Windows 10 IoT Enterprise Activation Guide

Version 2.0, updated November 2019

Contents

Introduction

This guide is intended to provide an overview and detailed guidance on how to activate and reactivate Windows 10 IoT Enterprise images in both the factory and the field.

All Windows 10 IoT Enterprise devices must be enabled for activation. Device activation may be completed by having devices contact Microsoft activation verification servers directly through an Internet connection or indirectly via a proxy tool. Alternatively, Windows 10 IoT offers a third option, allowing devices not connected to the Internet to remain in a deferred activation state, as described further below. This option is new to Windows 10 IoT.

This guide is primarily intended as a resource for individuals required to perform this activation process; however, it is also useful as a resource for administrators, planners, and technicians in other roles who need to understand how activation works or how to activate a device.

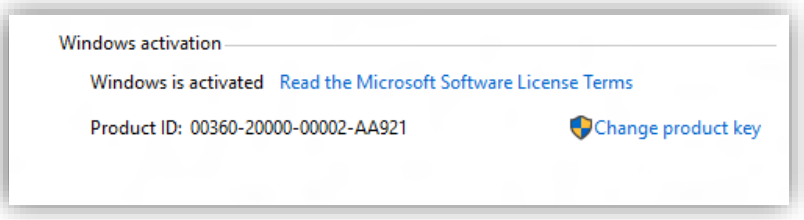
What is activation?

Activation is the process of registering Windows 10 IoT Enterprise with Microsoft to ensure the product is genuine. Activation is used to:

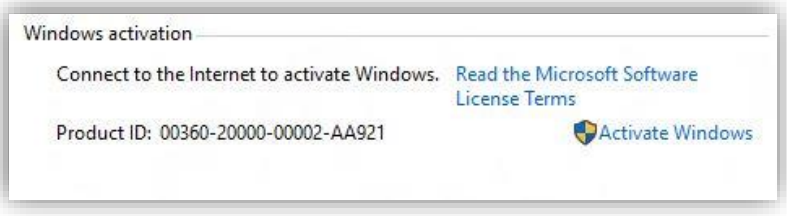
1. Reduce software piracy.
2. Protect the software industry, corporate intellectual property, software development investments, and product quality.
3. Ensure customers receive the product quality they expect.

By default, you must enable each device for activation. If the device is not connected to the Internet, it will remain in a deferred activation state. If the device is connected to the Internet, the device will automatically activate over the Internet. If the device connects to the Internet and the activation attempt fails due to an invalid licensing key or one that has exceeded its activation allotment, it will enter a not activated state. Thus, there are three potential device states:

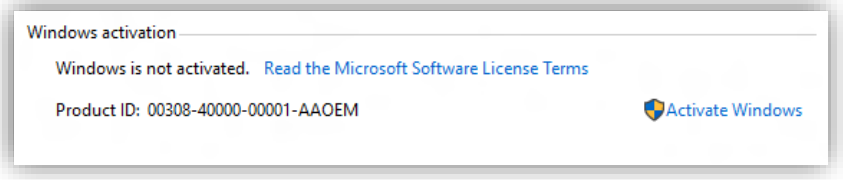
1. Activated state



2. Deferred activation state



3. Not activated state

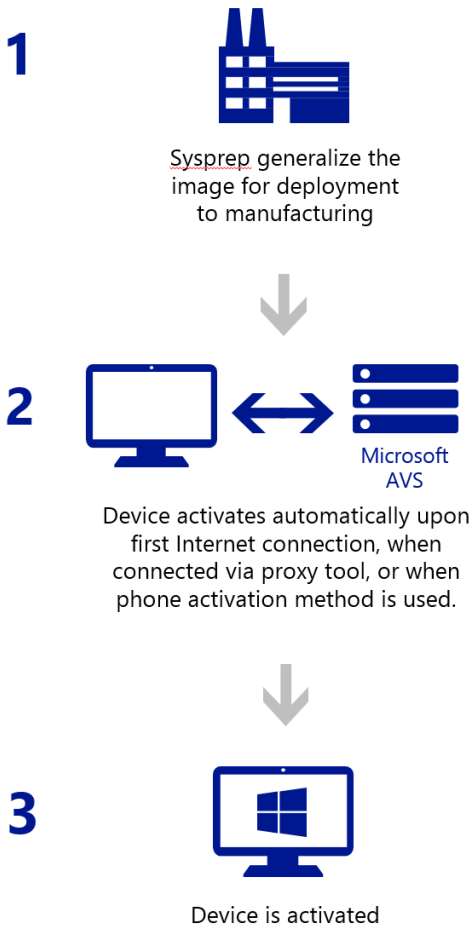


After a device has been activated, it will remain activated unless a significant change triggers a need to reactivate the device, such as a motherboard replacement or completely reimaging the device.

Activation process overview

Each device must have a valid license key to support activation, and the process of activation encompasses several distinct steps, as follows:

1. Obtain a product key and apply it to the device.
2. Retrieve the licensing status information from the device.
3. Connect for activation or leave in deferred activation state.
    a. Leave the device in a state of deferred activation.
    b. To activate: connect device to Internet directly; connect device to Internet indirectly using the proxy activation tool; or activate through Microsoft licensing servers using a telephone if no Internet connection is available. At this point, the device will automatically (or, in the case of telephone option, via user input) send licensing status. The device will then automatically:
        i. Retrieve a confirmation ID from the Microsoft licensing servers.
        ii. Apply the confirmation ID to your device. The device is now activated.
4. OEMs may have a sales-out reporting requirement to report licenses used.



Not activated behavior

When a Windows 10 IoT Enterprise device activation attempt fails due to an invalid licensing key or one that has exceeded its activation allotment, the device displays an immersive watermark on the lower-right corner of each attached display. This watermark appears 3 hours after the failed activation attempt. In addition, you cannot change the Windows personalization settings, such as the desktop background or the lock screen background, on a device that is not activated. These are the differences between a device that is not activated versus a device that is activated or in a deferred activation state.

Enabling Activation

The following sections describes the process for an OEM to build a device that is enabled for activation.

Product Keys

Product keys that apply to Windows 10 IoT Enterprise.

*E*mbedded Product Key Entry Activation (ePKEA)

ePKEA keys are distributed to and supported by an OEM. This type of product key is used to activate multiple devices, multiple times, up to the limit imposed on the key.

Product Key Entry Activation (PKEA) keys

PKEA keys are distributed to and supported by an OEM. This type of product key is used to activate a single installation of Windows per unique key.

OEM activation 3.0 (OA 3.0) key

OA 3.0 keys are obtained solely by using the OEM Activation 3.0 system. If you are interested in using this system, please contact your Microsoft representative.

Note: This document does not address the use of this product key specifically.

Finalizing the OEM Image

Customers receiving a device built via ePKEA or PKEA will be prompted for a license key that they do not have access to from the OEM. The following step suppresses the license key dialog that appears in the OOBE experience after Sysprep is run:

IMPORTANT: This step only applies to ePKEA and PKEA scenarios. It is not applicable for OEM 3.0 activation.

1. Insert your media into the target device and boot into Windows 10 setup
2. When prompted for product key, select “I do not have a product key” option
3. When you hit OOBE, enter Audit mode by pressing Ctrl+Shift+F3
4. After reboot, cancel the Sysprep dialog
5. In Audit mode, apply OEM ePKEA or PKEA using slmgr
    a. slmgr /ipk XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
6. Make any modifications required such as installing OEM value add applications, drivers, etc. Once complete continue with next step
7. At an elevated command prompt run: **reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\SoftwareProtectionPlatform" /v BackupProductKeyDefault /t REG_SZ /d "BBBBB-BBBBB-BBBBB-BBBBB-BBBBB" /f**
8. Next, type: **Slmgr /cpky**
9. Next, type: **Sysprep /oobe /generalize /quit**
10. Next, type: **reg add HKLM\Software\Microsoft\Windows\CurrentVersion\Setup\OOBE /v SetupDisplayedProductKey /t REG_DWORD /d 1**

11. Exit command prompt and shutdown
12. (capture and deploy if mass producing)

When the OEM's customer boots the device, they will proceed through OOBE (unless the OEM has automated the image with unattend.xml). Note: No prompt for Product Key entry will appear to the customer.

Activation methods

All Windows 10 IoT Enterprise images must be enabled for activation, which includes activation and deferred activation. If the device is never connected to the Internet, it will remain in a deferred activation state. If you decide to fully activate the image, rather than staying in deferred activation state, then the deciding factor in how and when to activate an image is usually what kind of Internet connection your device has available and the needs and expectations of the final customer.
The first factor in deciding how to activate your Windows 10 IoT Enterprise device is to determine what type of Internet connection is available to your device – direct Internet connection, Internet via proxy tool, or no Internet connectivity.

Direct connection

In this situation, a device has access to a public network so it can directly contact the Microsoft activation servers to complete the activation process. The device must be able to send and receive information across TCP ports 80 and 443.

Internet via proxy tool

In this situation, a device may have access to a private network but no access directly to the Internet. Proxy activation tools can be used in this case to complete the activation process between the device on the private network and the Microsoft activation servers on the public network.

For more information about activating a device in this scenario, see Volume Activation Management Tool Technical Reference: http://go.microsoft.com/fwlink/?LinkID=618654

No Internet connectivity

Situations in which there is no Internet connectivity include when the device has no networking capability, the factory has no Internet connectivity, the device is connected to a private network that does not have Internet connectivity, or the device cannot be connected (even indirectly through a proxy) to the Internet because of security considerations. In these situations, you can use a telephone to activate your device.

For more information about activating a device in this scenario, see How to Contact a Microsoft Product Activation Center by Phone: http://go.microsoft.com/fwlink/?LinkID=618655

Alternatively, you may choose to leave the device in deferred activation state.

