

# Microsoft Windows Embedded 8.1 Industry Pro and Windows Embedded 8.1 Industry Enterprise Privacy Statement

Last updated: June 2013

Microsoft is committed to protecting your privacy, while delivering software that brings you the performance, power, and convenience you desire in your personal computing. This privacy statement explains many of the data collection and use practices of Windows Embedded Industry Enterprise and Windows Embedded Industry Pro. It does not apply to other online or offline Microsoft sites, products, or services.

Windows Embedded 8.1 Industry is an operating system platform with a fixed feature set that provides functionality to enable OEMs and Enterprises to deliver rich targeted device experiences for industries such as Retail, Manufacturing, and Healthcare. Windows Embedded 8.1 Industry is available as two SKUs, Windows Embedded 8.1 Industry Pro and Windows Embedded 8.1 Industry Enterprise.

## Collection and Use of Your Information

The information we collect from you will be used by Microsoft and its subsidiaries and affiliates to enable the features you are using and provide the service(s) or carry out the transaction(s) you have requested or authorized. It may also be used to analyze and improve Microsoft products and services.

We may send certain mandatory service communications such as welcome letters, billing reminders, information on technical service issues, and security announcements to you. Some Microsoft services may send periodic member letters that are considered part of the service. We may occasionally request your feedback, invite you to participate in surveys, or send you promotional mailings to inform you of other products or services available from Microsoft and its affiliates.

In order to offer you a more consistent and personalized experience in your interactions with Microsoft, information collected through one Microsoft service may be combined with information obtained through other Microsoft services. We may also supplement the information we collect with information obtained from other companies. For example, we may use services from other companies that enable us to derive a general geographic area based on your IP address in order to customize certain services to your geographic area.

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as packaging, sending and delivering purchases and other mailings, answering customer questions about products or services, processing event registration, or performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the services and they are prohibited from using that information for any other purpose.

Microsoft may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the services; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers, or the public. We may also disclose personal information as part of a corporate transaction such as a merger or sale of assets.

Information that is collected by or sent to Microsoft by Windows Embedded 8.1 Industry may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union, the European Economic Area, and Switzerland.

## Collection and Use of Information about Your Computer

When you use software with Internet-enabled features, information about your computer ("standard computer information") is sent to the web sites you visit and online services you use. Microsoft uses standard computer information to provide you Internet-enabled services, to help improve our products and services, and for statistical analysis. Standard computer information typically includes information such as your IP address, operating system version, browser version, and regional and language settings. In some cases, standard computer information may also include hardware ID, which indicates the device manufacturer, device name, and version. If a particular feature or service sends information to Microsoft, standard computer information will be sent as well.

The privacy details for each Windows Embedded 8.1 feature, software or service listed in this privacy statement describe what additional information is collected and how it is used.

## Security of your information

Microsoft is committed to helping protect the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer systems with limited access, which are located in controlled facilities.

## Changes to this privacy statement

We will occasionally update this privacy statement to reflect changes in our products, services, and customer feedback. When we post changes, we will revise the "last updated" date at the top of this statement. If there are material changes to this statement or in how Microsoft will use your personal information, we will notify you either by posting a notice of such changes prior to implementing the change or by directly sending you a notification. We encourage you to periodically review this statement to be informed of how Microsoft is protecting your information.

## For More Information

Microsoft welcomes your comments regarding this privacy statement. If you have questions about this statement or believe that we have not adhered to it, please contact us at <http://go.microsoft.com/fwlink/?LinkId=260768>.

Microsoft Privacy  
Microsoft Corporation  
One Microsoft Way  
Redmond, Washington 98052 USA

## Specific features

The remainder of this document will address the following specific features.

### Activation

**Note: This feature is primarily used by OEMs and IT administrators.**

#### **What this feature does:**

Activation helps reduce software counterfeiting, helping to ensure that Microsoft customers receive the software quality they expect. Once the Windows Embedded software is activated by an OEM or IT administrator, a specific product key becomes associated with the computer (the hardware) on which the software was installed. This association prevents the product key from being used to activate the same copy of the software on multiple computers as counterfeit software. Certain changes to the computer components or the software may require software reactivation.

