

Security Controls 2024.3.1

Release Notes

About this Release	1
Installation Notes	2
Changes in Security Controls 2024.3.....	3
Known Issues	3
Removed Features	3
Resolved Issues	4

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2024.3.1. The GA version can be downloaded from this link:

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

The GA build is 9.6.9362.0.

You can upgrade to Security Controls 2024.3.1 from Security Controls 2022.2 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.

IMPORTANT! If you use distribution servers, you **MUST** update the Linux engine installer on all distribution servers before creating or updating policies to include Linux patch groups. If this is not done, and a new policy is used with an old engine, scans will not work and the old engine will interpret this policy to deploy all patches and not just the patches that were approved in the patch group.

IMPORTANT! If you use Linux contentless patching with Security Controls 2024.1, some new deployment history items could be lost, but you will see the current status of the advisory on an endpoint. Upgrading to 2024.2 or later will fix this issue.

Documentation

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

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

The Ivanti Security Controls Diagnostic Toolkit, which provides utilities to help diagnose your system and provide information to support is available from <https://forums.ivanti.com/s/article/Security-Controls-Diagnostic-Toolkit-Release-Notes>.

Installation Notes

System Requirements

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

- Windows Server 2012 family
- Windows Server 2012 R2 family

The following operating systems are no longer supported as Windows endpoints:

- Windows Server 2008
- Windows Server 2008 R2

Microsoft SQL Server 2012 is no longer supported. You must be using Microsoft SQL Server 2014 or later.

A new version of the Microsoft Visual C++ Redistributable for Visual Studio 2015 – 2022 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 2022.2 or later, you should [upgrade](#) to Security Controls 2024.3.1 (or 2022.2 if you require a Common Criteria certified version). 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 2024.3

This release contains the following changes:

- Individual packages can now be added to a contentless Linux patch group
- CVSS scores are now displayed for contentless Linux patches.
- A new set of database views has been added to the database to enable you to generate custom reports for contentless Linux patching.
- CentOS 7 and RHEL v7 have reached end of support with their vendors. As a result, Ivanti have deprecated support for CentOS 7 and RHEL v7 and will be removing support in a future update.
- The POST and DELETE methods sharewithservice have been removed from the Credentials function of the REST API.

Known Issues

False-positive missing advisories may be reported prior to patch deployment on some Linux distributions derived from the Red Hat Kernel

When using the original dnf package manager provided with Linux distributions derived from Red Hat Kernel versions 8.1 - 8.4, the dnf pre-deployment scan may generate false-positive advisories that do not appear in the post-deployment scan results. This was corrected by Red Hat in the package manager provided with version 8.5, and can also be corrected using the command **sudo dnf update dnf**.

Removed Features

Feature That Was Removed from 2024.3

The POST and DELETE methods sharewithservice have been removed from the Credentials function of the REST API.

Feature That Was Removed from 2023.4

The Security Controls console is no longer supported on the following operating systems:

- Windows Server 2012 family
- Windows Server 2012 R2 family

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 Will Be Removed in Future Releases

- VMware has ended support and technical guidance for versions 6.5, 6.7 and 6.7.1, and security updates are no longer published. Support for these versions will be removed in a future release, leaving the earliest supported version as 7.0.
- 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 will end in a future release. This capability is 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

2024.3.1

The following customer support issue has been resolved in this release:

Problem ID	Title
102248	Fixed an issue where the console crashed when Agentless Scanning initiated after upgrade to 2024.3.

2024.3

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

Problem ID	Title
100376	Fixed an issue where Schedule Power State jobs ignored the Add delay (days) setting.
101538	Fixed an issue that caused a crash in STTelemetryReporter.exe.
102102	Resolved an issue where CVEs without matching patches were not reported in the Unmapped CVE section of the CVE import dialog.