Activation and write filters

All activation processes require that the device has write filters disabled. Although activation initially succeeds if write filters are enabled, restarting the device resets the activation status, and you must reactivate the device.

Activation tools

You use the following tools in various activation scenarios.

Volume Activation Management Tool 3.1 (VAMT 3.1)

You can use VAMT 3.1 to centrally manage activation status for Windows 10 IoT Enterprise devices over a network. You can download this tool for free. For more information see What's New for ADK in Windows 10: http://go.microsoft.com/fwlink/?LinkID=618653

Just manually select **Volume Activation Management Tool (VAMT)** to install, because it is not selected by default. If you do not have a Microsoft SQL Server 2008 or later database available for VAMT to use, you should also select **SQL Server Express 2012** to install, because VAMT requires a connection to a SQL Server database. You can choose not to install any of the other features, because they are not required for VAMT.

For more information about VAMT 3.1, see Volume Activation Management Tool Technical Reference: http://go.microsoft.com/fwlink/?LinkID=618658

Windows Software Licensing Management Tool (Slmgr.vbs)

This command line tool enables you to manage product keys and activation status on a Windows 10 IoT Enterprise device. This tool is available on every Windows 10 IoT Enterprise operating system.

For more information about Slmgr, see Slmgr.vbs Options on TechNet: http://go.microsoft.com/fwlink/?LinkID=618656

Windows Activation UI (Slui.exe)

This tool launches the Windows Activation UI that allows you to enter a license key. This tool is available on every Windows 10 IoT Enterprise operating system.

Reactivation

Certain scenarios can cause a device to require to be reactivated. Any time a change is made to an activated device, the device is classified as either *in-tolerance* or *out-of-tolerance*. In many cases, you can make minor changes to the hardware, such as adding additional RAM or swapping out a hard drive, without requiring the device to be reactivated. Major hardware changes, such as changing the motherboard of a device, can cause a device to be considered out-of-tolerance, which sets the device back to a not activated state. A large number of small hardware changes made at once can also push a device to out-of-tolerance, even if the individual changes themselves would be considered in-tolerance.

Attaching and detaching USB devices or other peripheral hardware has no effect on the tolerance state of the device.

When a Windows 10 IoT Enterprise device requires reactivation, a watermark is displayed in the lower-right corner of each attached display, indicating that the device is not activated. In addition, you cannot change the Windows personalization settings, such as the desktop background or the lock screen background. The device continues to work as normal, and there are no other changes in the behavior of the device.

In most cases, you can reactivate the device in the same manner that you would activate a new device, as outlined in this guide. Depending on the type of product key you have used, reactivating a device has different implications. For ePKEA keys, reactivating a device can use up one of the pool of available keys, although multiple reactivations of the same device should reuse the reactivated key, as long as the hardware of the device has not significantly changed.

Activate a Windows 10 IoT Enterprise device by using a direct Internet connection

In most cases, a Windows 10 IoT Enterprise device directly connected to the Internet will activate automatically without user intervention. You can also use the following procedures to activate your device:

- Activate a Device Manually Using a Direct Internet Connection
- Activate a Device Over the Internet Using VAMT 3.1

Activate a device manually by using a direct Internet connection

If your device has a direct Internet connection, you can manually activate your device using either the command line or the Windows Activation UI.

Windows 10 IoT Enterprise provides the following two command line tools that you can use to manage your activation status:

- Slmgr.vbs – The Windows Software Licensing Management Tool lets you manage product keys and activation status.
- Slui.exe – This tool launches the Windows Activation UI.

Activate a device manually by using a direct Internet connection and the command line

Prerequisites:

- Windows 10 IoT Enterprise is installed on your device.
- Your device has a direct Internet connection.
- You have administrator rights on the device.

To activate:

1. On your device, open a command prompt as Administrator.
2. Navigate to the **<system drive>:\Windows\System32** folder, and then type **cscript slmgr.vbs /ato**
3. Type **cscript slmgr.vbs /dlv**, and then verify that the **License Status** now displays **Licensed**.

Activate a device manually by using a direct Internet connection and Windows Activation UI

Prerequisites:

- Windows 10 IoT Enterprise is installed on your device.
- Your device has a direct Internet connection.
- You have administrator rights on the device.

To activate:

1. On your device, do one of the following:
   a. Open a command prompt as Administrator and type the following command to launch the Windows Activation UI: **SLUI**
      -or-
   b. Open the Windows 10 Settings Menu, and navigate to **Open Settings**.
   c. Click **Updates & Security**.
   d. Click **Activation**.
   e. Click **Activate**.

2. After a few minutes, your device will be activated.

Automatically activate a device by using a direct Internet connection after setup

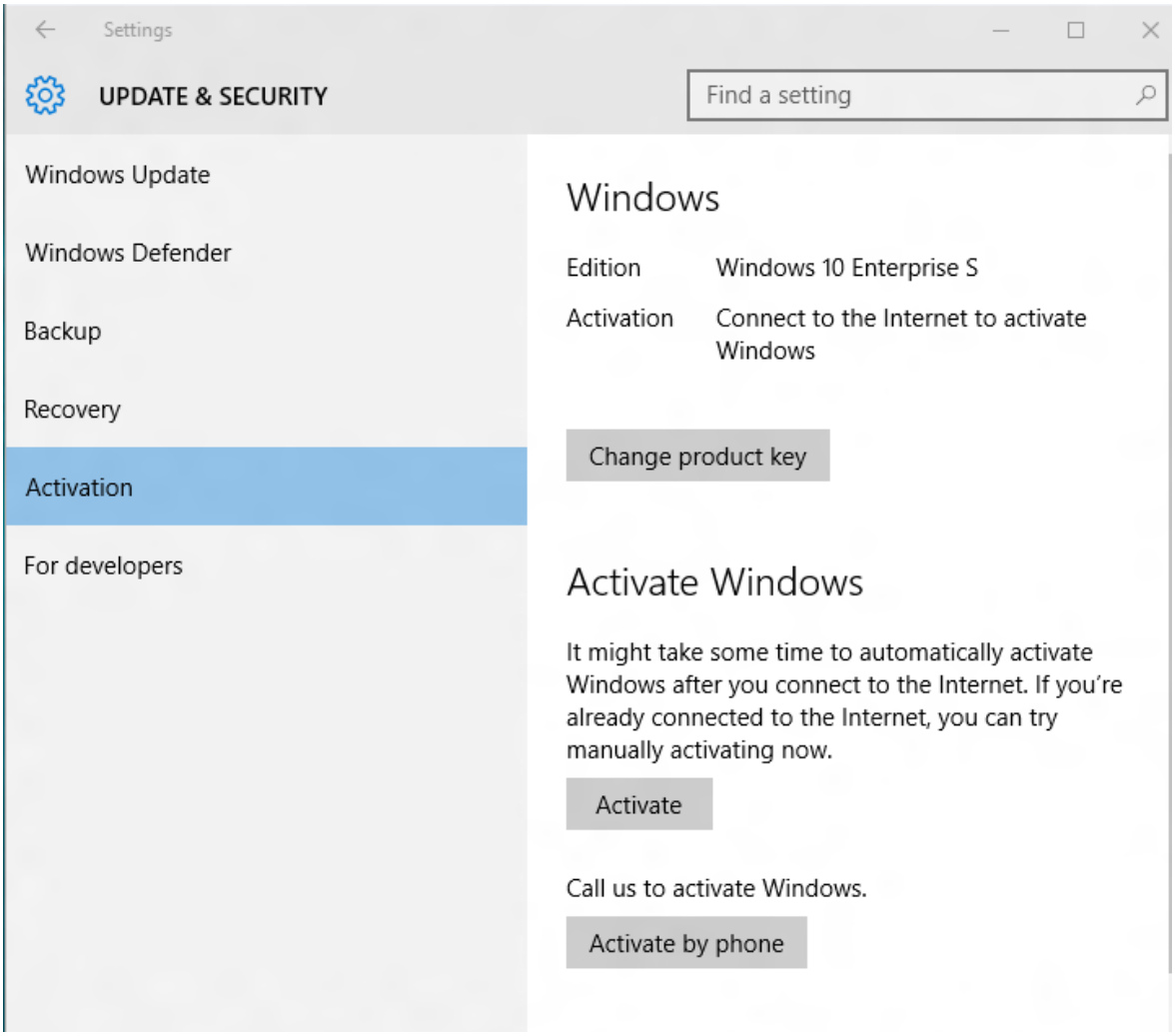
By default, Windows 10 IoT Enterprise devices will automatically activate upon first connection to the Internet.

Prerequisites:

- Direct Internet connection for your device.
- Your device's master image has been created with a valid product key.
- Administrator user rights to the master or reference image.

To activate:

Device will activate automatically when connected to Internet; however, if you would like to ensure this activation occurs at a specific time, then you can use this method:



1. On your master or reference device, open a command prompt as an Administrator.
2. Type the following to add the registry key to enable automatic activation:
   Reg add HkLm\Software\microsoft\Windows\CurrentVersion\RunOnce /v autoactivate /t REG_SZ /d "<system drive>:\windows\system32\slmgr.vbs /ato"
3. In the command prompt window, navigate to the **%systemdrive%\Windows\System32\Sysprep** folder and generalize your image by typing **sysprep /generalize**
4. Deploy the S**ysprepped** image to manufacturing. When this image is deployed to a device and the device is started for the first time, it will automatically attempt to activate when an Internet connection is available.

