



BIOS-SHIELD User's Guide

Rev 05 05/18/20



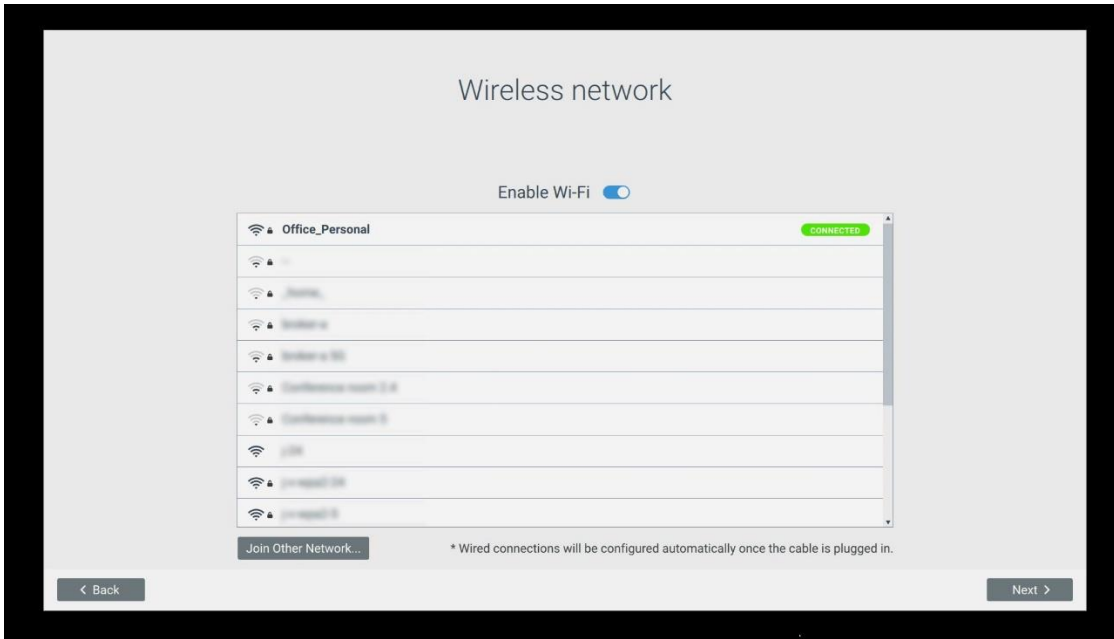
This User's Manual is designed for both new and experienced users to provide step-by-step guidance in setting up BIOS-SHIELD initially as well as activating key features. You can find more details on the features and functions on our website at <http://www.bios-shield.com>

Table of Contents

1. Connecting to Wireless	Page 3
2. Setting up the Snapshot Feature	Page 4
3. How to Restore a Snapshot	Page 7
4. Rename or Delete a Snapshot	Page 10
5. USB Control	Page 11
6. USB Encryption	Page 12
7. Bluetooth Setup	Page 16
8. Advanced Network Setup	Page 21
9. Secure Browser	Page 22
10. System Up-dates	Page 30
11. Re-setting the System	Page 31
12. Cloud Management	Page 32

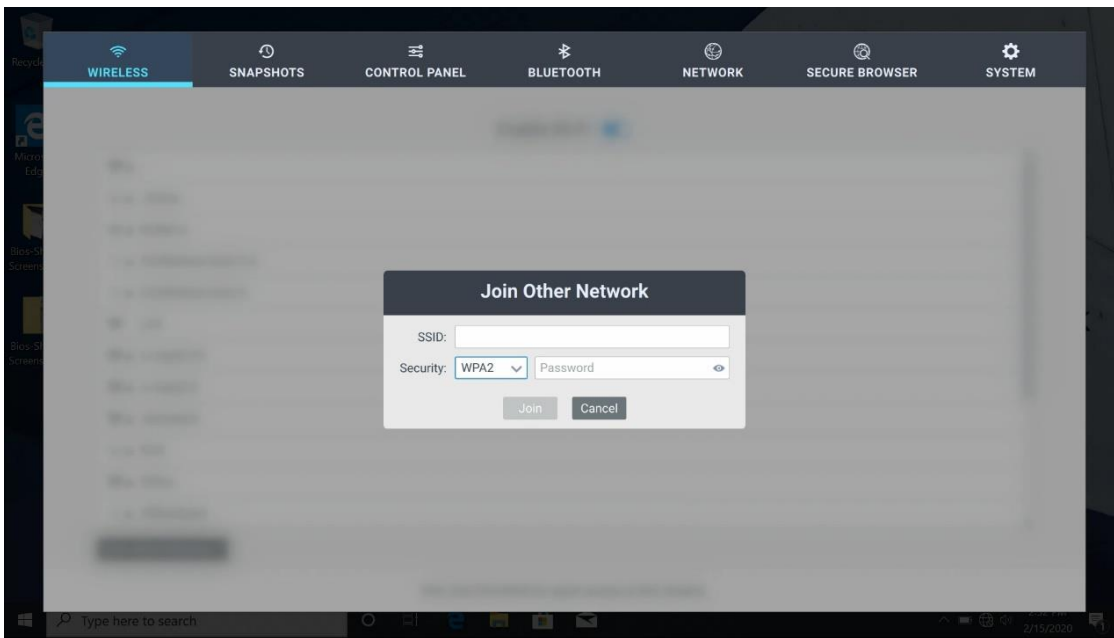
To begin, Use Ctrl-Alt-B to invoke BIOS-SHIELD GUI

1. Wireless connection:

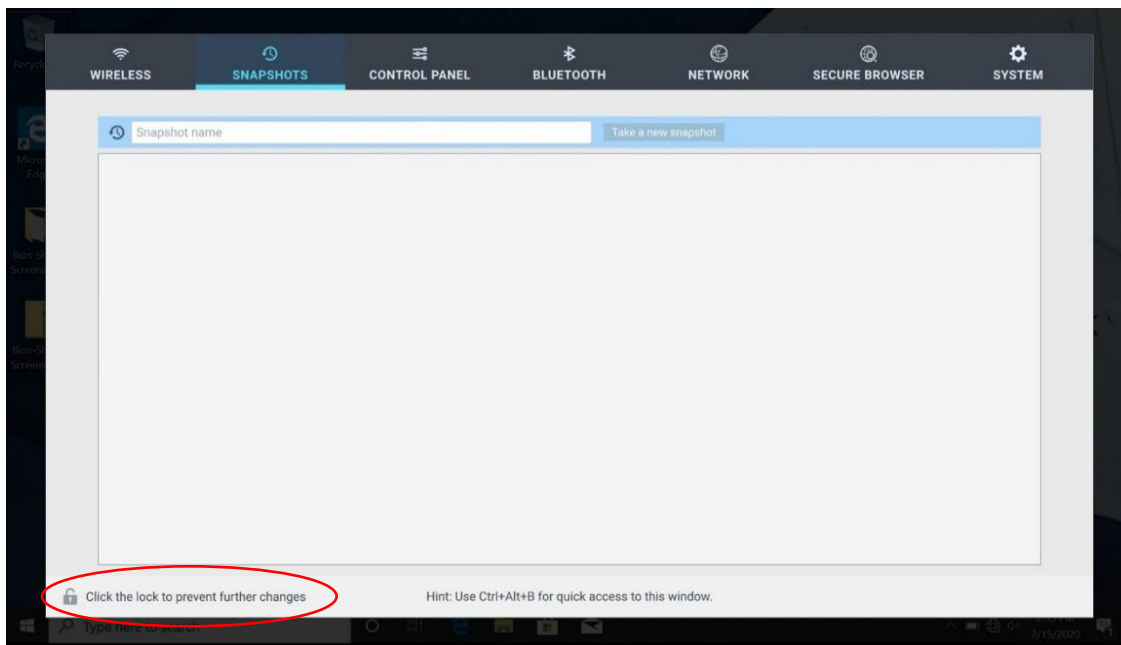


When the Wi-Fi is enabled, BIOS-SHIELD will scan nearby wireless access points. Select a wireless point and enter password to connect.

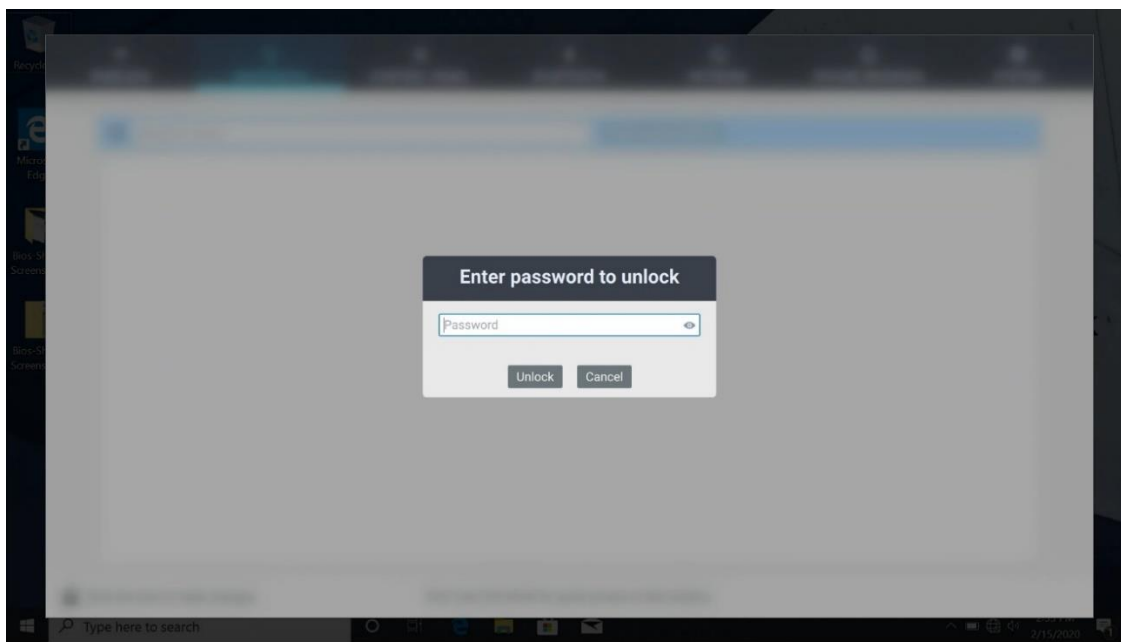
If a wireless access point is hidden (not broadcast), please click “Join Other Network” and enter SSID name, use pull down menu to select Security type and enter password. Then click “Join” to connect to wireless network.



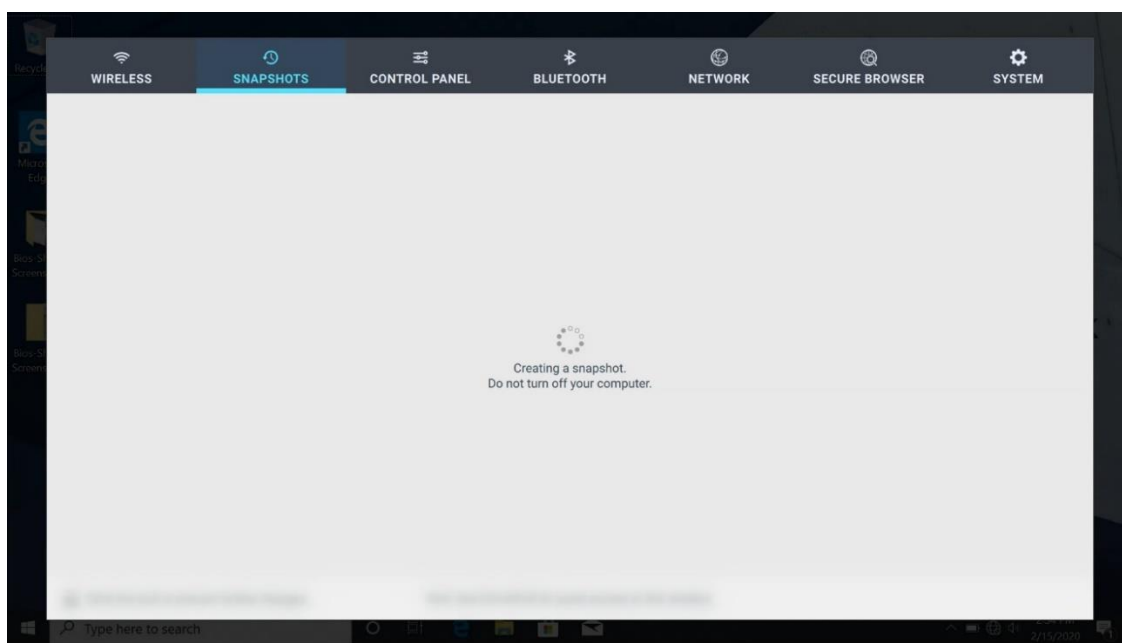
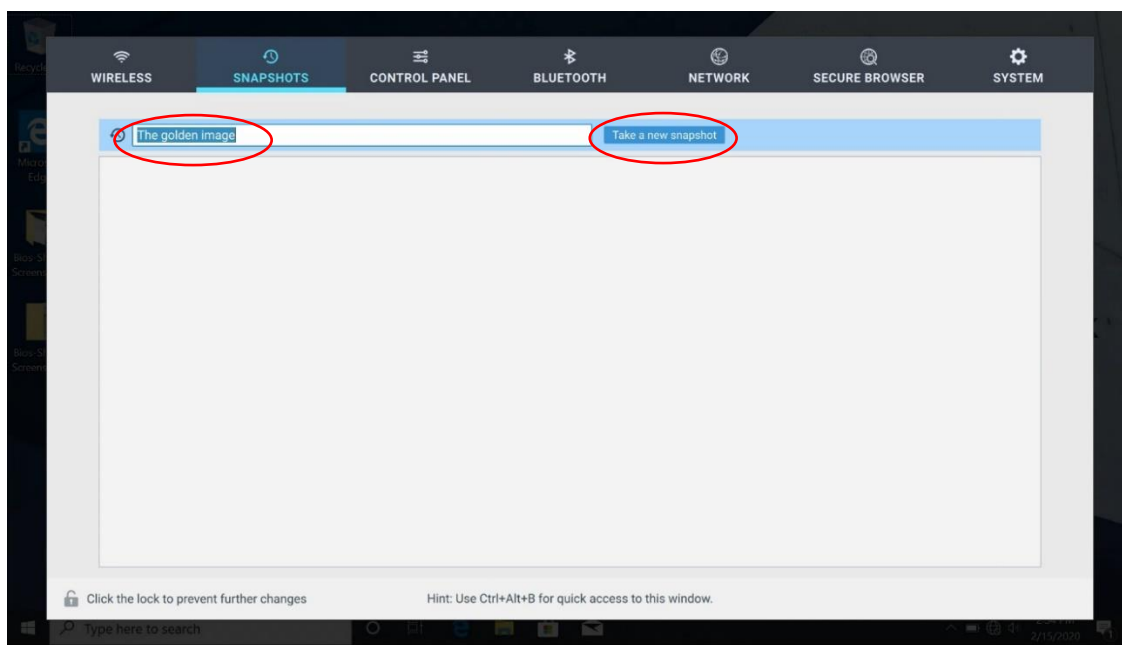
2. Setting up the Snapshot Feature:



Click the unlock icon and enter BIOS-SHIELD password

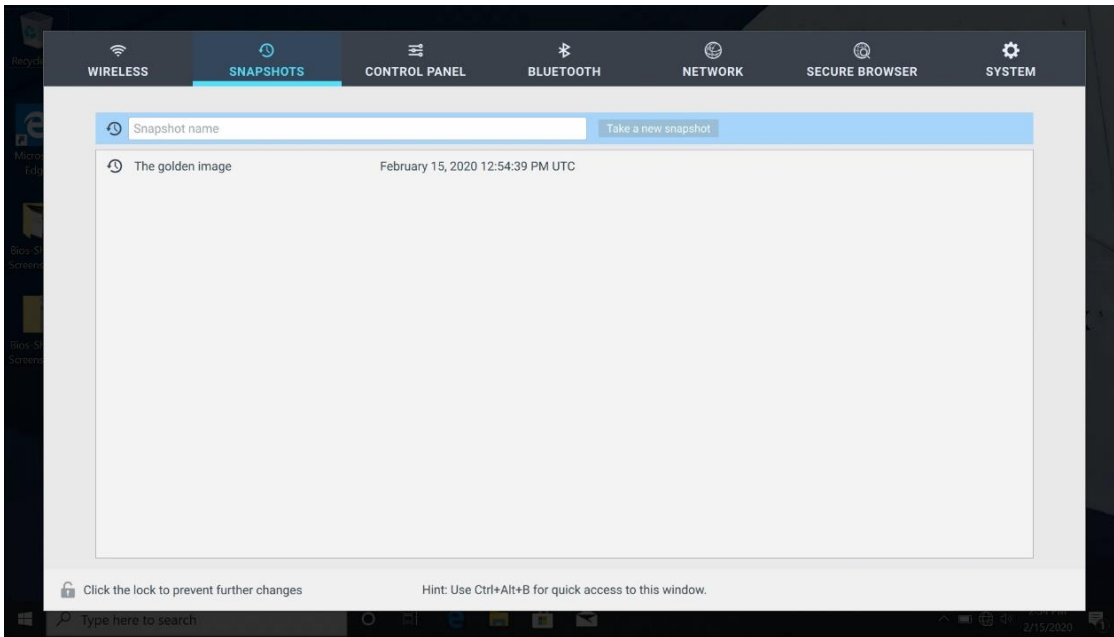


After entering the correct password, BIOS-SHIELD snapshot UI will be available. Enter the name of the first snapshot point. For example: “The golden image” and click “Take a new snapshot”

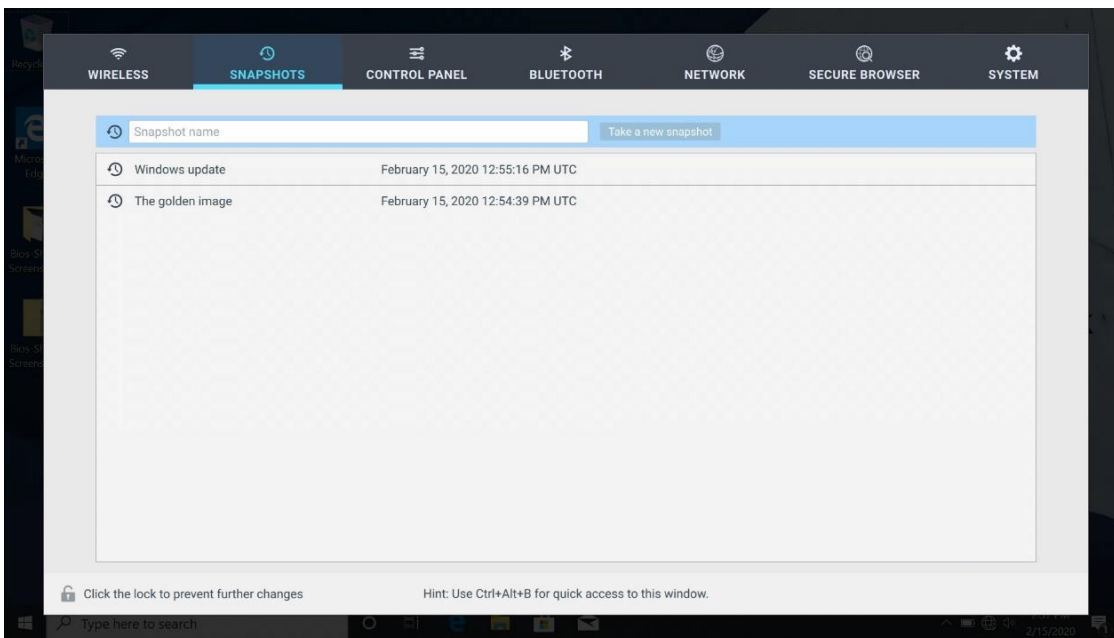


BIOS-SHIELD will create a new snapshot point. The time required for a snapshot point creation can vary. If your computer has a lot of active tasks and hard disk access (for example, Windows update running in background), it may take longer time.

Snapshot point created.

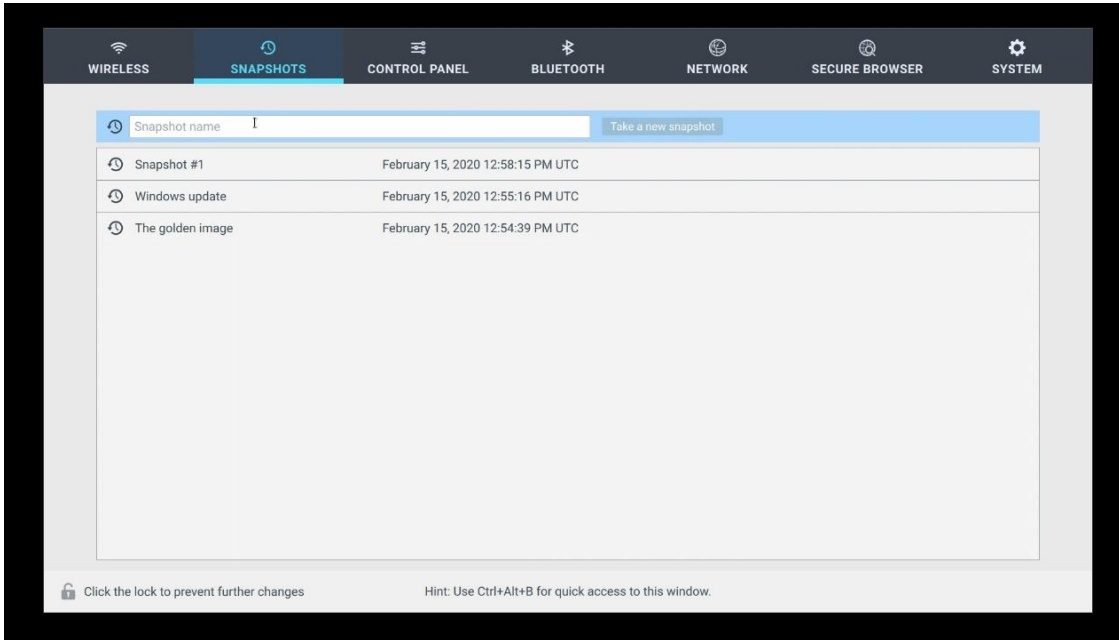


You can create snapshot points whenever they are needed. For example, it's a good idea to create a snapshot point after a major milestone such as "Windows Update".



