ManageEngine
Device Control Plus

Best practices to make the most of your device control solution

INTRODUCTION

In an organization where sensitive data resides in all three forms—at rest, in motion, and in use—you have to be wary of data theft and leakage. Throwing peripheral devices in this mix increases the chances of an uncertain environment.

A reactive approach to this is to have a solution that addresses these challenges. You also need to consider the following questions:

01

Is the solution best utilized?

02

Are you proactive in your approach to securing your business environment?

03

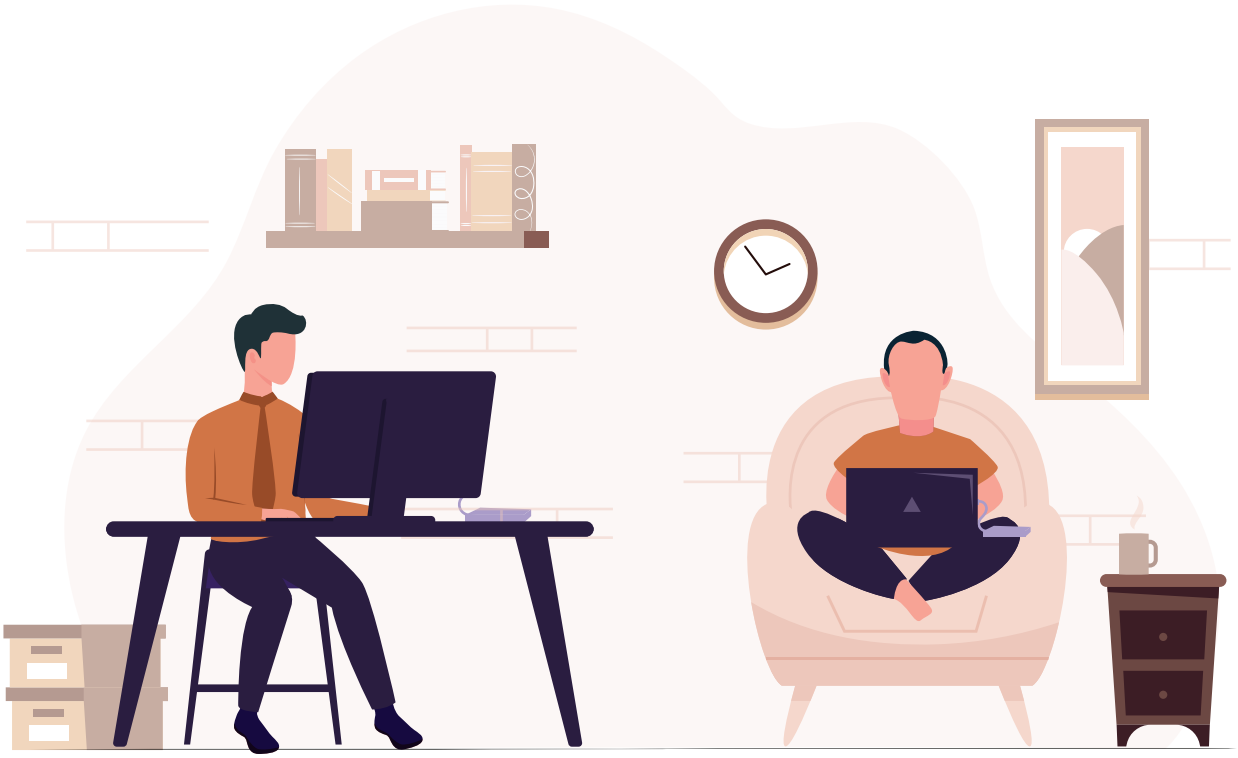
Is your approach effective enough to repurpose for multiple use cases?

The best practices included below will guide you in creating a secure environment for your organization and in managing its peripheral devices in the best possible way.

WHY BEST PRACTICES?

Best practices provide solutions for different scenarios while ensuring your organization's security is intact.

WHY BEST PRACTICES FOR **DEVICE CONTROL?**

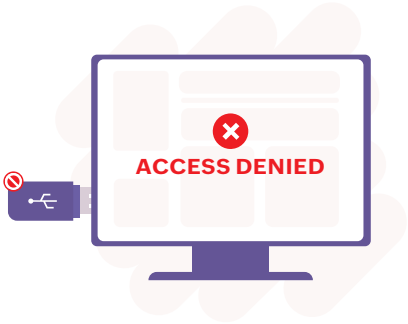


Now more than ever, organizations are favoring BYOD policies and facilitating the use of external devices to augment productivity. Be it a removable storage device to transfer critical files, a printer to print documents for your presentation, or even a wireless mouse or keyboard to work at your convenience, peripheral devices have evolved into a reliable and powerful medium to share business-related information easily.

With such dependence on these devices, it's important to define their purpose or role—after all, they work for the organization. Without a clear role defined, demarcating the devices that can be trusted from the rest could be demanding.

But lesser known are the threats such devices pose when unmonitored, and alarmingly, the best approach to alleviate such risks is often not taken. Following are some best practices regarding real-world scenarios and unprecedented use cases in device control.

