Switch limits access devices

Group policies on MS switches allow users to define sets of Access Control Entries that can be applied to devices in order to control what they can access on the network.

UniFi switches have Access Control Lists (ACLs), useful for isolating device traffic on the same VLAN. Networks with high-performance requirements can also use them to manage inter-VLAN routing, ...

Access Control is a built-in security feature that lets you choose which devices can and cannot connect to your network. This guide covers how to block devices connected to your Wi-Fi ...

This article explores various methods and tools available to help you effectively control internet access, ensuring that only designated devices can use your network freely.

This table lists the access-list number and corresponding access list type, and shows whether or not they are supported in the switch. The switch supports IPv4 standard and extended access lists, ...

By configuring a Failed-authentication GPACL or SGT, you can control and restrict the network resources accessible to devices that do not successfully authenticate, such as limiting ...

Discover how many devices your router can realistically support and learn practical tips to optimize your home or office network using WiFi and Ethernet connections.

Likewise, you should not allow unknown devices to connect to your network for security reasons. Let"s discuss some methods to restrict Internet access in more detail.

Visit your product"s support page, select the correct hardware version for your device, and check either the Datasheet or the firmware section for the latest improvements added to your product.

You can"t filter communications between devices. You can still filter communications between devices and the internet.

Web: https://safireschools.co.za