Ivanti Device and Application Control 5.2
Release Notes

Components in this Release

Component	Version
SK version	5.2.873
SCOMC version	5.2.874
SXS version	5.2.874
DB version	5.2.464
SMC version	5.2.874

Release Notes

We are pleased to announce the release of Ivanti Device and Application Control (IDAC) 5.2. Read these notes to find out what we have changed and what we've fixed.

Product Updates

Unlock tool for macOS

With this update we are bringing a macOS utility tool that provides the ability to read/write content from removable devices that were previously encrypted on Windows endpoints. Once the device is attached to the macOS endpoint, the user will have access to the data only after the password is provided. This provides transparent access through Finder when the device is attached.

Manage assets using Active Directory

We have improved our integration with Active Directory and with the 5.2 release you can enforce policies on AD Organizational Units. By default, this option is disabled and needs to be changed from the settings. After enabling this option, if an integration exists, the OUs from AD will be visible under **Machine-specific settings**. Now, you can assign permissions as you would do on any group.

Standalone endpoint management

5.2 update brings additional tools for managing endpoints that are not connecting to the central server. The client has the option to export details related to:

- Attached devices

- Local users and endpoint information

This data can be imported into the management console and based on that, the administrator can tailor policies that can be exported and imported in the isolated endpoint.

Stronger encryption

A big step in improving the product security was made by changing the encryption algorithms for:

- Password derivation – from SHA-256 to Argon-2id and PBKDF2

- Disk encryption – from AES-256-CBC to AES-128-XTS

The administrator will have to decide what happens with devices that were encrypted with older algorithms. Three options are available: for:

- Allow the use of this devices

- Upgrade the encryption and after this process the device can be used.

- Deny the use of device

Show/Hide unused device classes

This update adds the option to show/hide device classes. It brings a better management by providing a cleaner interface. The feature works only on device classes that are not in use.

Extended settings

Groups under **Machine-specific settings** have additional options when using the contextual menu. This brings the possibility to enforce permissions on all the groups.

Improved SIEM integration

To be able to support more SIEM applications with update 5.2, we are providing two new implementations. One brings the option to feed data directly into Windows Event Viewer. The second one brings data in JSON format. The majority of SIEM applications will be able to consume the logs in this way.

Device Control Server-side SDK

This update provides a better integration with 3rd party applications by exposing the SDK methods for the server application. You can enforce permissions on groups of endpoints and override the settings that you would usually do from the management console.

Hide status window

The client status window can now be hidden. The administrator can change this option from the default settings in the management console.

HDD better detection

With this update, you can fine-tune the HDD detection by choosing how this kind of device should be identified. Based on the lack of removable capabilities, reported by the operating system, or by also taking into consideration the buses. The option can be enabled/disabled from the default settings

Security improvements

We have made several security improvements in this release.

Customer Issues Fixed in 5.2

The following customer issues have been resolved in this release:

Problem ID	Title
649020	During DVD encryption the 'Time Stamp' on certain file types change.
643195	Traced On (Console time) or Transferred On (Console time) does not work properly in Log Explorer
669367	A bug in the Schedule tab of log template
667115	Two output files generated for one scheduled template in Log Explorer
640403	Scheduled Log Explorer report and Database Maintenance do not work due to UTC time
685967	Removed shadowing option from modem class
685962	Remove Wireless NICs class from user limited bucket
624491	Improve TLS cert selection, check both server and client in enhanced usages
629621	sxs.exe was crashing in some situations
657324	Updated description for "Portable Encryption Capacity"
660706	Chrome Printing not working on Windows 8.1
665303	Relative time profiles generate wrong time interval when query time is below the UTC offset
675923	Fixed scheduler for 'Wireless NIC's' class.
682545	Added index on TransferredDate
693295	Export settings not saving '.dat' extension for custom names
697368	Keylogger detected after upgrade to 5.1.5
697416	AMD Ryzen reboot issue