Security Controls 2023.3

Release Notes

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2023.3. The GA version can be downloaded from this link:

https://forums.ivanti.com/s/article/Ivanti-Security-Controls-Download

The GA build is 9.5.9402.0.

You can upgrade to Security Controls 2023.3 from Security Controls 2019.3 or later. See the Upgrade Guide for complete details.

IMPORTANT! Ivanti recommends you create a backup of your current database before performing any upgrades. If you are using a full edition of SQL Server, you should use the SQL Server Maintenance Plan Wizard to perform the backup. SQL Server Express users who do not have access to the SQL Server Maintenance Plan Wizard can use the Ivanti Security Controls Database Maintenance tool.

Documentation

The complete library of Ivanti Security Controls 2023.3 documentation is available here:

www.ivanti.com/en-US/support/product-documentation

Installation Notes

System Requirements

The following operating systems are no longer supported for use by the Security Controls console:

- Windows 7
- Windows 8.1
- Windows Server 2008 family R2 SP1

The following operating systems are no longer supported for use by Windows clients:

- Windows 7
- Windows 8.1
- Windows Server 2008

Microsoft SQL Server 2008 and 2008 R2 are no longer supported. You must be using Microsoft SQL Server 2012 or later.

A new version of the Microsoft Visual C++ Redistributable for Visual Studio 2015 – 2019 is available, so this will likely be identified as missing during the prerequisite check of the installation process.

For a complete list of requirements for the console, your agentless clients and your agent-based clients, see System Requirements in the Help.

New Installation vs Upgrade

If you are an existing customer using Security Controls 2019.3 or later, you should upgrade to Security Controls 2023.3. This will enable you to maintain your current product database and configuration data.

If you are a new Ivanti customer or an Ivanti Application Control customer who is migrating to the Application Control feature in Security Controls, you will be performing a new installation.

Although the upgrade and new installation processes are similar, there are differences. For example, if you upgrade you will not be presented with the opportunity to create a new database or choose how users and services will connect to the database.

Disconnected Networks

If you are installing on a disconnected console machine, in addition to manually installing any prerequisite software, you must also manually download and install the product core files BEFORE you begin the installation process. For complete information on this process, see the Performing a New Installation topic in the Security Controls Help.

For information on how to manually manage your data files in a disconnected environment, refer to the following Ivanti Community post:

https://forums.ivanti.com/s/article/How-To-Download-Content-Data-Files-and-Patches-using-the-Download-PowerShell-Script

Changes in Security Controls 2023.3

This release contains the following changes:

- The Security Controls REST API has been extended to provide more control of machines.
- During the automatic cleanup of the download directory, core files are not deleted if the download directory is set to be used as a distribution server.
- Accessibility improvements.

Known Issues

None.

Deprecated Features

Feature That Was Removed from 2023.2

The Ivanti Scheduler has been removed. The Microsoft Scheduler has been improved to the point that the Ivanti Scheduler was no longer needed.

Feature That Was Removed from 2022.2

Support for Red Hat Enterprise Linux 6 has ended. This is because Red Hat has stopped providing maintenance support for Red Hat Enterprise Linux 6.

Features That Were Removed from 2021.2 Update 1

The following operating systems are no longer supported:

- The Security Controls agent is no longer supported on Windows 8 and CentOS 6 operating systems
- Agentless operations are no longer supported on Windows XP, Windows Server 2003, Windows Vista and Windows 8 operating systems.

Features That Were Removed from 2020.1

- The Security Controls console can no longer be installed on the following operating systems:
  - Windows 7 SP1
  - Windows Server 2008 family R2 SP1

  Security Controls will continue to patch these endpoints through the Custom Patch Support program.
- The ITScripts TrustedHosts list credential has been eliminated because it is not required. Machines can still be added to the list when a remote PowerShell prompt is launched from Machine View.

Features That Will Be Removed in Future Releases

- The database views are now organized using the Reporting2 namespace. The original Reporting namespace will be removed in a future release and should only be used by legacy queries. All new queries should be created using the Report2.* views. For more information about report views, see the Generating Custom Reports section in the ISeC Help.
- In the REST API, support for **servicecredentials** requests and the **sharewithservice** parameter will end in a future release. Those capabilities are contained in the new shared credentials functionality.
- In the REST API, support for the **/metadata/vendor Family.products** parameter will end in a future release. That capability is being replaced by the **Family.productVersions** parameter.

Resolved Issues

The following customer support issues have been resolved in this release:

Problem ID	Title
93744	Corrected a credentials-based license activation failure when the local license state was invalid. The application can now recover and reactivate under this condition.
93992	Fixed an issue where removed user accounts or duplicated credential sharing could result in an application crash when navigating to **Manage -> Users**.
94227	Fixed a regression where devices identified by only a IPV6 address could not be scanned from the Machine Group View.
94115	Corrected an issue prevention connection by fully qualified DNS name when scanning online Hosted virtual machines.
93832	Corrected an issue where the Product-level update deployment option grayed out when "Show informational items in patch scan results" is disabled.
94390	Fixed an issue in the MachineGroup REST API where an empty Next pagination link was generated when query filter parameters are supplied.
94396	Fixed Agent patch definitions download to initiate a recovery download when an invalid WindowsPatchData.zip achieve is encountered in the on the agent. Note that this does not directly resolve the issue, but mitigates it.