

Security Controls 2022.3.1

Release Notes

[About this Release](#)

[Installation Notes](#)

[Changes in Security Controls 2022.3](#)

[Known Issues](#)

[Deprecated Features](#)

[Resolved Issues](#)

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2022.3.1. The GA version can be downloaded from this link:

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

The GA build is 9.5.9338.0.

You can upgrade to Security Controls 2022.3.1 from Security Controls 2022.2, 2022.1, 2021.4, 2021.2, 2021.1, 2020.1 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 2022.3.1 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 SP1
- Windows Server 2008 family R2 SP1

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 2022.2, 2022.1, 2021.4, 2021.2, 2021.1, 2020.1 or 2019.3 customer, you should perform an [upgrade](#) to Security Controls 2022.3.1. 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 perform an 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 2022.3

This release contains the following changes:

- The ability to automatically clean up your patch download directory and your distribution server(s). Any patches that are unlikely to be used in the future will be deleted from these locations, saving disk space. This option is configured on the **Tools > Options > Downloads** tab. See the [Security Controls Help](#) for more information.
- The number of thread pools used when scanning machine groups that contain machines defined by an IP range, a domain or an organizational unit is now automatically capped. This will improve performance by limiting the number of machine groups that can be scanned at one time, keeping the console machine's processors from becoming overloaded. For more details, see the [Security Controls Help](#) for information on the **Global thread pool** option.
- Localized versions of the [agent user interface](#) are now available.
- You now have the option to [specify if the agent user interface will be installed](#). The agent client currently requires the use of .NET 6, and it will likely continue to be updated in the future to use newer versions of .NET as they become available. One of the reasons you may not want the [agent client](#) installed is if you have other applications on your machines that also require the use of .NET. If the agent client is not needed, you can shield those machines from the reboots and other effects that occur when an agent is updated to support a new version of .NET.
- Two new Linux patch attributes are now stored in the database and are available for reporting purposes: **InstalledOn** date and **Notification > Title**.
- In addition to checking for application updates and End-of-Life notices on launch, the Security Controls console will now check for updates and notices every 24 hours while the Security Controls console remains open. The administrator can snooze the notifications for up to seven days at a time.
- The [Security Controls Cloud](#) website has been refreshed. It now has an updated style that is consistent with other Ivanti sites, and modern client libraries are used to help ensure the most secure browsing experience.
- A number of [customer issues have been resolved](#).

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 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

- A new set of database views has been created and is organized using the Reporting2 namespace. The Reporting2 namespace now includes a view for CVSS scores. 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

2022.3

Problem ID	Title
902207	Resolved an issue where Microsoft .NET 5 and .NET 6 runtime components were not properly detected during installation of Security Controls.
936634	Resolved an issue where the STAgentUpdater.exe process would hang on an agent client.
937872	Resolved an issue where a custom patch would fail on agents due to an unnecessary custom patch license check.
944775	Resolved an issue where upgrading to Microsoft .NET 6.0.6 would cause the agent user interface to fail to respond.
945718	Resolved an issue where the patch file name that was returned as part of a REST API call was incorrect.
948323	Resolved an issue where the console would crash when searching for a user in the Users Manager dialog.
951567	Resolved an issue where the Application Control engine could not process a license count change when the entitlement was set to perpetual.

2022.3.1

Problem ID	Title
881609	Resolved an issue where a Linux patch shows as missing and needed, but the package was not installed on the machine.
962429	Resolved an issue where the patch clean up feature failed to detect missing patches.
962676	Resolved an issue where there was only limited logging for the patch clean up feature.
962678	Resolved an issue where credentials were not used or honoured by the patch clean up feature.