded Toolkit



ECM

tutorial

The configuration of the
Unified Write Filter



Servicing Model

Learn about the changes in the new Windows 10
Servicing Model.

Astro COAs

See what has changed with the new Astro
Certificates of Authenticity.

do you need more **embedded** news?



read our Embedded Magazine #1, #2 and #3 online at
www.elbacom.com/magazine

editorial



Sylvain Ekel

Microsoft OEM Technical Sales
Windows IoT EMEA Manager

The Internet of Things has gained tremendous traction in the past few years, and we have seen an unprecedented wave of innovation across all industries, driving digital transformation that is impacting all types of companies and business models.

Microsoft and its partners are in the forefront of this transformation, which requires solid platforms to build their solutions. From ThyssenKrupp elevators, to Rolls-Royce aircraft engines to addressing the world's water challenges with Ecolab, our partners are leveraging Microsoft's IoT platforms to build their solutions.

There are many reasons for our partners to work with Microsoft - openness of the platform, richness of services and products, partnership opportunities, and our overall ability to provide a connected, secure and productive end-to-end platform.

We are investing in open solutions for IoT. For instance, our Azure IoT client and gateway SDK are highly portable, and support a variety of languages and platform, and are all available on GitHub. This create a real choice for our partners to maximize their existing investments and reuse their existing data and processes.

Partnerships are inherent to the Microsoft strategy. From our Cloud Solution Provider programs, to our Microsoft Azure Certified for IoT program our partners can get started on their IoT projects quickly by connecting them with an ecosystem of partners that have offerings that can easily connect to the Azure IoT Suite.

Digital Transformation today is being enabled through connected devices – collectively referred to as the Internet of Things (or IoT). Whether gathering data, manufacturing components, monitoring security, enabling productivity on-the-go, or fulfilling one of countless other ever-evolving needs, the edge intelligence provided by connected IoT devices and smart endpoints is becoming the centerpiece of Digital Transformation across industries and around the world. With the balance of IoT computing shifting toward edge intelligence, successful IoT solutions will increasingly demand robust edge computing capabilities, supported by the base of our IoT offerings: our Windows 10 IoT line of products.

Providing connectivity for devices out of the box while giving you the choice of how your device connects. We have support and partnerships with OPC-UA and OCF. We have heavily invested in Windows 10 security features, with encryption, secure and measured boot, which is illustrated by our virtual-based security features. In addition, our platforms are more productive than ever, following the application development investments on the Universal Windows Platform, our Azure APIs and SDKs, as well as technology such as Microsoft Cognitive Services, building the road for the innovative devices of the future.

Microsoft has also dramatically improved the accessibility of Windows to power your Internet of Things devices, illustrated by Windows 10 IoT Core, a low footprint, locked-down operating systems, available for free and allowing you to develop with the latest and greatest development tools.

With this, I wish you to enjoy this Elbacom Embedded Magazine as much as I enjoy reading them myself, to learn and drill down, with Wolfgang Unger and his team, on some of the key technologies available today from Windows IoT!

Sylvain Ekel

Windows IoT Core for your Devices

<https://www.windowsforiotdevices.com/>

Azure IoT Suite

<https://azure.microsoft.com/en-us/suites/iot-suite/>

Ecolab - Solving global water challenges with Microsoft cloud technologies

<https://customers.microsoft.com/en-US/story/ecolabcustomerstory>

ThyssenKrup AG – The Internet of Things gives the world's cities a major lift

<https://customers.microsoft.com/en-US/story/the-internet-of-things-gives-the-worlds-cities-a-major>

Rolls-Royce and Microsoft collaborate to create new digital capabilities

<https://customers.microsoft.com/en-US/story/rollsroycestory>

6

Page

Embedded News



7

Page

Astro COAs

Windows 10 IoT
Enterprise

Lockdown Features

8

Page

12

Page

Windows 10 IoT
Core Pro

20

Page

Windows 10
Servicing Models

Content



?

22

Tutorial

Page

16

Page

Elbacom
Embedded Toolkit



Windows
Offline Configurator



Windows
Deployment Tool



DISMUI



Recovery Creator



Media Creator

Embedded
Configuration
Manager

18

Page

21

Page

Industry 4.0



EMBEDDED NEWS

The new Elbacom website is online

We have relaunched our website with a new modern design. You will always find the latest information about Windows IoT/Embedded products there. It also features a new customer area that is filled with important information about Windows IoT/Embedded products. Please also check out our events page so you do not miss the next events in your area!

Visit our website at www.elbacom.com

Elbacom Embedded Toolkit updated to v2.5

We released a big update for our Elbacom Embedded Toolkit. All tools have been updated to support Windows 10 IoT Enterprise 2016 LTSC. Please check page 16 to see an overview of the most important changes.

We now also offer an evaluation version of the toolkit. If you are interested in testing the latest version, please contact us!

Value-based Pricing Model

Microsoft has created a new value-based pricing model for Windows 10 IoT Enterprise. Until now Microsoft offered different licenses for different verticals. In the new pricing model the licenses are bound to the computing capability of the devices. That means that low performance devices get a cheaper license than a high-end device.

Find more details on page 11.

CLA 6.0 extended

Microsoft has extended all currently active and new Customer License Agreements (CLA) 6.0 until the August 31, 2021. Any prior versions of the CLA will expire on their current end dates. To renew, OEMs are required to sign a new CLA 6.0. Once signed, the CLA will have the end date of August 31, 2021.

Servicing Model

Microsoft introduced a new Servicing Model for Windows 10. There are different Servicing Models available for the normal customer, for a devel-

oper, for a company and for the embedded channel. Have a look on page 20 to read about the four ways how you can get your updates.

Virtualization

In July 2016, Microsoft has finally introduced virtualization for the embedded channel. It is a per VM licensing model with no limit on the number of VMs. It is allowed to run Windows Embedded 7 & 8/8.1 and 10 as the guest OS. There are two licensing models available depending on the host OS.

There is a difference between qualified host OS (QoS) such as Windows 10 IoT Enterprise,

Windows Server 2012 or their successor products and the non qualified OS (Non QoS).

Non qualified operating systems are all other non-Windows platform and Windows legacy platforms namely Windows 7, 8/8.1 and Windows Server 2008 R2 Standard and Enterprise.

The licenses only differ in pricing. The VM licenses running on non qualified host operating systems are more expensive than those running on a qualified host operating system.

Please contact us for more details about the virtualization for the embedded channel.

Virtualization Business Model

	Qualified Operating System*	Non Qualified Operating System**
OS for Host OS	QoS*	Non QoS**
Virtualization allowed?	Yes	Yes
Virtualization License	Embedded Usage Only	Embedded Usage Only
Price per VM	\$	\$\$
OS for guest OS	Windows Embedded 7 & 8/8.1, 10	Windows Embedded 7 & 8/8.1, 10

Astro COAs

All embedded devices must have a valid license sticker attached to proof that they are licensed correctly. These license stickers are called Certificates of Authenticity (COAs). There are different COAs types available:

Windows Embedded Standard and Windows Embedded Compact use the Thumbnail COA which is displayed below.

Windows Embedded Enterprise and Windows Embedded Server use the regular size COAs that can be found on regular desktop machines as well.

You will receive the Certificates of Authenticity in an envelope. The COAs are located on a strip where they can be easily removed to affix them on the devices.

The Astro COAs are available since January 2016. These thumbnail COAs will be the same size as the old ones. But the content of them will be a little bit different. The full product name is now only visible on the envelope. The new thumbnail COA only shows the product group (2) like "Win Emb POSReady" but you will not see a difference between the versions. For example POSReady 2009

and POSReady 7 products will have the same COA.

The full product title (5) will only be visible on the envelope.

If you order two different products of the same group, you can differentiate them by taking a look on the envelope. You can identify your product by the range of the serial number (3) on the COA and envelope later.

There will be also a 2D barcode (1) on the strip. This contains part of the POA of the COA which is also written in a readable format right below the code. This label must not be affixed to the device. You will also find the Microsoft part number (4) on the COA.

Please have a look at our licensing website for more details regarding the changes.

MICROSOFT®

ITEM
7WT-00050



Win Emb Std P 7 EMB ESD OEI (WS7P)

5

Elbacom elektronische Bauteile

B1600999



QUANTITY

10



LABEL ID

123456789



First POA 00012345678100



3

Last POA 00012345678109

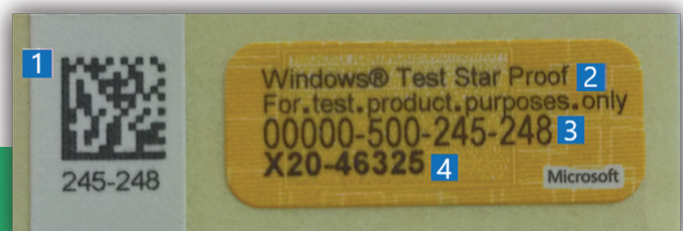


Sales Order: P12345678

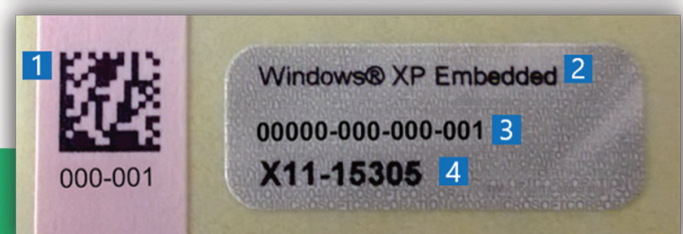
Mfg Date: 1/01/2016 08:15

Site: CZ

Astro COA



Old COA



Windows 10 IoT Enterprise

Windows 10 IoT Enterprise is an operating system specifically designed and optimized for medical devices, automated teller machines (ATMs), industrial automation and any other embedded device. It is based on the new Windows 10 technology with advanced lockdown capabilities, Win32 compatibility and universal windows app support. As the system is based on the full version of Windows 10 it offers full compatibility for applications, apps and drivers (Universal Windows Platform). It is available for the 32-bit and the 64-bit architecture. This article will give an overview about the new Windows 10 IoT Enterprise but also will have a look at the new Embedded Lockdown Features that are included in the OS.