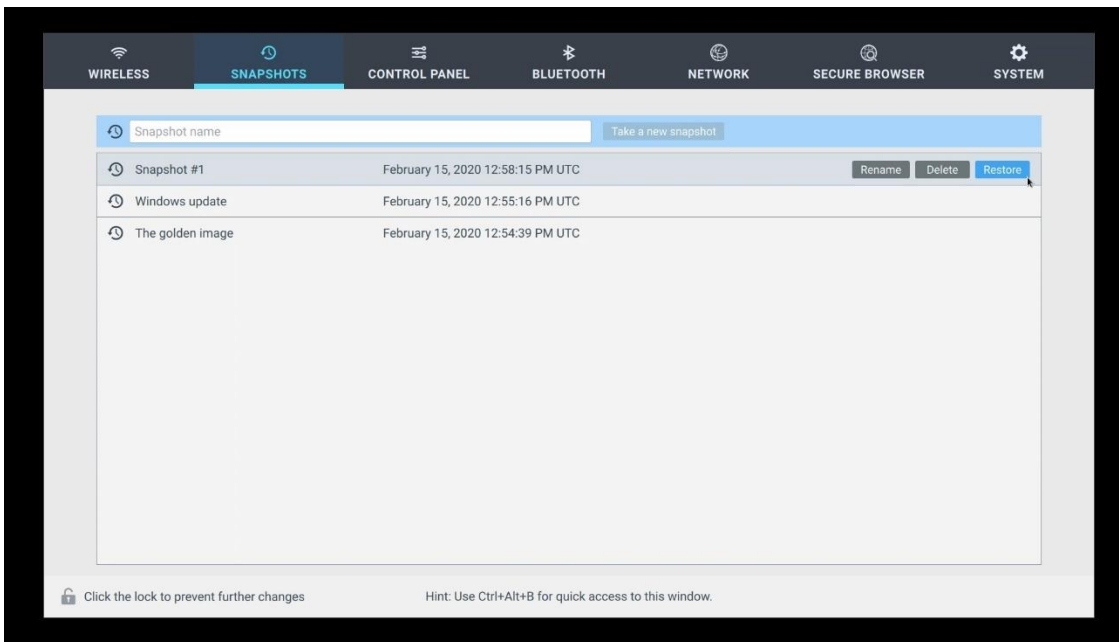
3. How to restore a snapshot:

Once you create some files on the desktop, you should go ahead and create a snapshot name “Snapshot #1”

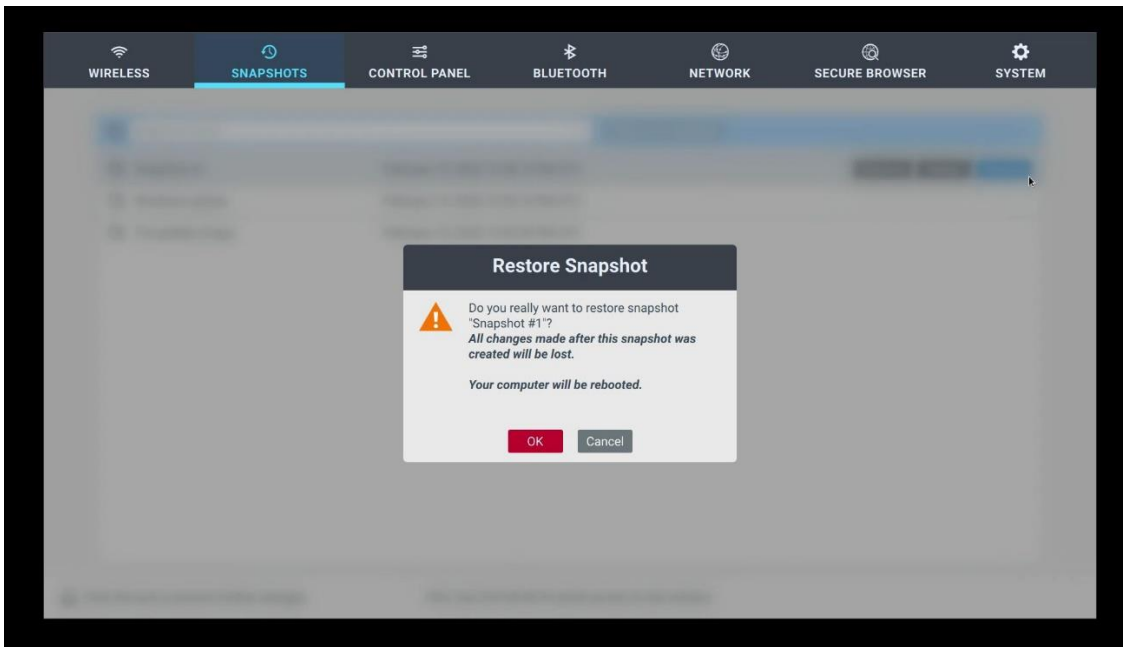


Afterwards, go to Windows desktop to delete those newly created files (file1 and file2)

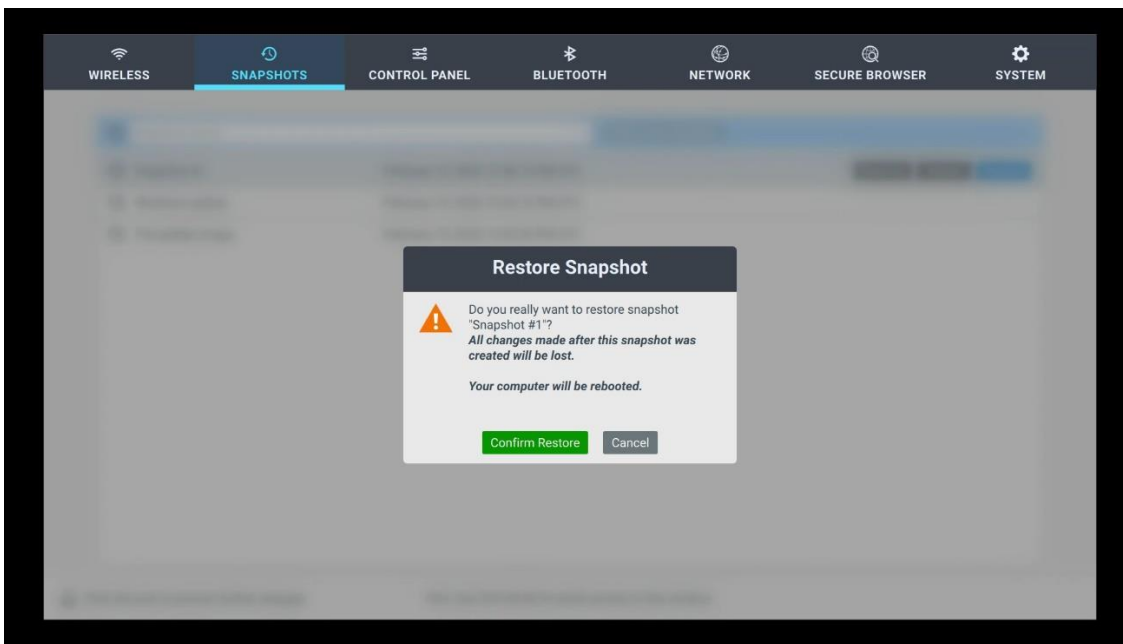
Ctrl-Alt-B to BIOS-SHIELD, select SNAPSHOTS tab, enter BIOS-SHIELD password to unlock, select snapshot #1 and click “Restore”



BIOS-SHIELD will remind users of any changes made after “Snapshot #1” will be lost. Press OK if you agree to proceed.



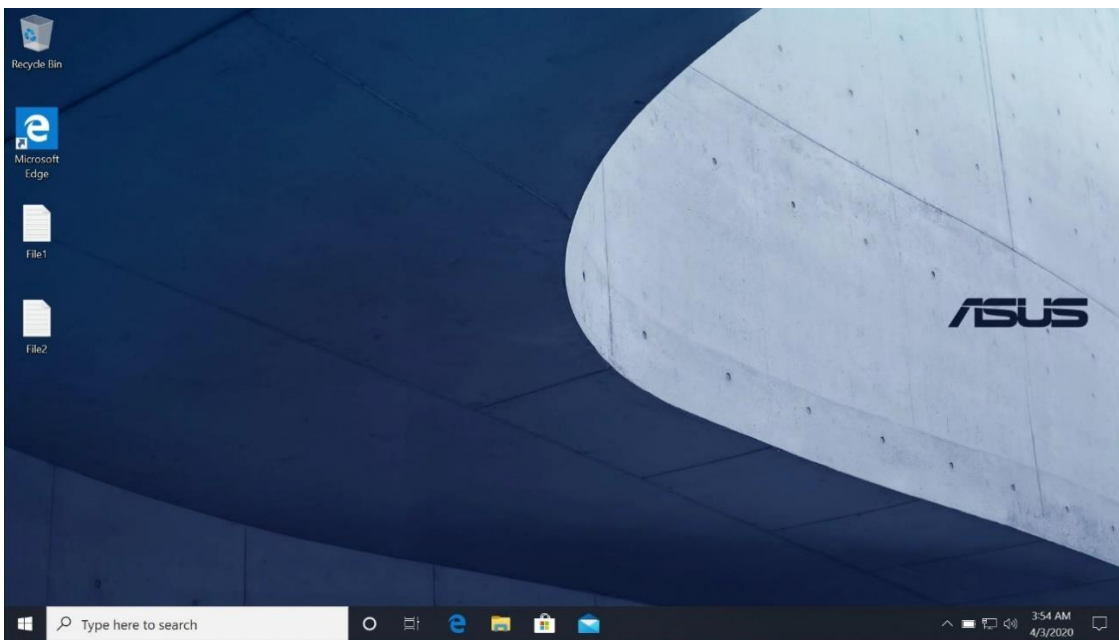
BIOS-SHIELD asks for confirmation. Click “Confirm Restore” to proceed.



Computer reboot



After snapshot restores, File1 and File2 will be restored to the Desktop.



4. Rename Snapshot:

You can also select a snapshot and rename it to a more descriptive name.

Delete Snapshot:

If you don't need a snapshot that you created 2 months ago, you can simply select it and delete it.

Best Practice:

It's recommended to create snapshots at regular intervals and at certain event. For example, prior to running a new software that you download. If you are unsure if it is compatible with your system, it's good idea to create a snapshot. Should the software conflict with your computer, you can quickly restore to it to the latest snapshot point.

Snapshot feature helps users protect their data. It does NOT provide virus protection. It's recommended to use Anti-Virus software and keep it up-to-dated.

Snapshot feature works in conjunction with an Anti-Virus solution.

5. Control Panel:

USB control: Enter BIOS-SHIELD password to enable USB control

USB control is done by device type

Mass Storage: USB hard disk, USB thumb drive, USB card reader, USB CD-ROM/DVD-ROM, SD-Card Reader

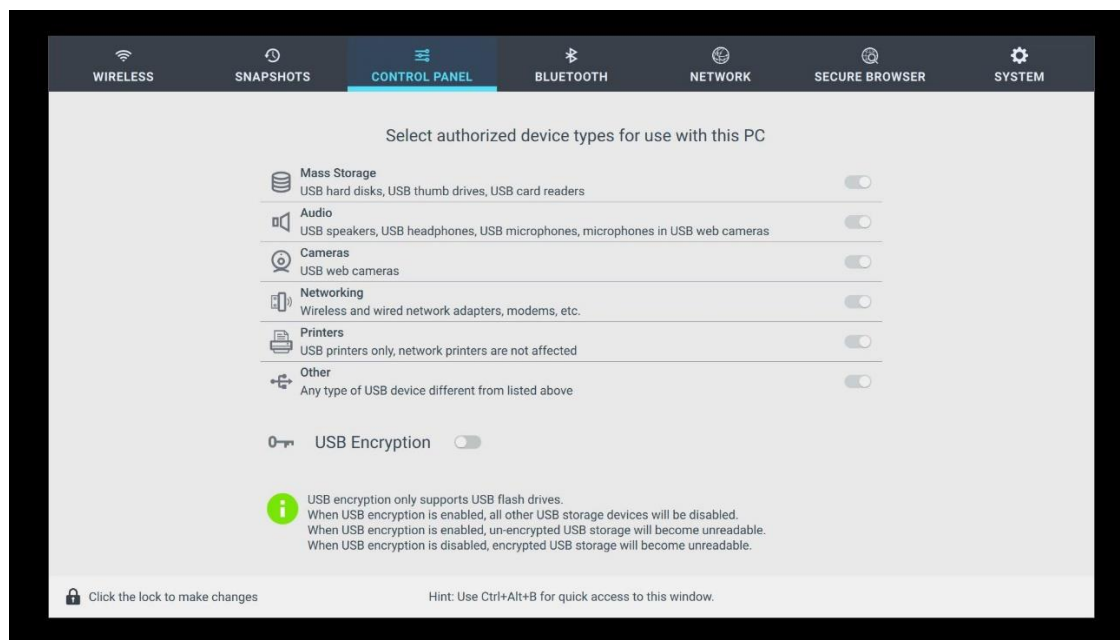
Audio: USB speaker, USB headsets, microphone built-in with USB Webcam

Cameras: Build-in camera in your laptop or USB Webcam

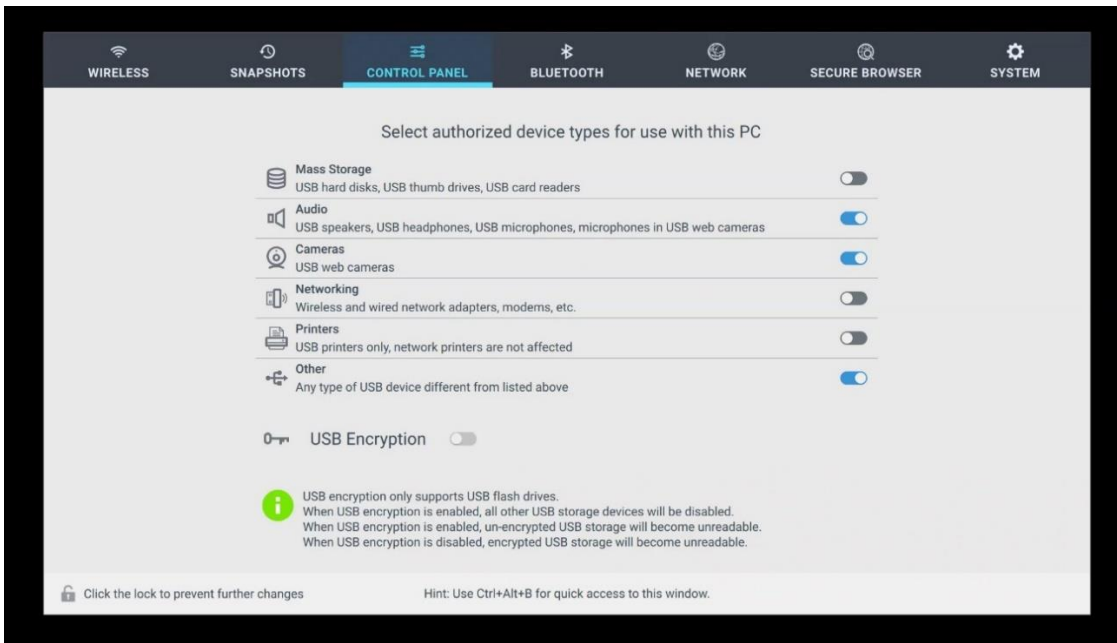
Networking: Wireless and wired USB network adapters

Printers: USB printers. Network printers is not affected.

Other: Any type of USB devices not included in the categories above



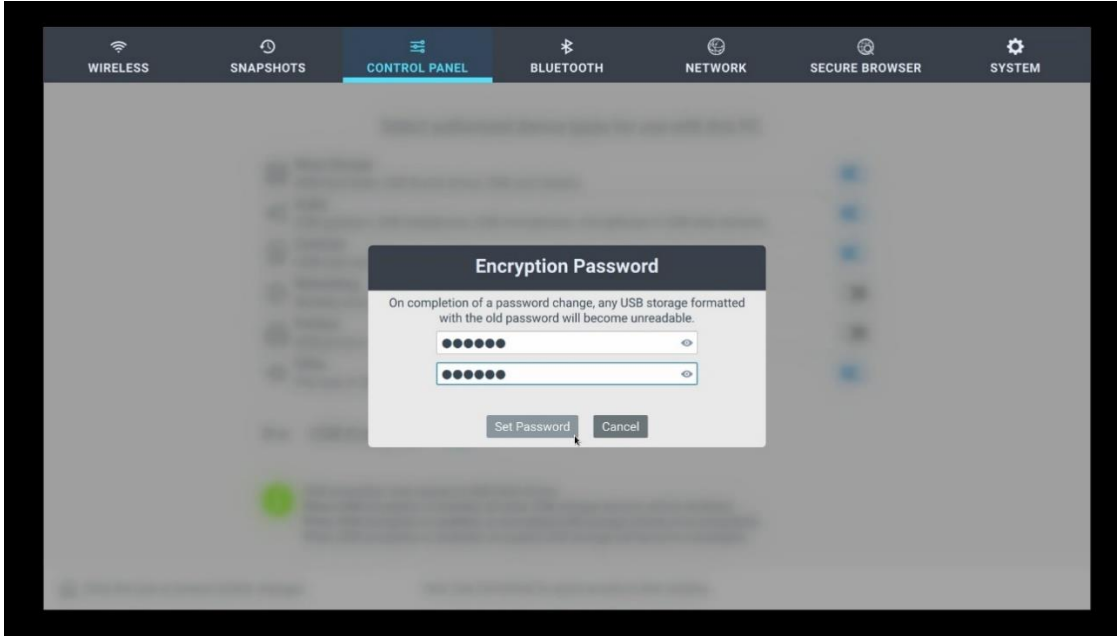
Example:



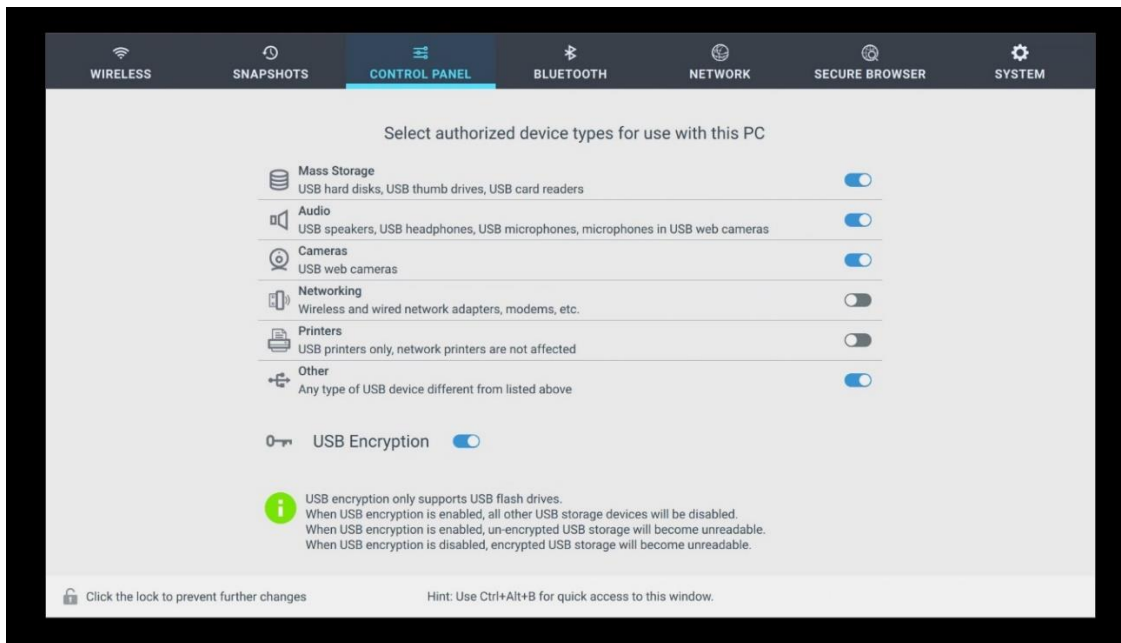
6. USB Encryption:

If you want to use USB encryption, you will need to enable Mass Storage and then turn on USB Encryption switch

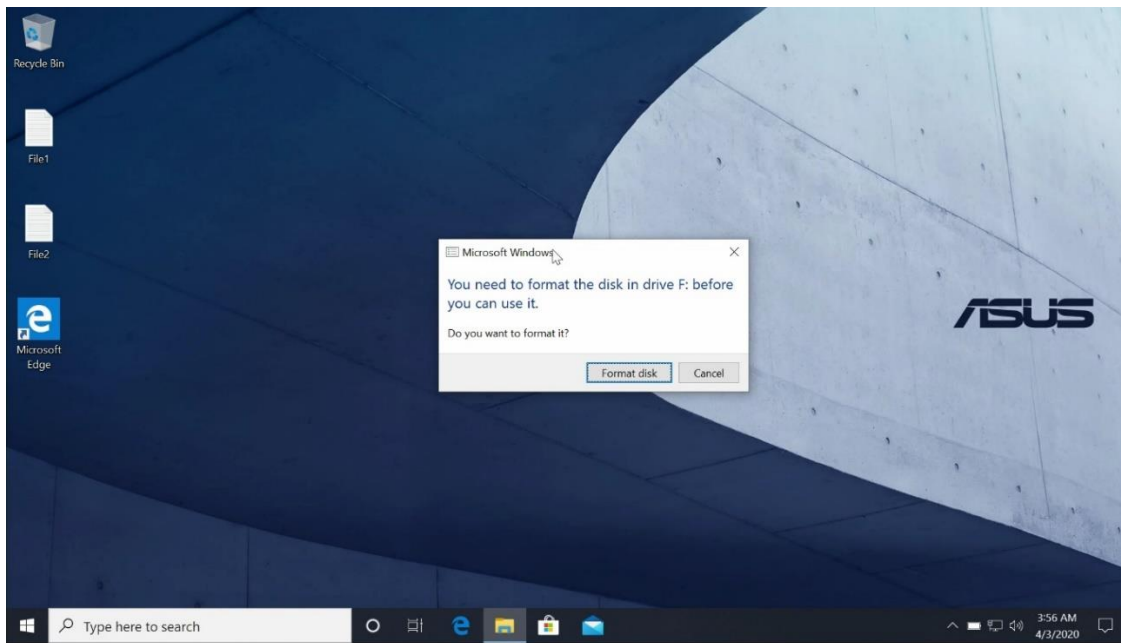
Enter USB Encryption Password.

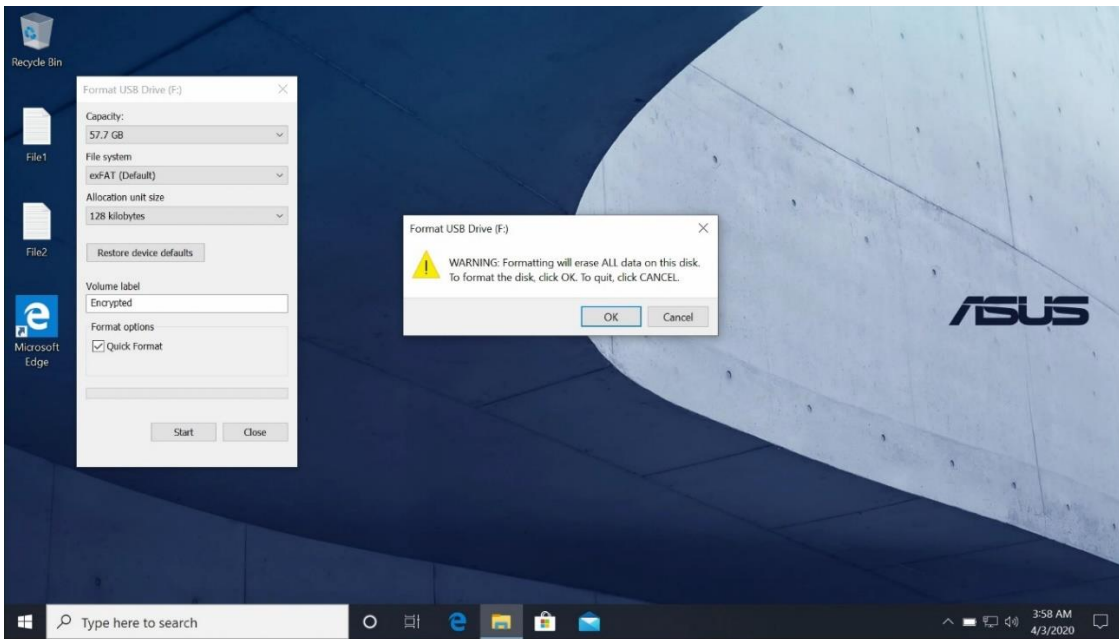
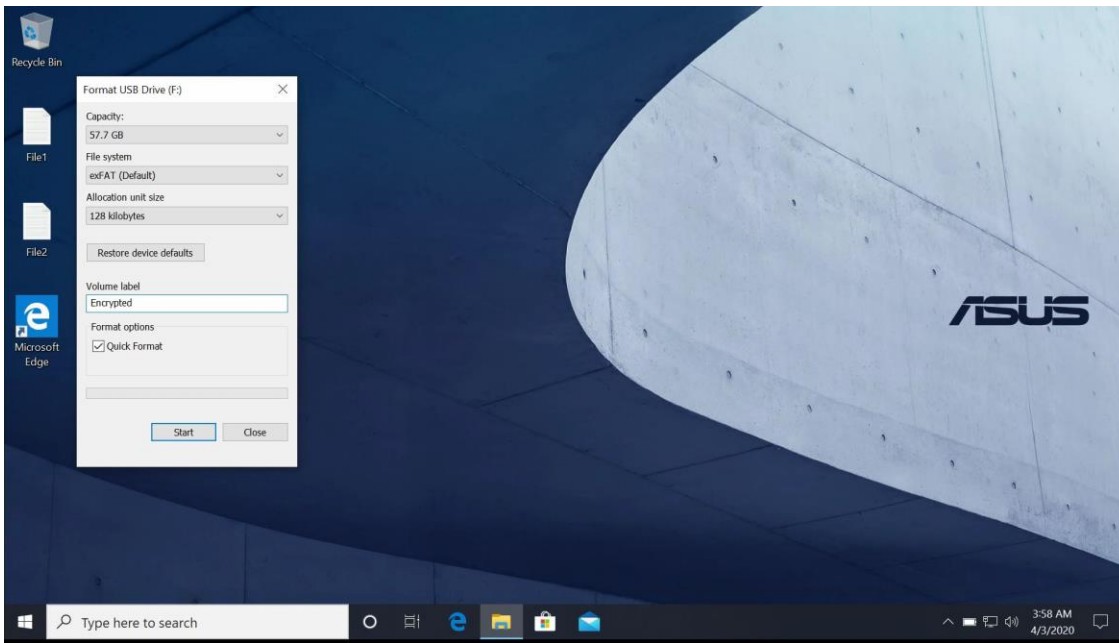


After entering the encryption password, USB Encryption function is turned ON.