Activate a device over the Internet by using VAMT 3.1

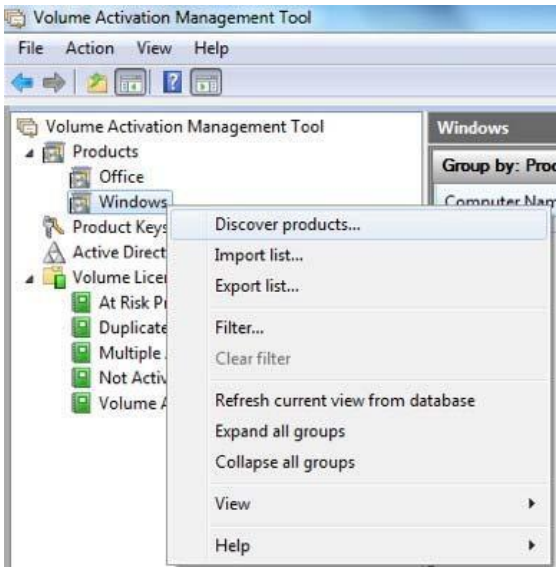
If your device does not have a display or does not have a method of user input, or if you have a large number of devices on a network and you want to activate them remotely, you can use the Volume Activation Management Tool 3.1 (VAMT 3.1) to remotely activate devices on a network. This tool is distributed for free.

For more information about VAMT 3.1, please see Volume Activation Management Tool Technical Reference: http://go.microsoft.com/fwlink/?LinkID=618656

To activate a device over the Internet by using VAMT 3.1

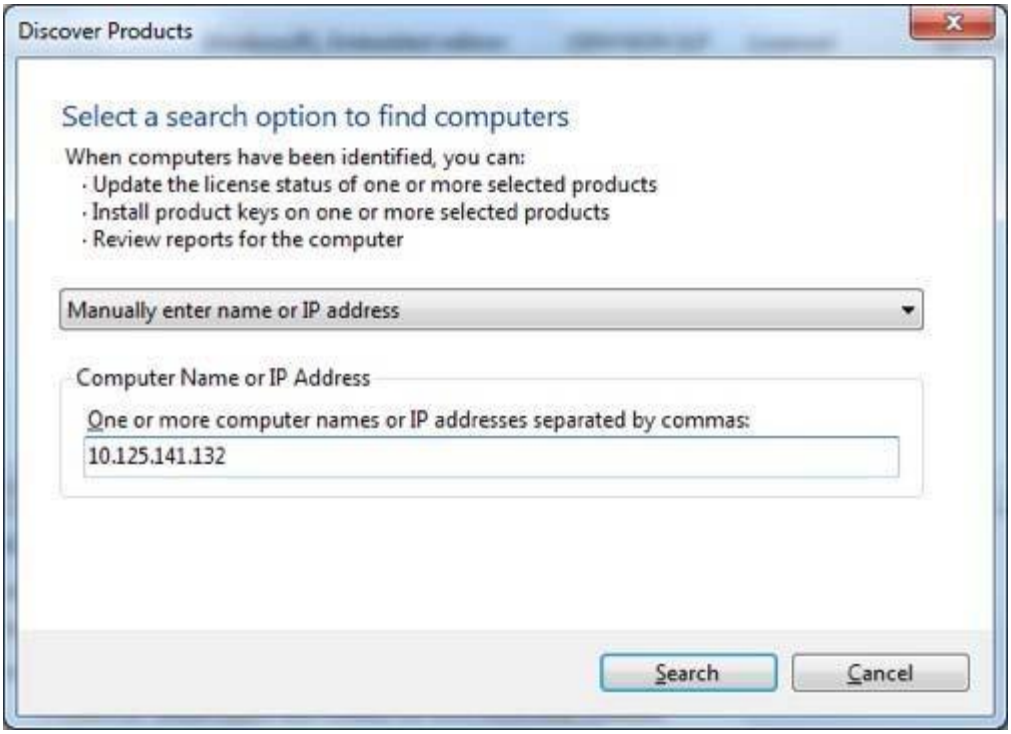
Prerequisites:

- VAMT 3.1 host, which includes the following:
  - VAMT 3.1 tool is installed.
  - The VAMT 3.1 host has Internet access.
  - The VAMT 3.1 host has private network connectivity.
- Windows PowerShell 4.0 is installed.
- The device to be activated contains the following:
  - Configured WMI/PowerShell remote access.
  - For more information, see Allow WMI/PowerShell Remote Access on a Device: http://go.microsoft.com/fwlink/?LinkID=618657
  - Private network connectivity.
  - Direct Internet connectivity.
  - An administrator account with a password.



To activate:

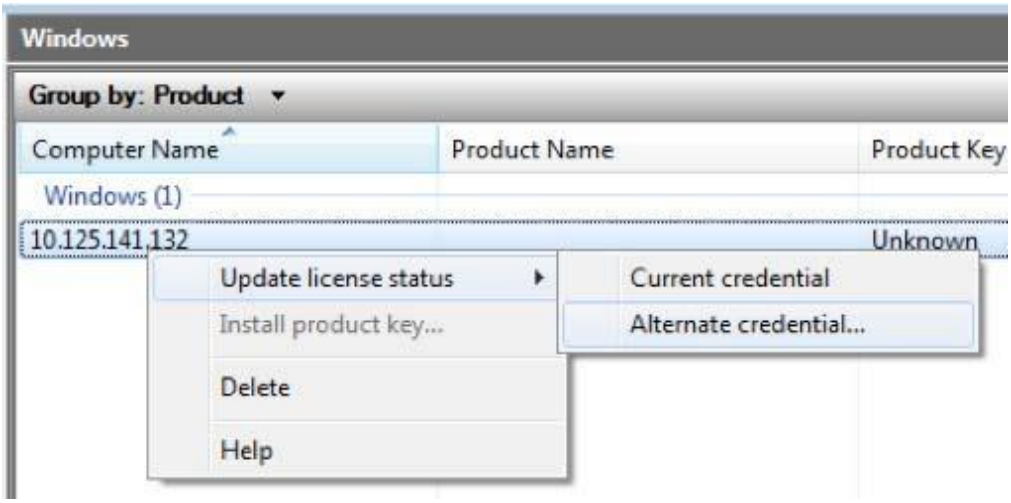
1. On the VAMT 3.1 host, open VAMT 3.1.
2. In the left pane, expand the **Products** node, right-click the **Windows** node, and then click **Discover products**.
3. In the **Discover products** dialog box, select **Manually enter name or IP address**, and then enter the name or IP address of the device you are going to activate.



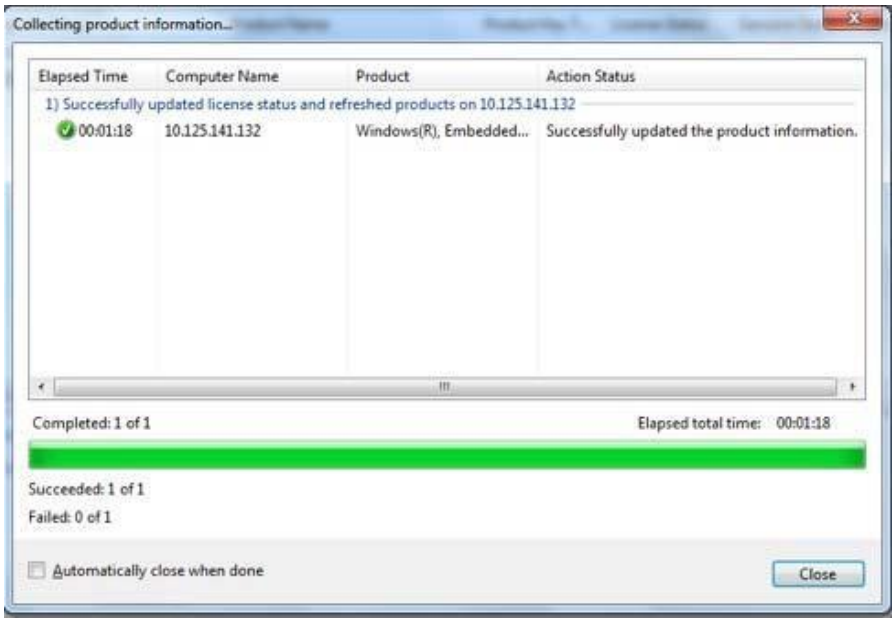
4. When VAMT 3.1 successfully locates the device, it will display it in the center pane.

Note: You can search for the device or devices you want to activate in several different ways. For information about the other options, see Volume Activation Management Tool Technical Reference: http://go.microsoft.com/fwlink/?LinkID=618656

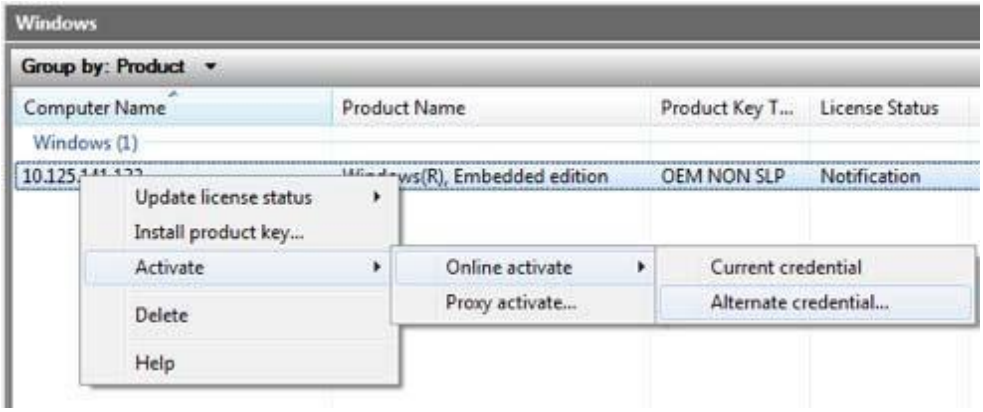
5. Right-click the device in the center pane, click **Update license status**, and then click **Alternate credential**.



