Security Controls 2021.2

Release Notes

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2021.2. The GA version can be downloaded from this link:

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

The GA build is 9.4.34798.0.

You can upgrade to Security Controls 2021.2 from Security Controls 2021.1, 2020.1, 2019.3 or 2019.2. 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 2021.2 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 SP1
- Windows Server 2008 family R2 SP1

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.

Customers upgrading from Ivanti Security Controls 2019.2 should note the following new console requirement:

- Microsoft .NET Framework 4.8 or later (was 4.7.2)

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 2021.2, 2020.1, 2019.3 or 2019.2 customer, you should perform an upgrade to Security Controls 2021.2. 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 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 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

New Features Introduced in Security Controls 2021.2

Major New Features

Sideload Patches

Sideloading refers to the process of managing patches that cannot be automatically downloaded. The sideload feature greatly simplifies this process. You will need to manually download the patch file, but after that the sideload feature takes over and provides a number of automated services. Specifically, the feature will verify the contents of the manually downloaded patch, rename the file if needed and then automatically save the patch file to the patch download directory. Once there, the patch is ready to be deployed using the normal deployment process.

Automatically Delete Inactive Machines from the Database

The ability to automatically delete inactive machines from the database has been added to the Database Maintenance tool. An inactive machine can be a machine that has not had an agent check in with the console, been assessed or been included in a patch deployment for the specified number of days. This is important, because inactive machines do not accurately depict the current state of your organization.

Continuous Agentless Scanning

You now have the option to configure agentless patch scanning operations on intervals as short as three minutes. This provides the ability to perform nearly continuous scans of a designated machine group.

Scripted Scans and Deployments Using CVEs

A detailed series of PowerShell scripts is provided that show how to scan for and deploy patches using input from a CVE file. The scripts invoke the REST API and perform a number of tasks, including:

- Parsing a CVE file and converting the content to a patch group
- Creating a scan template that scans for the patches contained in the patch group
- Optionally deploying any missing patches

Workstation and Server License Information

Additional details about your current license status are now available in two different locations. You can:

- Select **Help > About Ivanti Security Controls** on the console to view the number of deployment license seats currently used for both your servers and your workstations.
- Generate a **Detailed License Status** report that shows the number of available licensed seats, the number of seats used, how and when the seats were consumed and when they will be available again.

Minor New Features and Enhancements

- Added a new Configuration method in the REST API that enables you to display version information for the Security Controls console.
- In the Patch Deployments method in the REST API help, a **DeploymentResult** table has been added containing the codes that identify the various states of a deployment.
- In the Machines method in the REST API help:
    - Added the **credentialId** field to the output model
    - Added new PUT operations for assigning and unassigning a credential to a machine
- Added Port 902 information to the **Port Requirements** table in the System Requirements

Deprecated Features

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.
- Support for CentOS 6 Linux clients will end in a future release. This is because Red Hat has stopped providing maintenance support for CentOS 6.
- Support for SQL Server 2008 and SQL Server 2008 R2 will end in a future release.
- 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
781715	Resolved an issue where a full cloud synchronization fails with an internal server due to large patch groups.
783388	Resolved an issue where Security Controls Cloud synchronization would stop and would not restart if a cloud synchronization is due while SQL is turned off.
784257	Resolved an issue where the action button on the Database Setup Tool are not visible due to the screen resolution when using a web browser to access a virtual machine.
784439	Resolved an issue where the telemetry registry switches were not disabling event logging in the operational event log.
784901	Resolved an issue where a crash would occur when attempting to access credentials following an upgrade to Ivanti Security Controls 2021.1.
792913	Resolved an issue within Application Control Retrieve Events where users thought the agent command was failing based on the message that was displayed when a user attempted to retrieve events without generating new events on the target by updating the status message. Resolved a check-in loop that could be created when issuing a retrieve event command.
792525	Resolved an issue where a high DPI percentage caused the scroll bars to be missing when creating a patch task within an agent policy.
795122	Resolved an issue that prevented the save action when adding a vCenter server due to an FK constraint violation.
797234	Resolved an issue where a PowerShell API command to run a scan and deployment sent two deployment notification email reports.
797631	Resolved an issue where the “Reboot may be required / installation failed” deployment status copy was not displayed consistently in the Deployments reports.
798072	Resolved an issue where requests to the REST API for a specific hostname returned the matched host, but the next href did not include the parameters passed in for the subsequent request.
799012	Resolved an issue where the counter limit for the database table Protect.[dbo].[AssetValue] was reached due to an issue with asset scan
799084	Resolve an issue where a customer received bad files that were generated by a machine reporting a bad file path for Microsoft Edge.
801941	Resolved an issue with a Windows patch scan where the listening agent connections changed from FQDN to Hostname after a patch scan task runs.

Problem ID	Title
803976	Resolved a Linux agent installation issue that was causing a console crash when the resolver script timed out.
807506	Resolved an issue where superseded patches were reported missing when included in a Linux patch group.