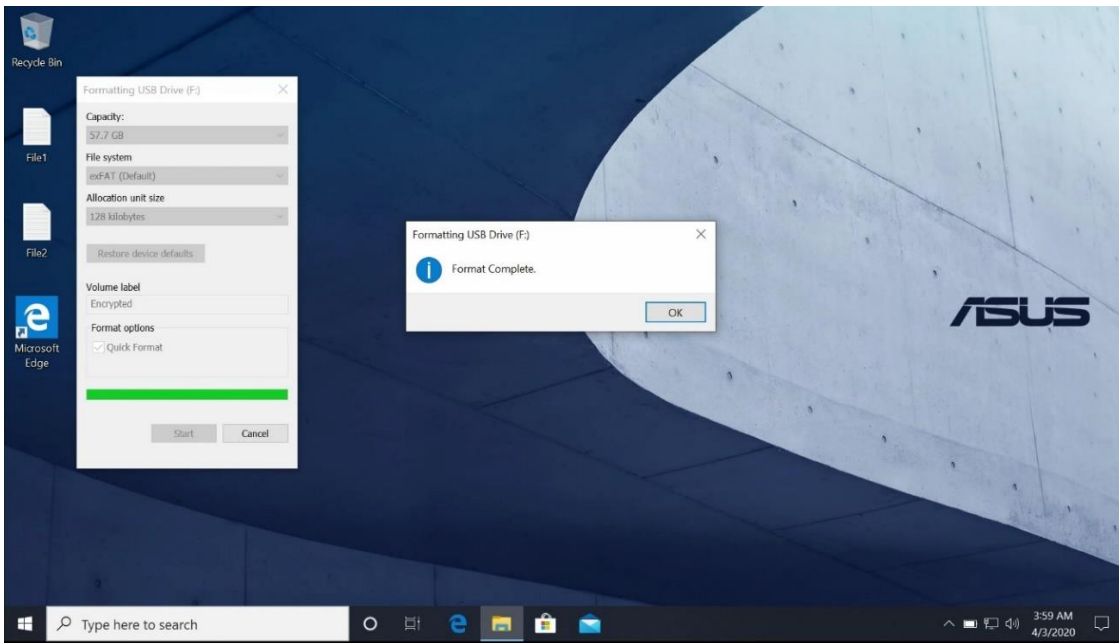


Ctrl-Alt-B takes you back to Windows. Once you plug in an USB thumb drive, Windows® will ask you to format this thumb drive. Please make sure to back-up the content on the drive first. Once Windows formats this thumb drive, all data will be lost.

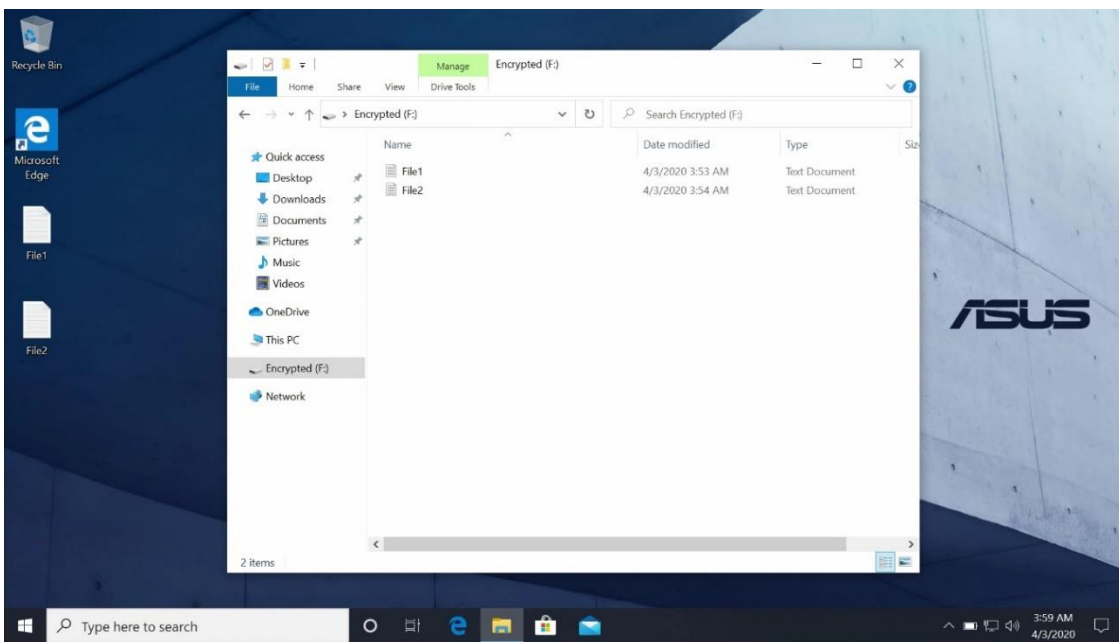




Format complete.



User can use this USB thumb drive like a regular USB thumb drive.

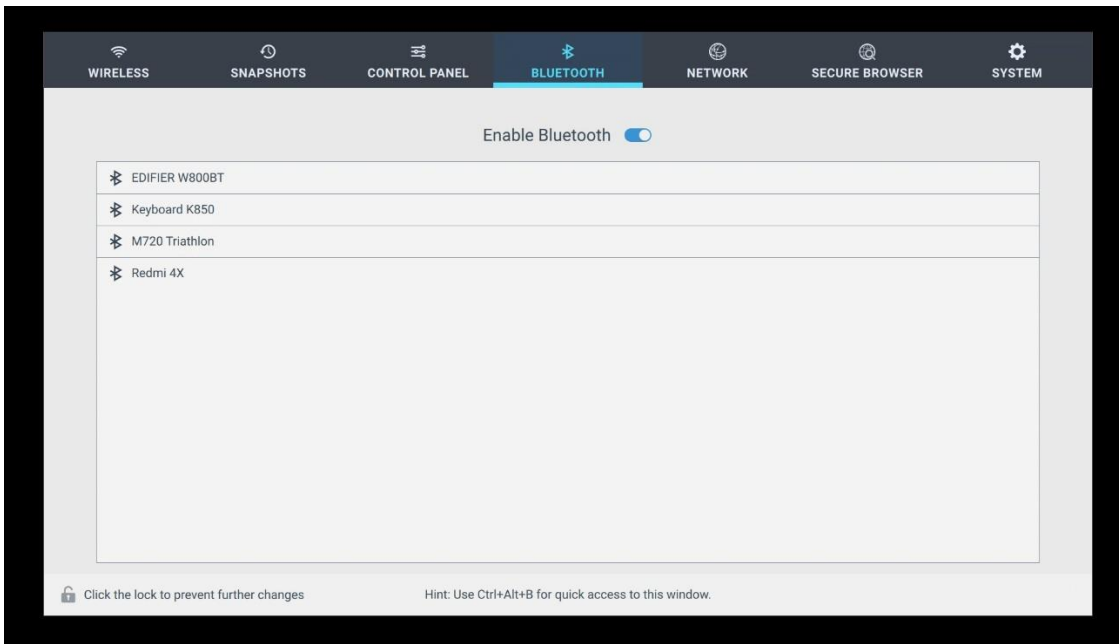


USB thumb drives cannot be read from other computers that do not have the same encryption key. In the event the USB thumb drive is lost, the data inside is still secure because the USB thumb drive is encrypted.

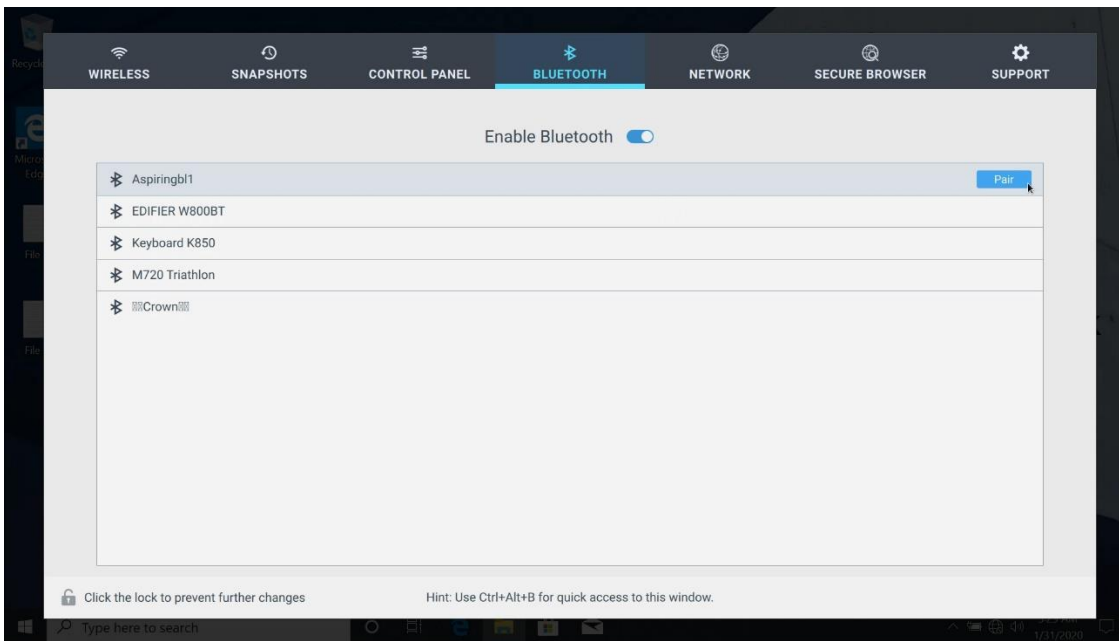
Only BIOS-SHIELD PC with the same USB encryption password can read this USB thumb drive.

7. Bluetooth Setup:

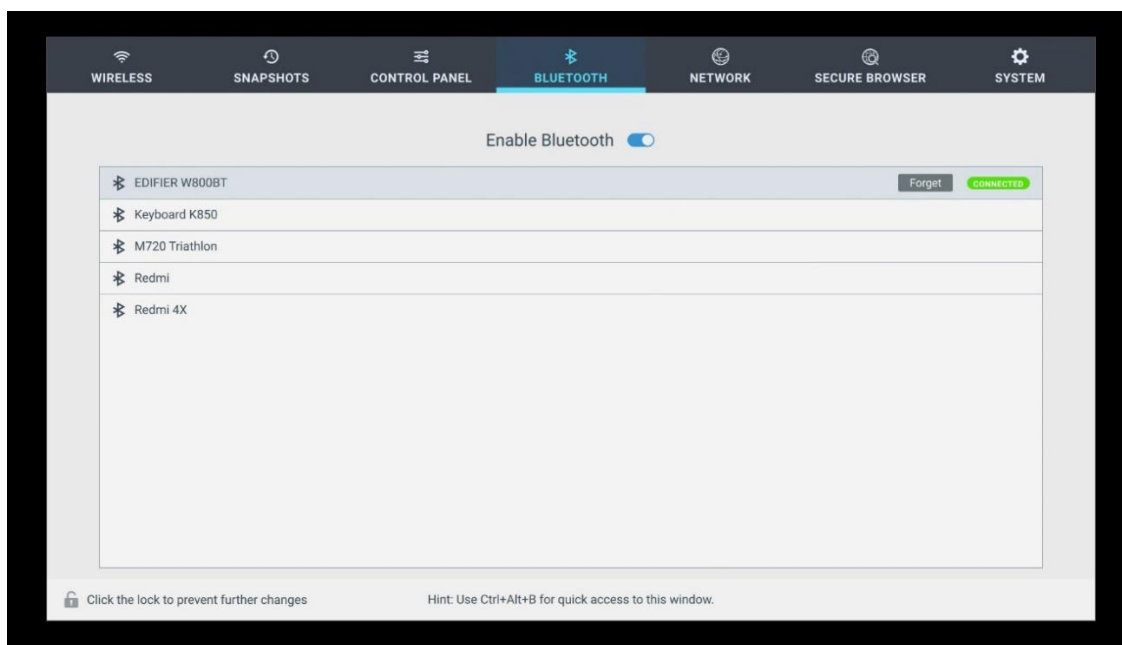
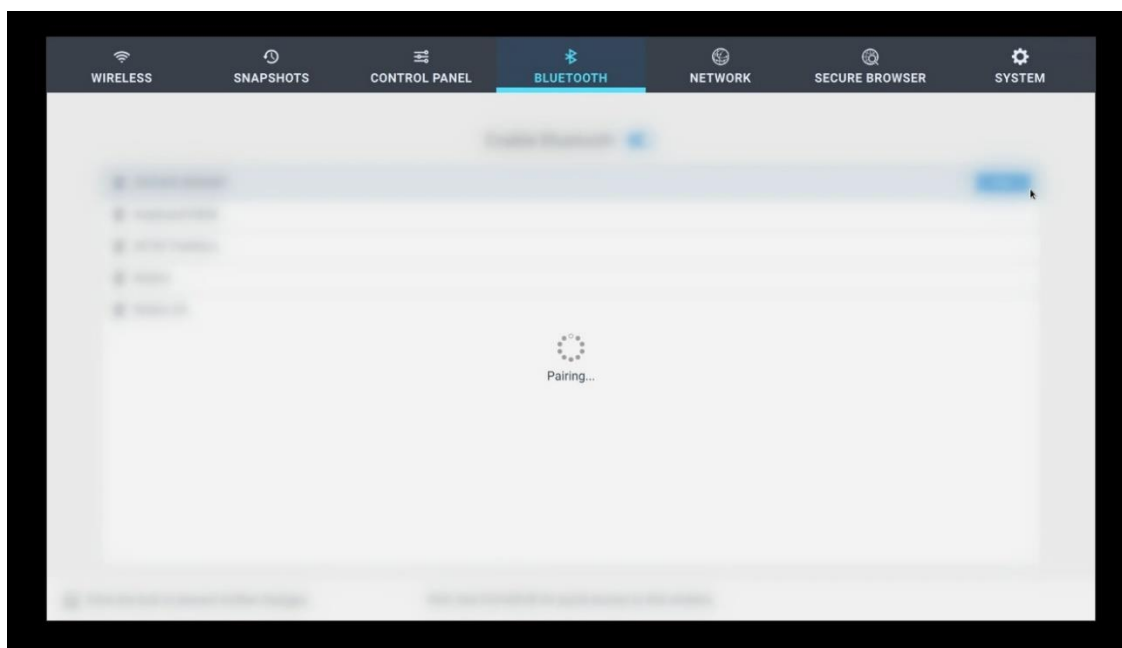
BIOS-SHIELD enables the PC to be configured and controlled through Bluetooth inside BIOS-SHIELD. To set this up, first put the Bluetooth devices in discovery mode (ready for pairing)



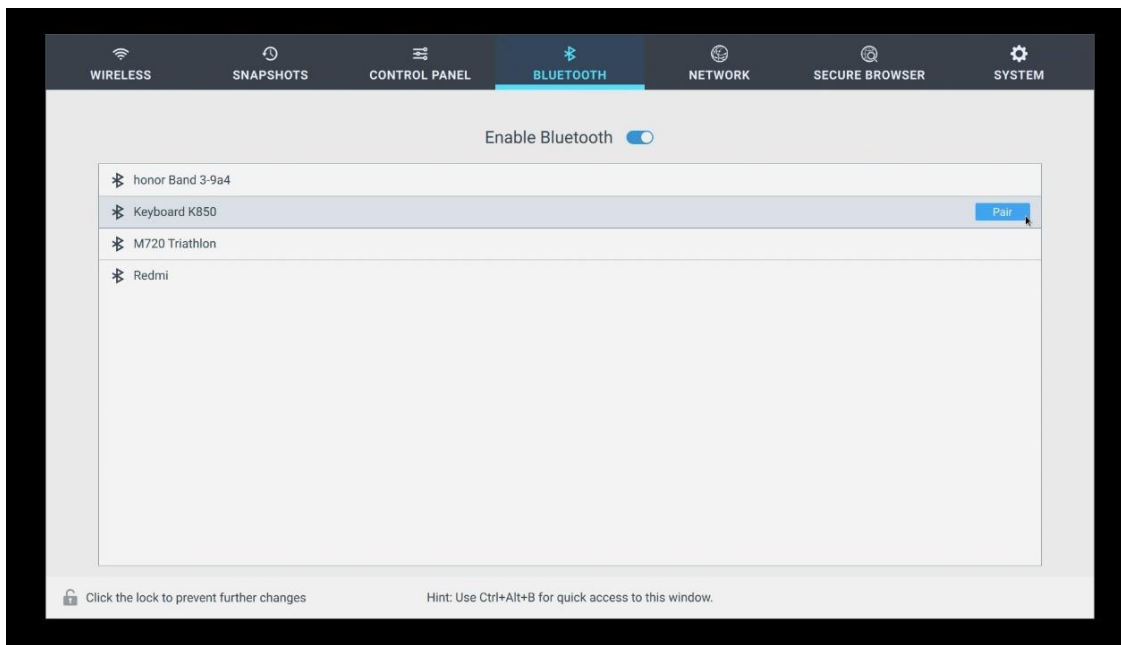
Select the Bluetooth device and click “Pair”



Once successfully paired, it will display “Connected”.

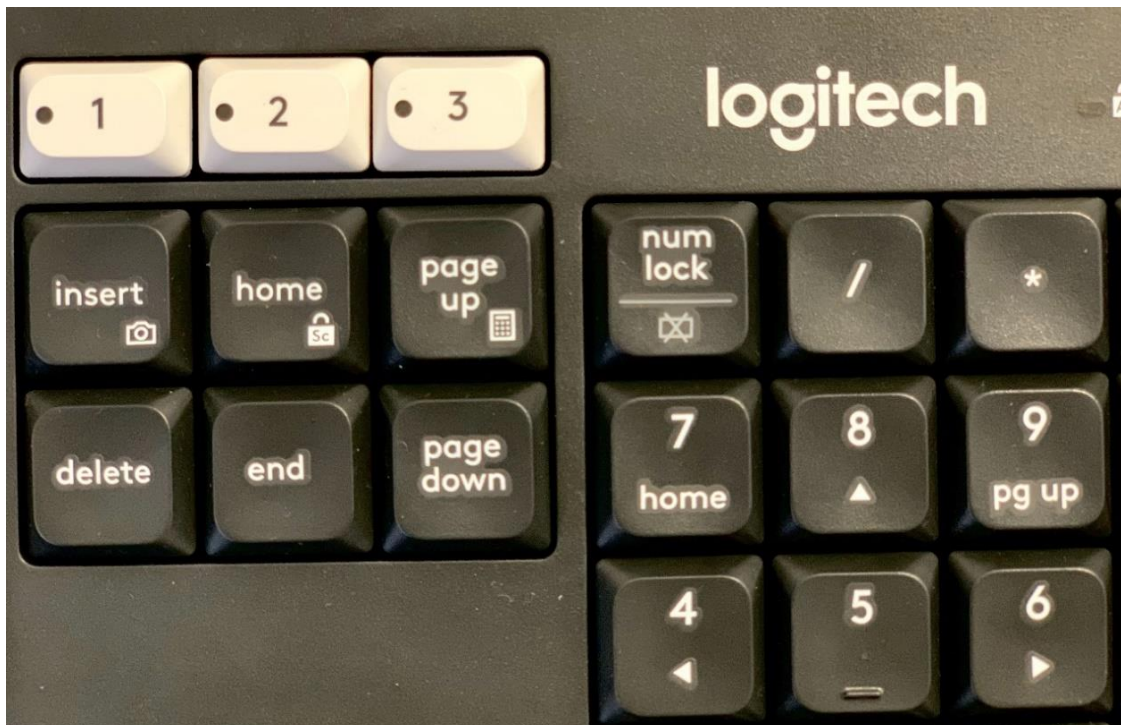


Next pair a Bluetooth keyboard

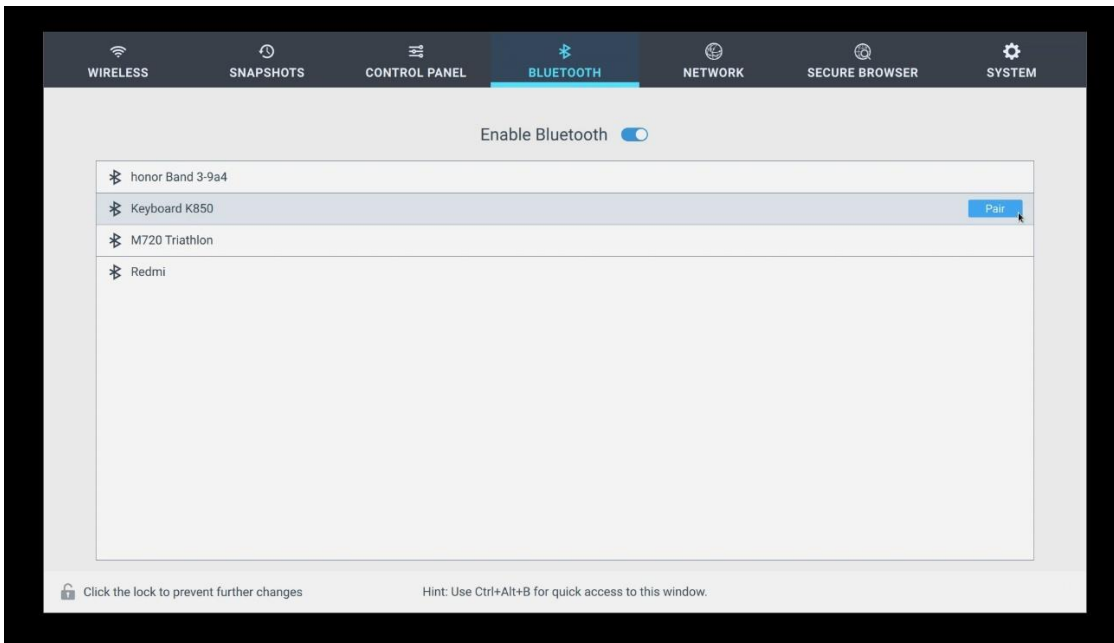


Example: Logitech Bluetooth keyboard

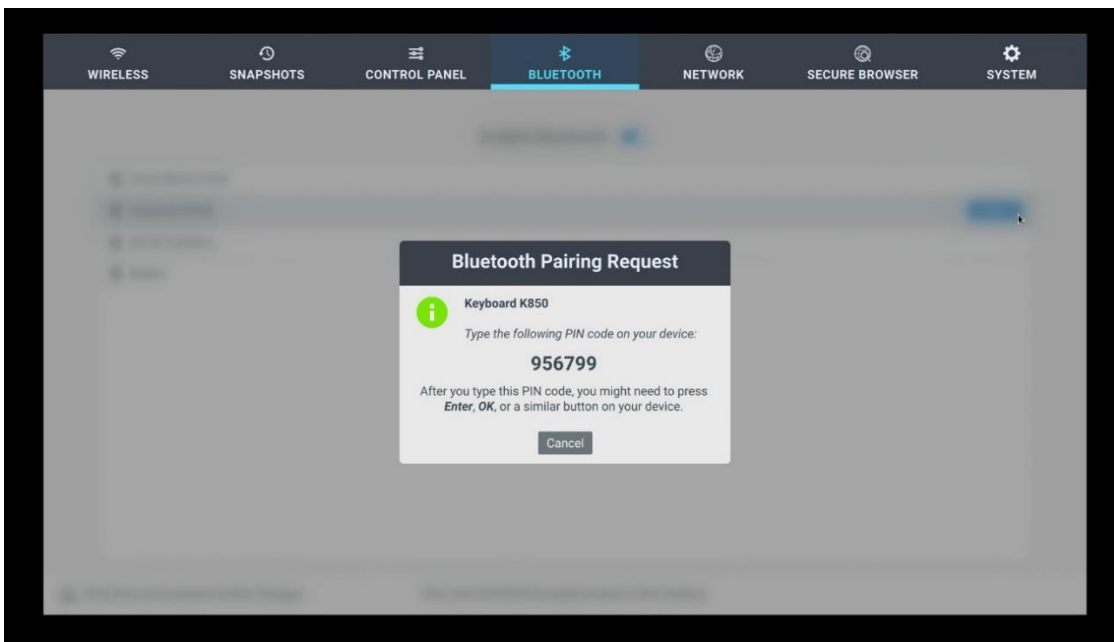
Press and hold key 1, LED will blink - ready to pair. (Please refer to your Bluetooth keyboard user's manual for instruction.)



