Security Controls 2023.2

Release Notes

About this Release

Installation Notes

Changes in Security Controls 2023.2

Known Issues

Deprecated Features

Resolved Issues

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2023.2.
The GA version can be downloaded from this link:

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

The GA build is 9.5.9387.0.

You can upgrade to Security Controls 2023.2 from Security Controls 2023.1, 2022.4, 2022.3, 2022.2, 2022.1, 2021.4, 2021.2.1 or 2019.3. 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 2023.2 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 Security Controls 2023.1, 2022.4, 2022.3, 2022.2, 2022.1, 2021.4, 2021.2.1 or 2019.3 customer, you should upgrade to Security Controls 2023.2. 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 2023.2

This release contains the following changes:

- The Ivanti Scheduler has been removed. The Microsoft Scheduler has been improved to the point that the Ivanti Scheduler was no longer needed. The Microsoft Scheduler is now the default scheduler service and is used when performing power state and patch deployment tasks on remote machines. The scheduler is used to initiate the tasks at the specified time, whether immediately or at some specified time.

  NOTE: With the deprecation of the Ivanti Scheduler, port 5120 is no longer required to be an allowed port in your firewall settings. In addition, when you are certain that all scheduled tasks still using the Ivanti Scheduler have been run, you should remove the Ivanti Scheduler from your target machines.

- A deployment tool is now being pushed to target machines when a patch deployment is performed from the console. The tool is used to execute a deployment package on the target machine. The capabilities of the deployment tool are not new; they used to be included with the Ivanti Scheduler. With the deprecation of the Ivanti Scheduler, however, the deployment tool is now being delivered as a separate component. It will automatically be pushed to target machines when needed. If needed, you can remove the deployment tool from a target machine by right-clicking the machine in Machine View and using the Uninstall deployment tool command.
- For offline virtual machines, patching products installed on virtual disks with the disk mode set to either Independent – Persistent or Independent – Nonpersistent is not supported. If a virtual machine has both dependent and independent disks, you can still install patches for products that are installed on the dependent disks.
- Support for ESXi 6.0 has been dropped and support for ESXi 8.00 and 8.0.1 added. The supported versions of VMware ESXi hypervisors are now ESXi 6.5, ESXi 6.7, ESXi 7.0, ESXi 8.00, and ESXi 8.0.1.
- Removed Microsoft Visual C++ Redistributable for Visual Studio 2013 as a prerequisite software requirement for the console

Known Issues

Deploying patches that use Red Hat Enterprise Linux 8 application streams is not supported. Detection of these patches is fully supported.

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
1026081	Corrected a VMware Workstation 17 compatibility issue. Support for the new NVMe offline disk type was added.
1028795	Corrected an issue where Application Control command line validation rules did not parse registry key arguments with various Regedit options.
1030338	Resolved an issue where a Linux agent would not be installed on a Red Hat 8 machine that contained an additional repository. This is a data droppable fix that corrects all versions back to V2021.4.
1038554	Linux RedHat 8 patch scans now correctly account for directly installed patches, independent of the module install status.
1044053	Corrected an issue where a code signing certificate change required Agent Policy re-generation before new content could be downloaded.
1047051	Corrected outdated prerequisite download links.
2190438	Corrected an issue where VMware Templates failed to scan with Error 800 Unable to retrieve OS info.