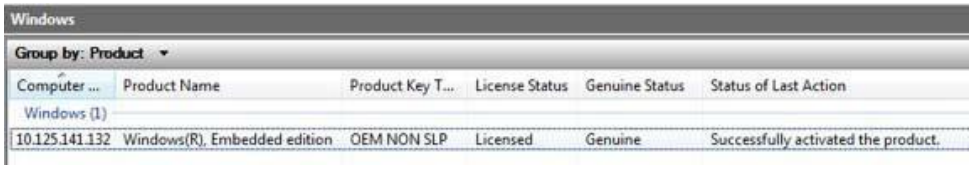
6. In the **Windows Security** dialog box, enter the username and password for an account with Administrator user rights on the device, and then click **Ok**. Note that the administrator account must have a password or VAMT 3.1 will fail.
7. A window will open and display the status of the attempts by VAMT 3.1 to update the device's information. This update can take several minutes to complete.



8. When the process has completed, click **Close**. VAMT 3.1 now displays the **License Status** value of the device as **Notification** in the center pane.
9. Right-click the device in the center pane, click **Activate**, click **Online activate**, and then click **Alternate credential**.



10. In the Windows Security dialog box, enter the user name and password for an account with Administrator user rights on the device and click **Ok**.



11. A window displays the status of the attempts by VAMT 3.1 to activate the device over the Internet. After a few minutes, the device will be activated. Note that the value in the **License Status** column has now changed to **Licensed**.

Activate a Windows 10 IoT Enterprise device by using a proxy connection to the Internet

If your device is (or can be) connected to a private network, but does not have direct access to the Internet, you can use a proxy server to act as an intermediary between the device and the Internet. The proxy server functions as a bridge between the private network and the Internet, and enables the device to communicate indirectly with the Microsoft activation servers.

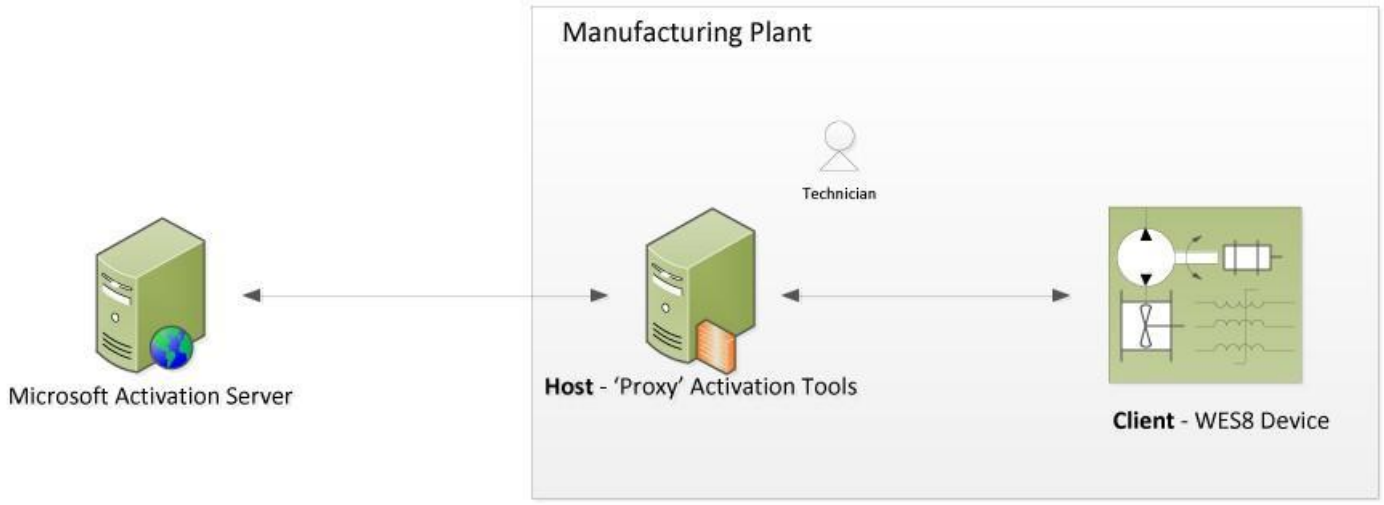
The tool that enables you to use a proxy server to activate Windows 10 IoT Enterprise devices over a network is the Volume Activation Management Tool 3.1 (VAMT 3.1). This tool is distributed for free. For more information about VAMT 3.1, please see Volume Activation Management Tool Technical Reference: http://go.microsoft.com/fwlink/?LinkID=618656

Activate a device over a private network by using VAMT 3.1 on a proxy computer

The basic flow of this process is:

1. Connect your proxy computer, which has VAMT 3.1 installed on it and access to the Internet, to the private network that your Windows 10 IoT Enterprise device is on.
2. Use VAMT 3.1 to discover your device and add your device information to the VAMT 3.1 host's database.
3. The VAMT 3.1 host contacts the Microsoft activation server over the Internet and transmits the license information of the device.
4. The Microsoft activation server returns a Confirmation ID (CID) for the device to the VAMT 3.1 host.
5. The VAMT 3.1 host applies that confirmation ID to the device. The device is now activated.

This process can be done on a device-by-device basis but is also scriptable to allow for automation or multiple-device activation.



The following procedures below describe this process in greater detail:

- Activate an Individual Device over a Private Network by Using VAMT 3.1
- Activate Multiple Devices as a Batch over a Private Network by Using VAMT 3.1

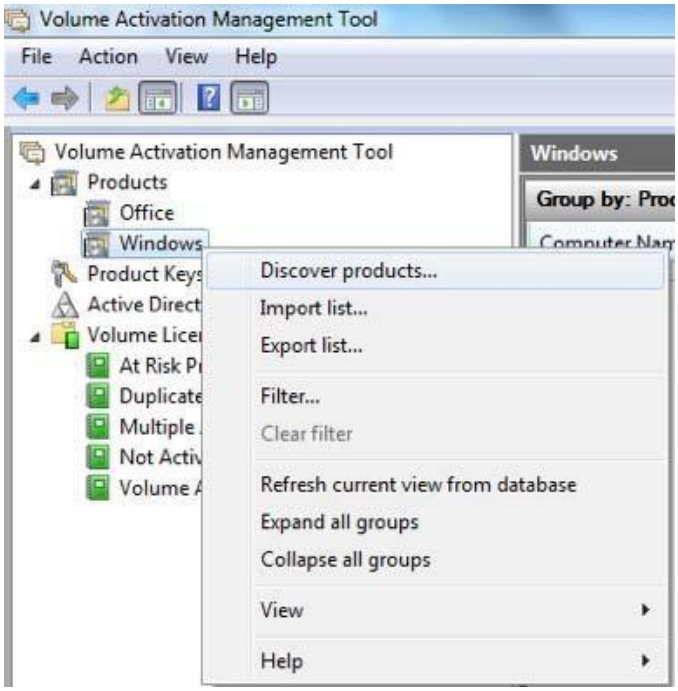
Activate an individual device over a private network by using VAMT 3.1

Prerequisites:

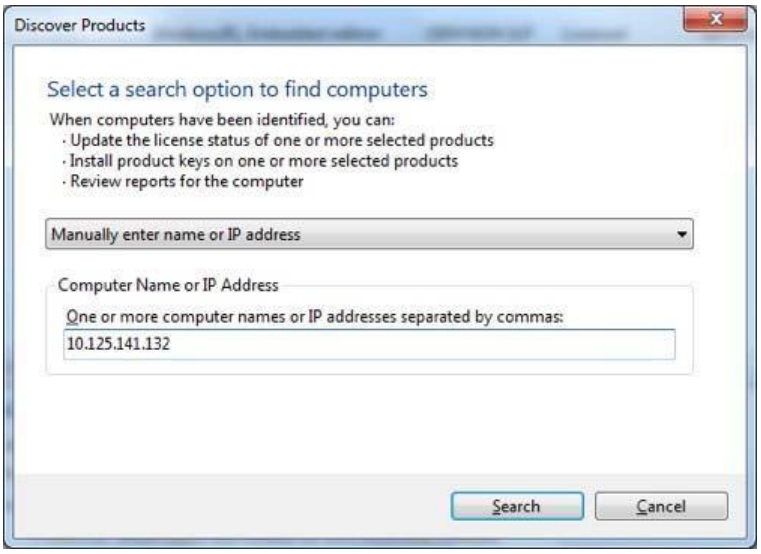
- VAMT 3.1 host, which includes the following:
  - VAMT 3.1 is installed.
  - A SQL Server database is installed.
  - The VAMT 3.1host has Internet access.
  - The VAMT 3.1 host has private network connectivity.
  - Access to TCP ports 80 and 443.
- The device to be activated contains the following:
  - Configured WMI/PowerShell remote access.
- For more information, see Allow WMI/PowerShell Remote Access on a Device: http://go.microsoft.com/fwlink/?LinkID=618657
  - Private network connectivity.
  - An administrator account with a password.

To activate:

1. On the VAMT 3.1 host, open VAMT 3.1.
2. In left pane, expand the **Products** node, right-click the **Windows** node, and then click **Discover Products**.



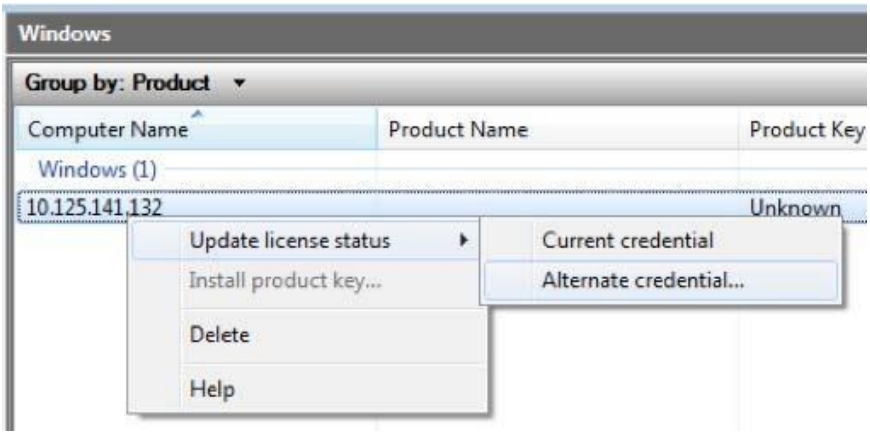
3. In the **Discover Products** dialog box, select **Manually enter name or IP address**, and then enter the name or IP address of the device you are going to activate.