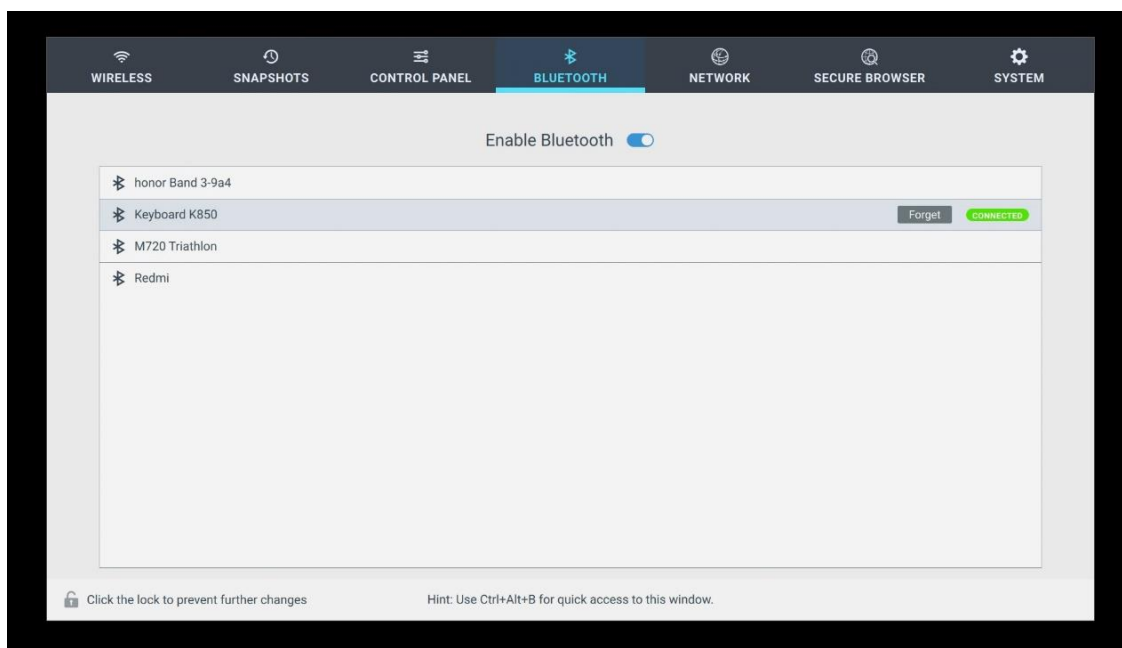
Click “Pair”



To pair a Bluetooth keyboard, BIOS-SHIELD will display a 6 number PIN code. Please enter this PIN code on your Bluetooth keyboard and press Enter.

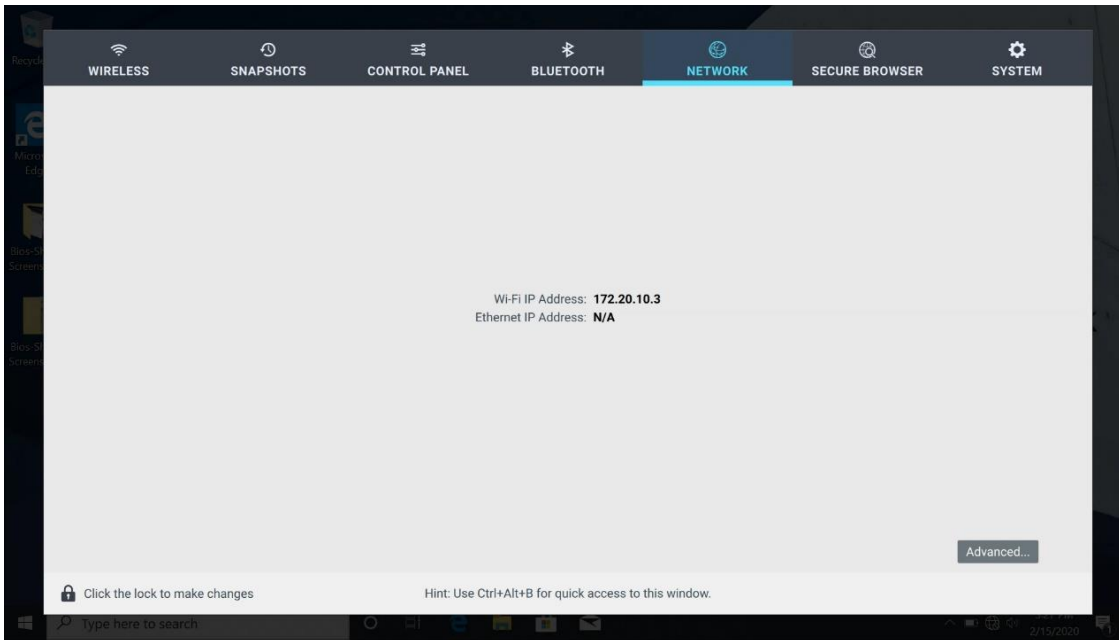


If a PIN code is correct, your Bluetooth keyboard will connect to the system.



8. Advanced Network:

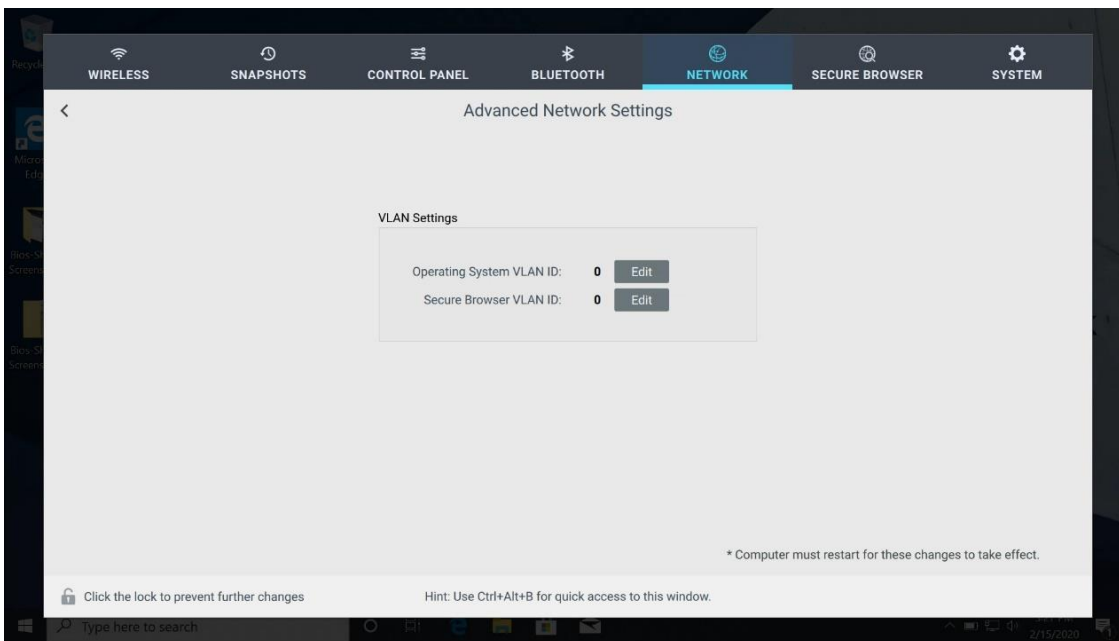
IP address is displayed on this page, if the laptop is connected to a network via wireless connection.



Click “Advanced”, this allow enterprise user to configure VLAN settings.

In order to use VLAN function, enterprise must have VLAN capable ethernet switch and configure VLAN properly. IT Administrator setup VLAN ID. BIOS-SHIELD can use different VLAN for Operating System (Windows®) and Secure Browser for maximum network security.

VLAN function applies to Ethernet. (not wireless)

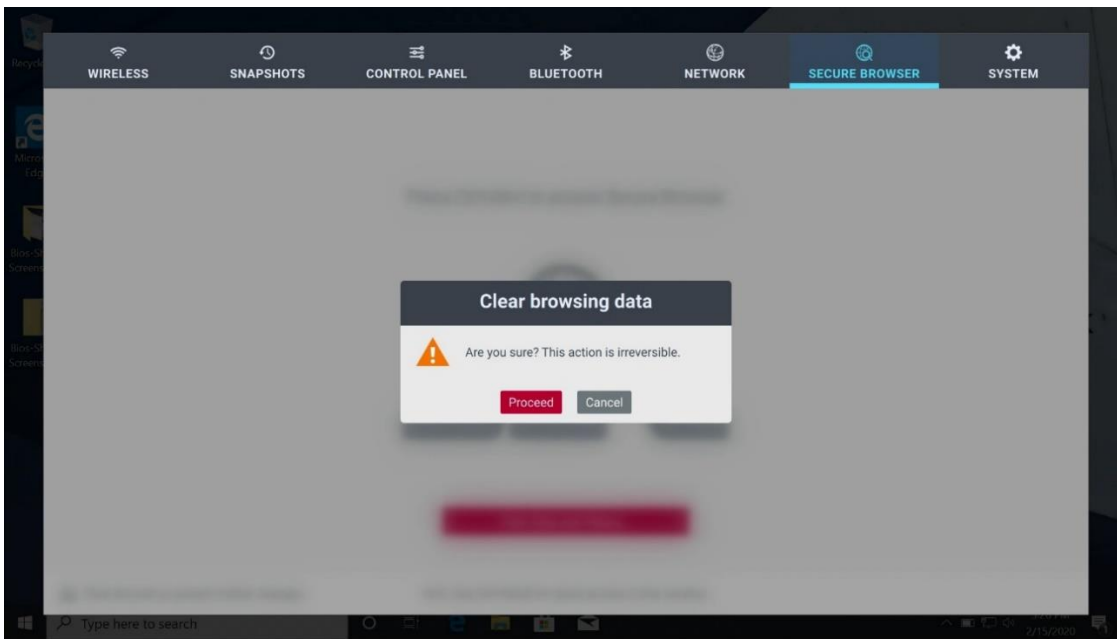
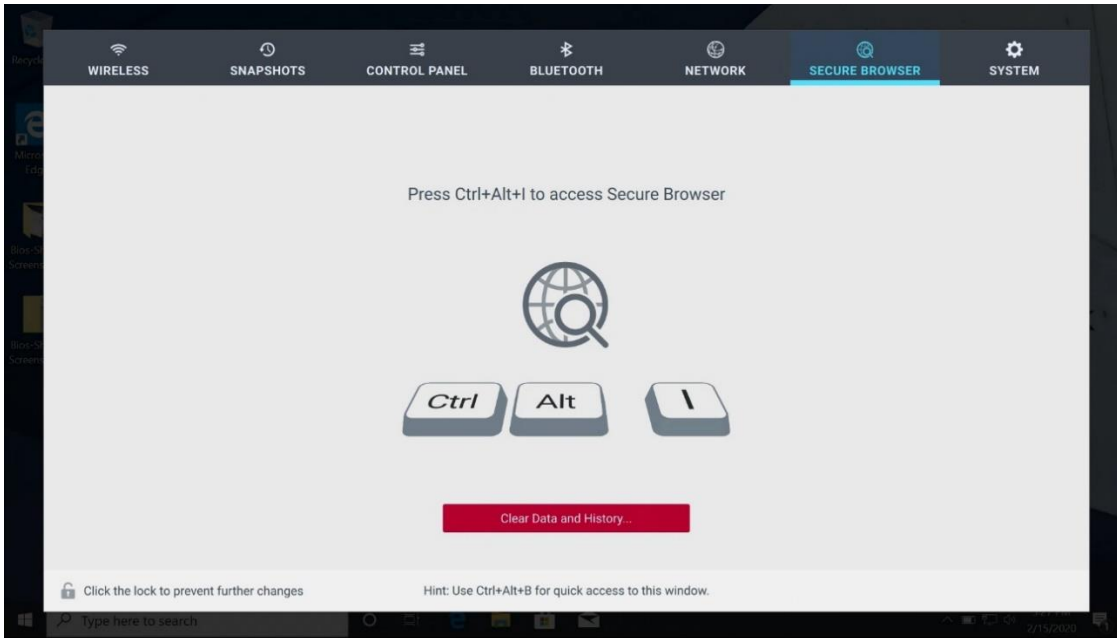


9. Secure Browser

BIOS-SHIELD has a built-in Secure Browser function. You can use the Secure Browser to browse Internet. If you browse a website that introduces malware, it will NOT affect your Windows®.

Secure Browser will start fresh in every boot.

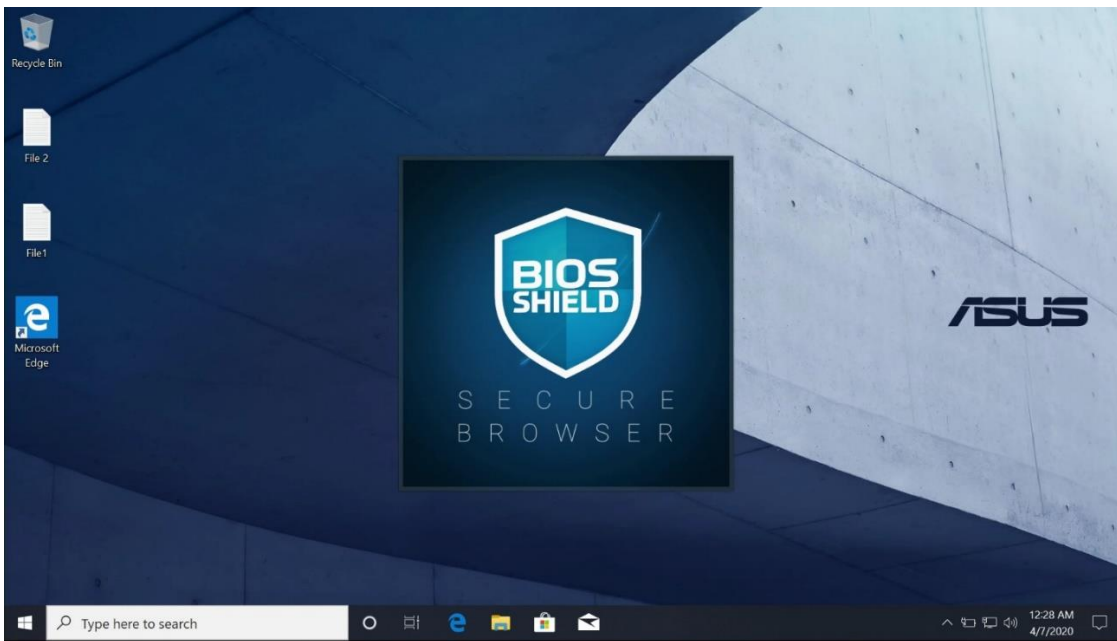
Secure Browser allows the user to save bookmarks. To reset your Secure Browser history and bookmarks, please click “Click Data and History”



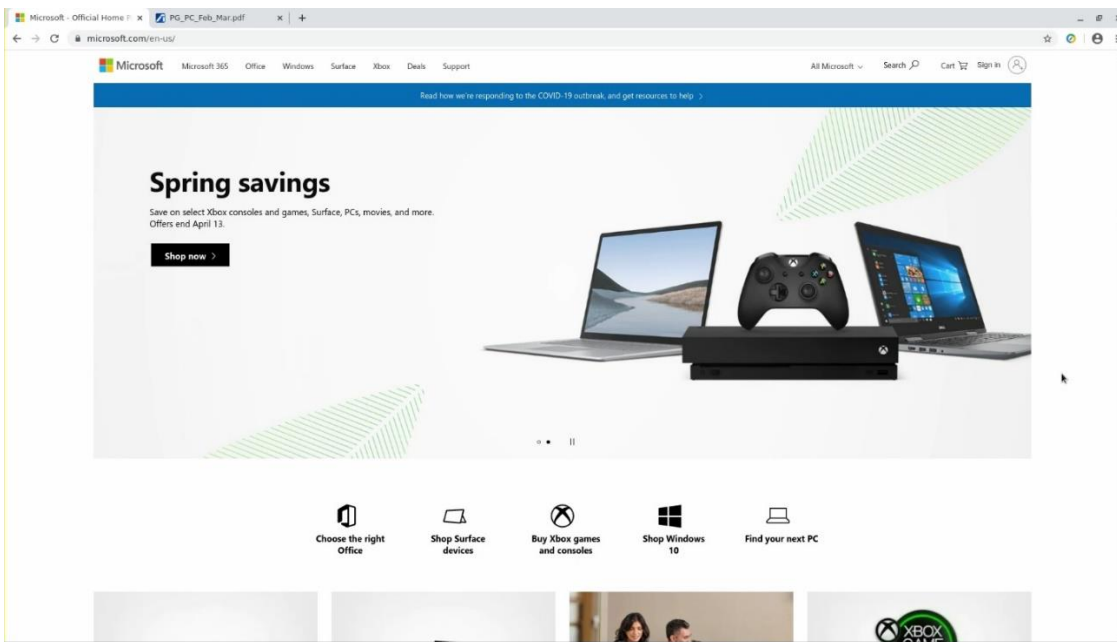
How to use Secure Browser

While Secure Browsers provide great security, user may still want to copy screenshots, photos or PDFs from the internet to Windows. The Secure Browser provide a protected channel to bring this information to Windows®.

Use Ctrl-Alt-I to launch Secure Browser



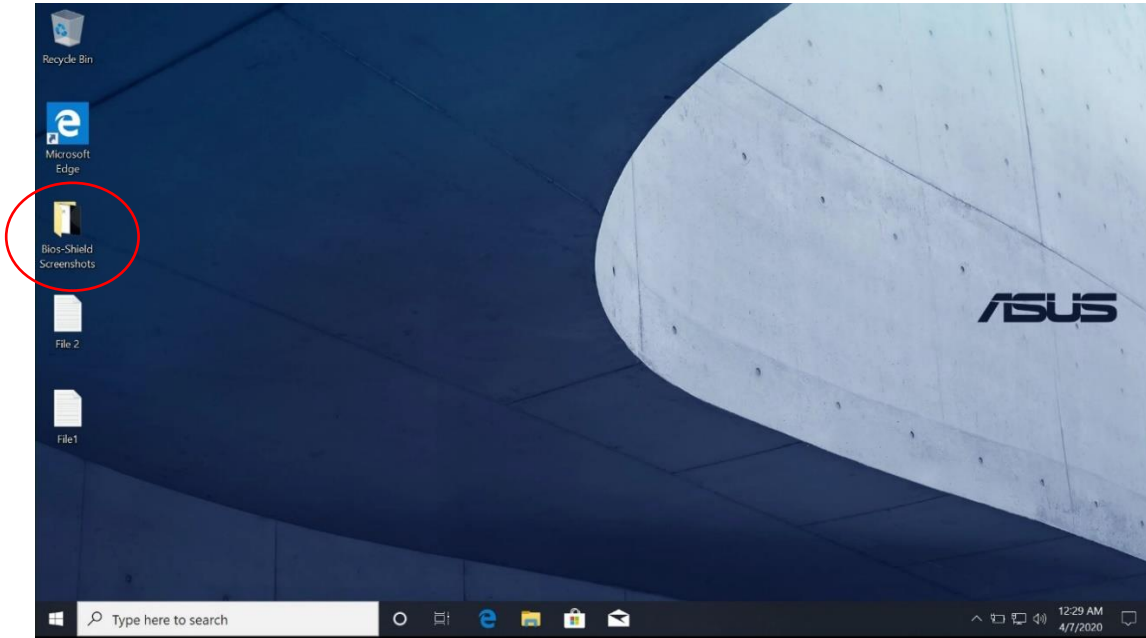
Browser internet www.microsoft.com website



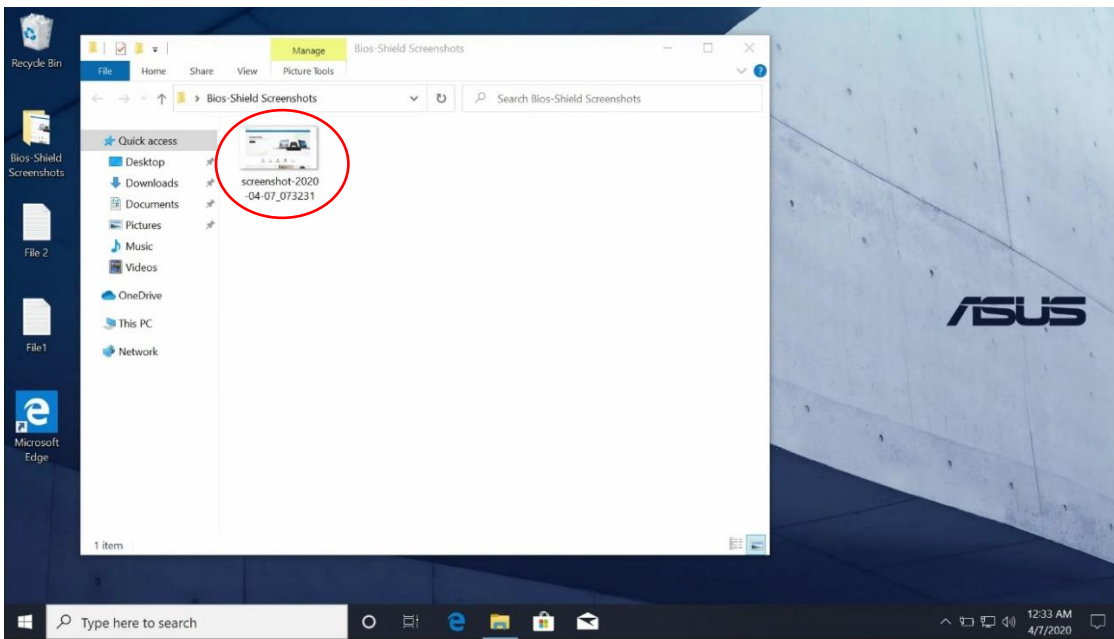
Screenshot in Secure Browser

If you want to do a screenshot from your Secure Browser to Windows®, use Ctrl-Alt-P to do screenshot in Secure Browser.

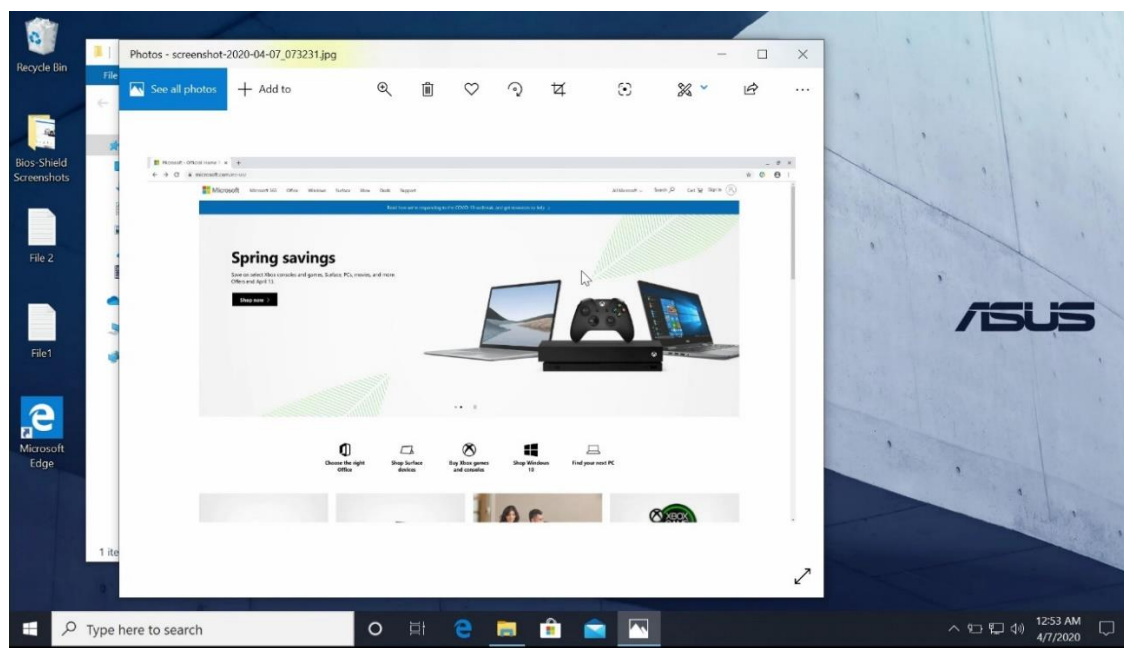
The screenshot will be sent to Windows® Desktop inside “Bios-Shield Screenshots” folder.