#### **Information collected, processed, or transmitted:**

During activation, product key information is sent to Microsoft along with a hardware hash, which is a non-unique number generated from the computer's hardware configuration. The hardware hash does not represent any personal information or information about the software. The hardware hash cannot be used to determine the make or model of the computer and it cannot be backward calculated to determine any additional information about the source computer. Along with standard computer information, some additional language settings are collected.

#### **Use of information:**

Microsoft uses the information described above to confirm that you have a licensed copy of the software, and then it is aggregated for statistical analysis. Microsoft does not use the information to identify you or contact you.

#### **Choice and control:**

Activation is mandatory and must be completed within a predefined grace period. If you choose not to activate the software, you cannot use it after the grace period expires. If the software is not correctly licensed, you will not be able to activate it.

### Embedded Lockdown Manager

**Note: This feature is primarily used by OEMs and IT administrators.**

**What This Feature Does:**

The Embedded Lockdown Manager (ELM) is a snap-in to the Microsoft Management Console (MMC) application. ELM provides an easy to use UI for OEMs and system administrators to configure certain lockdown features – namely, Dialog Filter, Unified Write Filter, Shell Launcher, and the Keyboard Filter - on a Windows Embedded 8.1 Industry device. The Embedded Lockdown Manager automatically detects which lockdown features exist on an embedded device, and only displays configuration options for those features. IT administrators can use ELM directly on a Windows Embedded 8.1 Industry device if the OEM included it as a feature in a custom image, or administrators can use it via a Windows Desktop or Windows Server machine to remotely configure a Windows Embedded 8.1 Industry device.

**Information Collected, Processed, or Transmitted:**

Each device will be identified on the IT-managed network via a unique computer name. The state of an embedded device can be viewed, monitored, and updated real-time by the IT administrator and it provides the ability to export a device's configuration settings to a Power Shell script for broader deployment. None of this information is sent to Microsoft. The IT administrator requires administrator permissions to each device that is being managed.

**Use of Information:**

Microsoft does not use this information. It is available to the IT administrator.

**Choice/Control:**

The IT administrator requires administrator permissions to each device that is being managed. The user of the device cannot enable or disable this management tool. The IT Administrator can remove the tool from the MMC Snap-in console.

**Windows 8 Features**

**Note: These features are relevant to all device users.**

**What this feature does:** Windows Embedded 8.1 Industry Pro and Windows Embedded 8.1 Industry Enterprise include the Windows 8.1 client operating system.

**Use of information:** Windows 8.1 client operating system contains features that can send information to Microsoft. To learn more about the information sent and its privacy impact, please see the Windows 8.1 Privacy Statement at <http://go.microsoft.com/fwlink/?linkid=280262>.

**Choice and control:**

Some of the Windows features that send information may be turned on by default. The first time an OS image is run on a device, the user will be presented with an interface that has toggles for turning off/on delivery of information. Please note that for Windows Embedded Industry Pro, some device owners may receive a preconfigured image and thus will not be presented with the initial user interface.

Users can also later turn off delivery of information as described in see the Windows 8.1 Privacy Statement at <http://go.microsoft.com/fwlink/?linkid=280262>.

**Customer Experience Improvement Program**

**Note: This feature is relevant to OEMs, IT Administrators, and all device users.**

**What This Feature Does:**

The Customer Experience Improvement Program ("CEIP") collects basic information about your hardware configuration and how you use our software and services in order to identify trends and usage patterns. CEIP also collects the type and number of errors you encounter, software and hardware performance, and the speed of services. CEIP reports do not intentionally contain any contact information about you (such as your name, address, or phone number). **However, some reports from Windows features might unintentionally contain individual identifiers (other than the GUID), such as a serial number for a**

**device that is connected to your computer.** Microsoft filters the information contained in CEIP reports to try to remove any individual identifiers that they might contain.