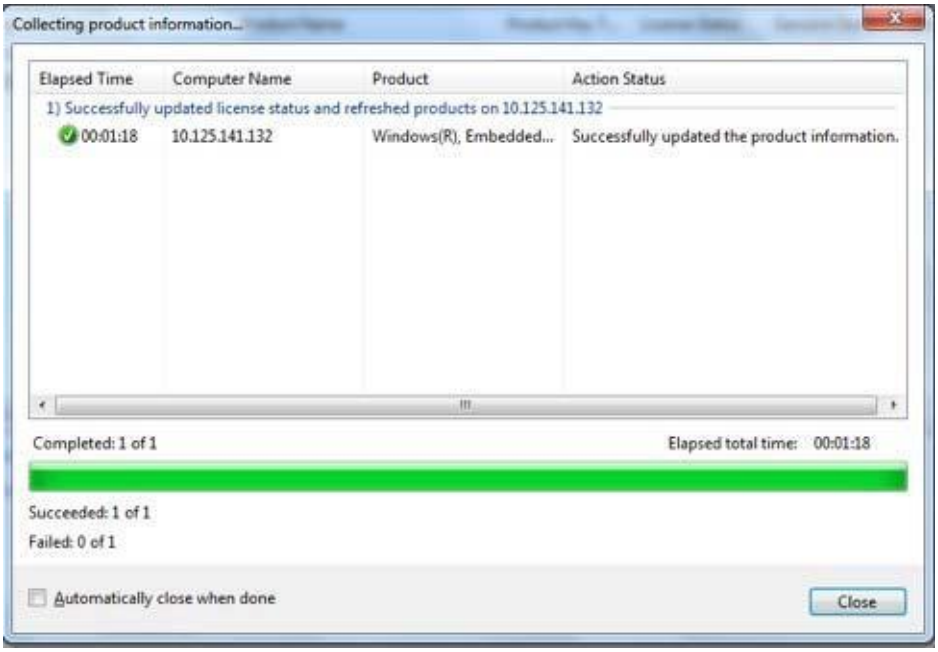
When VAMT 3.1 successfully locates the device, it will display it in the center pane.

Note: You can search for the device or devices you want to activate in several different ways. For information about the other options, see Volume Activation Management Tool Technical Reference: http://go.microsoft.com/fwlink/?LinkID=618656

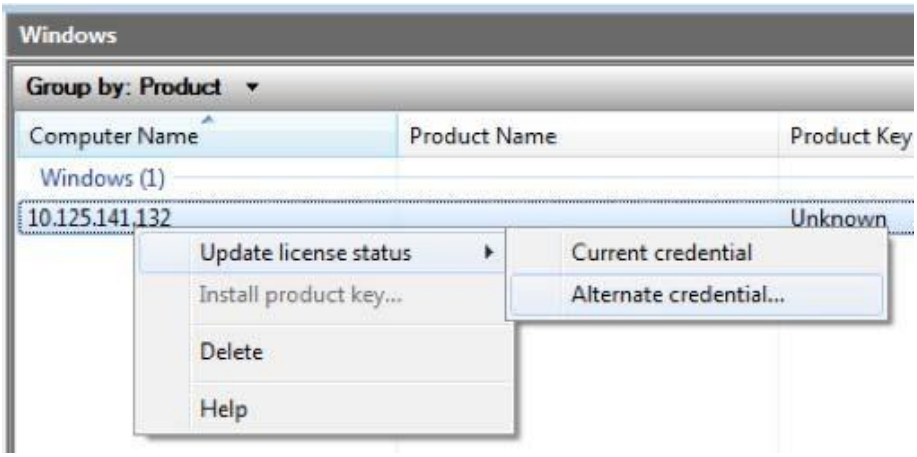
4. Right-click the device in the center pane, click **Update license status**, and then click **Alternate credential**.



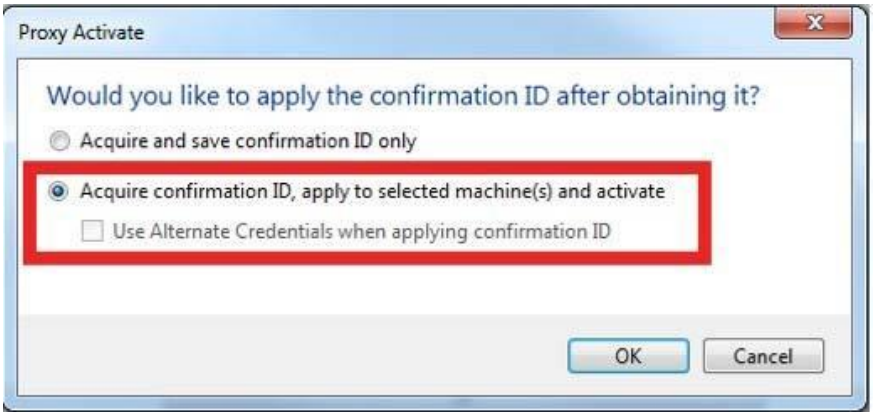
5. In the **Windows Security** dialog box, enter the username and password for an account with Administrator user rights on the device, and then click **Ok**. Note that the administrator account must have a password or VAMT 3.1 will fail.
6. A window will open and display the status of the attempts by VAMT 3.1 to update the device's information. This update can take several minutes to complete.



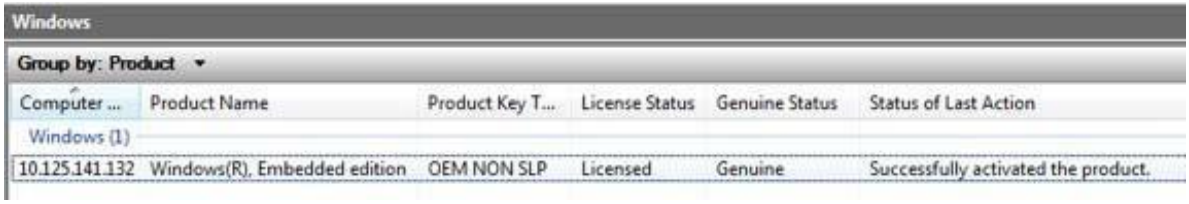
7. When the process has completed, click **Close**. Note that the center pane will now have the value **Notification** in the **License Status** column for this device.
8. Right-click the device in the center pane, click **Activate**, and then click **Proxy Activate**.



9. In the **Proxy Activate** dialog box, select **Acquire confirmation ID, apply to selected machine(s) and activate**, select the checkbox **Use Alternate Credentials when applying confirmation ID**, and then click **Ok**.



10. In the **Windows Security** dialog box, enter the username and password for an account with Administrator user rights on the device and click **Ok**.
11. A window displays the status of the attempts by VAMT 3.1 to activate the device over the Internet. After a few minutes, the device will be activated. Note that the value in the **License Status** column has now changed to **Licensed**.



Activate multiple devices as a batch over a private network by using VAMT 3.1

Windows 10 IoT Enterprise provides a Windows PowerShell command line interface script and two associated files that you can use to automate mass activation tasks. This script enables you to create a scheduled task that periodically runs the activation script and activate your devices.

The default location for these files is **%systemdrive%\Windows Embedded Standard 8\Toolset\Activation**. The files are:

- **activationHelper.ps1** Windows PowerShell script file
- **Config.xml** Configuration file
- **Config.xsd** Configuration schema file

The steps taken by the activationHelper.ps1 script are:

1. Import the VAMT module into Windows PowerShell.
2. Parse the Config.xml file to get the device IP address/name information and generate a machine list.

3. Add the machines into the VAMT database by specifying the device name or IP address. This is done as a background job.
4. Sends the device's license information to Microsoft AVS. This is a background job.
5. Obtains a confirmation ID from AVS for the device. This is a background job.
6. Applies the confirmation ID to the device. This is a background job.
7. Enables Unified Write Filter (UWF), if the flag is set in the configuration file.
8. Shuts down the device, if the flag is set in the configuration file.

Prerequisites:

- VAMT 3.1 host, which includes the following:
  - VAMT 3.1 is installed.
  - A SQL Server database is installed.
  - The VAMT 3.1 host has Internet access.
  - The VAMT 3.1 host has private network connectivity.
  - The Activation Script from the Standard 8 Toolkit has been copied to the VAMT 3.1 host and is correctly configured for your environment.
  - Windows PowerShell 4.0 is installed.
  - Access to TCP ports 80 and 443.
- The device to be activated contains the following:
  - Configured WMI/PowerShell remote access.
- Private network connectivity.
- An administrator account with a password.