Open this folder

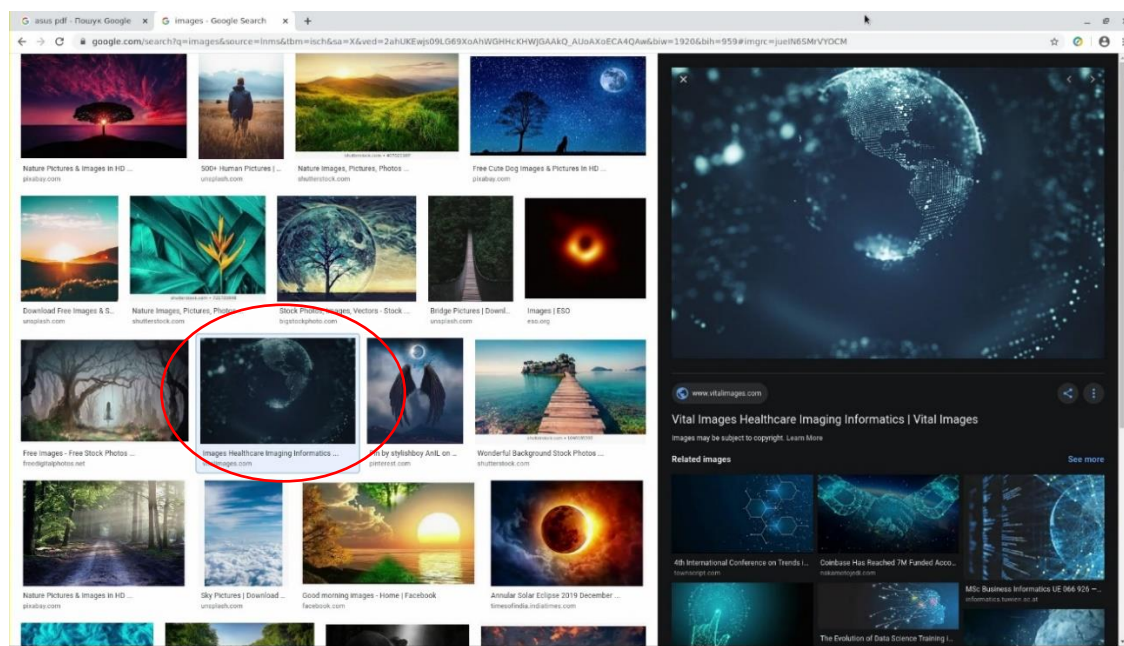


Open the screenshot file

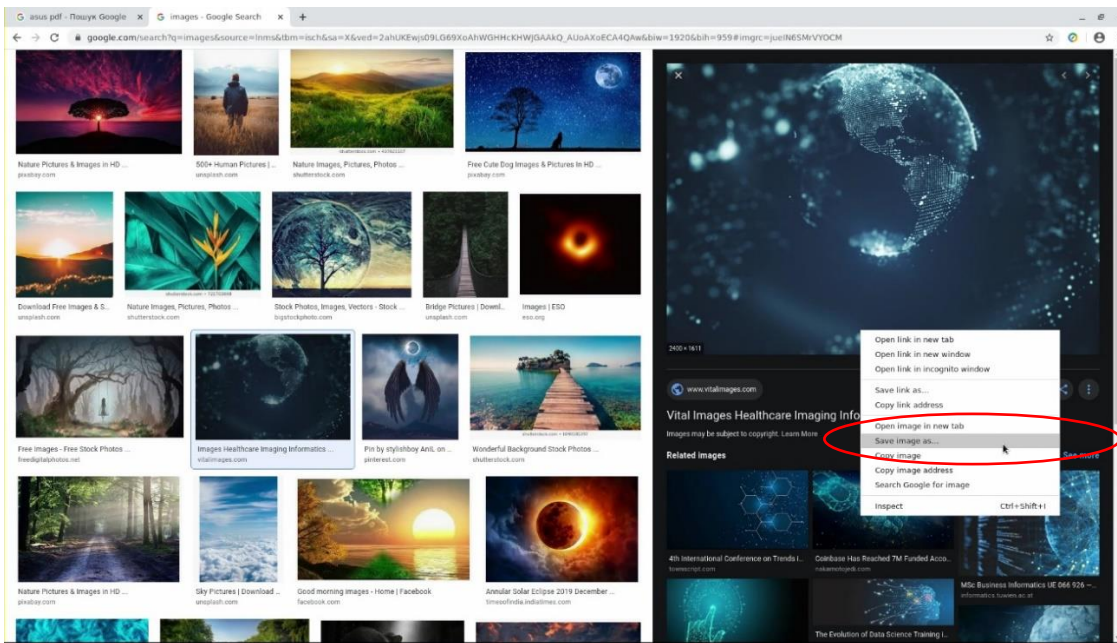


Transfer Photos from Secure Browser to Windows®

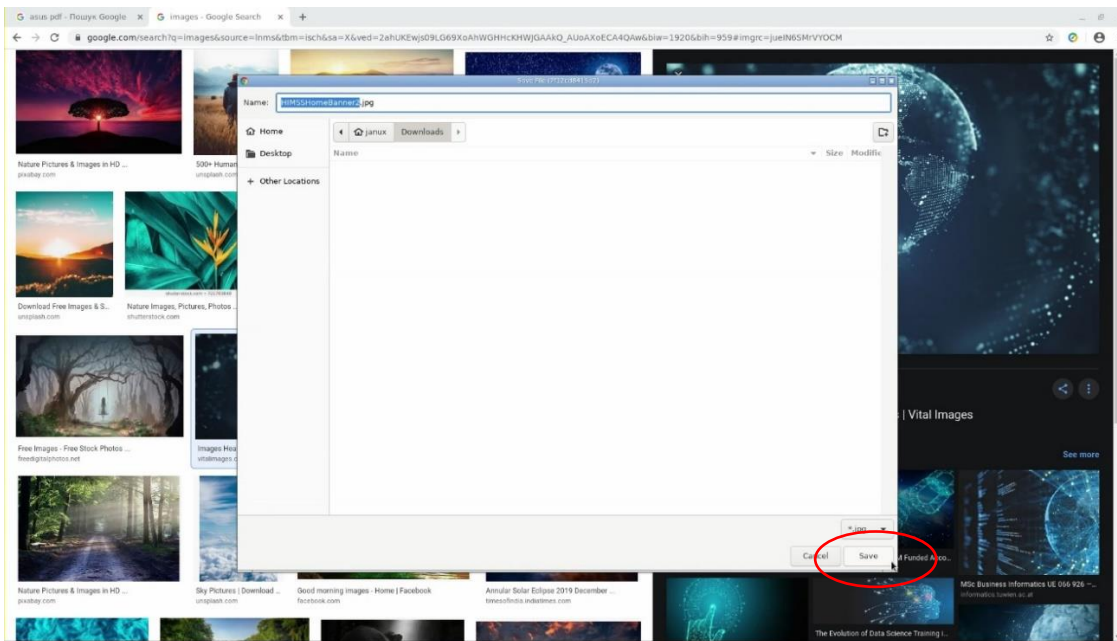
When browsing the internet in Secure Browser, you may find a photo you want to transfer to Windows®, select the photo and right click



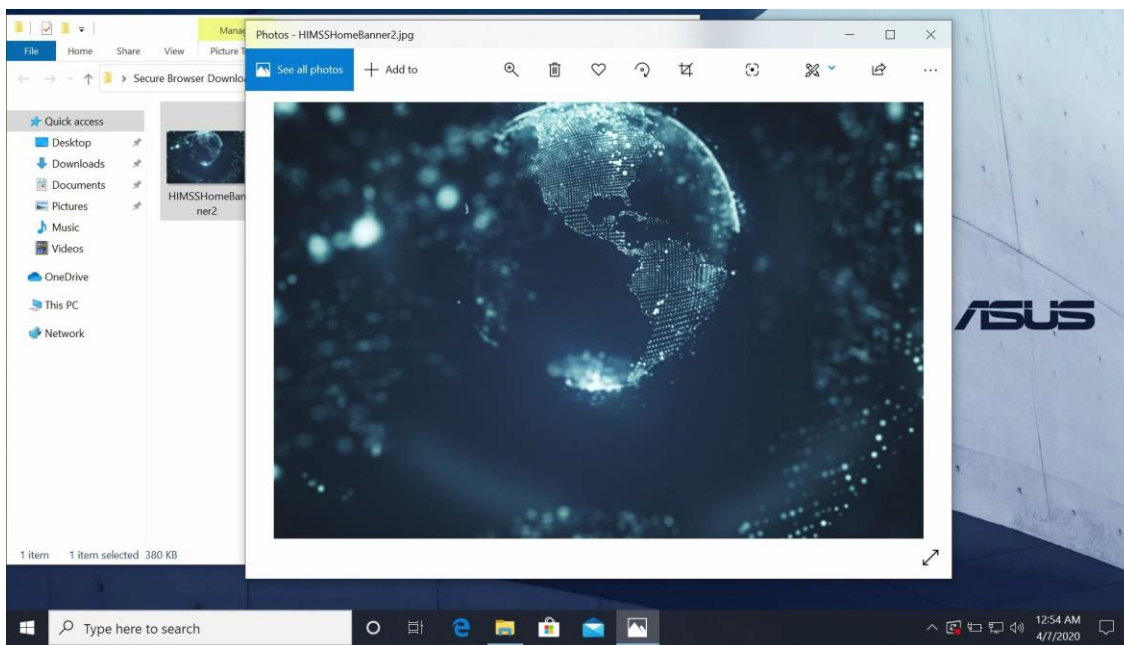
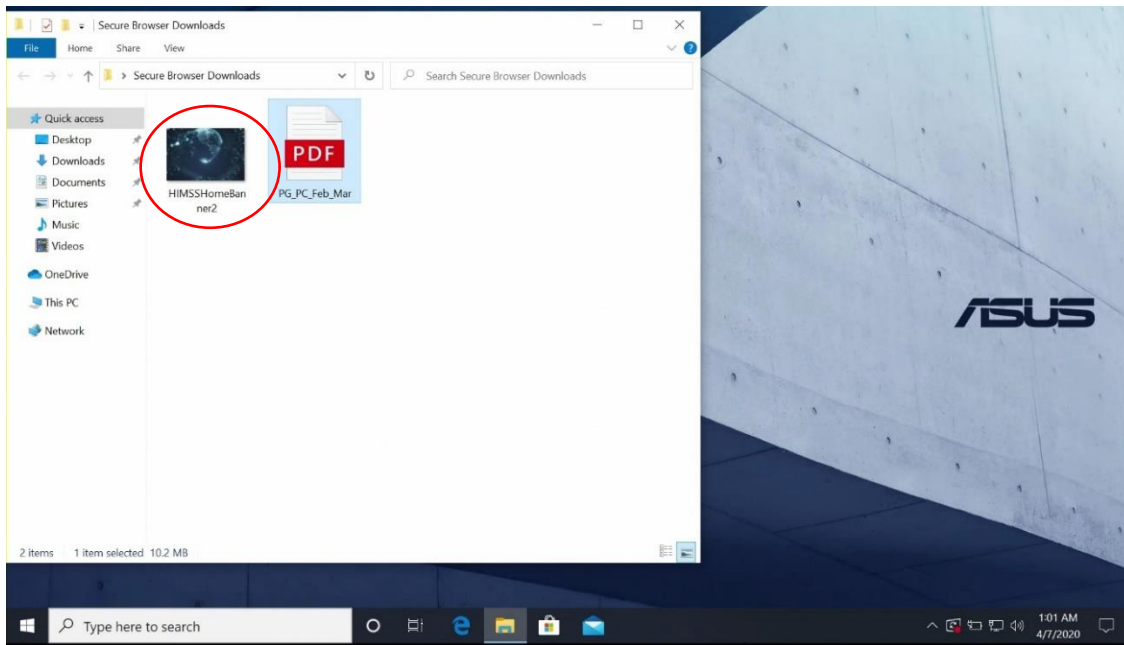
Save image as...



Click “Save” in lower right corner



Go to Windows® Desktop, click into “Secure Browser Downloads”

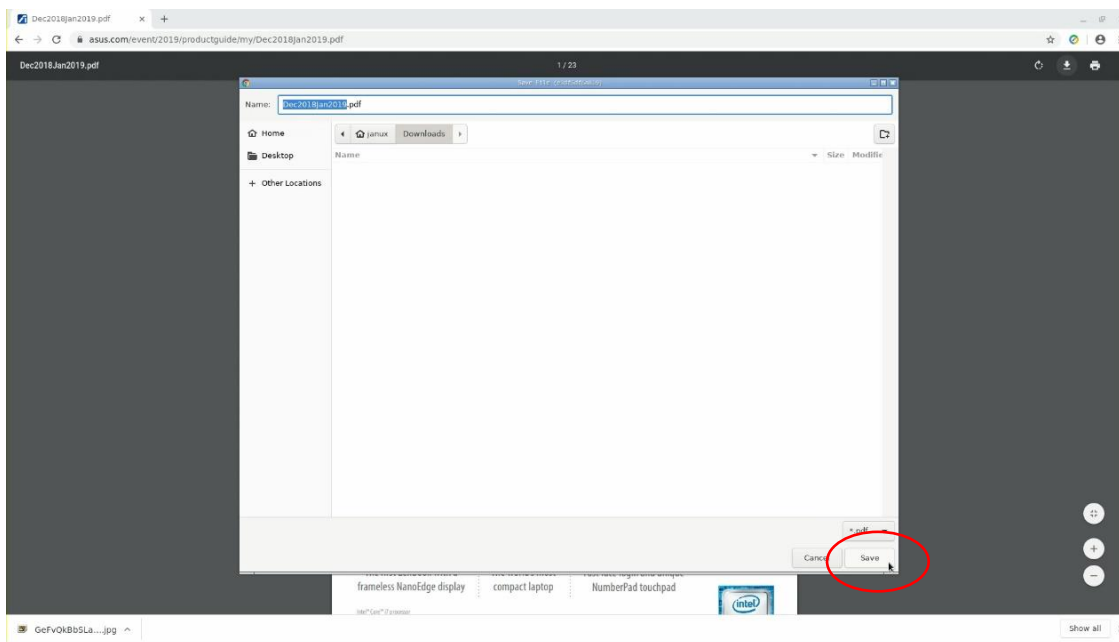


Transfer the PDF file from Secure Browser to Windows®

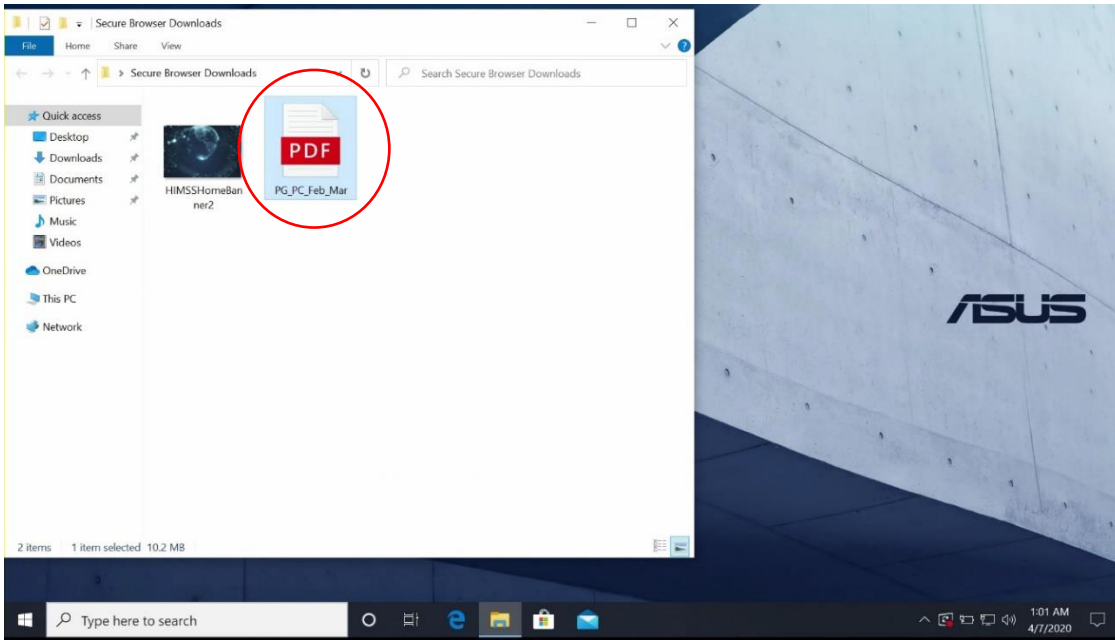
When browsing the internet, you may find a pdf file you want to transfer to Windows®, open the PDF file and click “Download”



Click “Save”



Go to Windows® Desktop, check “Secure Browser Downloads” folder, you will see PDF file transferred from Secure Browser to here.



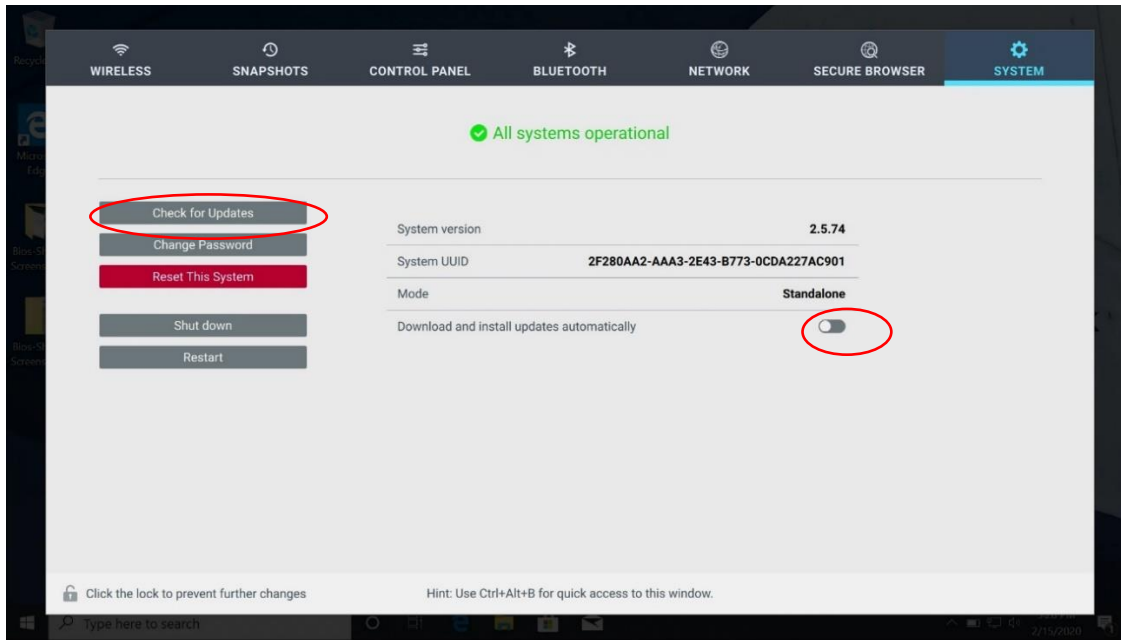
Open the PDF file



When using the Secure Browser to transfer photos or PDF files to Windows®, BIOS-SHIELD will filter these files and make sure there is no embedded malicious code inside when transferring to Windows®.

10. System Up-dates

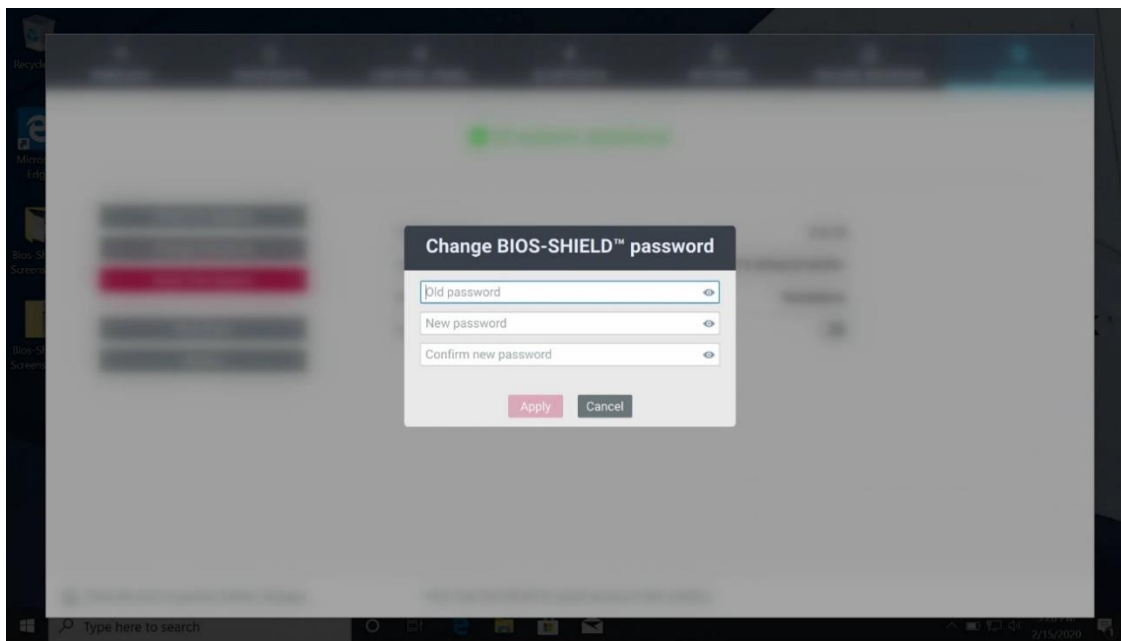
System status will display System version, UUID, Mode (Standalone mode or Cloud Management mode)



“Download and install updates automatically. If this feature is turned on, BIOS-SHIELD will check the internet. If there is a newer version of BIOS-SHIELD available, it will download and install it. In next re-boot, a new version of BIOS-SHIELD will be used.

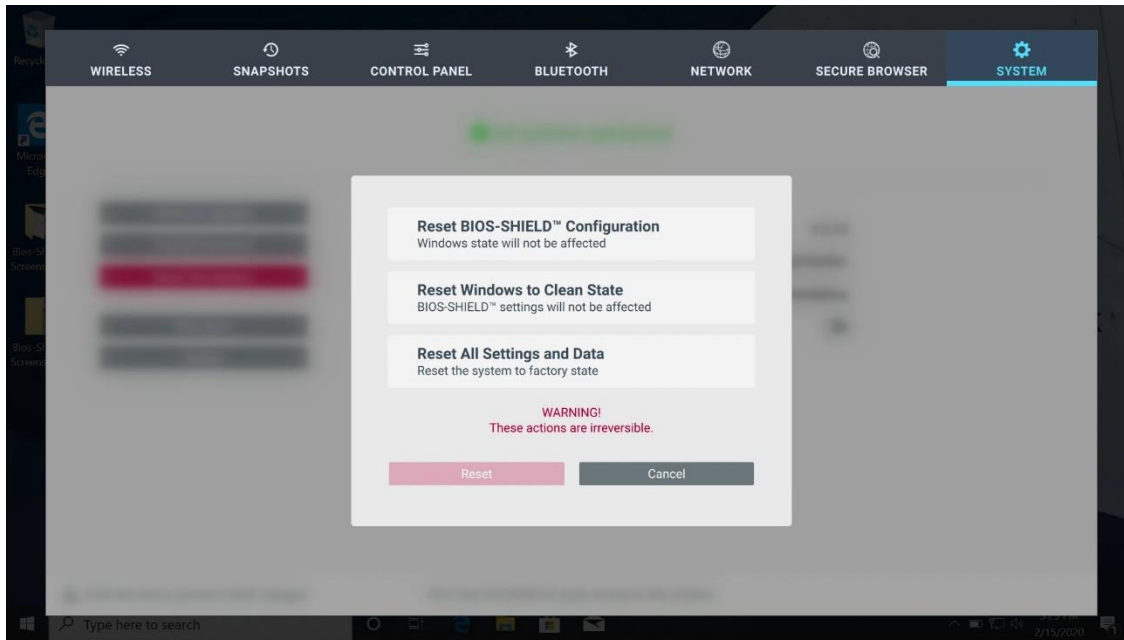
Check for Updates: Manually check for Updates

Change Password: Change BIOS-SHIELD Password



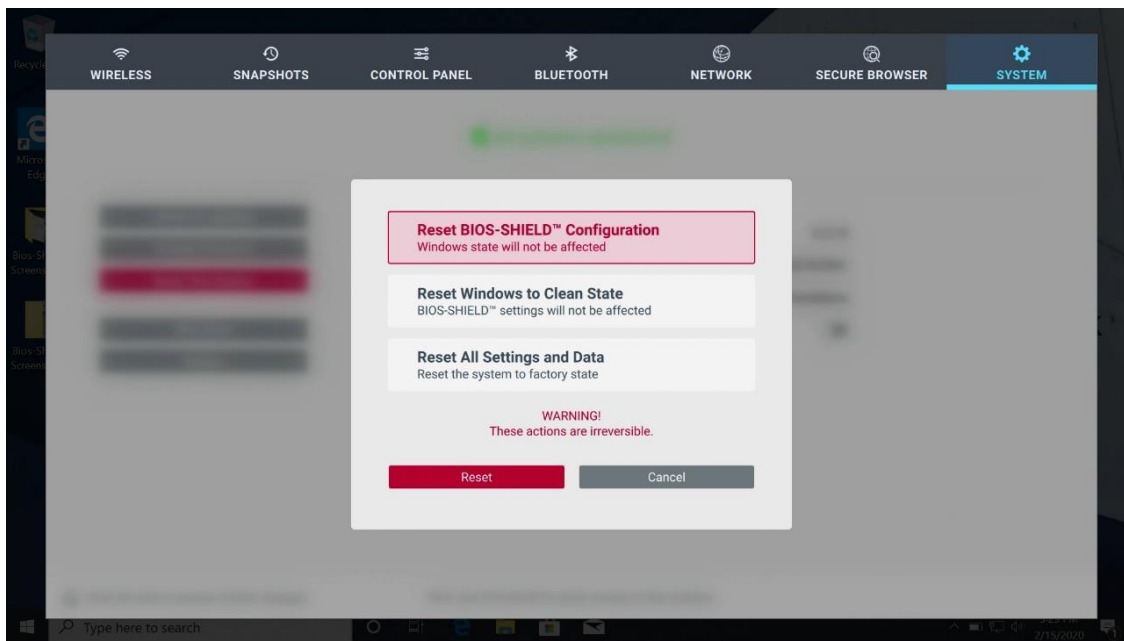
11. Reset This System

Enter BIOS-SHIELD password to unlock this.