As with previous versions, the new system will be supported by Microsoft for at least 10 years.

Installation

The installation is using the same principle as Windows Embedded 8.1 Industry Pro. Windows 10 IoT Enterprise uses the same setup as the retail version. This allows to use the same known

tools to install and deploy the operating system on the devices. Once this is done the installation can be cloned onto other devices.

The second tool, the Imaging and Configuration Designer allows creating pre configured systems to run the setup completely unattended. Also OOBE (Out-Of-The-Box-Experience) and possible application setups can be automated with it. The configuration including the settings will be stored in ppkg file that is called "provisioning package". This file includes the configuration with XML files. This provisioning package can be used for two purposes:

You can use the file to save your configuration for the Imaging and Configuration Designer (ICD) or you can deploy the file to an already installed OS to do the configuration.

Different SKUs

There are three different SKUs of the Windows 10 IoT Enterprise 2015 LTSC

are different SKUs which must be used depending on the field of application. The first version is the SKU called "Windows 10 IoT Enterprise". This version is used for ATMs, industrial devices or medical devices. The next version is the SKU called "Windows 10 IoT Enterprise for Retail and Thin Client" which is the SKU for point of service (POS) devices like cashier systems, kiosks or digital signage devices. This makes it the direct successor of Windows Embedded 8.1 industry Pro Retail. The last version is the SKU "Windows 10 IoT Enterprise for Tablets" which is, as the name says, for tablets with a specific form factor.

Windows 10 IoT Activation

The activation changes a little bit with Windows 10 IoT because there is mostly no activation anymore. You do not have to activate the Windows 10 IoT Enterprise version - but only if the device never connects to the

internet.

Another benefit is, that devices will not show activation reminders and they will not reboot in case of the device is not yet activated. The functionality of the device will never be compromised!

If the Windows 10 IoT Enterprise device connects to the internet - it should be activated. As known from Windows Embedded 8.1 Industry Pro, Windows 10 IoT Enterprise implements ePKEA. This means that only one product key must be entered when creating the master image. After cloning, the key must not be changed - the device only needs to be activated once.

Activation can be automated easily via PowerShell scripts and can also be triggered from your own application.

Please contact us if you would like to receive the scripts or more details regarding Windows Activation.

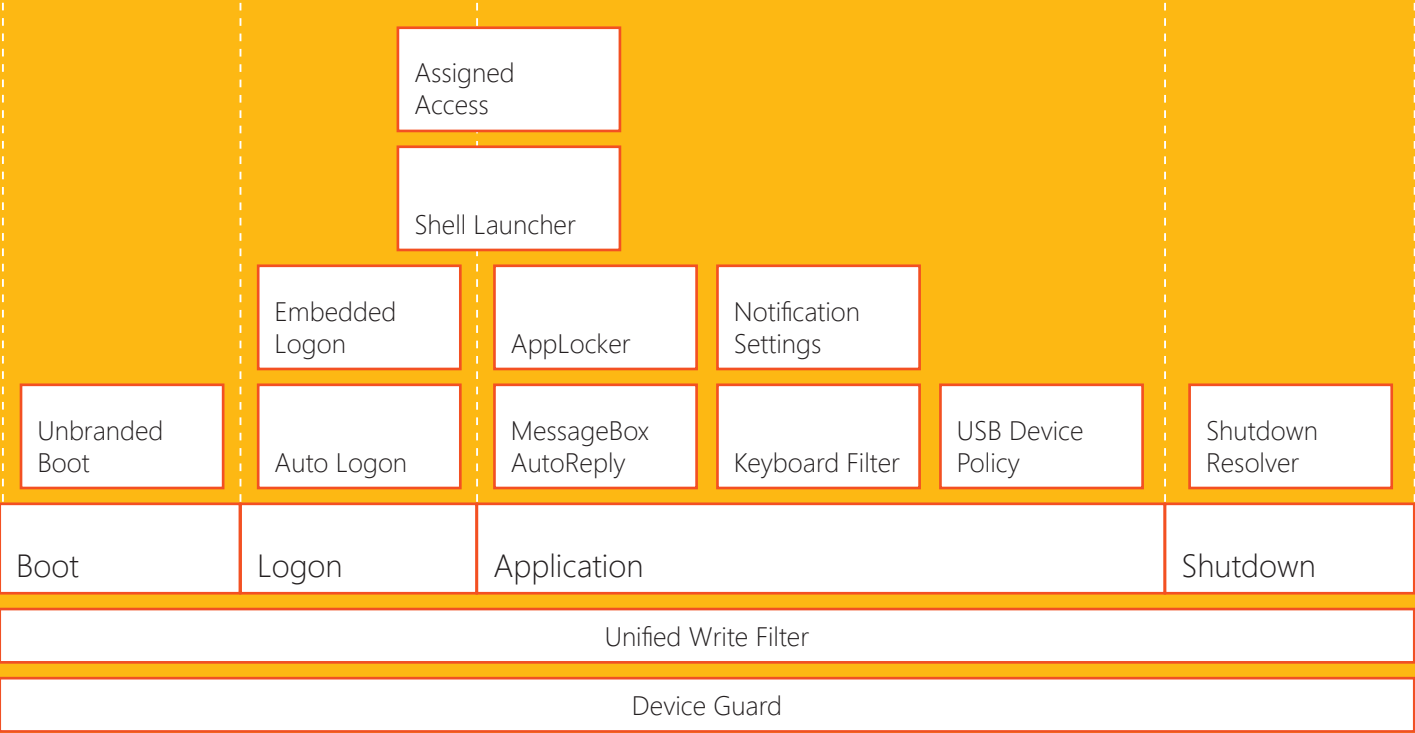
Windows 10 IoT Enterprise 2015 LTSC

EPKEA

PKEA

Embedded Lockdown Features

The Embedded Lockdown Features of Windows 10 IoT Enterprise offer branding options and protection for every cycle in the device runtime. The Unified Write Filter can protect the device from unwanted changes to the disk - whereas the Unbranded Boot, Embedded Logon and Assigned Access or Shell Launcher can help brand the device to a corporate design and hide the Windows logos completely. The Device Guard is the most secure way to protect a device at the moment.



Brand the Device

The Embedded Lockdown Features can be used to secure a device or to make the Windows operating system completely invisible behind an application. This overview shows you all Embedded features that are included in Windows 10 IoT Enterprise.

Unbranded Boot

The Unbranded Boot feature makes it possible to suppress the Bootlogo, the Status Ring and the Status Text during the boot. This can be done one by one or you can also hide all together. If the device is an UEFI supporting device, it is also possible to change the bootlogo in the firmware to your own one. There

is the possibility to block the access to the F8 and the F10 menu during the boot. This prevents starting the recovery mode or booting another system or device through the bootloader. Another feature is that you can show a black screen instead of a bluescreen. But in this case the device will create a dump file for you in the background and the device will make an automatic restart so nobody can recognize the crash of the device.

Embedded Logon

With the Embedded Logon feature it is possible to hide the login screen completely if there is an automatic logon configured. This allows you to

show an application right after the boot screen. The features also allows you to customize the log-in screen by hiding some elements.

Shell Launcher

With the Shell Launcher, you can open a classic Win32 program automatically. The Shell Launcher changes the classic desktop shell to another program. Additionally you can configure what should happen if the program crashes or if someone closes the program. In this case the device can do a restart or shut down. It can also just restart the device or do nothing. There is also the possibility to configure different shells for different users. That means that you can

set up for example two accounts and use one account with your own program as shell and the other account with the classic desktop shell for administrative things.

Assigned Access

The similar feature to the Shell Launcher for modern applications is the Assigned Access. This feature provides a direct boot into a modern application. There is also a way to hide notifications and you can block some touch or mouse gestures that are required for example to open the action center. There will be also some key combinations blocked but it is still possible to get out of the application by using a specific breakout key.

The breakout key will bring you to the logon screen if you press it five times in a row.

AppLocker

This feature helps you by blocking applications which you do not allow to run. You can configure this by creating a black- or a whitelist. You can allow an application to run for example by the path of the execution file, by a hash or you can only allow application from a specific manufacturer to run.

USB Device Policy

With the USB Device Policy it is possible to protect your system from unwanted USB devices. There is a way to block a USB device based on the device ID. You can also block devices based on a device class, for example all bluetooth devices, or you can block all removable devices in general. The policy can be bypassed for administrators so they can still connect any device to the system during maintenance work.