Use a "no room for error" approach by denying peripheral device access to allnetwork endpoints



Devices newly entering the organization's network or those deployed without a policy are more prone to unauthorized access, be it an unencrypted wireless mouse, a USB device suffering from a badUSB attack like Rubber Ducky and posing as a keyboard, or even a badUSB attack intercepting input signals from the keyboard and relaying them to the hacker's computer.

Why risk this when you can devise a policy that blocks all devices unanimously from connecting to computers, keeping any chance of data leakage at bay?

Frame policies to allow peripheral device access for privileged users' endpoints

When it comes to managers and C-level executives in the organization, you have to tread lightly while creating a policy that includes them. After all, a one-size-fits-all approach tends not to work in an organization with varying user roles and departments.

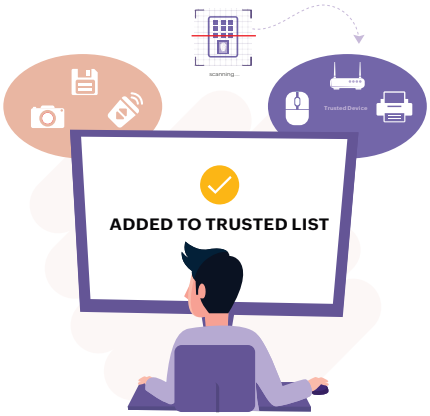
Instead of having to tiptoe, leverage the concept of user roles while creating a policy. Create one specific to high-privileged users, and allow them permissions to access all devices without risking their productivity.

Allow access to specific users using user group exclusion without creating additional policies

You don't always have to rely on policies to circumvent device-based concerns, as a customizable user group is another recourse. An organization with a block policy is secure but restricts administrators' activities. Without creating overhead with another policy for administrators, you can deploy the existing block policy to an existing custom group along with a user group exclusion.

This concept allows you to demarcate standard accounts from esteemed accounts so that multiple users can have separate policies, all effective on a single computer. Create a user group excluding technicians or administrative users, thus forming concordance between their device needs and the "allow all" policy.

Add your organization's peripheral devices to a trusted device list



Admins and peripheral devices are always in disagreement. While the tussle to strike the right balance between security and productivity is riveting, often, enterprise-approved devices get caught up in the middle of this conundrum. Adding such devices to a trusted device list comes in handy when corporate devices want to stand out from other devices.

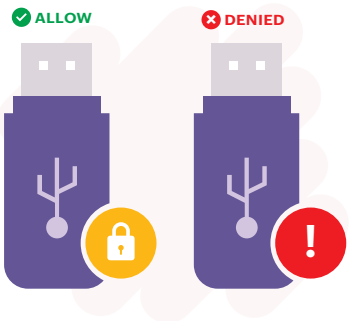
Creating a CSV file with enterprise-approved devices and uploading it to the trusted device list reduces the workload of manually adding devices and automatically allows all enterprise-approved devices to be active in the network.

Use a permanent solution for temporary peripheral device needs

As always, more than designing a solution, it's the follow-up that needs meticulous attention; after all, there could be a fatal issue or a flaw that exploits the task itself. Revoking admin access cannot be overlooked, yet being spot on is not always guaranteed. Instead of basing your confidence on laborious activities like handpicking the devices to add to the trusted list or manually picking out the devices to revoke admin access, you can create a temporary access list for device access in special cases and enable this option on policies.

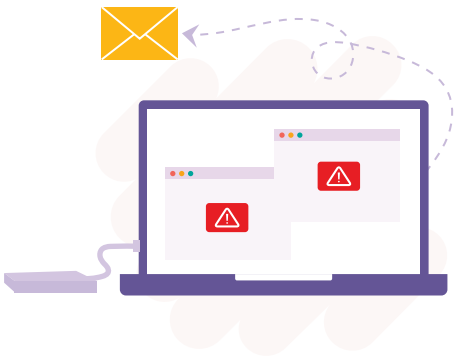
You can configure a policy to enable temporary access that hands the control to the end user, who can then request temporary device access. Once the duration for device access ends, the special rights are revoked automatically, creating a hassle-free environment.

Hold the door only for encrypted peripheral devices



Encryption is the go-to solution for secure data transmission, and the one offered by BitLocker is a solution intact, making it harder to bypass and expose your enterprise data. You can never go wrong when you allow only BitLocker-encrypted peripheral devices—this can come in handy while configuring a policy to avoid exposing your endpoints to unencrypted wireless devices, keeping potential keyloggers at bay.

Configure alerts and notifications for unauthorized device-based actions



Configuration is the key to establishing a flow and deputing alternate solutions in case of anomalies. Once you have configured your mail server settings, you can customize the alert email notification and its intended recipients. These alerts are sent when a restricted device enters an organization's network, and notifications are sent to technicians when temporary access is requested by a user.

Stay compliant by configuring device auditing and data mirroring reports

Adhering to industry regulations and guidelines is important to avoid financial and reputational losses. Every organization has its own compliance strategy and, per your enterprise's needs, you can configure file auditing and file shadowing reports to ensure such configurations are security compliant.

The GDPR, HIPAA, and PCI DSS, just to name a few, are some of the compliance standards which your organization can adhere to using a solution like ManageEngine Device Control Plus.

FREE TRIAL LEARN MORE