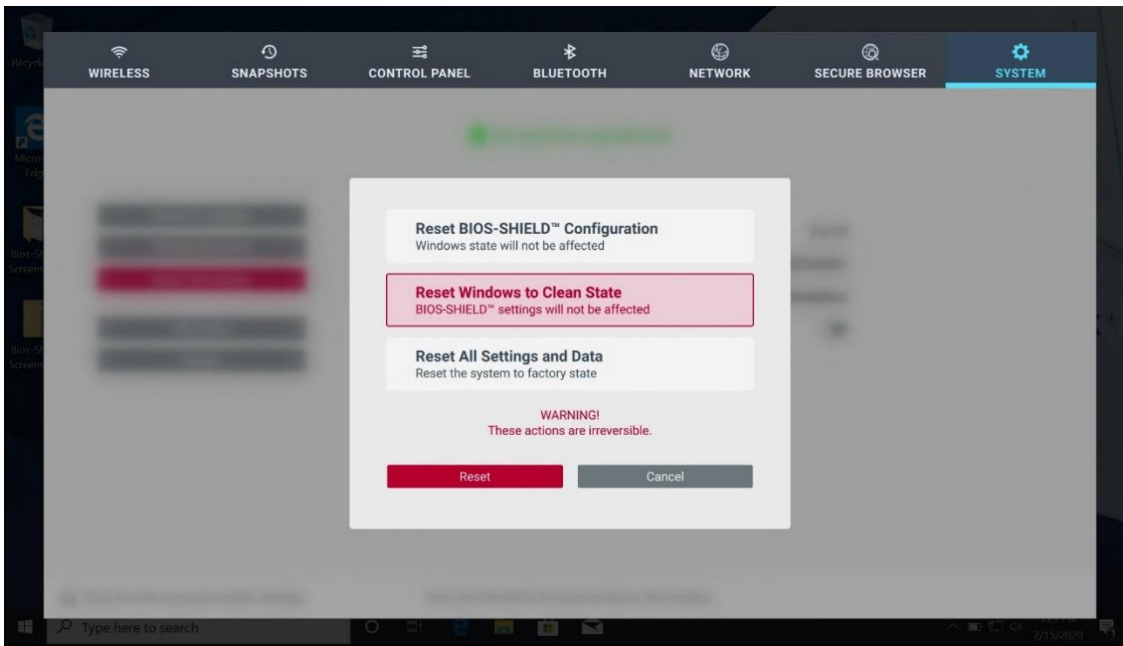
11.1 Reset BIOS-SHIELD configuration:

When you have a BIOS-SHIELD enabled PC in standalone mode and want to switch to Cloud Management mode, you can use this function. It will reset BIOS-SHIELD and allow it to connect to Cloud Management without resetting the end user data.



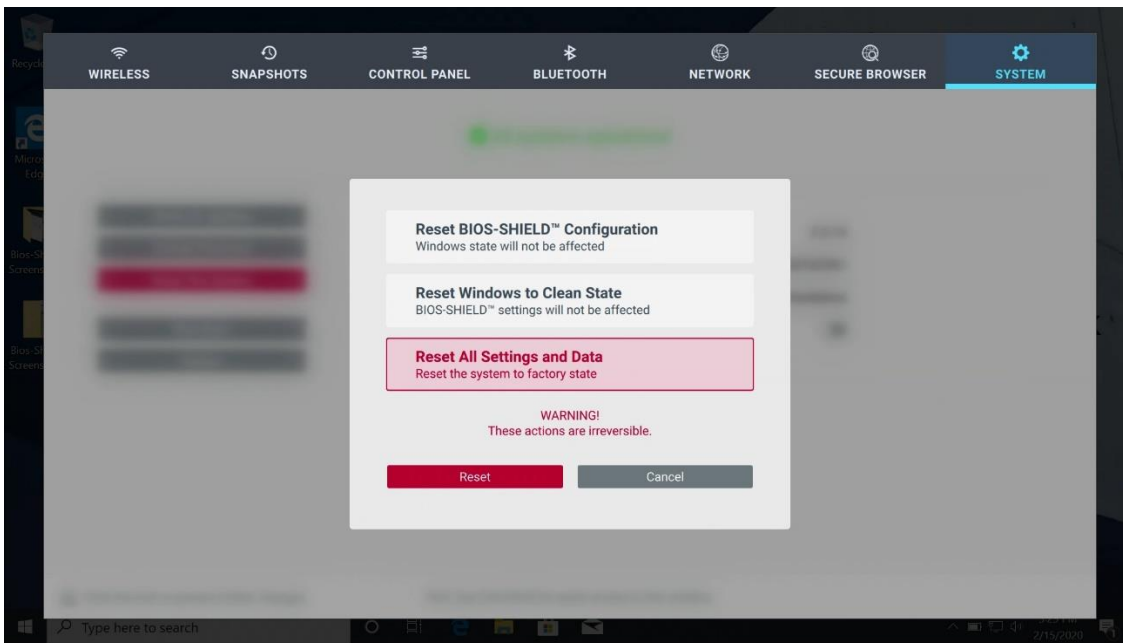
11.2 Reset Windows to Clean State:

BIOS-SHIELD can reset Windows to factory image. This will erase all end user data. BIOS-SHIELD settings such as password, control panel settings, wireless and Bluetooth settings will not be affected.



11.3 Reset All Settings and Data

BIOS-SHIELD will reset the system to factory default. It will erase all user data and BIOS-SHIELD settings.



Reboot: BIOS-SHIELD will shut down Windows and reboot PC

Shutdown: BIOS-SHIELD will shut down Windows and shutdown PC

12. Cloud Management

BIOS-SHIELD support two different ways to manage your computer, standalone mode and cloud management mode. If you are an end user who operate from a single computer, you can choose either standalone mode or cloud management mode. If you are using a computer belonging to a company and plan to manage more than one computer, then you should choose Cloud Management mode. Cloud Management mode provides additional benefits such as remote device management with PC enablement/disablement, secure PC reboot/shutdown, ease of group policy creation and deployment and remote wipe of end-user data.

To choose your cloud management, you need to:

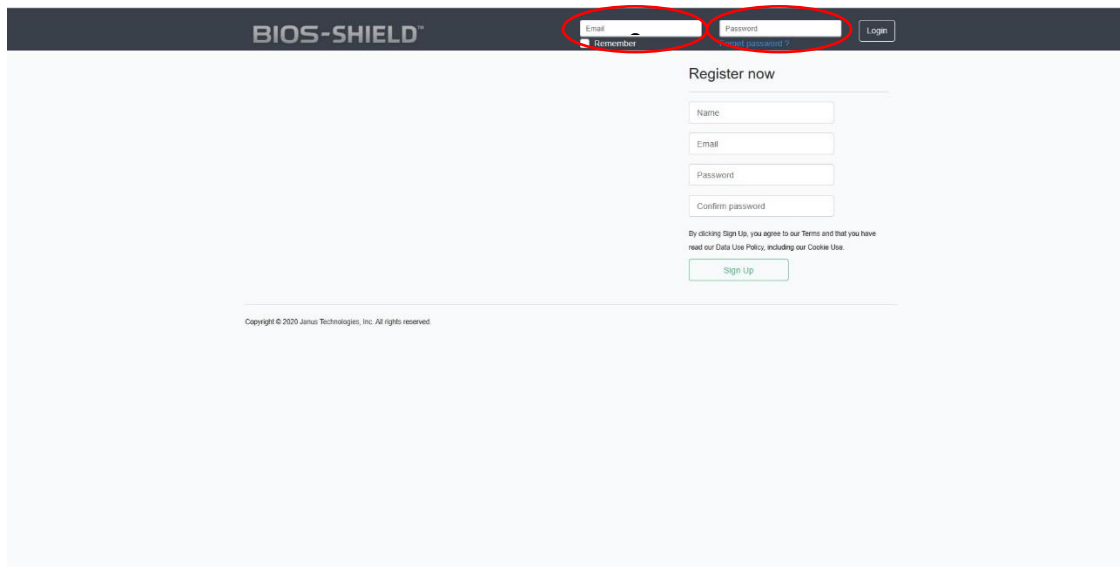
1. Create a cloud account
2. Setup your PC to use Cloud Management mode

To create a cloud account, please go to <https://cloud.asus.bios-shield.com> to create a cloud account. You can refer to Quick Start Guide page 5 for more detail about creating a cloud account and setup your PC to use Cloud Management.

Login to Cloud Management Portal

Please use <https://cloud.asus.bios-shield.com> to access BIOS-SHIELD Cloud Management Portal

Enter your login name (email address) and password and click “Login”



The screenshot shows the BIOS-SHIELD Cloud Management Portal interface. At the top, there is a dark header with the BIOS-SHIELD logo on the left. In the center of the header, there are two input fields: 'Email' and 'Password'. The 'Email' field has a red circle around it, and the 'Password' field has a red circle around it. To the right of the 'Password' field is a 'Login' button. Below the header, there is a 'Register now' section. This section contains four input fields: 'Name', 'Email', 'Password', and 'Confirm password'. Below these fields is a small text line: 'By clicking Sign Up, you agree to our Terms and that you have read our Data Use Policy, including our Cookie Use.' Below this text is a 'Sign Up' button. At the bottom of the page, there is a small copyright notice: 'Copyright © 2020 Janus Technologies, Inc. All rights reserved.'

Set configuration password for target computer: It's highly recommended to set configuration password for each target computer.


The screenshot shows the BIOS-SHIELD dashboard. At the top, there are three summary cards: 'All computers' with a count of 1, 'Active computers' with a count of 1, and 'Blocked computers' with a count of 0. Below these is a table titled 'Computers' with columns: Name, Status, Firmware, Group, Description, and Actions. The first row in the table is for 'John_Smith', with status 'Active', firmware '2.6.31', and group 'Accounting'. The 'John_Smith' text in the 'Name' column is circled in red. The dashboard footer includes 'Copyright © 2020 BIOS-SHIELD Cloud Management. All rights reserved.' and 'Version: 2.6.15'.


The screenshot shows the 'System' configuration page for the 'John_Smith' computer. On the left, under the 'CONTROL PANEL' tab, there is a 'Change Password' button circled in red. Other buttons in this panel include 'Reset All Settings and Data', 'Detach this Computer', 'Lock this Computer', 'Shut down', and 'Reboot'. The main area shows system details: 'All systems operational', 'System version: 2.6.31', and 'System UUID: AAC36D3-EE41-A443-87BE-8BAA1EF3A56'. There are input fields for 'Name' (containing 'John_Smith') and 'Description' (containing 'John Smith laptop (accounting)'). The footer includes 'Copyright © 2020 BIOS-SHIELD Cloud Management. All rights reserved.' and 'Version: 2.6.15'.

Please enter password and confirm password. Please note this password is required for users to access specific features areas from a target computer such as Snapshot, Bluetooth Setup, Advanced Network Configuration, Clear Secure Browser Data and History, change System Configuration settings.


The screenshot shows a 'Change BIOS-SHIELD™ password' dialog box. It has two input fields for password entry, each with a green checkmark indicating a valid password. Below the fields is a note: 'This password allows to manage BIOS-SHIELD™ functions directly on the computer'. At the bottom are 'Apply' and 'Cancel' buttons.


To configure setting form an individual computer: click Dashboard to display all the computers belonging to this account and click on the computer you want to manage.


BIOS-SHIELD 



Dashboard  Dashboard

Groups




All computers  1

Active computers  1


Blocked computers  0


Computers   Add

Show 5 entries per page Showing 1 to 5 of 1 entries Filter Clear


Name	Status	Firmware	Group	Description	Actions
John_Smith	Active	2.6.31	Accounting		  


Copyright © 2020 BIOS-SHIELD Cloud Management. All rights reserved. Version: 2.6.15


BIOS-SHIELD 



Dashboard  Dashboard

Groups




All computers  1

Active computers  1

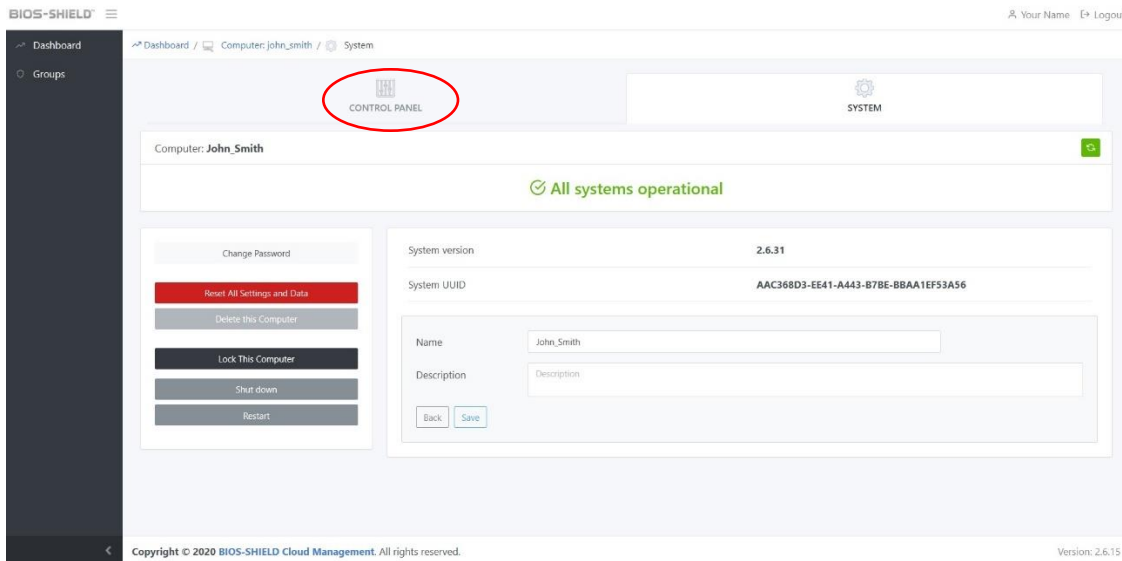
Blocked computers  0

Computers   Add

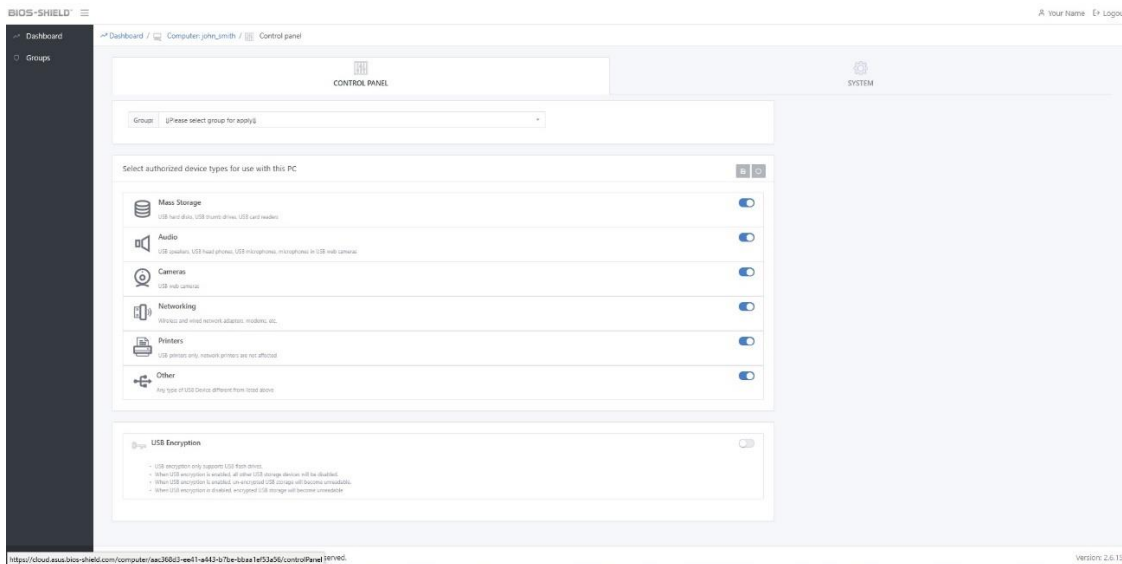
Show 5 entries per page Showing 1 to 5 of 1 entries Filter Clear

Name	Status	Firmware	Group	Description	Actions
John_Smith	Active	2.6.31	Accounting		  

Copyright © 2020 BIOS-SHIELD Cloud Management. All rights reserved. Version: 2.6.15



Click “CONTROL PANEL”

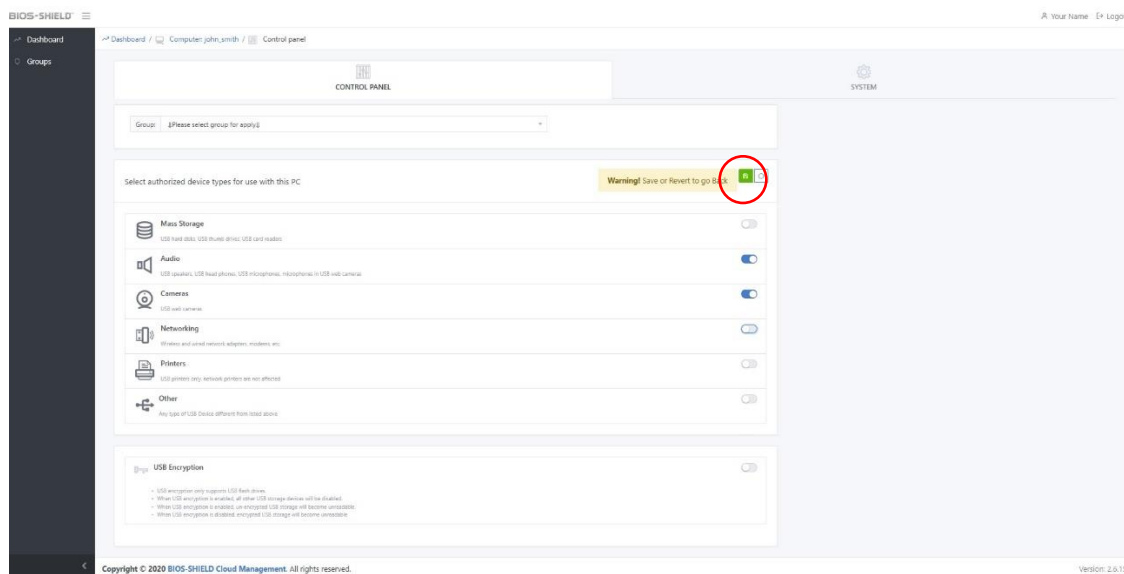


You can adjust the USB device control to fit your needs. For example, if you want to restrict your employees ability to use the USB thumb drive and protect company confidential data, you can disable the Mass Storage.

You can also :

- enable the audio and camera to allow your employees to conduct video conference calls.
- disable the “USB wireless” and “USB Ethernet” dongle
- disable the USB printers.
- disable any other USB devices that do not belong to any type of devices listed above.

After you adjust USB settings, please click “Save” button to make the settings apply.



You can go to the target laptop (John Smith’s laptop) and plug in a USB thumb drive, even if the USB thumb drive is connected to your computer, it will not detected it in Windows.

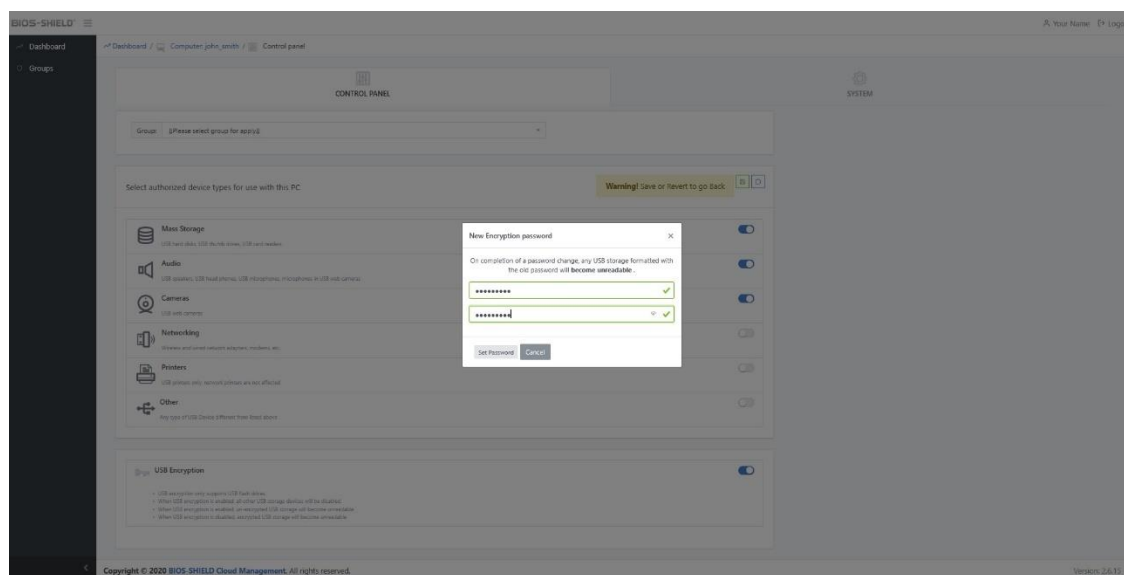
USB Encryption:

If you want to allow your employee to use the USB thumb drive feature to transfer data between BIOS-SHIELD computer, but you need to make sure confidential data won’t leak outside of the company, you can enable the USB encryption.

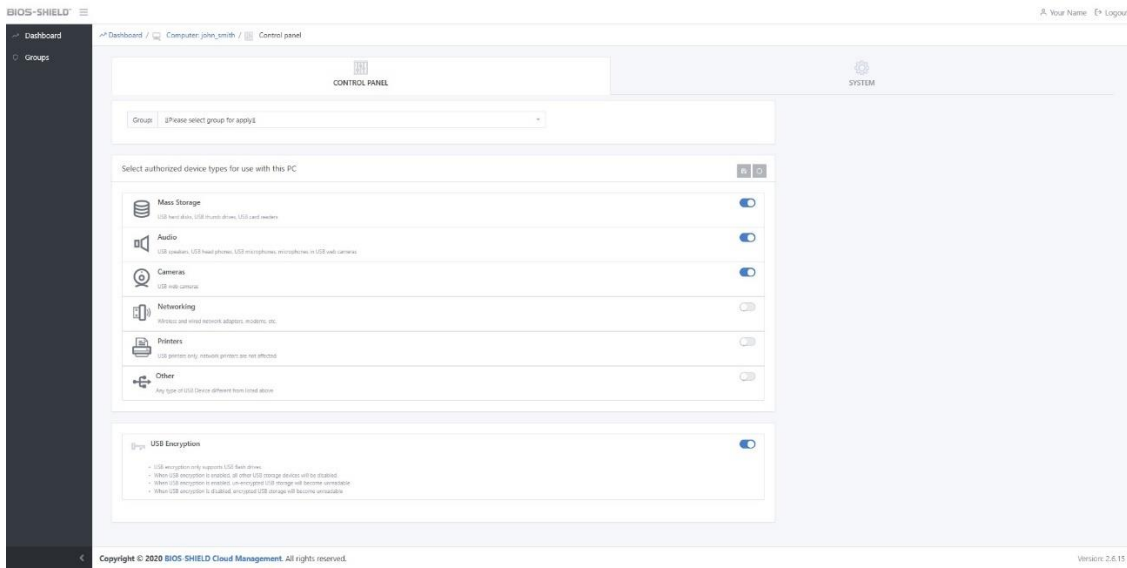
To do this, first, enable Mass Storage.

Then enable USB Encryption. It will prompt you to enter an encryption password. Please enter your encryption password and hit confirm - click “Save Password”.

(Please note, you need to remember this encryption password if you want to setup another computer to be able share the USB thumb drive.)



After Setting applied to computer, your Cloud Management UI look like this.