Unified Write Filter

One of the most important features in the embedded channel is the Unified Write Filter. This filter protects the hard disk from unwanted changes. If you activate this filter, new data will be only written in the RAM and not to the physical hard disk. So all changes will not affect the hard disk and will be gone after a restart.

But in case, there is a file or a folder that must be updated on the disk, like a database for example, you can create exclusions for specific files or folder. There is also a servicing mode available that lets you update the device with an activated filter. Servicing mode restarts the device into an unprotected mode. During this, the Unified Write Filter is deactivated and there will be a fullscreen screensaver which you cannot exit. In the background your device will do all windows and application updates. When finished, it will restart again and the Uni-

fied Write Filter will protect the device again.

Device Guard

The Device Guard is a combination of many security features that Microsoft created in the past. With Device Guard you can store a certificate in the firmware and Windows will only run applications that were signed by this certificate. No other applications can run on the system.

Additionally all applications run in their own virtual memory and they cannot access memory from any another application.

At the moment this is the safest way to run Windows because no viruses or malware can run on the system.

BitLocker

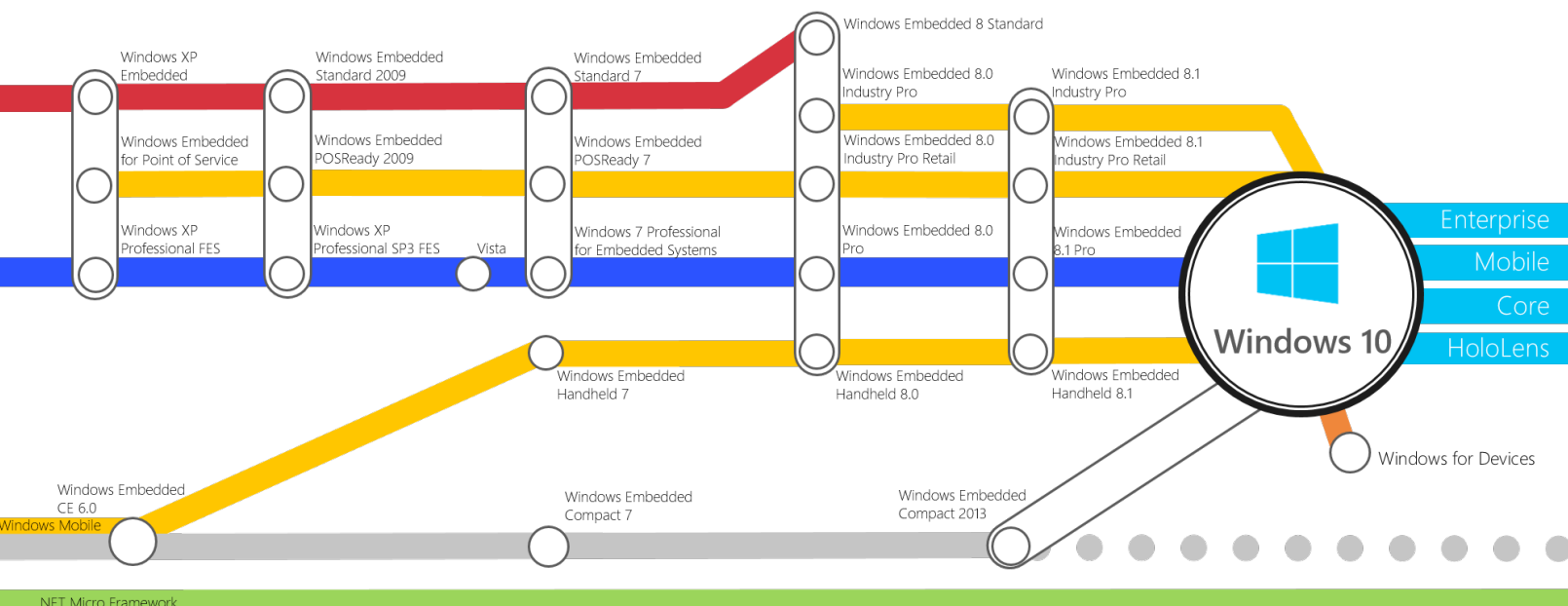
With the BitLocker you can completely encrypt your drive including the hibernation file and the pagefile. There are different possibilities how to use the BitLocker on the device: You can store the encryption key in the

TPM chip - then the disk will only work on this specific device. If someone removes the hard disk it is completely encrypted. But in the device it will boot normally. Alternatively you can also store the encryption key on a removable device. Then the device will only boot if the removable device is connected as well.

BitLocker also supports entering a PIN during boot up - however this is not an embedded-friendly option, as the devices will no longer boot unattended.

Language Packs

Windows 10 IoT Enterprise supports over 30 different language packs (MUIs). If you also count the language interface packages (LIPs) like en-UK or en-US, you can use over 100 different language packs. You have to use at least one language pack but you can use as much as you want. There is no limitation from licensing.



Anniversary Update Windows 10 IoT Enterprise

Windows 10 IoT Enterprise 2016 LTSB & CBB

Microsoft has released the new Windows 10 IoT Enterprise 2016 LTSB version at the end of July 2016. The 2016 LTSB version is based on the anniversary update of the classic Windows and includes some new embedded features in the IoT version. Also the IoT version is now available with Current Branch for Business (CBB) servicing model allowing for more frequent feature updates.

The CBB version also includes all standard applications from the classic Windows like the Edge Browser or the Windows Store application. Also included are Cortana and Windows Hello.

License Upgrade

Customers will be able to upgrade their Windows 10 IoT 2015 LTSB license to the 2016 LTSB or CBB version with a free field upgrade (COA costs may apply). It is also possible to do a field upgrade from any other embedded system to the Windows 10 IoT Enterprise 2016 LTSB or CBB version.

Keyboard Filter

One of the new features is the Keyboard Filter. We already know the filter from Windows Embedded 8.1 Industry Pro but with Windows 10 IoT Enterprise 2016 LTSB & CBB the Keyboard Filter is back. The configuration of this feature can be done via PowerShell (WMI) or the Embedded Configu-

ration Manager (ECM) from Elbacom. Please find more details about the ECM on page 18.

New Pricing

With the anniversary update of Windows 10 IoT Enterprise, Microsoft switched to a value-based pricing model aligned to computing capability. This model replaces the "Retail or Thin Client" SKU for POS devices or separate SKUs for tablets. With the new Windows 10 IoT Enterprise 2016 LTSB or CBB version it depends on the CPU that you are using. There are three different SKUs for the LTSB and three different SKUs for the CBB version. The same model has been introduced for Windows 10 IoT Enterprise 2015 LTSB.

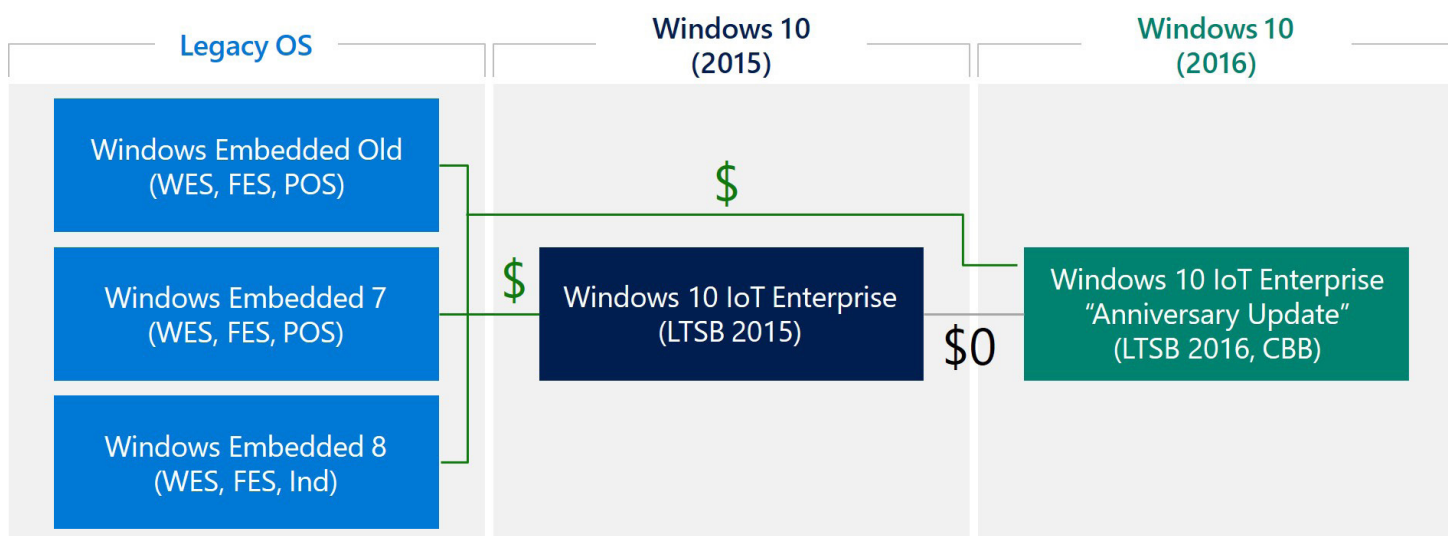
SKUs

The "High-End" SKU is for devices that contain a Intel Core i7, Intel XEON or selected AMD FX models.

