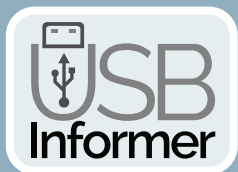
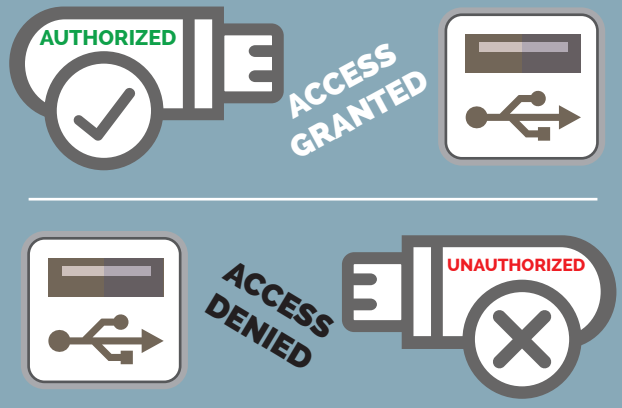
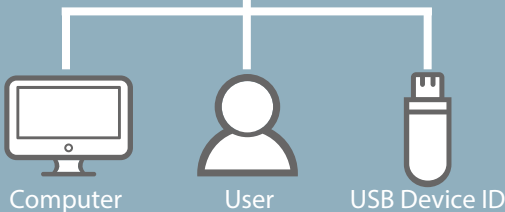


USBInformer

USBInformer® provides USB port security on every Windows based endpoint on your network. You can mitigate threats introduced through USB connections by enforcing a policy that only administrator authorized devices are allowed. USBInformer® uses a real-time monitoring service that stops access to any USB device that is not approved. The web portal then allows administrators to remotely grant or reject user access to new & existing USB devices as requirements change.



Provides Granular Control over USB ports based on a combination of:



USBInformer® continues to protect, enforce, & report on portable devices even when they are away from your network. All activity is locally cached & reported to administrators when the endpoint returns to the network, giving administrators a clear record of any activity that occurred while the device was away.

Policy flexibility is a key component to USBInformer®. Every network is unique with its own set of users & devices. USBInformer® caters to your network and is able to customize & enforce policies based on any combination of computer, user & USB device.

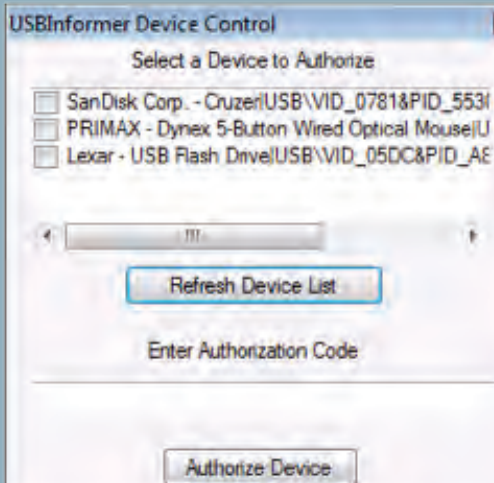
Computer	Authorized Devices	Unauthorized Devices	User-Unauthorized Devices	Date Added	Last Checkin
USBA_PC	4	0	2	6/23/2016 11:53:44 AM	6/23/2016 11:53:44 AM
MW01PC010	0	0	1	7/20/2016 11:53:44 AM	7/20/2016 11:53:44 AM
USBA_PC2	0	0	1	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
WIN7CL1	3	3	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
WIN7CL2	2	0	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
WIN7CL3	1	1	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
WIN7CL4	4	0	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
WIN7CL5	6	7	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
WIN7CL6	7	0	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
WIN7CL7	5	1	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
WIN7CL8	28	3	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
USBA_PC3	0	0	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
USBA_PC4	3	3	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
USBA_PC5	4	4	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
USBA_PC6	0	0	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
USBA_PC7	0	0	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
USBA_PC8	1	2	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
USBA_PC9	0	0	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM
USBA_PC10	0	0	0	8/23/2016 11:53:44 AM	8/23/2016 11:53:44 AM

Device ID	Description	Date Added	Status
USBA_PC10	SanDisk Connect Wireless	8/23/2016 11:53:44 AM	OK
USBA_PC10	SanDisk Connect Wireless	8/23/2016 11:53:44 AM	OK
USBA_PC10	SanDisk Connect Wireless	8/23/2016 11:53:44 AM	OK

The recent release of USBInformer® 2.0 has brought some major new features and updates.

Physical Keylogger Detection

We have improved our device detection and in USBInformer® 2.0 we are now able to mitigate the risk of a physical keylogger being plugged into your computer systems. Using deep USB analytics and analysis we can alert on and block physical keyloggers.



One Time Use Device Authentication Codes

This new feature allows your IT staff to help your mobile employees. Now when your employees take their laptop off the network, your IT can help authorize devices without the need of connecting back to the network. These one time use codes authorize a single device and can never be used again. When the user returns the computer to the network, the authorized device will be placed into the database and can be further managed by your IT staff.

Managing Computers and Devices has never been easier. With the new Management view, you can quickly manage any computer and the devices connecting to it. The revamped interface allows for smaller learning curves for your help desk. [See Screenshots on Page 1]

Improved Features:

- ✓ **Stability & Efficiency**
- ✓ **Lower Network Communication Footprint**
- ✓ **Communication Security w/Message & Transport Encryption**

We have worked hard to improve every aspect of the system to make it more stable, secure and silent. With 2.0 we have improved how and when the clients report back to the server. We have decreased the traffic needed to perform these actions and we have enhanced the security of the in data that is transmitted across the network. USBInformer® 2.0 is the best USB protection solution we have ever produced.



What Will It Take to Secure My USB Ports?



The first step to locking down your USB ports will be to setup your server.



S
E
R
V
E
R

This server will be a Windows 2008 or greater setup with SQL Server Express, IIS, &.NET Framework 4.0.

After the server is set up we can deploy our Clients to the endpoints we want to protect.

USBInformer® Client requires Windows Vista or newer & .NET Framework 4.0.

The client can be deployed by:
» Easy to use MSI installer
or
» Command line installer

C
L
I
E
N
T



Once these services are set up, then USBInformer® Admin can be installed using the MSI Installer.



C
O
N
T
R
O
L

Once the Client has been installed then all control is established through the Server, including updates & policy management.

Server Minimum Requirements:

- » Windows Server 2008 R2
- » IIS 7.5
- » .NET 4.0
- » SQL Server Express 2008

Client Minimum Requirements:

- » Windows 7, 8, 10 or Server 2008 or 2012
- » .NET 4.0
- » Administrative Privileges (for setup only)