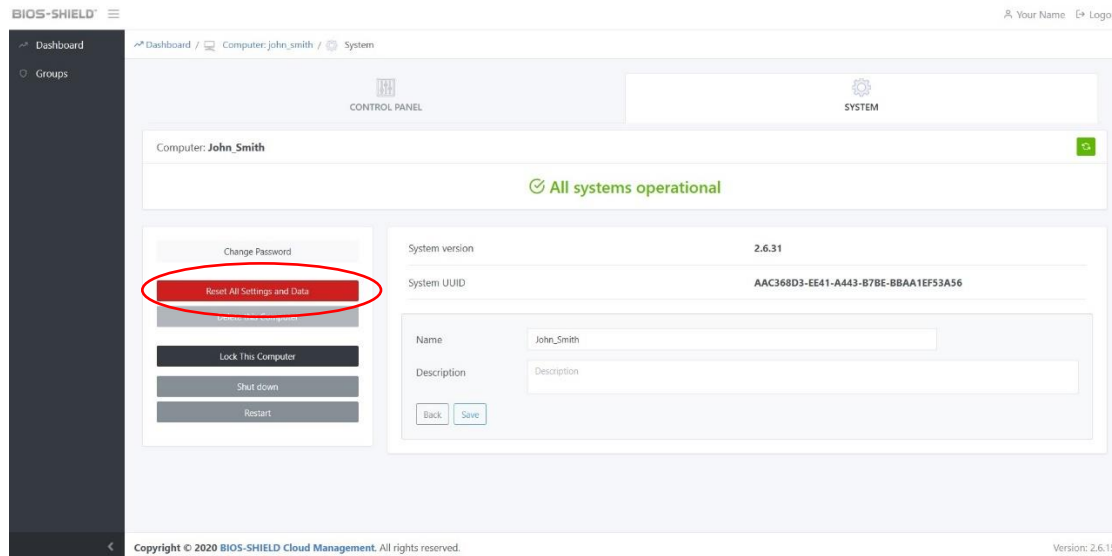


You can refer to [section6](#) for how to use USB encryption.

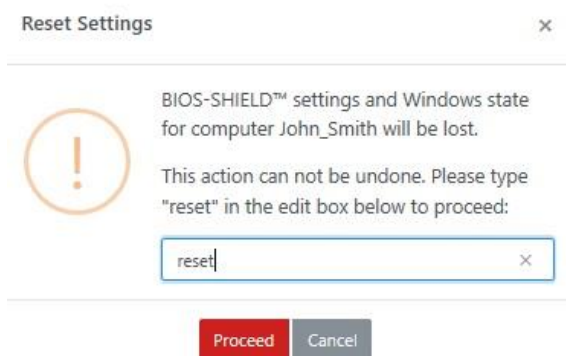
System Control:

When you use BIOS-SHIELD Cloud, you will have remote management capabilities such as “Reset Computer”, “Lock This Computer”, “Shutdown” and “Restart”.

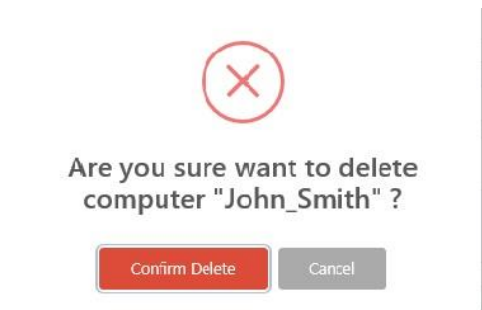
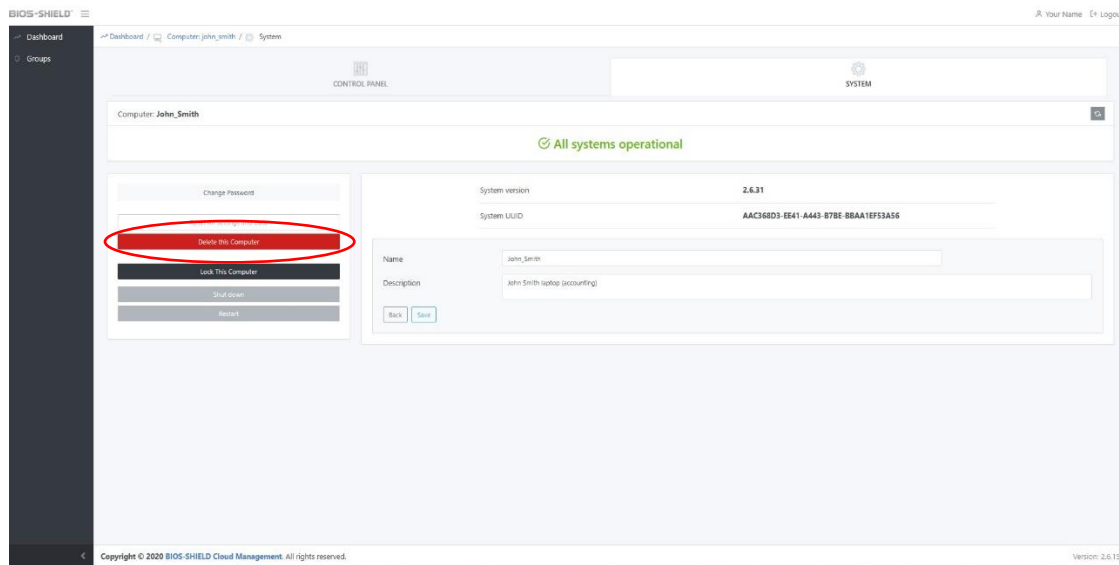
Reset All Settings and Data: This will Reset your computer to “factory settings”. It’s the same as describe in [section 11.3](#). You can use this feature to set your computer and re-distribute to your other employee to use. Or the other common use of this features like “Remote Wipe End User data”. If employee report a computer is lost, you issue this command as remote wipe. When the client computer connects to the internet, it receives this command and the computer will reset back to the factory settings and all end user data will be lost. Please use this feature carefully.



A confirmation page displayed, please type “reset” and click “Proceed” to issue factory reset. Please note that this is **not** reversible, the target computer will reset and all end user data will be lost. Your target computer will reboot and show “Welcome to BIOS-SHIELD™ Page”.

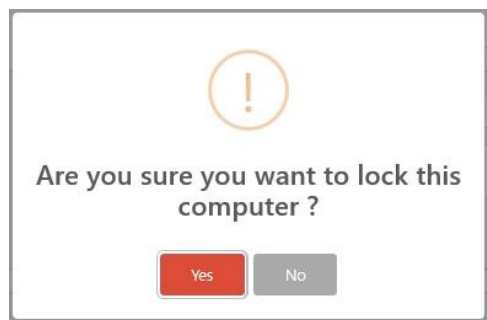
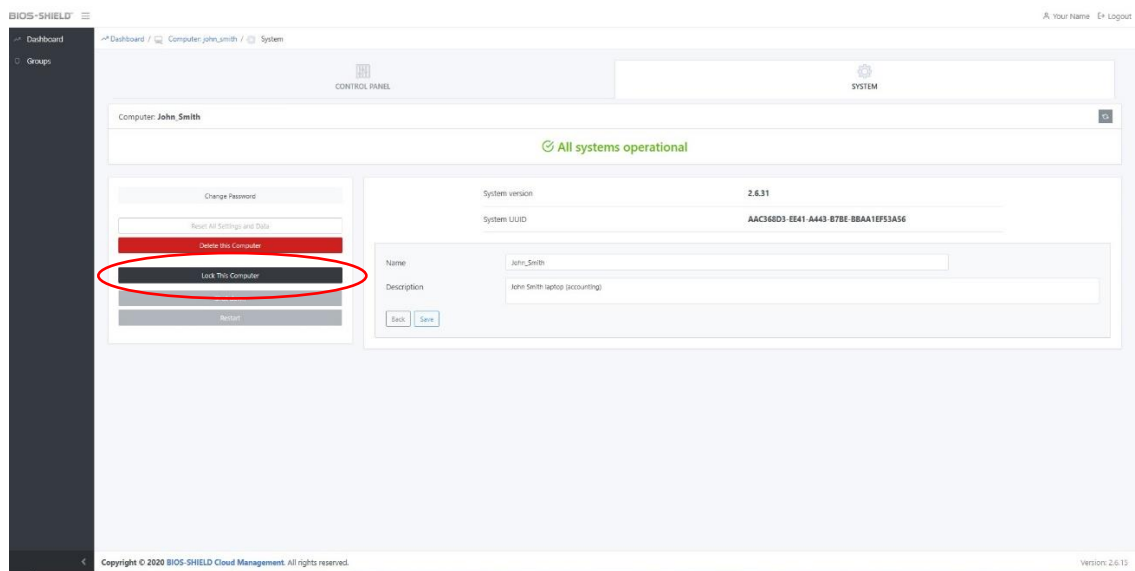


Delete This Computer: When you want to disconnect a computer from the Cloud Management Portal, you can use this function. While the computer is connected to the Cloud Management Portal, this button will gray out. You will need to shut-down the computer and disconnect from the Cloud Management Portal, this button will now be active. Click “Delete This Computer”. A confirmation window will appear, click “Confirm Delete” to proceed.

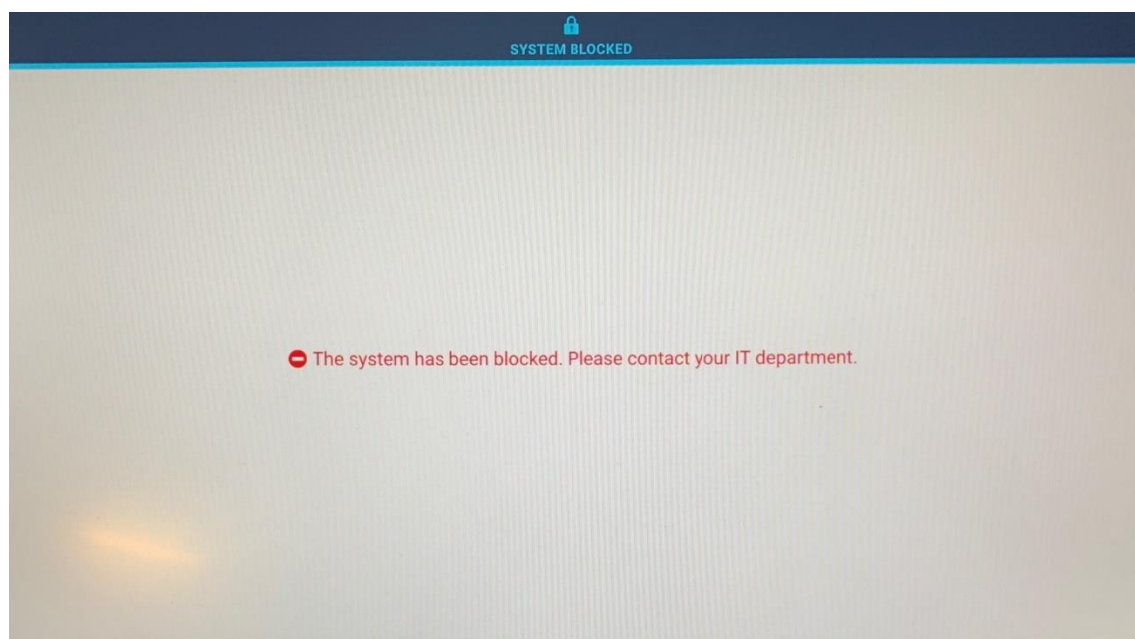


Once the target computer is disconnected from Cloud Management Portal, the computer settings (such as USB settings, USB encryption settings, etc) will remain the same. If you want to change the settings (like use is as Standalone Mode or Join to a new Cloud Management Account), you should use Ctrl+Alt+B and go to SYSTEM – Click the lock to make changes - Enter Password and click “Unlock”. Then click “Reset This System” – “Reset BIOS-SHIELD™ Configuration” – “Reset” then type “reset” in confirmation window and click “Proceed”. System will reset and go to BIOS-SHIELD™ Welcome page. You can decide if you want to use the “Standalone mode” or “Cloud Management mode”.

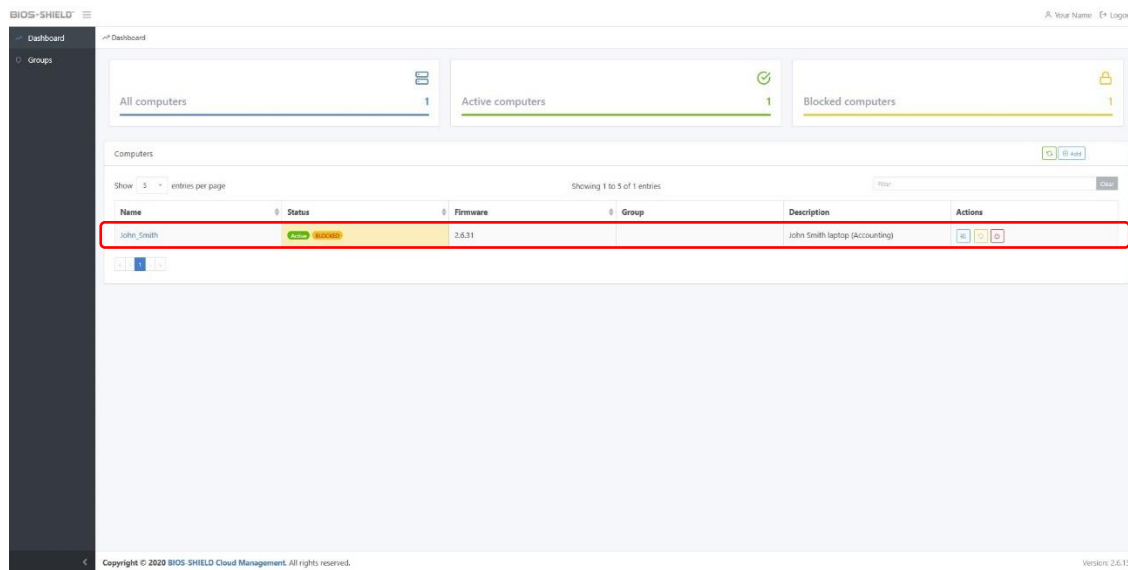
Lock This Computer: BIOS-SHIELD provides PC Enablement/Disablement function. In the event of a computer misplaced, employee should notify their company’s IT administrator or manager immediately. For best security, IT administrator can Lock this computer.



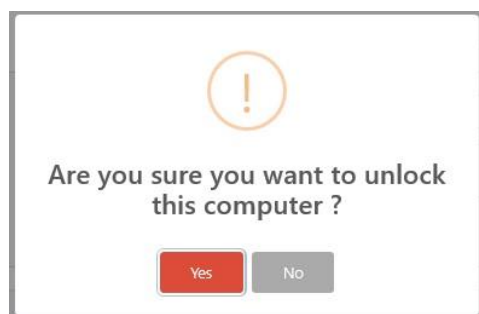
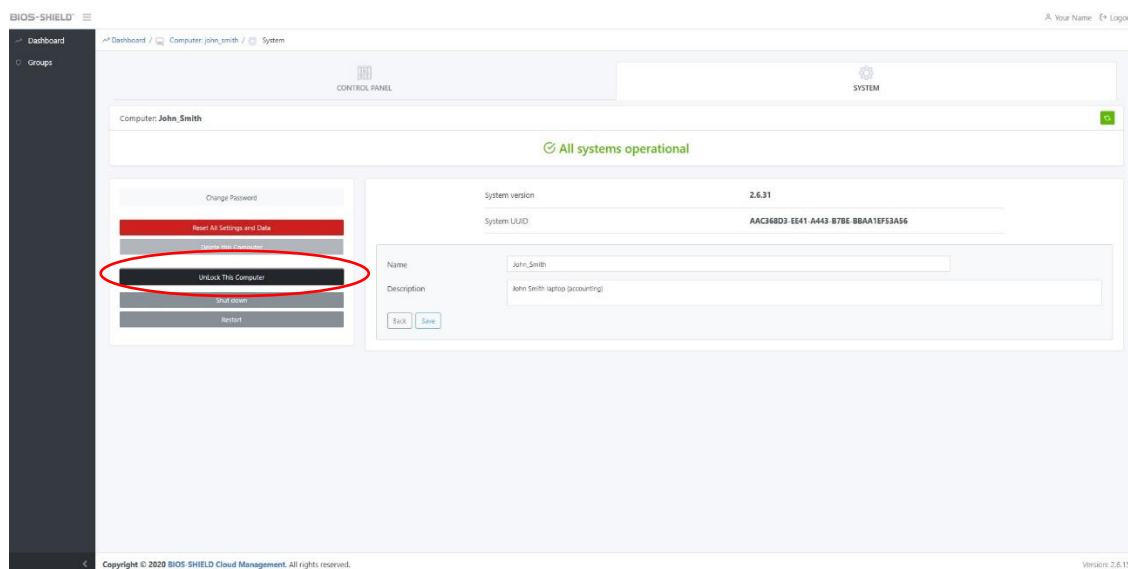
The target computer will be blocked and display the following message. It will NOT boot to windows.



On the Cloud Management Portal, you will see the following:

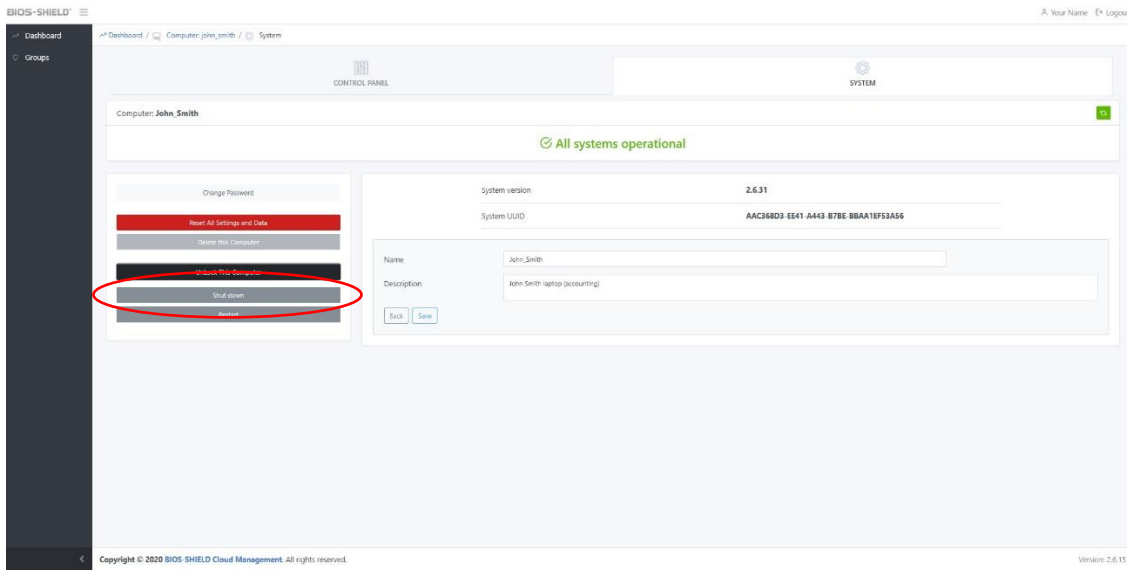


If the computer been recovered, IT administrator can unlock this computer by click “Unlock This Computer”

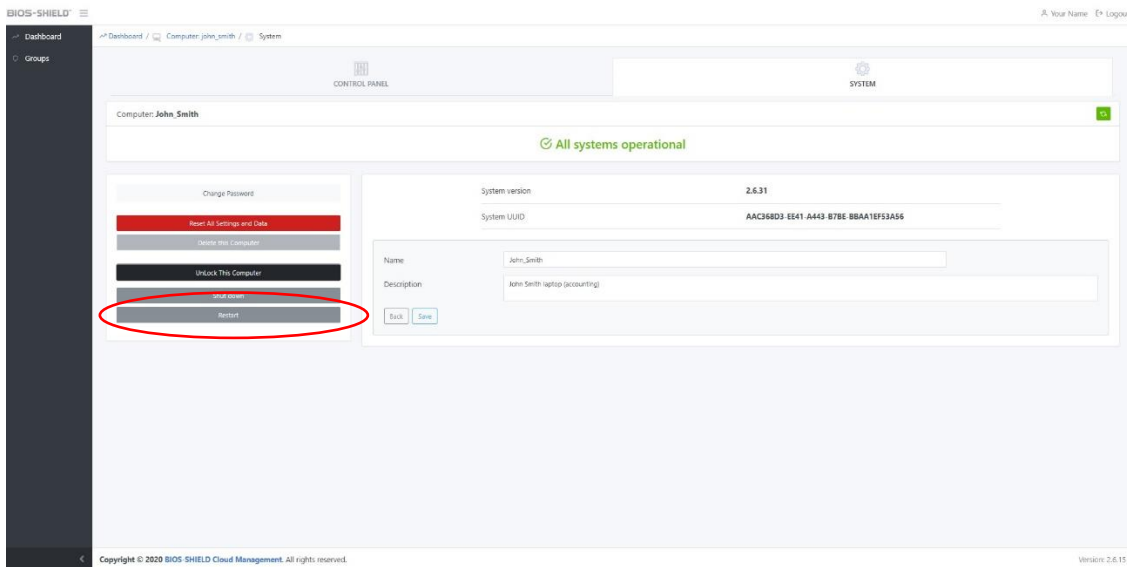


After click “Yes” on confirmation page, the target system will unlock and boot to Windows.

Shut Down: If you want to remote shut down the target computer, you can click “Shut Down”.

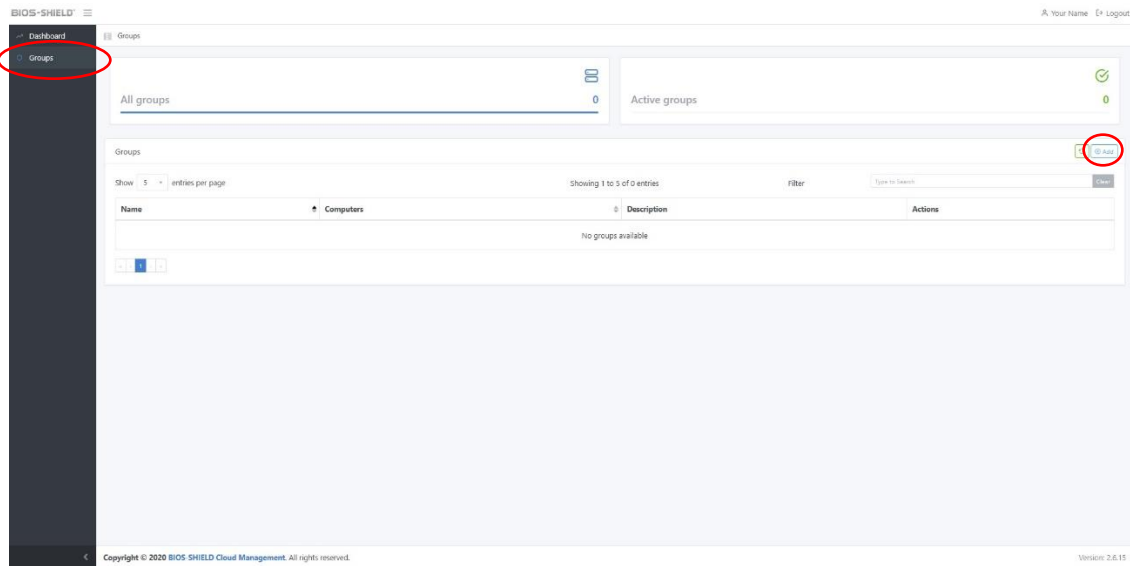


Restart: If you want to remote restart the target computer, you can click “Restart”.

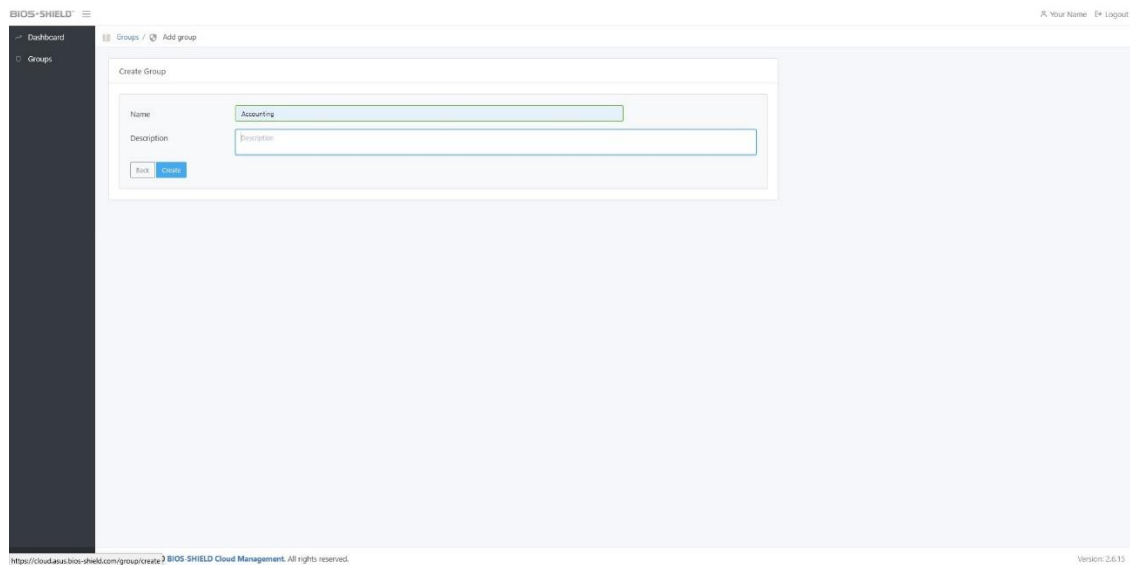


Group Management: BIOS-SHIELD™ supports Group Management capability. In a typical company, you can define employee's role by groups. For example, accounting group may have different settings compares to engineering group. IT administrator can create group, then assign target computer(s) into group, then configure settings to group. Then the group settings will apply to all the computers within the group.