The "Value" SKU is for devices with a CPUs such as the Intel Core i3, i5 or AMD R-Series, A10, A8 and the rest of the FX models.

The "Entry" SKU is for devices with a very low computing capability and CPU models like Intel Atom or selected Celeron and AMD E1, E2, A4, A6 or G-series.

The "Entry" SKU has the lowest price, whereas the "High-End" SKU has the highest price. The "Value" SKUs price lies in between the two.



Windows 10 IoT Core Pro

The new Windows 10 IoT Core is a minimized version of Windows 10 that runs on the following devices: The Raspberry Pi 2 and 3, the DragonBoard 410c and the MinnowBoard MAX.

Microsoft already had a minimized version of Windows 8.1 running on small footprint devices such as the Intel Galileo board. Now they have released the final version based on Windows 10 called Windows 10 IoT Core.

Microsoft released this version of Windows 10 at the same time as the Windows 10 IoT Enterprise system.

Windows 10 IoT Core is a great operating system for small footprint devices or as an endpoint for the cloud.

There are many great features included in this version. Some of them are described in the following article.

Operation Modes

Windows 10 IoT Core is designed for only one Graphical User Interface Application (GUI) but it is possible to run as many applications as you want in the background (background workers). You can use a Windows 10 IoT Core running device in two different modes: headed and headless.

The headless mode means that you do not have to connect a display because you can connect to the device remotely. You can use the headless mode if you do not need a Graphical User Interface.

UWP

All applications that should run on Windows 10 IoT Core must be Universal Windows Apps. These are applications are based on the new Universal Windows Platform (UWP). The Universal Windows Platform is a new platform from Microsoft for Windows 10 devices. This means that, if you write an application once based on the UWP, you can use it on any Windows 10 running

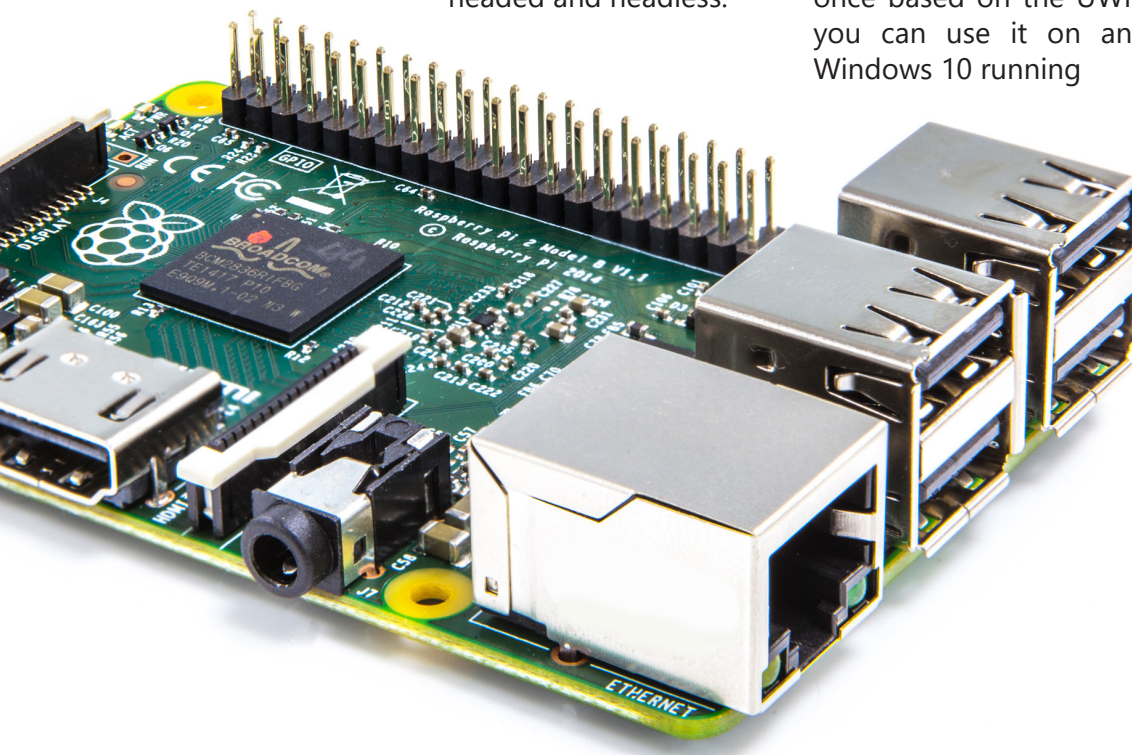
device - it doesn't matter if it is Windows 10 Enterprise, Windows 10 Mobile, Windows 10 IoT Core, Xbox or HoloLens.

Porting

To port existing applications to the Universal Windows Platform, Microsoft designed some tools to analyze the source code of the existing Windows applications. If you use these tools, they will tell you what part of the source code you have to change to build an Universal Windows App.

Architectures

One of the most interesting things is, that this operating system runs on two different architectures. For example: The Windows 10 IoT Core version on the Raspberry Pi 2 and 3 is ARM-based and the Windows 10 IoT Core version on the MinnowBoard MAX runs on x86-based architecture. There is a 32-bit and a 64-bit version available. If you use the x86-based version, it is possible to use the drivers from the classic Windows 10 devices. For the ARM version it is required to compile the drivers.



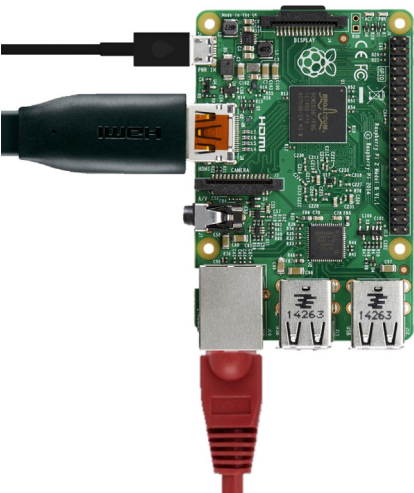
Windows 10 IoT Core Installation and Configuration

The new Windows 10 IoT Core is designed for one Graphical User Interface application and as many applications in the background as you want. But how can you configure all this in this new operating system and how does the installation look like?

Prepare to install

Please prepare a microSD card and get one of the supported devices to can run Windows 10 IoT Core. To install the new operating system, please download the IoT Core Dashboard tool - it will guide you through the installation of Windows 10 IoT Core.

You can download it from windowsondevices.com



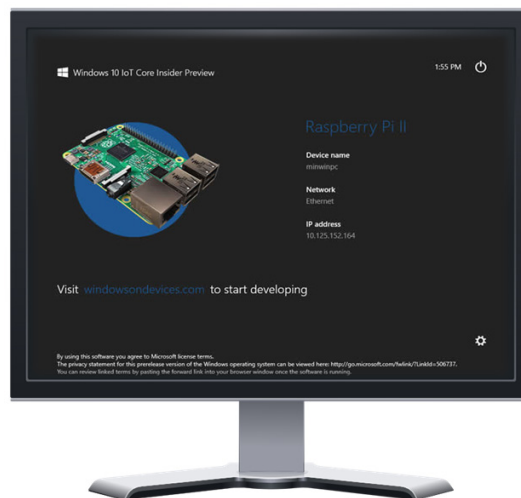
Installation

To start the installation, please run the IoT Core Dashboard and select "Install".

Then you just have to select your device type and the microSD card and hit the "Install" button. After doing this, a file called "Flash.ffu" will be downloaded automatically. This .ffu-file is similar to a .wim file but includes the content of a full disk with the Core system on it. The difference between a .wim-file and a .ffu-file is that a .ffu-file also includes complete disk partitions and not just files.

Now the tool will flash the image on your microSD card. After this has completed, you can hook up your board and start it. The first boot will take about two minutes. Then you will see the Windows 10 IoT Core default application instead of a classic desktop shell.

This default application shows you some details about the device like the name, the IP address or how it is connected to the network. You can configure things like the language, bluetooth or network settings.



PowerShell

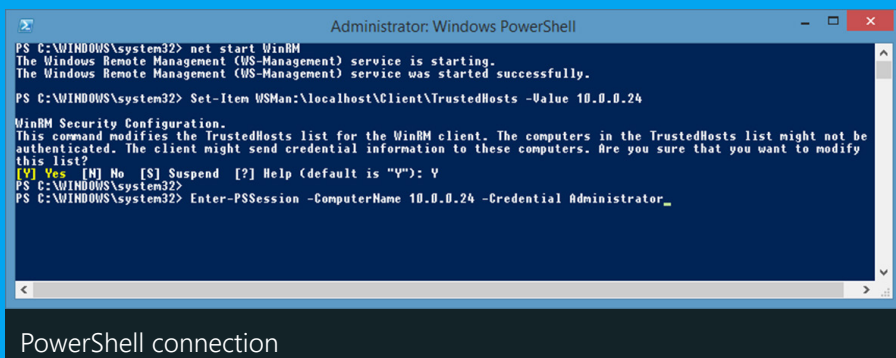
After the installation it is possible to connect to your Windows 10 IoT Core device remotely by using the PowerShell.

You just need to start the PowerShell as an administrator and type in two commands. The first to start the Windows Remote Management Service and the second to connect to the device remotely.

