

How to Disable USB2 Hub Downstream Ports for Server Security Applications



External devices such as USB drives play a dual role, they enhance productivity by enabling quick data transfers but pose significant security risks simultaneously. Companies across industries face challenges in safeguarding their sensitive information, as unregulated use of USB devices can lead to unauthorized data access, malware infiltration, and compliance violations.

Managing external devices has become one of the critical part of security strategies. With the increasing complexity of device security threats, workplaces require stricter controls over device usage to protect data integrity and prevent operational disruptions. The ability to regulate USB access is a technical measure and a critical part of enforcing company-wide security policies and meeting regulatory standards.

Disabling USB ports on Windows PCs and servers helps companies prevent unauthorized data transfers, reduce malware exposure, enforce security policies, and protect sensitive business information.

Why should a user disable USB ports on computer system?

USB drives are a convenient way to transfer files, but they also pose significant security risks, especially in professional and sensitive environments like servers. Here are key security concerns that necessitate disabling USB ports on computers:

1. Preventing data loss, breach, or theft
USB drives make it easy for individuals to transfer sensitive information out of an computer system without leaving a trace, highlighting the risks such devices pose to data security. Whether intentional or accidental, the unauthorized transfer of proprietary data or customer information can have major consequences. Businesses could face lawsuits, reputational harm, or financial losses from leaked data. By disabling USB ports, companies can prevent such incidents and maintain better control over their critical data.
2. Protect USB devices using security measures against malware and viruses

External USB drives are a notorious entry point for malware, including viruses and spyware. A single infected USB device can bypass traditional security measures and introduce malware or increase compromise risk, especially on systems running Windows. High-profile ransomware attacks often originate from simple actions like plugging in an unverified USB drive. To counter these risks, IT admins not only disable specific USB ports but also configure policies to deny read access or deny write access on removable drives. These measures help prevent infections that can disrupt operations, steal sensitive data, or even demand hefty ransoms.

3. Preventing unauthorized access through USB storage

USB drives can serve as tools for unauthorized individuals to access sensitive corporate systems. A malicious actor could use USB to execute commands, install backdoor programs, or steal data unnoticed. This is particularly concerning in shared work environments where device access might not always be closely monitored. By disabling USB ports using unauthorized USB device blocking tools, organizations restrict access for unauthorized users to exploit company devices, enhancing overall security.

How to disable USB ports on computer system?

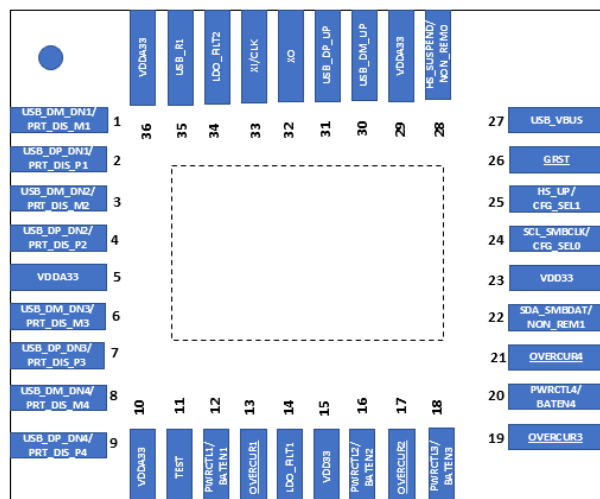
To stop people from plugging in USB drives on a Windows PC or server, there are a few ways to do it.

USB access can be disabled through Device Manager, Group Policy, Registry Editor, BIOS/UEFI settings, or an endpoint management solution to block USB storage and unauthorized peripheral access, depending on scale and control requirements.

This document discusses how to disable USB ports with TUSB2514B USB2 hub.

- 1: Disable USB ports in hub pin-strap mode.
 - 1. TUSB2514B pin mapping:

Figure 1 is the TUSB2514B pinout map

**Figure 1. TUSB2514B Pinout Map****2. TUSB2514B pin-strap mode implementation:**

To configure TUSB2514B into pin-strap mode, CFG_SEL[1,0] is 00. To disable hub downstream ports in pin-strap mode, need to adding 10k pullup resistor on DP/DM signals.

USB_DM_DNx/USB_DP/DNx pins will be sampled at the rising edge of GRST signal to determine if USB port is disabled or not. Tabel 1.1 shows how to disable USB ports in pin-strap mode

Table 1. TUSB2514B Implementation in Pin-Strap Mode

Pin No	TUSB2514B Pin Name	TUSB2514B Implementation
1,3,6,8	USB_DM_DNx/ PRT_DIS_Mx	USB high speed transceiver (negative) for downstream portx Adding 10k pullup option to disable portx
2,4,7,9	USB_DP_DNx/ PRT_DIS_Px	USB high speed transceiver (positive) for downstream portx Adding 10k pullup option to disable portx

2: Disable USB ports in hub SMBUS mode

To configure hub into SMBUS mode, CFG_SEL[1,0] is 01.

Here is the procedure to disable hub downstream ports with SMBUS.

1: Configure CFG_SEL[1,0] to 01, pin 22 (SDA_SMBDATA) and pin 24 (SCL_SMBCLK) are pulled up to 3.3v with 10k resistor

2: SMBUS address is 0x44

3: Power on TUSB2514B

4: Read TUSB2514B register with SMBUS and I2C master controller to make sure SMBUS connection works.

5: Set register 0x07h bit [7] to 1

6: Set register 0x08h bit [0,3] to 1 to disable any downstream ports you want

7: set register 0xF8h bit [0] to 1 to clear cfgActive bit to exit SMBUS programming mode

8: You will see TUSB2514B will be enumerated as generic USB2 hub under device manager or USBTreeView

Summary

Disabling USB ports on Windows PC and server is a smart way to protect your system and prevent data loss by being copied or shared without permission. It helps companies prevent unauthorized data transfers, reduce malware exposure, enforce security policies, and protect sensitive business information. This application brief mainly discussed how to disable USB ports with TI TUSB2514B USB2 hub either in pin-strap mode or SMBUS mode.

Trademarks

All trademarks are the property of their respective owners.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to [TI's Terms of Sale](#), [TI's General Quality Guidelines](#), or other applicable terms available either on [ti.com](https://www.ti.com) or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Copyright © 2026, Texas Instruments Incorporated

Last updated 10/2025