Login to Cloud Management Portal, click “Groups” and click “Add”



Create Group - Accounting



Create Group – Engineering

Add computer(s) to Group

Click Accounting Group

BIOS-SHIELD

Dashboard Groups

All groups 2 Active groups 0

Groups

Show 5 entries per page Showing 1 to 2 of 2 entries Filter Type to Search Clear

Name	Computers	Description	Actions
Accounting	Computer		Add Edit Delete
Engineering	Computer		Add Edit Delete

Copyright © 2020 BIOS-SHIELD Cloud Management. All rights reserved. Version: 2.6.15

Click "COMPUTERS"

BIOS-SHIELD

Dashboard Groups Accounting System

CONTROL PANEL SYSTEM

Edit group : Accounting

Name Accounting Description

Back Save

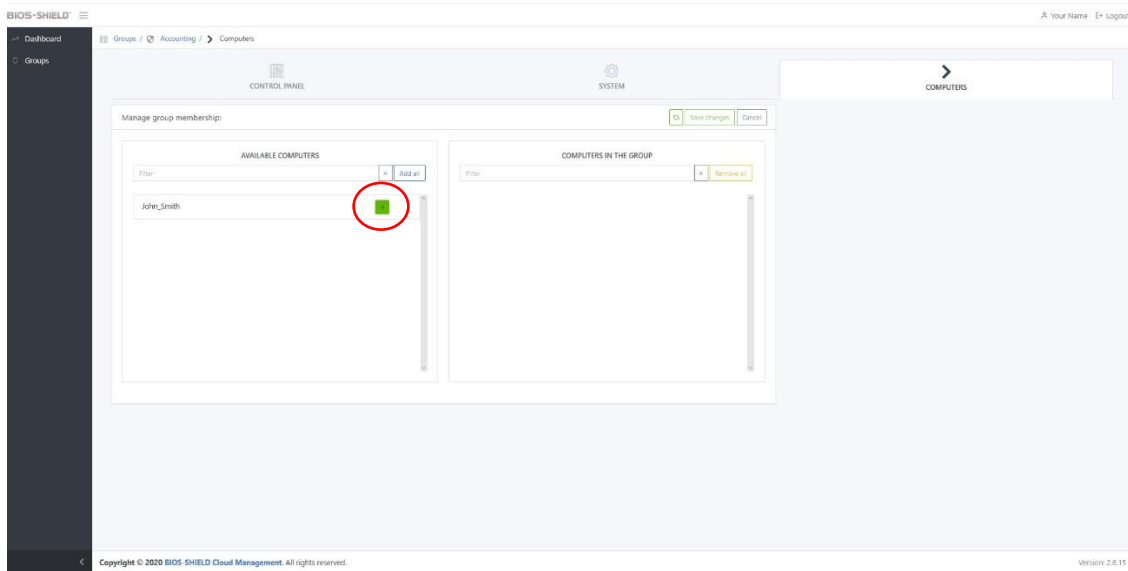
Change Password

COMPUTERS

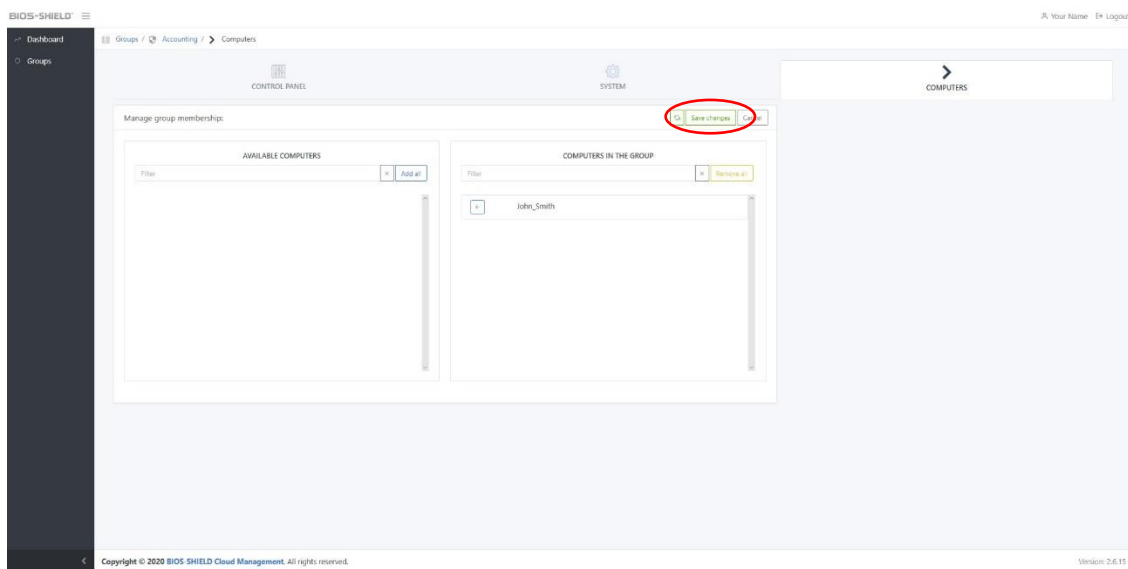
Copyright © 2020 BIOS-SHIELD Cloud Management. All rights reserved. Version: 2.6.15

Select computer(s) from AVAILABLE COMPUTERS and join to Group.

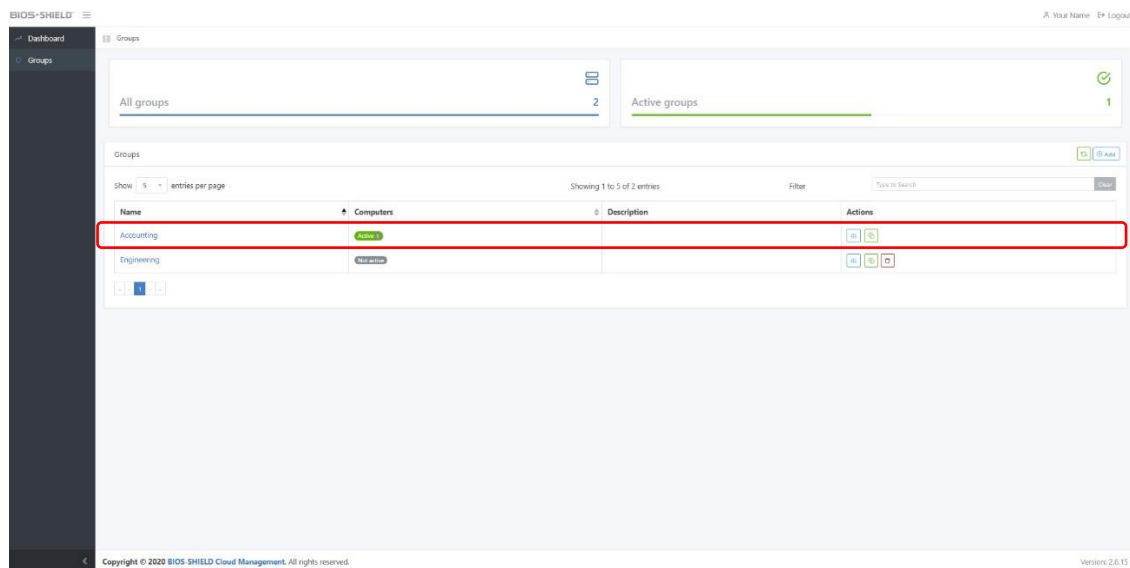
Click “➔”



Click “Save changes”

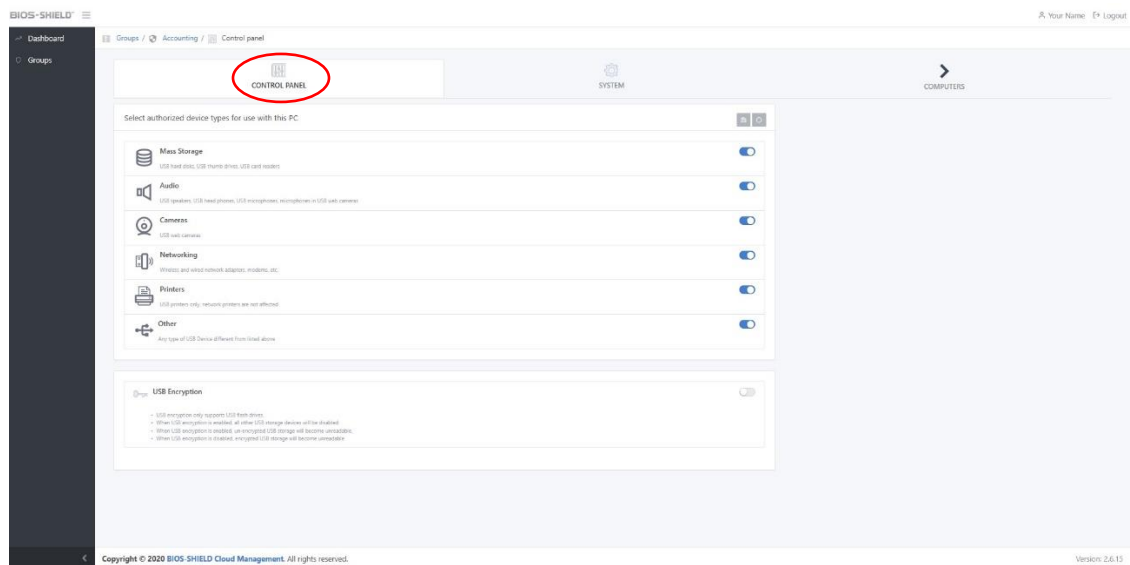


The computer “John_Smith” belongs to “Accounting” group now.

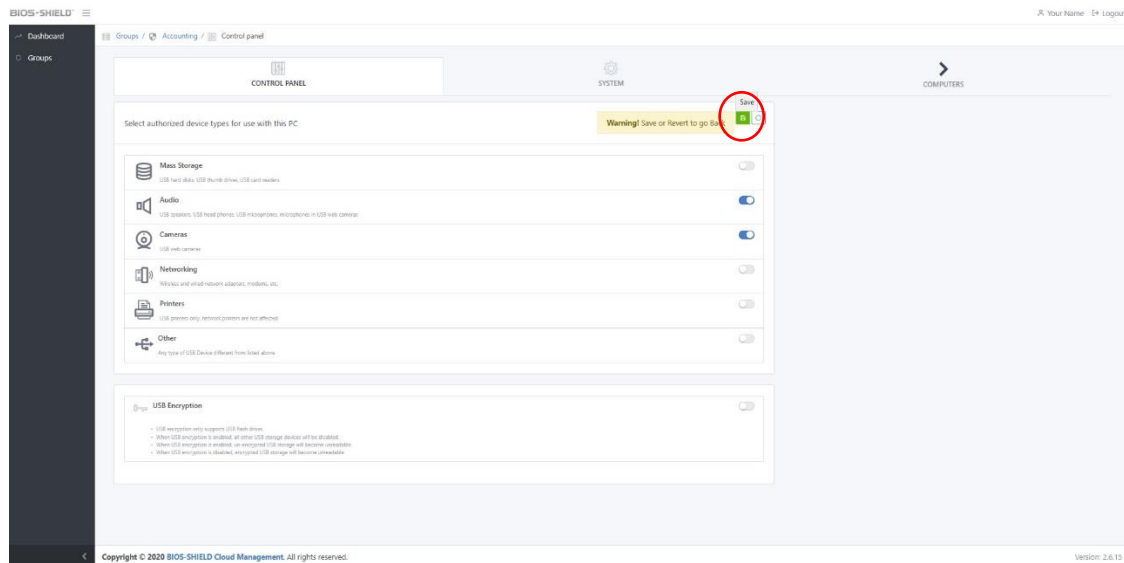


Edit Group settings

Click “Accounting” group then “CONTROL PANEL”

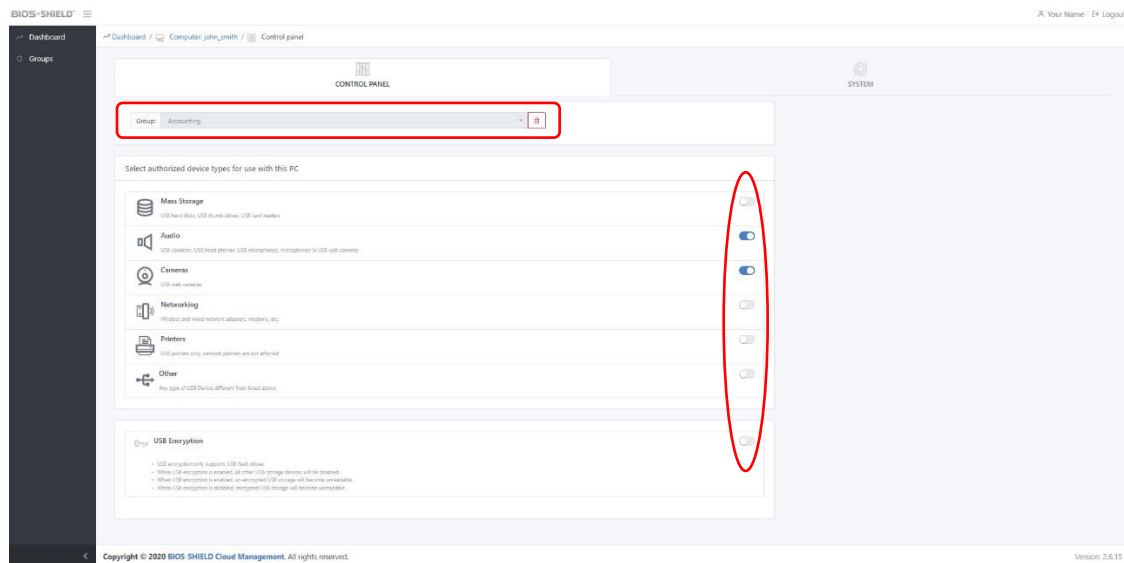


Please set proper group settings and then click “Save”

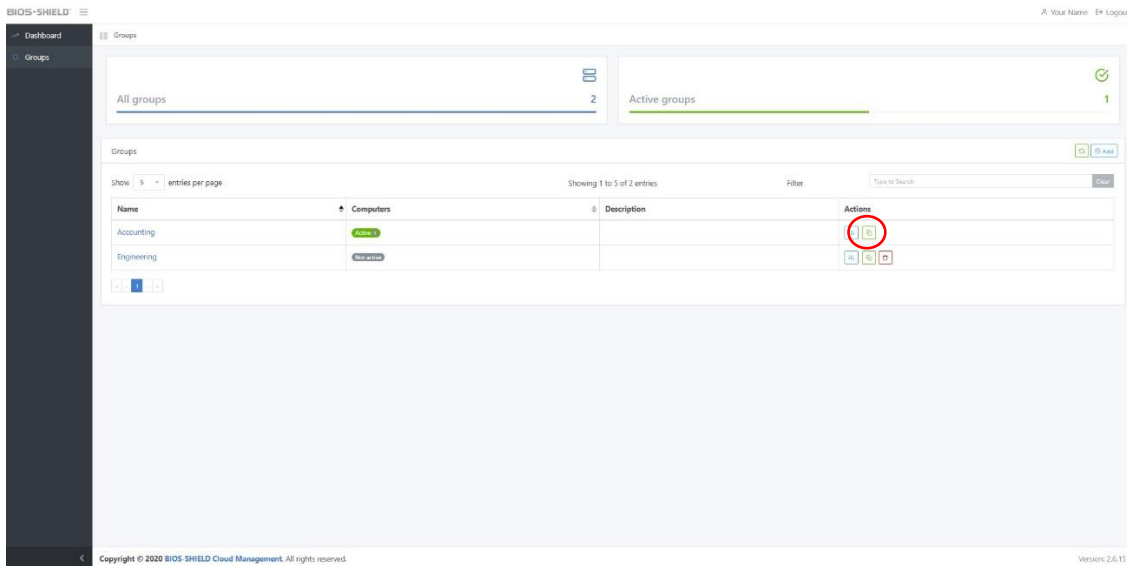


Group settings will be applied to all the computers in this group.

If you click “John_Smith” computer and go to “CONTROL PANEL”, you will find you **can not** modify the settings on right hand side. It’s because this computer belong to Accounting group and settings was defined in the Accounting Group.



Clone a group setting: When you try to setup a Group and its policy is very similar to an existing group, you can use the “Clone” function. For example, you try to create a “Sales” group and the settings is similar to “Accounting” group, you can do the following: client “Clone”



Change name to “Sales” and click “Clone”

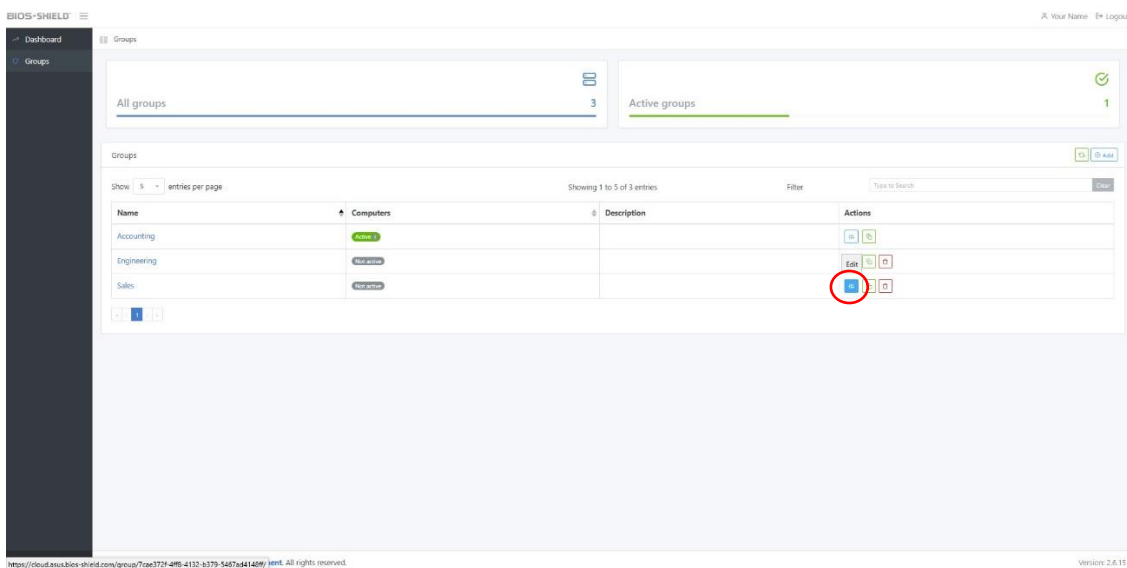
Duplicate group: Accounting

Name

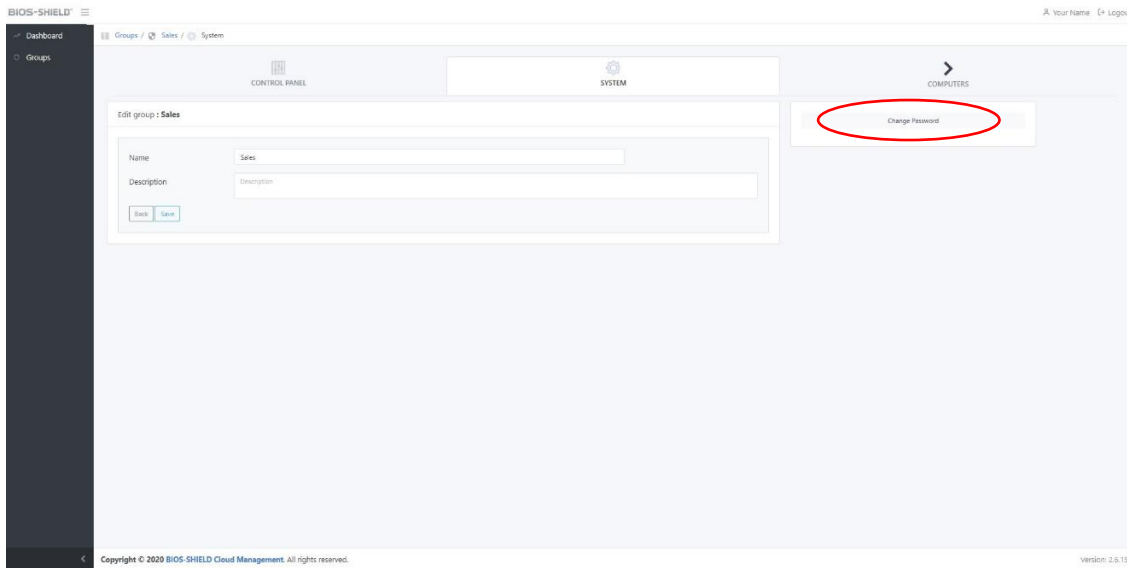
Sales

Clone Cancel

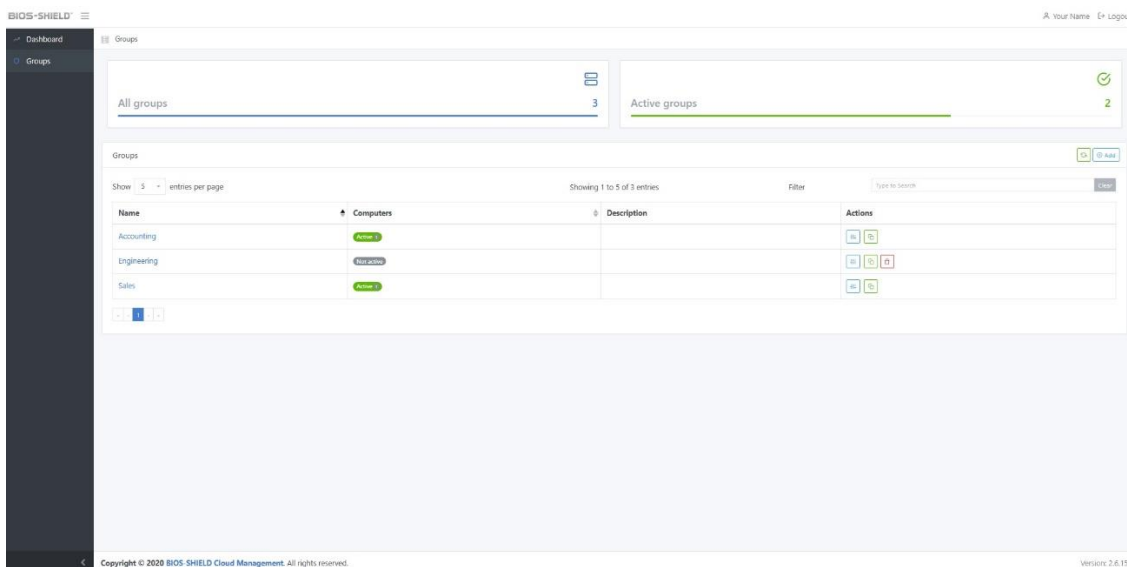
Then do final edit of “Sales” group settings by click “Edit”



Change Group Password:



Delete Group: You can only delete a group that has no computer assigned to it. In the following screen, both Accounting and Sales group have computer assigned to it. So, there is no “Delete” button. Engineering group has no computer in there, you can click “Delete” button to delete this group. When you need to delete a group, please remove computers from it and then delete group. When you remove computers from a group, please make sure these computers have proper settings apply to them to ensure their security.



Best practices will typically include turning on USB encryption so that employees can securely use a USB thumb drive to transfer data securely. Companies may decide to setup different groups based on employee functions. Each group can be assigned a different USB encryption password. By doing this, USB thumb drives will work within a designate group but not across an unassigned group. For example, an Engineering computer will not be able to read the USB thumb drive from the Accounting group. When USB encryption is turned on, the computer will not be able to read a USB thumb drive written from an “un-authorized” computer. This will reduce the risk of importing malware from an un-authorized USB thumb drive.