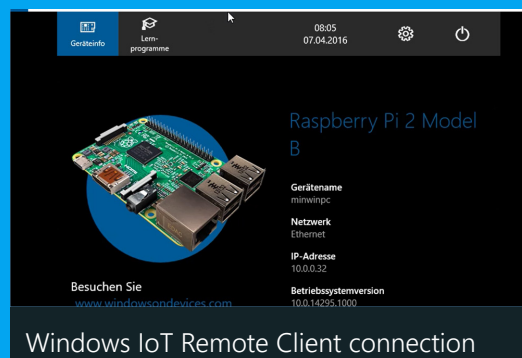
Via this connection it is possible to configure a few things like the name of the device or the password, which is recommended because all devices have the same password after the first boot. You can also retrieve a process list and setup a startup application.

Remote Client

It is also possible to connect to a Windows 10 IoT Core running device remotely with the Windows IoT Remote Client. You can download this application from the Windows Store. The Remote Client shows you a list of all Windows 10 IoT Core running devices in your network and you can select a specific device you want to connect remotely. After the connection is established, you will see the devices screen content and can use your mouse and keyboard to control the device. This allows to run the device headless and still be able to control and configure it easily.



PowerShell connection



Windows IoT Remote Client connection

Windows IoT Core Dashboard & Device Portal

The IoT Core Dashboard allows you to see a list of all Windows 10 IoT Core running devices connected to your network. You can click on a specific device and select "Open in Device Portal". There is a great web interface for your Windows 10 IoT Core device which lets you configure many things much easier than with the PowerShell remote connection.

1. START PAGE

It is possible to do important standard configurations like changing the name of the device or the password of the administrator account here. You can also change the time zone or configure the display resolution and the display orientation here. Many things listed here are also displayed in the default application on the device itself.

2. APP MANAGER

In this section you can configure your applications. You can change the default GUI application and you can do the installation of all applications by just browsing for the AppX files to install them on the device. You can also uninstall applications which you do not need on the device anymore.

3. PERFORMANCE

This point gives you a great overview about the utilization of your device. It shows you the graph

of the CPU and the RAM memory. You can also see how much memory is installed and in use. There is also the graph of the GPU utilization visible if your device supports it and you can take a look on the I/O of the device.

4. DEVICE MANAGER

There is also a simplified Device Manager as on a normal Windows 10 running device. You can update drivers in there and export a list of all devices into a file.

5. NETWORKING

If you have a WiFi adapter you can configure it here. You can also load and save different network profiles and check other network related settings.

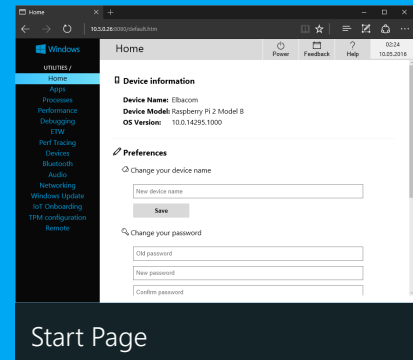
6. WINDOWS UPDATE

Windows 10 IoT Core devices search automatically for new updates.

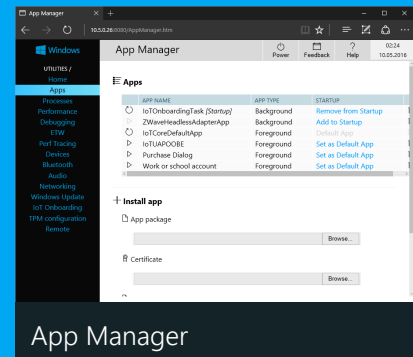
This configuration page lists you all available Windows Updates and will show you some information during an installation progress.

If the device has scheduled an update installation, you can also start the process immediately here.

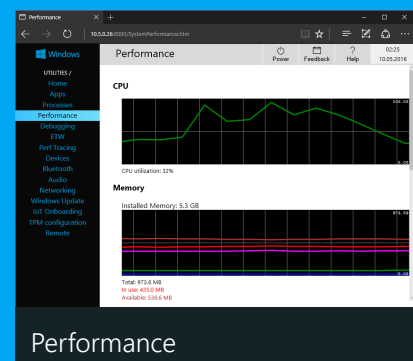
Microsoft is continuously improving the web interface on Windows 10 IoT Core to allow you to set-up the device more easily. The most recent version could already include more than shown here!



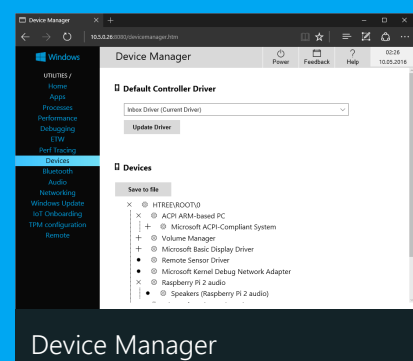
Start Page



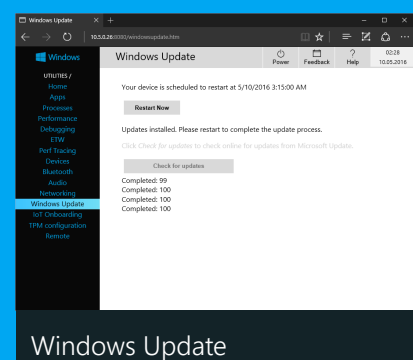
App Manager



Performance






Device Manager



Windows Update

Comparison: Windows IoT Core vs Windows IoT Core Pro

Lets take a closer look on the two different versions of Windows 10 IoT Core. There two different versions available: The normal "Windows 10 IoT Core" version and the "Windows 10 IoT Core Pro" version. Technically they are nearly the same but in general the Pro version has some advantages which are very important for the embedded channel.

Windows 10 IoT Core vs. Windows 10 IoT Core Pro	
LIABILITY	
Windows 10 IoT Core is for makers (hobbyists). That means commercial projects must be registered. They have to sign an agreement for Microsoft. This agreement contains licensing terms which are similar to our ATs and they get very limited liability from Microsoft.	 Windows 10 IoT Core Pro is covered through the Customer License Agreement (CLA).
WINDOWS UPDATE	
In the normal version, you have to install all updates and the devices can update themselves at any time in the field. This is a big problem because if an application doesn't work with the new update all devices are not functional anymore and it is not allowed to deactivate the updates.	 In the Pro version the Current Branch for Business is available. That means that you have control over the updates. You can defer them for at least 4 months and test the updates before you update all your devices. There is also the possibility to deactivate them completely.
LICENSE STICKER	
For the normal version you get no COAs and you have to sign an agreement for the commercial usage for Microsoft.	 For the Pro version you can pay a small fee to receive a Tracking label.

How to get Windows 10 IoT Core Pro

Windows 10 IoT Core Pro can be ordered as OEM Pre-Installation Kit (OPK) from Elbacom. The OPK contains the full installation media.

Visit www.elbacom.com for more information or contact us via email: info@elbacom.com

Option One Windows 10 IoT Core

If being connected to the internet and automatically receiving the latest updates is part of your device scenario, then you can sign up through the Windows 10 IoT Core Commercialization process. All you need is a Microsoft account (formally Windows Live ID). This Windows 10 IoT Core product is well suited for early adopter businesses looking to create and commercialize their innovative devices.

If you are already a licensed partner with Microsoft or indirectly through an authorized Microsoft distributor, you do not need to go through this commercialization process. Contact your Microsoft representative or distributor for more information.

To get started, sign in below to review and accept the commercialization terms.

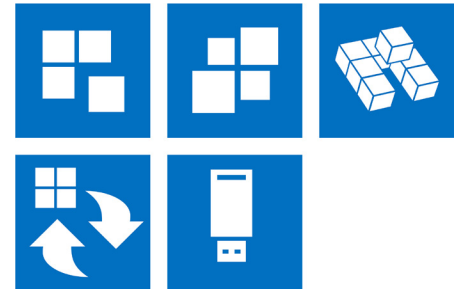
Sign In

Option Two Windows 10 IoT Core Pro

If you want control with fewer upgrades, the flexibility to stage and deploy updates when you want, or even the ability to turn off auto updates then Windows 10 IoT Core Pro is what you need. Contact your Microsoft representative or find a distributor to learn more about licensing Windows 10 IoT Core Pro.

Find a Distributor Near You

Elbacom Embedded Toolkit



As Microsoft Embedded Distributor we get lots of feedback and problem reports from customers about the Windows Embedded products. Over the years we were found out that most of the issues can be grouped into five segments:

1. Installation
2. Deployment
3. Servicing
4. Recovery
5. Updates

With the Elbacom Embedded Toolkit we created a collection of tools that help and improve the image development process radically.

The latest release of the Elbacom Embedded Toolkit includes support for the latest Windows 10 IoT Enterprise 2016 LTSB & CBB versions! This means that all Windows Embedded versions, starting with Windows Embedded Standard 7 are now supported!

The toolkit is now also available in different packages and includes other tools, the Driver Extractor and Keyboard Filter, as add-on!

Each one of the three packages includes a different tool set.

The **EET CREATE** package includes the Windows Offline Configurator, Windows Online Configurator and DISMUI. These are tools for the installation of Windows Embedded/IoT operating systems and also for servicing existing installations.