Information can be collected through CEIP from:

- the Embedded Lockdown Manager (“ELM”) Microsoft Management Console snap-in that is used by IT Professionals or administrators to manage deployed devices; and from
- the features within the OS image once it has been deployed to a device

#### **Information Collected, Processed, or Transmitted:**

For more information about the information collected, processed, or transmitted by CEIP, see the CEIP privacy statement at <http://go.microsoft.com/fwlink/?LinkID=52097>.

#### **Use of Information:**

We use this information to improve the quality, reliability, and performance of Microsoft software and services.

#### **Choice/Control:**

##### Embedded Lockdown Manager

You can choose to enable or disable CEIP in the Customer Experience Improvements Program dialog that is presented when ELM is launched for the first time after installation, or can link to this dialog when ELM is running in Microsoft Management Console (“MMC”) by clicking the Join the Customer Experience Improvement Program link in the tool description pane.

##### Features within the OS image

For Windows Embedded 8.1 Industry devices, the first time an OS image is run on a device, the user will be presented with an interface that has toggles for turning off/on delivery of information. Please note that for Windows Embedded Industry Pro, some device owners may receive a preconfigured image and thus will not be presented with the initial user interface.

You can also later turn off delivery of this information by launching Control Panel, selecting System and Security, selecting Action Center, selecting Change Action Center Settings, and then selecting Customer Experience Improvement Program settings. The Customer Experience Improvement Program settings interface presents checkboxes for turning off/on delivery of information. If you have Unified Write Filter enabled on your device, you may need to disable the write filter and restart your device before making any changes to your CEIP settings.

## **Microsoft Error Reporting**

**Note: This feature is relevant to OEMs, IT Administrators, and device owners.**

#### **What This Feature Does:**

Microsoft Error Reporting provides a service that allows you to report problems you may be having with Windows Embedded 8.1 Industry to Microsoft and to receive information that may help you avoid or solve such problems.

Information can be collected through Error Reporting from:

- the ELM snap-in that is used to manage deployed devices; and from
- the features within the OS image once it has been deployed to a device

#### **Information Collected, Processed, or Transmitted:**

For information about the information collected, processed, or transmitted by Microsoft Error Reporting, see the Microsoft Error Reporting privacy statement at <http://go.microsoft.com/fwlink/?linkid=50293>.

#### **Use of Information:**

We use the error reporting data to solve customer problems and improve our software and services.

**Choice/Control:**

When Microsoft needs additional data to analyze the problem, you will be prompted to review the data and choose whether or not to send it. You can change your Microsoft Error Reporting settings at any time.

**Embedded Lockdown Manager**

ELM is hosted inside Microsoft Management Console (MMC) , and runs on an OS image or on a desktop system if an IT Professional downloaded the standalone version of the tool. On a system (custom OS image or desktop) where Microsoft Error Reporting is enabled, MMC will forward on the stack to the error reporting service to show which snap-in, if any, failed. Error handling information is not handled directly in ELM itself.

**Features within the OS Image**

The first time an OS image is run on a device, the user will be presented with an interface that has toggles for turning off/on Windows Error Reporting. Please note that for Windows Embedded Industry Pro, some device owners may receive a preconfigured image and thus will not be presented with the initial user interface.

You can also later turn off Microsoft Error Reporting by launching Control Panel, selecting System and Security, selecting Action Center, selecting Change Action Center Settings, selecting Problem Reporting Settings and selecting one of the radio button options. Note that some of these settings may be controlled within a managed network environment via Group Policy. To turn it off, select "Never check for solutions."

**Important Information:**

If you turn off Microsoft Error Reporting, it will be turned off for all features in Windows. Enterprise customers can use Group Policy to configure how Microsoft Error Reporting behaves on their computers. Configuration options include the ability to turn off Microsoft Error Reporting. If you are an administrator and wish to configure Group Policy for Microsoft Error Reporting, technical details are available at <http://technet.microsoft.com/en-us/library/cc709644.aspx>.