



# Device and Application Control

powered by HEAT Software

## Release Notes

5.1 Update 1

## Release Notes

Ivanti is pleased to announce the release of Ivanti Device and Application Control 5.1 Update 1! This update includes a variety of fixes for issues reported in previous releases.

# Issues Resolved

The 5.1 Update 1 release resolves the following issues:

ID	Description
RM 253838	Fixed an issue that caused upgrades from 4.6 SR3 to 5.1 to fail when using Default Keys.
RM 253750	Fixed an issue where application of policies to x86 machines would fail.
RM 254076	Fixed a policy issue that allowed access to blocked removable storage devices if no permissions were applied.
RM 254292	Fixed an issue that caused network printing jobs to fail when users inserted USB Type C docking stations into their devices.
RM 254268	Fixed a blue screen error that would occur when attempting to burn a CD.
RM 252894	Fixed a blue screen error that would occur after connecting laptop devices to docking stations.
RM 248257	Fixed an issue that prevented third-party applications from starting when the device had both Ivanti Device and Application Control and Kaspersky Endpoint Security with AES Crypto Module installed.
RM 252969	Fixed an issue that blocked scripts assigned to an unauthorized file group when Macro and Script Protection were set to Disabled.
RM 253532	Fixed an issue that caused Windows 10 to crash when running reports.
RM 253807	Fixed an issue that disrupted access to CD and DVD drives on devices with TrendMicro OfficeScan installed.
RM 253819	Fixed an issue that prevented access to portable encrypted USB flash drives. This issue occurred after removing a USB flash drive without first ejecting it from Windows.
RM 254266	Fixed a logging issue that caused some recorded device events to disappear.
RM 253210	Fixed an issue that prevented users from saving policy export DAT files consistently.

# Known Issues

The 5.1 Update 1 release ships with one known issue.

## Issue

When using Secure Volume Browser to copy a file from an encrypted device to another location, the copy does not complete successfully.

## Symptoms

This issue occurs under the following conditions:

### Before the file is copied

- You are using only Secure Volume Browser to copy a file, and not Windows Explorer.
- The file being copied is stored on a device with Portable Encryption.
- The file being copied is 4 GB or larger.
- You are copying the file *from* the device *to* another location.

### After the file is copied

- The size of the copied file is less than the size of the original file.
- When you attempt to open the copied file, the file is corrupted.

## Resolution

Instead of copying the file using only Secure Volume Browser, copy the file from Secure Volume Browser to Windows Explorer.

1. From Secure Volume Browser, unlock the device using the password set during the initial encryption process.
2. Open an instance of Windows Explorer. Browse to the path that you want to copy your file to.
3. Copy the file from Secure Volume Browser to Windows Explorer.

Very large files may take a few minutes to complete.

**Result:** Your file is successfully copied to your destination.