EET RECOVER includes the Recovery Creator, Recovery Wizard and the Windows Deployment Tool. These are all required tools to easily create master images and customized recovery media.

EET COMPLETE is the complete package that contains all mentioned tools and helps through the complete image development and upgrade cycle.

Every ordered tool ships with a 16GB USB flash device that is bootable. With the USB stick you can immediately begin working

with the Elbacom Embedded Toolkit.

Continue reading to find out more details about each tool included.

Windows Offline Configurator

The Windows Offline Configurator allows the installation of every Windows Embedded operating system on your fast development machine. This can be very helpful if your target device does not have high computing capabilities. In extreme scenarios installations can take 2-3 hours to complete on a low-end target device - whereas the installation with Windows Offline Configurator can finish within 15 minutes on a fast development machine.

The tool is very easy to use - just connect the hard disk of the target device to the development machine and insert the setup media - then launch Windows Offline Configura-

tor. The tool will automatically recognize the setup media and Windows version that should be installed. The user interface will look very similar to the original Windows setup. However it will offer many more options. For example, it allows to fully customize Windows Embedded POSReady 7, Windows Embedded 8.1 Industry Pro and Windows 10 IoT Enterprise 2015 & 2016 LTSB & CBB prior the installation. So you can have the same flexibility as with the fully componentized operating systems. The tool also includes the Out-Of-The-Box experience (OOBE) settings so everything is already configured when you first boot the image on the target hardware. After everything has been configured, the tool asks for the installation tar-

Windows Online Configurator	Recovery Creator	Windows Online Configurator
Windows Offline Configurator	Recovery Wizard	Windows Offline Configurator
DISMUI	Windows Deployment Tool	DISMUI
Driver Extractor	Driver Extractor	Recovery Creator
Keyboard Filter	Keyboard Filter	Recovery Wizard
Media Creator	Media Creator	Windows Deployment Tool
CREATE	RECOVER	Driver Extractor
		Keyboard Filter
		Media Creator
		COMPLETE

get. This can either be the hard disk drive of the target device or you can create a VHD file and install everything into the virtual hard disk. The benefit here is that Windows supports booting from this VHD file - so no further image creation tool is required!

Windows Online Configurator

This tool is similar to the Windows Offline Configurator, however the Online version can be used directly on the target device. The benefits to use this tool instead of the original setup are the advanced customizability and OOB options.

Windows Deployment Tool

After the installation and configuration is done, the next step would be to create a master image. This can be done very easily with the Windows Deployment Tool. After booting from the Elbacom Embedded Toolkit USB device, you can start the tool from the launcher. The tool will guide you through the image creation process and will include several security checks. For example, it will check if the boot manager is missing from the image selection. If so it will ask to add it automatically. The tool will use the Microsoft Windows Image file format (WIM) to store the image. The advantage by using this format is, that it is a file based image. Because of that you can store multiple images

of the same operating system in the same WIM file. The files for the OS will only be stored once because it recognized identical files - this saves a lot of storage!

During the image creation process the Windows Deployment Tool will also save a snapshot of the partition layout which can be automatically restored during deployment.

The deployment process is also very easy. Just select the WIM file and the images within the file that you wish to restore. If the image was created with the Windows Deployment Tool, you can restore the original partition layout. The tool will show a preview of what will be done when recreating the layout. When deploying the image, the tool will also perform additional checks to make sure that the image will boot afterwards. For example it will create a new boot manager in case the image did not contain one.

Recovery Creator

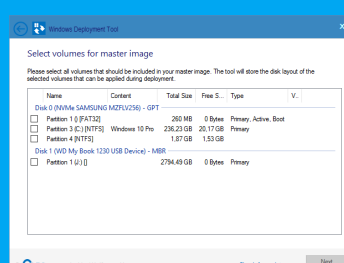
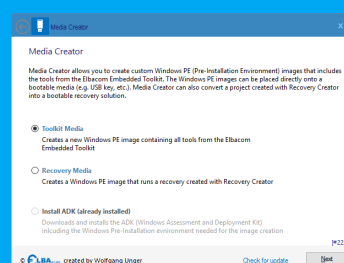
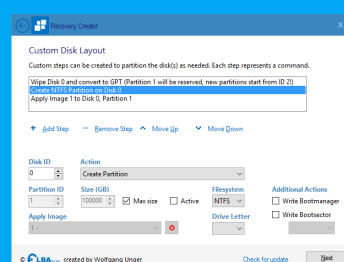
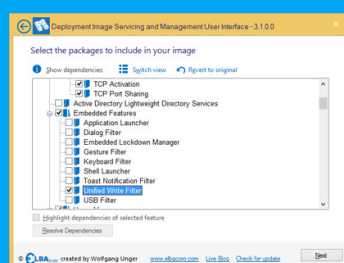
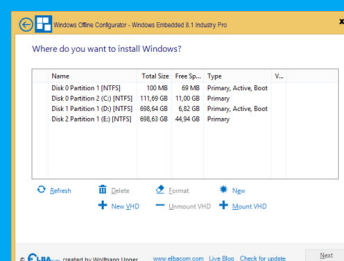
With the Recovery Creator you can easily create a fully customized recovery media. The wizard will guide you through the complete recovery creation process so the media is finished within a few minutes. It allows to specify the wizard pages that should be shown during the recovery and also the image file. Also it allows to change all graphics and texts that are displayed during the recovery process.

The Recovery Creator can also be used to create upgrade media. As the tool allows to customize the recovery process, you can create a custom step that will only format the C: partition and deploy a new version of the image afterwards. Also the tool can execute a script before and after deployment to backup and restore custom data.

DISMUI

The Deployment Image Servicing and Management User Interface (DISMUI) tool allows you to easily modify and service existing Windows installations. It is a very helpful tool for the componentized versions of Windows Embedded because it allows to add and remove certain feature packages and modules at any time in a secure way. It includes dependency checks and conflict checks to ensure that the image will still work properly after the modification. For the newer operating systems it also allows easy feature enabling and disabling while the operating system is offline!

For more details please visit our website at www.elbacom.com/eet



EVALUATION VERSION

We are offering a free evaluation version of the Elbacom Embedded Toolkit. The evaluation version allows you to test the most important features of the toolkit. Please contact us to receive a free evaluation copy!

Elbacom Embedded Configuration Manager

Windows Embedded 8.1 Industry Pro included a handy tool for configuring the Windows Embedded Lockdown Features called Embedded Lockdown Manager. Unfortunately this tool was not carried over to Windows 10 IoT Enterprise - this makes it hard to configure the lockdown features on the new systems.

Elbacom has created a solution for this called the Embedded Configuration Manager.

The Embedded Configuration Manager has even more functionality than the original Microsoft Embedded Lockdown Manager. The new tool can be used as a central management place for all Embedded related settings. It allows to activate or deactivate features and also to manage and configure them with ease. The

tool is designed to work with Windows Embedded 8 Standard, Windows Embedded 8.1 Industry Pro, Windows 10 IoT Enterprise 2015 LTSB, Windows 10 IoT Enterprise 2016 LTSB & CBB.

CONFIGURATION WITH EASE

To find out which embedded lockdown features are available for your Windows installation, just launch the Embedded Configuration Manager. On the first configuration page you will get a complete list of all available features. To enable them, just toggle the switch in front of their name and click on "Apply". After a reboot the features are available for configuration.

The tool will list all available features that can be configured on the left side. Every setting is de-

scribed in detail and can be configured with just a few mouse clicks.

ASSIGNED ACCESS

With the Assigned Access configuration you can easily select a modern Universal Windows Platform App that should be the default shell for a specific user.

With the "Enable Kiosk-Mode" functionality, that is only available through the Embedded Configuration Manager on Windows 10 IoT Enterprise 2016 versions, you can also completely suppress the Windows Desktop to ensure the user cannot exit the app!

EMBEDDED BOOT

The Embedded Boot settings allow to easily brand the boot experience. You can disable the boot logo, text and status ring, or block access to the F8 and F10 boot menu. These

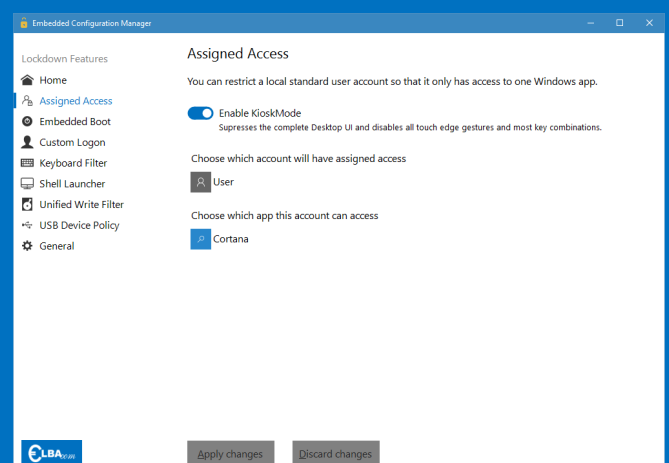
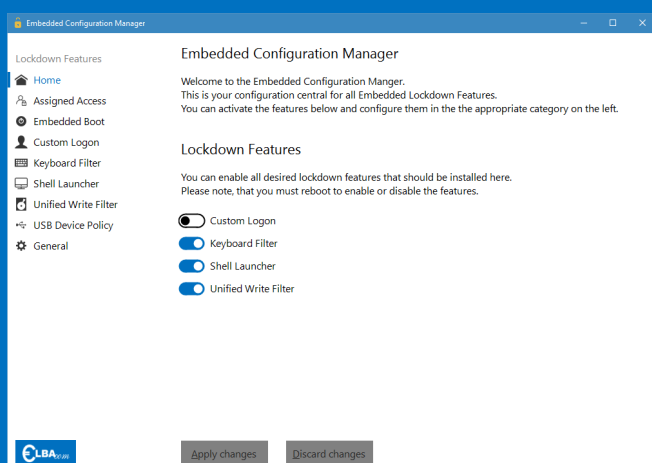
settings are important if you want to build a completely branded device.