To activate:

Before setting up this periodic activation process, you must modify the activation script's configuration file for your environment. The following snippet is a sample of the Config.xml configuration script:

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
    <Vamt
        InstallLocation="C:\Program Files (x86)\Windows Kits\8.0\Assessment and
Deployment Kit\VAMT 3.0"
        maxThreads="3"
        checkConnectivity="false"
    />
   <Machineidentity
        Prefix="192.168.0."
        Start="100"
        End="105"
    />
    <UserAccount
        UseAlternateCredential="true"
        Username="john"
        Password="1234"
    />
    <PostActivationTasks
        EnableUWF="false"
        ShutDownMachine="Shutdown"
    />
    <LogInfo
         Level="ErrorOnly"
         Logfile="script.log"
    />
</Configurations>
```

The settings that you use for the periodic activation process are described in the following table.

Note: The element and attribute names are case sensitive.

Element/Attribute	Description	Schema
VAMT	Specifies VAMT 3.1 related info, including installation path, maximum threads count, and check Connectivity flag.	<xs:complexTypename="vamtInfo"> <xs:annotation> <xs:documentation>VAMT infomation</xs:documentation> </xs:annotation> <xs:attributename="InstallLocation"use="required"type="xs:string"/> </xs:complexType>
maxthreads	Specifies the maximum threads running in the background.	<xs:simpleType name="smallInteger"> <xs:restriction base="xs:nonNegativeInteger"> <xs:maxInclusive value="100" /> <xs:minInclusive value="1" /> </xs:restriction> </xs:simpleType>
checkConnectivity	Specifies whether toping the machine to check connectivity first, instead of passing whole list into VAMT directly. Client machines must enable network discovery for ping operation.	<xs:attributename="checkConnectivity"use="optional"type="xs:boolean" default="false"/>
machineIdentity	Specifies the element that will be used to generate the machine ID. The rule is Prefix+index [index is from Start to End]; this sample uses IP address as a prefix string; you can easily change it to computer name like "MS-machine".	<xs:complexType name="MachineIdentityInfo"> <xs:annotation> <xs:documentation>Machine discovery phase to generate machine list, MachineNameis{Prefix+[Start..End]}</xs:documentation> </xs:annotation> <xs:attributename="Prefix"use="required"type="xs:string"/> <xs:attributename="Start"use="required"type="xs:int"/> <xs:attributename="End"use="required"type="xs:int"/> </xs:complexType>
UserAccount	Specifies whether an alternate credential is needed; if yes, then specify the username and password; if no, all the operations inside the script will use the current credential.	<xs:complexType name="useraccountInfo"> <xs:annotation> <xs:documentation>Needed to perform remote operation</ xs:documentation> </xs:annotation> <xs:attributename="UseAlternateCredential"use="required" type="xs:boolean"/> <xs:attributename="Username"type="xs:string"/> <xs:attribute name="Password" type="xs:string"/> </xs:complexType>
EnableUWF	Specifies whether to enable UWF on target machine after activation is complete.	<xs:attributename="EnableUWF"use="optional"type="xs:boolean" default="false"/>
Shutdowntype	Specifies the post-activation operations. You can specify any of the following options: • Reboot • Shut down • Log off • Power off • Do nothing	<xs:simpleType name="shutdownType"> <xs:annotation> <xs:documentation>Post-activationphasetoperformshudown operation</xs:documentation> </xs:annotation> <xs:restriction base="xs:string"> <xs:enumerationvalue="NO"/> <xs:enumerationvalue="LogOff"/> <xs:enumeration value="Shutdown"/> <xs:enumeration value="Reboot"/> <xs:enumerationvalue="PowerOff"/> </xs:restriction> </xs:simpleType>
LogInfo	Specifies the log level and log file location.	<xs:simpleType name="loglevelType"> <xs:annotation> <xs:documentation>Tospecifytheloglevel</xs:documentation> </xs:annotation> <xs:restriction base="xs:string"> <xs:enumerationvalue="NoLog"/> <xs:enumerationvalue="ErrorOnly"/> <xs:enumeration value="Info" /> </xs:restriction> </xs:simpleType>

After you set up your configuration file and save it as Config.xml, you can set up the scheduled task, by using the following steps:
On your VAMT 3.1 host, add the location of the script files to the **%path%** system variable.

1. Open the Task Scheduler by doing either of the following:
   - In Windows 10, in **Control Panel**, click **System and Security**, click **Administrative Tools**, then double-click **Task Scheduler**.
2. In **Task Scheduler**, click **Action**, and then click **Create a basic task**.
3. In the **Create basic task wizard**, enter a name and description for your task, and then click **Next**.
4. On the **Task Trigger** page, click **Next**.
5. On the **Daily** page, click **Next**.
6. On the **Action** page, select **Start a Program**, and then click **Next**.
7. On the **Start a Program** page, browse to or enter the full path to **powershell.exe** on your machine in the **Program/script box**.

Note: It is important to run the x86 version of Windows PowerShell with this script because of a VAMT 3.1 requirement. If you are running this script on an x64 system, the default path for the x86 Windows PowerShell application is **%SystemRoot%\syswow64\WindowsPowerShell\v1.0\powershell.exe**.

8. In the **Add Arguments** box, enter the script location using the **–File parameter** and the full path to the **ActivationHelper.ps1** file, and then click **Next**.
9. On the **Summary** page, select the **Open the properties dialog for this task when I click finish**, and then click **Finish**.
10. In the **Properties** dialog box:
    a. On the **General** tab, select the **Run with highest privileges** checkbox.
    b. On the **Conditions** tab, clear the **Start the task only if the computer is idle** checkbox.
    c. On the **Conditions** tab, clear the **Start the task only if the computer is on AC power** check box if it is selected.
