Interactive BIOS simulator

Welcome to the interactive BIOS simulator for the
HP Spectre x360 Convertible PC

Here's how to use it...

**BIOS Utility Menus:** (Click the link to navigate to the individual menus)
On this page you will find thumbnail images of each of the product's BIOS utility menus. To view a specific menu in greater detail, simply click that thumbnail. Just as in the live BIOS, on each menu, you can select the tab of each of the other utility menus to navigate directly to that menu.

**Menu options:**
While the menu options cannot be toggled, many of them offer item specific information about that option. To view this information, use the cursor to rollover the option and the information will present in a pane on the right of the BIOS screen.

That's it!

On every page there is a link that brings you back to either this Welcome page or the BIOS Utility Menus page enabling you to navigate to whatever BIOS option you wish to review.
BIOS Utility Menus

Back to Welcome Page
## Main Menu

### System Information
- **System Time:** [00:09:34]
- **System Date:** [01/01/2019]
- **Product Name:** HP Spectre x360 Convertible 13-aw0xxx
- **System Family:** HP Spectre
- **Product Number:** X3A5KU4#ABA
- **System Board ID:** 86FA
- **Born On Date:** 07/22/2019
- **Processor Type:** Intel (R) Core (TM) i7-1065G7 CPU @ 1.30GHz
- **Total Memory:** 16 GB

### BIOS Information
- **BIOS Vendor:** AMI
- **BIOS Revision:** B.08
- **Device Firmware Revision:** SCD92622KS
- **UUID Number:** 39444335-3632-3232-4B35-353236324435
- **System Board CT Number:** PX3ANBD8JCE01I
- **Factory installed OS:** Win10
- **Primary Battery SN:** 2B0306 06/07/2018
- **Build ID:** 19WW2RAT6ai#SABA#DABA
- **Feature Byte:** 3K6b 7N7W aBaH apaq asaw bVbh bzc b dUdx dUdp fPhz kf .2T
## Security Menu

**Main | Security | Configuration | Boot Options | Exit**

<table>
<thead>
<tr>
<th>Item</th>
<th>Setting</th>
<th>Item Specific Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator Password</td>
<td>[Clear]</td>
<td></td>
</tr>
<tr>
<td>Power-On Password</td>
<td>[Clear]</td>
<td></td>
</tr>
<tr>
<td>Intel Software Guard Extensions (SGX)</td>
<td>[S/W Controlled]</td>
<td></td>
</tr>
<tr>
<td>HP Sparekey</td>
<td>[Disabled]</td>
<td></td>
</tr>
<tr>
<td>HP Sparekey Enrollment</td>
<td>[Not Enrolled]</td>
<td></td>
</tr>
<tr>
<td>TPM Device</td>
<td>[Available]</td>
<td></td>
</tr>
<tr>
<td>TPM State</td>
<td>[Enable]</td>
<td></td>
</tr>
<tr>
<td>Clear TMP</td>
<td>[No]</td>
<td></td>
</tr>
<tr>
<td>Restore Security settings to Factory defaults</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fingerprint Reset On ReBoot</td>
<td>[No]</td>
<td></td>
</tr>
</tbody>
</table>

Back to Welcome Page
## System Configuration Menu

### Main Security Configuration

<table>
<thead>
<tr>
<th>Item</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Language</td>
<td>[English]</td>
</tr>
<tr>
<td>Virtualization Technology</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Fan Always On</td>
<td>[Disabled]</td>
</tr>
<tr>
<td>Action Key Mode</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>USB Charging</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>Battery Remaining Time</td>
<td>[Enabled]</td>
</tr>
<tr>
<td>UEFI HII Configuration</td>
<td></td>
</tr>
</tbody>
</table>
# Boot Options Menu

## POST HotKey Delay
- 0

## USB Boot
- [Enabled]

## Network Boot
- [Disabled]

## Network Boot Protocol
- IPv4+IPv6 (UEFI)

## Legacy Support
- [Disabled]

## Secure Boot
- [Enabled]

## Platform Key
- [Enrolled-MSFT]

## Pending Action
- None

### Clear All Secure Boot Keys
- None

### Load HP Factory Defaults Keys
- None

### Load MSFT Debug Policy Keys
- None

## UEFI Boot Order
- **OS Boot Manager**
  - USB Flash Drives/USB Hard Disk
  - USB CD/DVD ROM Drive
  - USB Network Adapter

## Legacy Boot Order
- Internal Hard Drive
- USB Flash Drive/USB Hard Disk
- USB CD/DVD ROM Drive
- USB Network Adapter

---

**Back to BIOS Utility Menus**

**Back to Welcome Page**
Exit Menu

Back to BIOS Utility Menus

Back to Welcome Page
## Device Firmware Revision

<table>
<thead>
<tr>
<th>Device Firmware Revision</th>
<th>Intel ME (Management Engine)</th>
<th>12.0.6.1120</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>GOP (Graphic Output Protocol)</td>
<td>9.0.1079</td>
</tr>
</tbody>
</table>

### Item Specific Help

Back to BIOS Utility Menus

Back to Welcome Page
### System Log

![System Log Table]

**Main**

**System Log**

<table>
<thead>
<tr>
<th>Result</th>
<th>Time: 010109-000039</th>
</tr>
</thead>
<tbody>
<tr>
<td>0502</td>
<td>- No Data -</td>
</tr>
</tbody>
</table>

**Item Specific Help**

---

Back to BIOS Utility Menus

Back to Welcome Page
## Device Options

### Back to BIOS Utility Menus

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Item Specific Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Options</td>
<td></td>
</tr>
<tr>
<td>Serial Port</td>
<td>[3F8-3FF; IRQ4]</td>
</tr>
</tbody>
</table>

### Back to Welcome Page
# Thermal

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Item Specific Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>Thermal</td>
<td></td>
</tr>
<tr>
<td>CPU Fan Speed</td>
<td>: N/A</td>
</tr>
</tbody>
</table>

Back to BIOS Utility Menus

Back to Welcome Page
UEFI HII Configuration

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Item Specific Help</th>
</tr>
</thead>
<tbody>
<tr>
<td>UEFI HII Configuration</td>
<td></td>
</tr>
<tr>
<td>Realtek PCIe GBE Controller (MAC: 10:E7:C6:29:62:00)</td>
<td></td>
</tr>
</tbody>
</table>

Back to BIOS Utility Menus

Back to Welcome Page