CUSTOM LOGON

These settings allow to easily setup an automatic logon for a specific user and allows you to configure the branding settings. With the branding settings, you can easily suppress the complete Logon UI and hide certain elements, such as the power button or ease of access button from the logon screen!

KEYBOARD FILTER

The Keyboard Filter settings allow you to simply block keys or key combinations, such as Ctrl+Alt+Del. These combinations can be selected from a wide range of pre-defined keys, or you can easily add a custom combination that should be blocked. The keyboard filter allows to block keys



based on the key ID, such as Z, the keys will be blocked regardless of the keyboard layout. If the keyboard layout changes and the key wanders to a different location it will be blocked there as well. Alternatively the keys can be blocked based on the keys scan code. In this case the physical key on the keyboard will be blocked, ignoring what key is currently mapped from the keyboard layout.

The keyboard filter also allows to change the breakout key or to completely disable it.

The breakout key allows a user to break out of an account that is locked down, e.g. with a custom shell. Pressing the breakout key 5 times in a row will get the user to the Welcome screen so he can login with another user account.

Per default the breakout key is the Windows key. It is recommended to change the key or to completely disable the functionality and handle this scenario solely through the custom shell application.

SHELL LAUNCHER

The Shell Launcher allows to setup different shells for different users or groups. With the Embedded Configuration Manager the programs that should be used as shell for a specific user can be configured very easily.

With the shell launcher you can configure a default shell for the standard users, so they can use the shell application only but cannot access anything else in the system.

Administrators however, can be configured to boot into the regular Windows Explorer shell so they can use the full desktop experience to configure and service the devices.

UNIFIED WRITE FILTER

The write filter that can protect your system from any unwanted changes can be configured in detail as well.

The tool allows to configure the overlay settings, such as size and type.

You can easily add volumes to the protection and create exclusions based on files or folders and registry keys under HKEY_LOCAL_MACHINE.

USB DEVICE POLICY

The USB Device Policy allows you to create blacklists of devices that are not allowed to be connected to the system. Simply select a currently connected device and add it to the blacklist. The next time the device is being connected to the system it will no longer be allowed to be installed.

The filtering can be done based on the device ID or device classes. With the device classes you can block devices within a class in general, such as Bluetooth devices.

The tool also allows you to disable the filtering for Administrators or block removable devices in general.

TOUCH GESTURES

Additionally the tool allows you to disable touch gesture, such as the swiping from the right side to open the Action Center. This is very helpful to ensure users stay within the application on touch based devices.

It also allows to completely disable the whole touch functionality on a device. This can be use-

ful on tablets where the touchscreen should not be used for interaction with the device.

NOTIFICATIONS

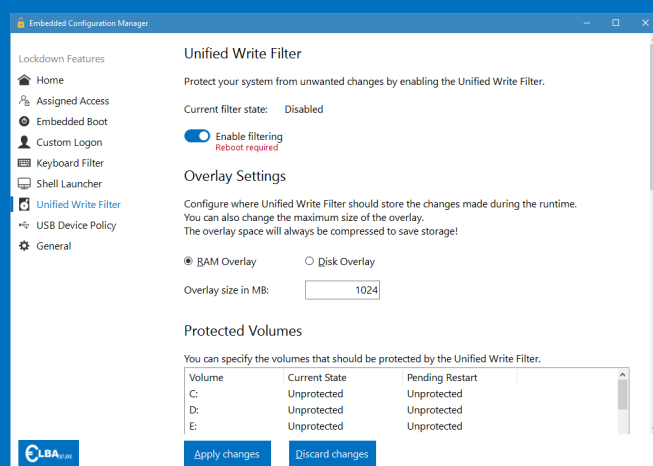
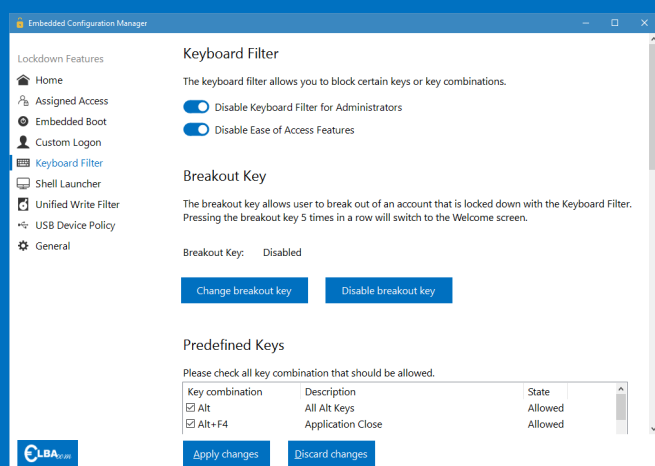
With a simple click the tool can also disable all toast notifications within Windows. This is important to remove any unwanted notifications from other applications or Windows itself.

ONEDRIVE

In most scenarios OneDrive is not needed on embedded devices. Therefore the tool allows you to easily turn off OneDrive so it does no longer run in the background and ask for a configuration.

In case OneDrive should not be disabled completely, the tool also supports to just remove OneDrive from the File Explorer and file open and save dialogs.

For more details please visit our website at www.elbacom.com/ecm



Windows 10 IoT Servicing Model

With Windows 10, the Servicing Model of Windows changed completely. Now, there are four different ways how to get your updates.

The first branch is the Windows Insider Preview Branch. This branch is a beta-program by Microsoft. If you are a Windows Insider, you will get every feature and security update as fast as possible. It is also possible to send some feedback back to Microsoft regarding the new updates.

The next one is the Consumer Branch. This branch is, as the name says, for the classic Windows consumers. They get mostly monthly updates and they have to do every update on their

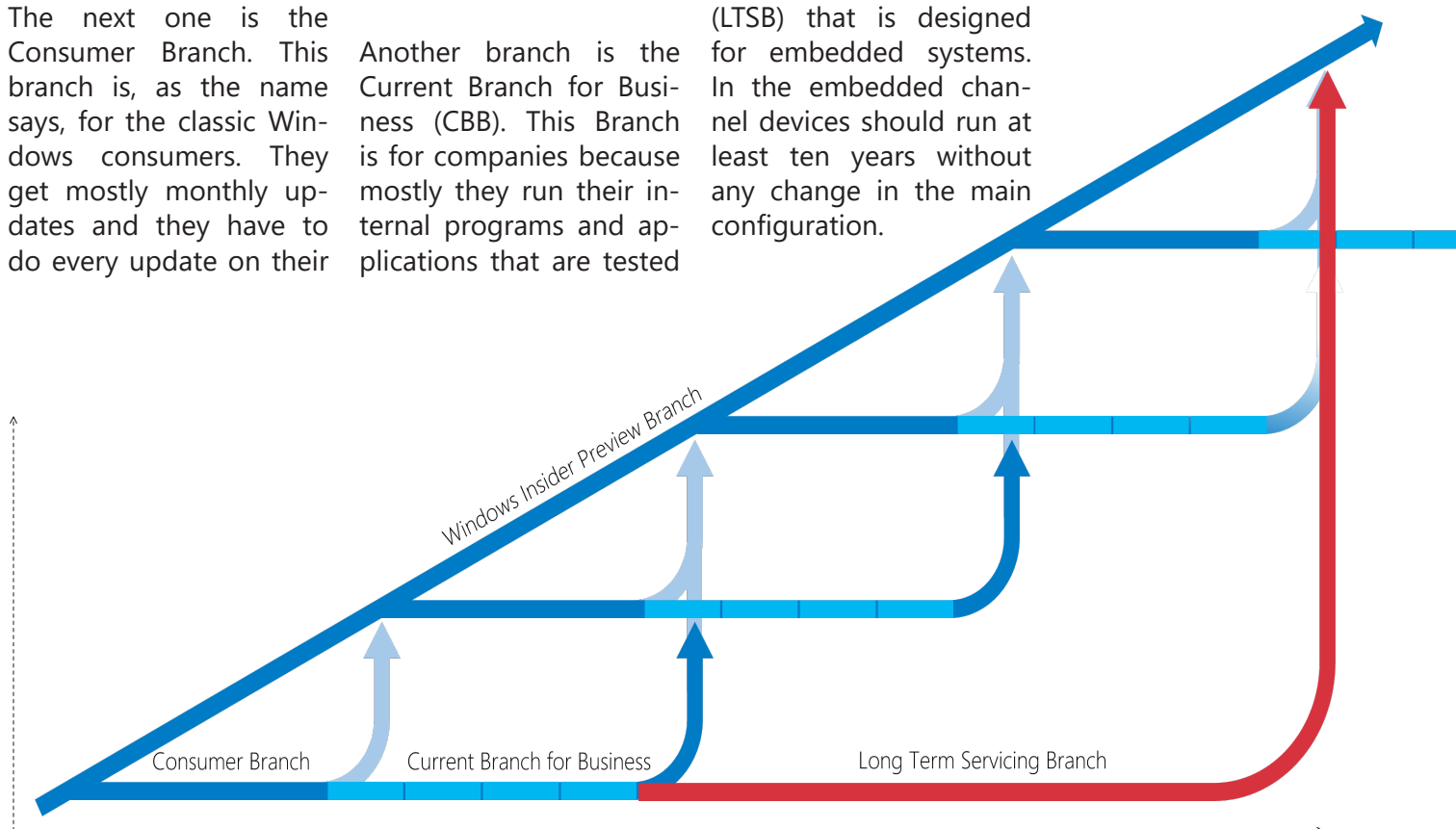
device. It is not possible to deactivate the updates or to miss an update and jump to the next one. This is also good for application developers because if they develop their application for the new Windows Insider Preview version, they can be sure that their application will work on every consumer device. Because they can release their application with the next consumer update and they can be sure that most of the consumers will be on the new version of Windows 10 within 2 or 3 weeks.