11. Click **Ok** to complete scheduling this task.

Activate a Windows 10 IoT Enterprise device by using a telephone

If your Windows 10 IoT Enterprise device is not connected to the Internet or you can't connect your device to the Internet either directly or via a proxy connection from a private network, you must use a telephone and the Windows Software Licensing Management Tool (SLMGR) command line tool to activate the device. Alternatively, you may leave your device in deferred activation state.

If your device is connected to the Internet, but you still want to use telephone activation, you can use either SLMGR or the Windows Activation UI (SLUI).

Activate a device by using a telephone

You can activate your device by using a telephone to call the Microsoft Product Activation Center. You will need to provide your information and your 63-digit Installation ID, and you will receive a 48-digit confirmation ID from the Microsoft Product Activation Center.

You must then use either SLMGR or SLUI to activate the device by entering the confirmation ID onto the device. Your device must be connected to the Internet to use SLUI.

- Activate a Device by Using a Telephone and SLMGR.
- Activate a Device by Using a Telephone and SLUI.

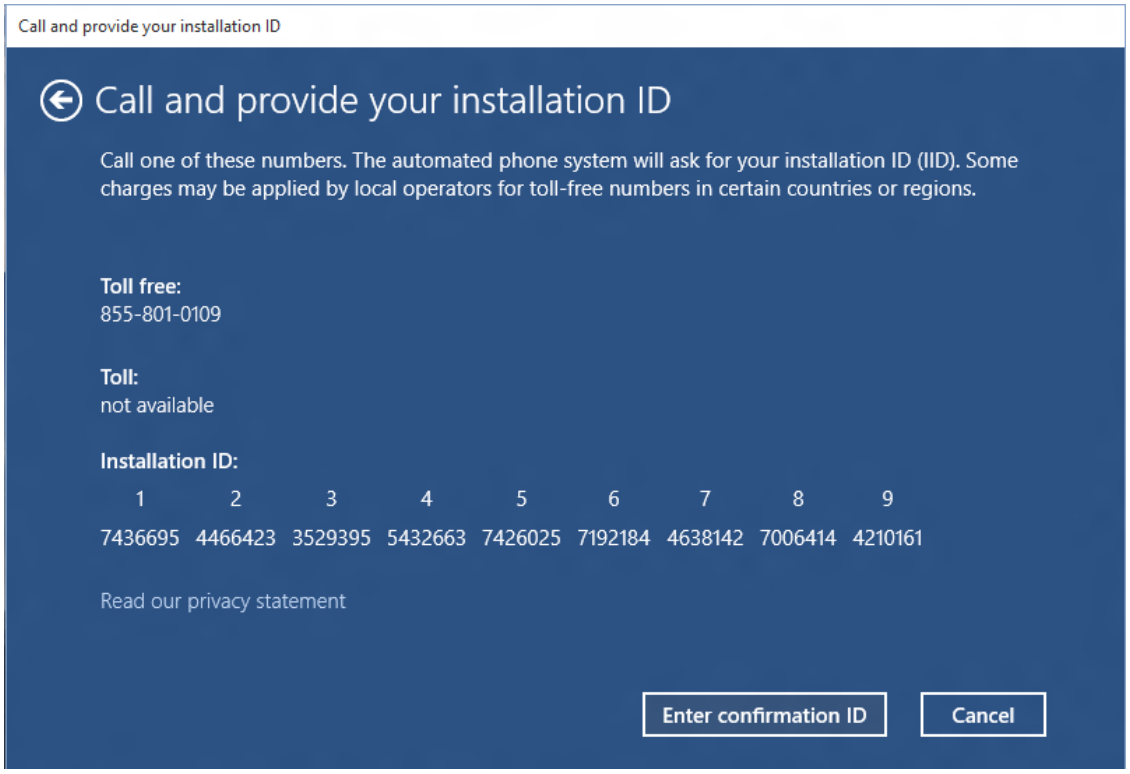
Activate a device by using a telephone and Slmgr

Prerequisites:

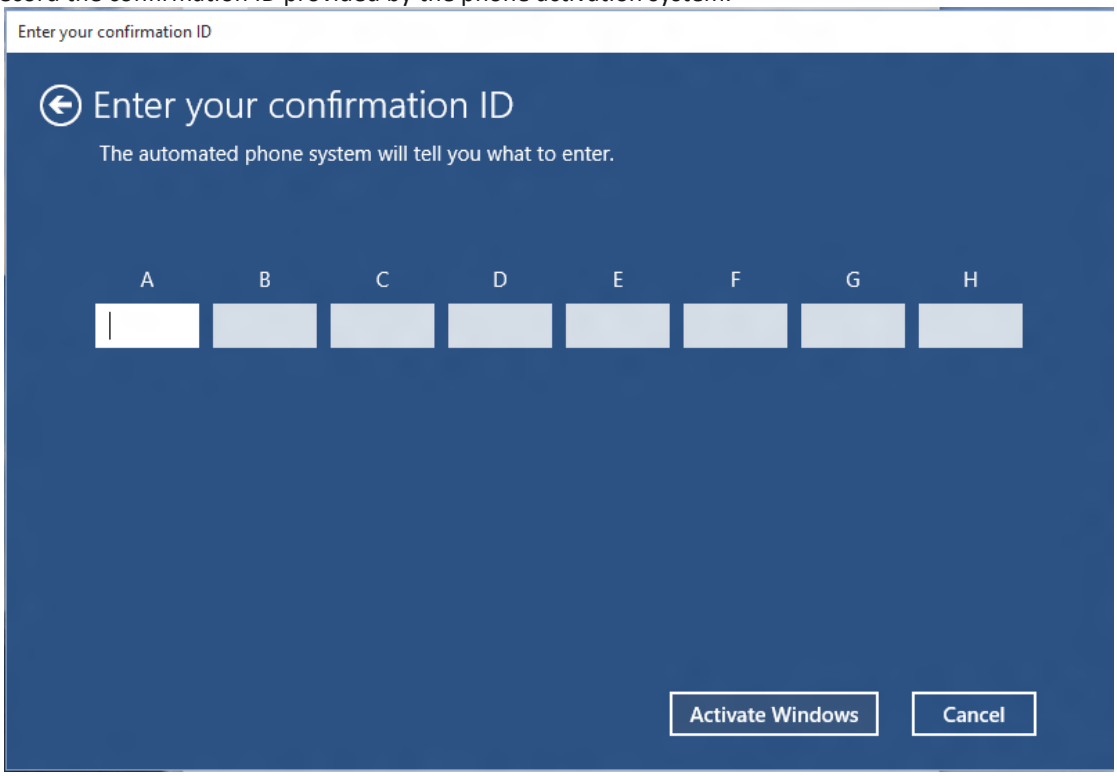
- Telephone.
- Windows 10 IoT Enterprise is installed on your device.
- You have Administrator user rights on the device.

To activate:

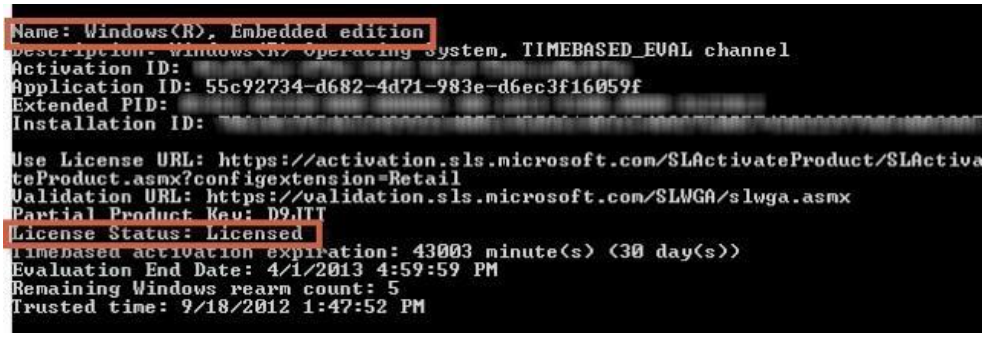
1. On your device, open a command prompt with Administrator user rights.
2. Navigate to the **<system drive>:\Windows\System32** folder, and then type: **cscript slmgr.vbs /dti**
3. Record the 63-digit **Installation ID**.



4. Call the Microsoft Product Activation Center. In the United States, call (855) 801-0109. For a list of other phone numbers, see How to Contact a Microsoft Product Activation Center by Phone: http://go.microsoft.com/fwlink/?LinkID=618655
5. Follow the automated instructions and provide the 63-digit Installation ID when prompted.
6. Record the confirmation ID provided by the phone activation system.



7. On your device, in the command prompt window, type the following, where **<confirmation id>** is the confirmation ID provided by the phone activation system. **cscript slmgr.vbs /atp <confirmation id>**



8. Type **cscript slmgr.vbs /dlv** and then verify the License Status now displays **Licensed**.

Note: Each device must be activated separately. Batch activation is not supported.

Activate a device by using a telephone and SLUI

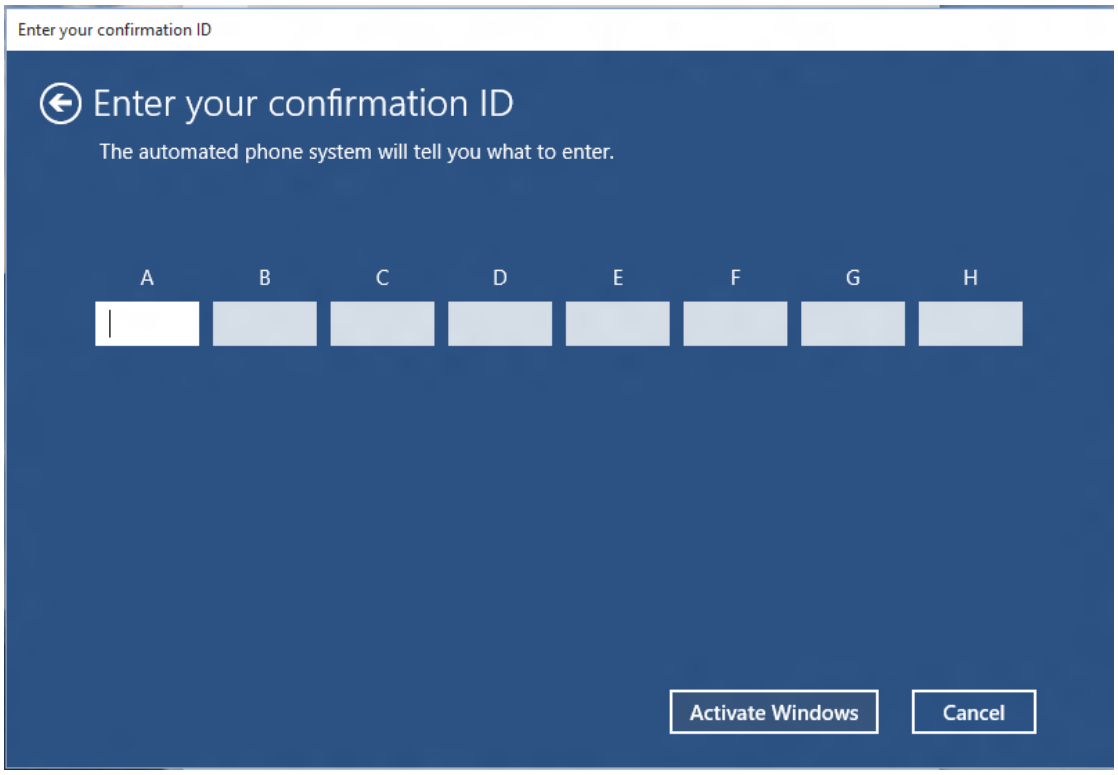
Prerequisites:

- Telephone.
- Windows 10 IoT Enterprise is installed on your device and includes the following:
- Windows Security Center module (**Features** > **Security**)
- Telephony API Client (**Features** > **Application Development Frameworks** > **Legacy Support**)
- Administrator user rights on the device.

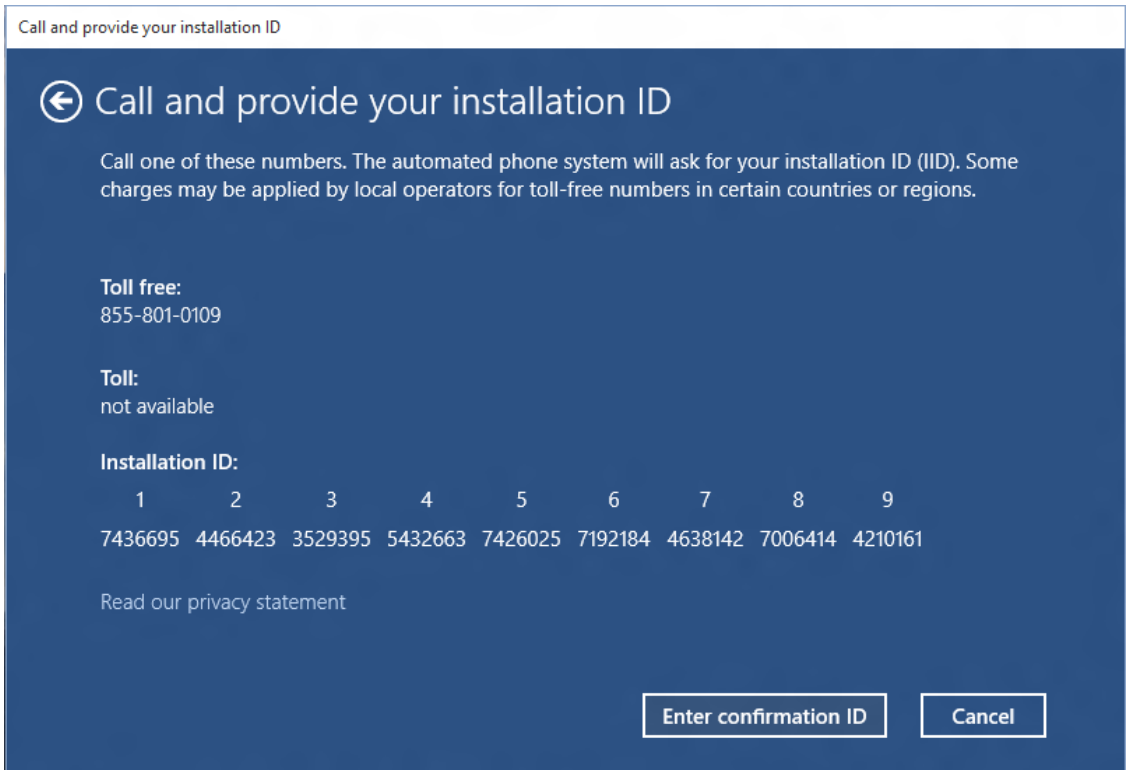
To activate:

1. On your device, open a command prompt as Administrator and launch SLUI by typing: **SLUI 4**
   Note: The 4 option instructs SLUI to launch the telephone activation UI.
2. In the **Windows activation** tool, on the **Click the nearest location** page, click **Next** to continue.
3. Call the Microsoft Product Activation Center. In the United States, call (855) 801-0109. For a list of other phone numbers, see How to Contact a Microsoft Product Activation Center by Phone: http://go.microsoft.com/fwlink/?LinkID=618655
4. Follow the automated instructions and, when prompted, provide the 63-digit Installation ID.

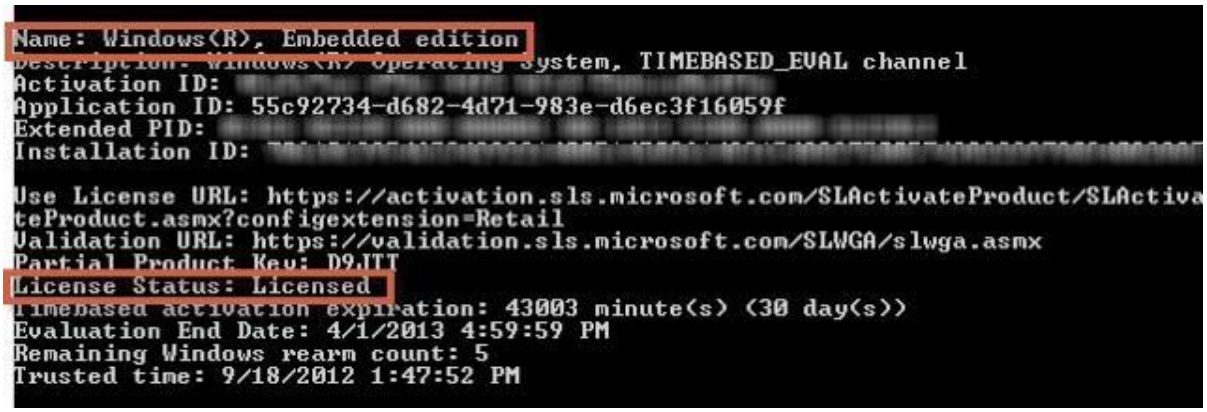
5. Enter the confirmation ID provided by the phone activation system, and then click **Activate Windows**.



6. To verify the licensing status, open a command prompt as Administrator on the device.



7. Navigate to the **<system drive >:\Windows\System32** folder, type **cscript slmgr.vbs /dlv** , and then verify that the License Status now displays **Licensed**.



Note on activation changes for Windows 10 IoT Enterprise May 2019 Update (19H1) or later

Windows 10 IoT Enterprise has always used the same binaries as Windows 10 Enterprise. While testing the May 2019 Update, our partners found an issue with the new Reserved Storage feature specific to embedded devices with a small amount of storage space. To address this, Windows 10 IoT Enterprise now has new keys, which allow settings to be included or excluded resulting in a default configuration which is different from the defaults in standard Windows 10 Enterprise. This will also allow future Windows 10 IoT Enterprise scenarios to be tailored for IoT, enabling or disabling additional features specifically for IoT devices. No new media is required to utilize this capability. Customers should continue to use the latest Windows Enterprise OPK starting with Windows 10, version 1903, but it will require new product keys starting with the 19H1 release.

Update November 25, 2019: The solutions outlined below also apply to Windows 10, version 1909. Please ensure that you have all of the Latest Cumulative Updates applied to ensure seamless installation experience.

Update Oct. 25, 2019: New product keys were introduced for the Windows 10 IoT Enterprise, version 1903 release of Windows 10 IoT Enterprise which allows features to be included or excluded, resulting in enabling a default configuration which is different from the defaults in Windows 10 Enterprise.
Partners have experienced several issues when activating or updating Windows 10 IoT Enterprise. These issues have been resolved and details are listed below.

1. Partners leveraging Windows 10 IoT Enterprise, version 1803 or Windows 10 IoT Enterprise, version 1809 with the Product Keys released with Windows 10 IoT Enterprise, version 1903 or later may experience activation failures. Please ensure that you have the Latest Cumulative Update (LCU) installed. Specifically, partners need to install the September 10 update or later available on Windows Catalog.