Another branch is the Current Branch for Business (CBB). This Branch is for companies because mostly they run their internal programs and applications that are tested

for a specific version of Windows. So if there are new updates, they can defer them for at least four months and test all updates. During this time they still get security updates for their devices but no unwanted feature updates. When they finished their tests, they can simply update to the new version of Windows, or if it is available, even to the next version. This is also helpful for the embedded channel.

The last branch is the Long Term Servicing Branch (LTSB) that is designed for embedded systems. In the embedded channel devices should run at least ten years without any change in the main configuration.

As many devices are connected to the internet nowadays, security updates are important. The LTSB model is designed for this scenario - offering only security related updates but no feature updates. These updates are guaranteed for ten years! Also the LTSB version allows to disable updates completely if desired. With the LTSB version Microsoft is supporting the Industrial Life Cycle Model and gives OEMs full control over their devices update behavior.



INDUSTRY 4.0

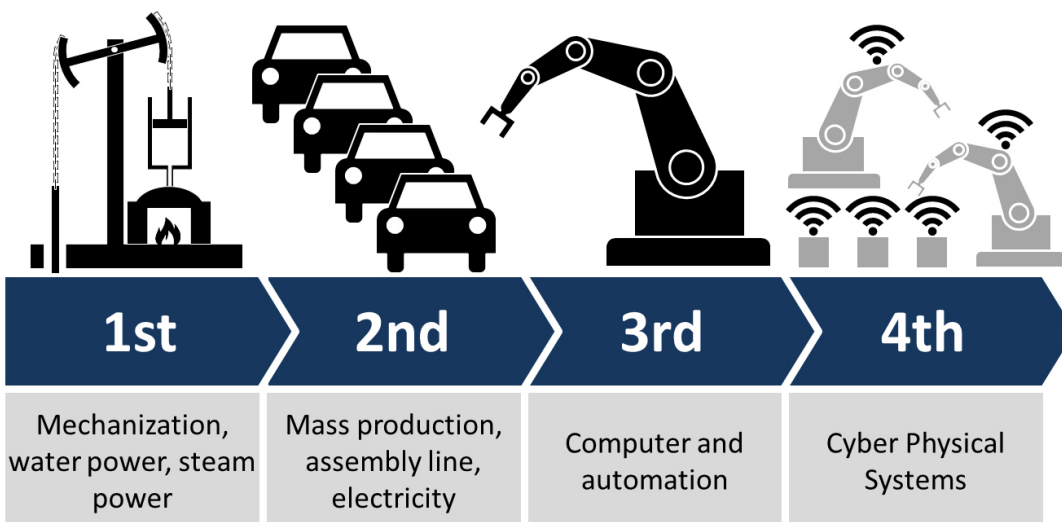
CONTROL
SECURITY
CLOUD CONNECTIVITY
AZURE
MICROSOFT
NETWORK
INTERNET OF YOUR THINGS
SERVICES
UPDATES
REMOTE CONNECTION
EMBEDDED
WMP
DATA
INTERNET
Core
10 IoT

Industry 4.0 is the fourth industrial revolution. The first industrial revolution was the mechanization of production using water and steam power. The second industrial revolution introduced mass production with the help of electric power. The third industrial revolution was also called digital revolution and the use of electrics to further automate production. Industry 4.0 is the current trend of automation. This includes

cyber physical systems, cloud computing and the Internet of Your Things (IoT). A very good example for this is the Smart factory compared to a traditional factory. The traditional factory needs maintain technicians on site to determine and resolve issues. It takes days or weeks to reroute and reconfigure devices and the search for data is needed for root-cause analysis. In the smart factory you can access devices remotely

to diagnose and resolve issues. You can complete corrections within hours, including rerouting processes and reconfiguring machines and you have access to very comprehensive data almost immediately to perform root-cause analysis. There are other good examples with smart retail devices or smart homes. The retail employee can take a look on a real-time inventory and don't need to track the deliveries manu-

ally. All alarm sensors and cameras in a smart home can communicate with another and to user devices 24/7. There is the possibility for cloud-connected temperature controls that can download predictive weather modeling and sense when the user is at home to apply resources most efficiently. With IoT, devices and embedded computing sensors will be communication and delivering real-time responses. Everything will be connected to the cloud. Because networked machines will be able to perform more efficiently and the more data you get the better will be your experience.



Now it is all about information. Connect your existing embedded devices to the Microsoft Cloud and allow them to do more!

tutorial

The Unified Write Filter is one of the most important Embedded Features in the Windows Embedded Channel. This filter is very useful to protect the device from unwanted changes. After enabling this feature, all changes will be written to a virtual overlay and will not affect the hard disk. Then all new files or changes will be only written into the RAM memory and after a restart all changes will be dropped.

This feature is also recommended for devices with a instable power supply for example. You can protect your system in this case from getting corrupt files after a power failure.

The usage of HORM is currently not supported for Windows 10 IoT Enterprise but it is expected to be added in the future.

You can configure the Unified Write Filter from the command line. This tutorial shows you the most important commands for the Unified Write Filter configuration.

Use the Unified Write Filter (UWF) via CMD

Enable the Unified Write Filter

```
uwfmgr filter enable
```

Disable the Unified Write Filter

```
uwfmgr filter disable
```

Protect a volume

```
uwfmgr protect <volume>
```

```
uwfmgr protect C:
```

Set Exclusion for a file or folder

```
uwfmgr Add-Exclusion <file or folder>
```

```
uwfmgr Add-Exclusion C:\Data\exclusion.txt
```

```
uwfmgr Add-Exclusion C:\Data
```

Remove Exclusion for a file or folder

```
uwfmgr Remove-Exclusion <file or folder>
```

```
uwfmgr Remove-Exclusion C:\Data\exclusion.txt
```

```
uwfmgr Remove-Exclusion C:\Data
```

Get a detailed list of existing Exclusions

```
uwfmgr Get-Exclusions
```

Get detailed information about the full UWF configuration

```
uwfmgr Get-Config
```

Enable Hibernate Once/Resume Many (HORM)

```
uwfmgr Enable-HORM
```

Disable HORM

```
uwfmgr Disable-HORM
```

Set Overlay size in MB

```
uwfmgr Set-Size <size>
```

```
uwfmgr Set-Size 2048
```

ELBACOM LOGISTICS CENTER

+43 2174 26604 0
info@elbacom.com

AUSTRIA

+43 2236 866 886 0
austria@elbacom.com

BOSNIA AND HERZEGOVINA

+43 664 260 57 45
bosnia@elbacom.com

BULGARIA

+359 887 311 230
bulgaria@elbacom.com

CROATIA

+43 664 260 57 45
croatia@elbacom.com

CZECH REPUBLIC

+420 602 464 089
czech@elbacom.com

ESTONIA

+48 71 3399247
estonia@elbacom.com

GERMANY

+49 89 1894 756 0
germany@elbacom.com

HUNGARY

+36 30 748 0458
hungary@elbacom.com

ITALY

+49 89 1894 756 0
italy@elbacom.com

KOSOVO

+43 664 260 57 45
kosovo@elbacom.com

LATVIA

+48 71 3399247
latvia@elbacom.com

LITHUANIA

+48 71 3399247
lithuania@elbacom.com

MACEDONIA

+43 664 260 57 45
macedonia@elbacom.com

MONTENEGRO

+43 664 260 57 45
montenegro@elbacom.com

POLAND

+48 71 3399247
poland@elbacom.com

ROMANIA

+36 30 748 0458
romania@elbacom.com

SERBIA

+43 664 260 57 45
serbia@elbacom.com

SLOVAKIA

+421 911 464 089
slovakia@elbacom.com

SLOVENIA

+43 664 260 57 45
slovenia@elbacom.com

SWITZERLAND

+41 32 512 14 41
switzerland@elbacom.com

UKRAINE

+43 2236 866 886 0
ukraine@elbacom.com





www.elbacom.com



Microsoft Partner
Gold Distributor