    - Windows 10, version 1803 Microsoft Update Catalogue [Link] (KB4516045)
    - Windows 10, version 1809 Microsoft Update Catalogue [Link] (KB4512578).
    - Windows 10, version 1903 Use the latest LCU from the Microsoft Update Catalogue
2. When upgrading from Windows 10 IoT Enterprise, version 1803 or Windows 10 IoT Enterprise, version 1809, using the Product Keys released with Windows 10 IoT Enterprise, version 1903 or later, OEMs need to review the IoT Enterprise Activation Guide updated in October 2019 as it

pertains to ePKEA/PKEA activation. Specifically, there is an important step, “Slmgr /cpky” outlined in document that is required for successful upgrades.

3. Partners who try to use a Windows 10 IoT Enterprise ePKEA/PKEA key issued prior to Windows 10 IoT Enterprise, version 1903 or later will experience activation

Below is an example of how the new 1903 keys will affect feature configurations like Reserved Storage which should be disabled on Windows 10 IoT Enterprise when using the new keys:

Starting Point	Operation	Result
Windows 10, version 1809 (10.0.17763.737 or later); OR Windows 10, version 1803 (10.0.17134.1006 or later)	Update device to Windows 10, version 1903	Device is activated as expected. Reserved Storage is not enabled on update.
Windows 10, version 1903 (10.0.18362.356)	Clean install with new 1903 key	Device activates as expected. Reserved Storage not enabled at installation when using a new key
Windows 10, version 1809 (10.0.17763.737 or later); OR Windows 10, version 1803 (10.0.17134.1006 or later)	Clean install with new 1903 key	Device activates as expected.
Windows 10, version 1903 (10.0.18362.2356 or later)	Clean install with key issued prior to 1903	PKEA and ePKEA: keys issued prior to 1903 will fail activation. See Supply Chain Guidance section below for instructions to obtain new key(s). OEM Activation 3.0: Device activates as expected when adequate storage is provided. Reserved Storage is enabled automatically with a clean install using an old key. Note: if a device has inadequate storage to accommodate the Reserved Storage feature, setup steps will fail.
Windows 10, version 1809 (10.0.17763.737 or later); OR Windows 10, version 1803 (10.0.17134.1006 or later)	Clean install with key issued prior to 1903	Device activates as expected. Reserved Storage not enabled at installation when using an old key with pre-1903 media.
Servicing	Use MBR key to repair a Windows 10 IoT Enterprise device	The Reserved Storage feature and edition identification will remain in the original state which was set by the first key activation of the media (either new or old keys)

Q: How can I tell the difference between the new keys and the old keys?

A: There is no way to distinguish the keys by range or format. However, using the new keys, the edition will show up as "Windows 10 IoT Enterprise" in 1903 and later.

SUPPLY CHAIN GUIDANCE

Product Key Entry Activation (PKEA) – Indirect

a. Authorize Replicators (ARs) will continue to ship the old Windows 10 Enterprise PKEA keys printed on COAs until **August 31, 2019**.
b. Starting on **September 1, 2019**, ARs will stop shipping the old keys and will start shipping the new Windows 10 IoT Enterprise PKEA keys.
c. The old and new PKEA keys can be identified by locating the Base Label Stock (BLS) Part Number printed on the COA.
    i. The old PKEA keys are printed on three different BLS: X21-95364, X21-95365, X21-95366
    ii. The new PKEA keys are printed on three different BLS: X22-14281, X22-14283, X22-14282

Embedded Product Key Entry Activation (EPKEA) - Indirect

d. Please note that you will be able to request the old Windows 10 Enterprise EPKEA keys until **August 31, 2019**.
e. Starting on **September 1, 2019**, any key requested will be the new Windows 10 IoT Enterprise EPKEA keys.
f. To ensure that you get the new Windows 10 IoT Enterprise EPKEA key, please fill out the key request form located here and submit to OASignh@microsoft.com.

Product Key Entry Activation (PKEA) – Direct

g. Authorize Replicators (ARs) will continue to ship the old Windows 10 Enterprise PKEA keys printed on COAs until **August 27, 2019**.
h. Starting on **August 28, 2019**, ARs will stop shipping the old keys and will start shipping the new Windows 10 IoT Enterprise PKEA keys.
i. The old and new PKEA keys can be identified by locating the Base Label Stock (BLS) Part Number printed on the COA.
    i. The old PKEA keys are printed on three different BLS: X21-95364, X21-95365, X21-95366
    ii. The new PKEA keys are printed on three different BLS: X22-14281, X22-14283, X22-14282

Embedded Product Key Entry Activation (EPKEA) - Direct

j. Please note that you will be able to request the old Windows 10 Enterprise EPKEA keys until **August 27, 2019**.
k. Starting on **August 28, 2019**, any key requested will be the new Windows 10 IoT Enterprise EPKEA keys.
l. To ensure that you get the new Windows 10 IoT Enterprise EPKEA key, please fill out the key request form located here and submit to OASignh@microsoft.com.

OEM Activation 3.0 - Direct

m. OEM customers will be able to order the old Windows 10 Enterprise OA3.0 keys until **August 27, 2019**.
n. On **August 28, 2019**, any keys ordered will be the new Windows 10 IoT Enterprise OA3.0 keys.
o. The same Licensable Part Number will be used to order the new Windows 10 IoT Enterprise OA3.0 key.
p. OEM customers are asked to take special precautions to segregate the older Windows 10 Enterprise OA3.0 keys and new Windows 10 IoT Enterprise OA3.0 keys to avoid an inventory mix up of old and new keys.
q. If preferred the OEM customer can return the old Windows 10 Enterprise OA3.0 keys, provided new Windows 10 IoT Enterprise OA3.0 keys are ordered to replace them. Please contact your Microsoft Operations Account Manager for additional details.
r. Your return and reorder must be completed by **September 30, 2019**. Any requests not completed by this date will be denied.

Microsoft