# Security Controls 2019.3

## Release Notes



## About this Release

### Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2019.3.

The GA build is 9.4.34582.0.

You can upgrade to Security Controls 2019.3 from Security Controls 2019.2, 2019.1.1, 2019.1, 2018.3 (non-AC users only) or Patch for Windows 9.3 Update 1. If you are currently using the Preview version of Application Control that was available in Security Controls 2018.3, you must perform a fresh installation. 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 2019.3 documentation is available here:

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

# Installation Notes

## System Requirements

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

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

Customers upgrading from Ivanti Patch for Windows 9.3 Update 1 should note the following new console requirements:

- Memory: 16GB of RAM is now recommended for high performance systems
- Disk space: 100GB is now recommended for the patch repository
- Microsoft .NET Framework 4.8 or later (was 4.6.2 or later)
- Microsoft Visual C++ Redistributable for Visual Studio 2013 (required for scanning offline VMs)
- Microsoft Visual C++ Redistributable for Visual Studio 2015-2019

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 2019.2, 2019.1.1, 2019.1, 2018.3 (non-AC) or Patch for Windows 9.3 Update 1 customer, you should perform an upgrade to Security Controls 2019.3. 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. If you are currently using the Application Control feature in Security Controls 2018.3, you must uninstall the program and all agents and then perform a fresh installation. See the Installation section in the Help.

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

# Major New Features

## Linux Listening Agents

Support is now provided for Linux listening agents. This means that the agents on Linux machines are now able to listen to the console for policy updates and commands.

## Additional REST API Functionality

The following functional areas are now available through the REST API:

- Agents
- Agent Deployments
- Agent Tasks
- Linux Patch Deployment Configurations
- Linux Patch Group
- Linux Patch Metadata
- Linux Patch Scan Configurations
- Policies
- Product Level Group

For complete information on using each of these new functional areas, see the REST API Help.

## Application Control Configuration Versioning

You can now create different versions of a configuration. Each time a modification is made a new version is created which enables the review and auditing of changes. It also means that previous versions of your configuration remain available which you can rollback to if required.

Specific versions of a configuration can be assigned to an Agent Policy.

Deletion of specific versions is now also possible.

For further details, see Manage AC Configurations.

## Application Control Configuration Comparison Tool

The configuration comparison tool has been introduced so you can easily compare two different configurations or two different versions of the same configuration. Change tracking can quickly be identified and located.

For further details, see Configuration Comparison Tool.

# Minor Features and Enhancements

## Improved Graphics

The icons and images in the main console have been updated to use a scalable vector graphics (SVG) format. This means the console has proper high DPI support and will scale correctly on machines that have font settings greater than 100%.

## Intelligent Linux Agent Installations

When installing an agent on a Linux machine, checks will be made to see if the Linux machine is properly configured to support all agent functionality. If something is amiss (for example, if the machine's Red Hat subscription is not current), the installation will fail and a message will be displayed informing you of the situation.

## Application Control Message Settings Enhancements

The message box enhancements include:

- Option to include a company logo as a graphic in the message box.
- Easily resize the message box in the preview, all values of the resize are retained when the preview is closed.
- Option to include a colored text banner in the message.
- More descriptive default text in the message body.

For further details, see Configuration Message Settings.

## Rule Collections

There is now only one type of Rule Collection, in previous versions this was split between Executable Control Rule Collections and Privilege Management Rule Collections. For further details, see Rule Collections.

# 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 SQL Server 2008 and SQL Server 2008 R2 will end in a future release.

# Resolved Issues

The following customer support issues have been resolved in 2019.3.

## Early Availability Release (November 2019)

| Problem ID | Title |
|---|---|
| 579384 | Resolved an issue where the “Add delay (days)” option did not work in an agent policy. |
| 593320 | Resolved an issue where the “Add delay (days)” option did not trigger in a console scheduled task. |
| 598140 | Resolved an issue where a patch scan initiated via the REST API did not work due to a credential problem. |
| 603838 | Resolved an issue where the console would fail when running an ITScripts template from the Tools > Run Console ITScripts menu command. |
| 604546 | Resolved an issue where a patch scan would fail when running against an ESXi host configured to use a proxy. |
| 606052 | Resolved an issue where upgrading from ISeC 2019.1.1 to ISeC 2019.2 would fail on non-English-based operating systems. |
| 606791 | Resolved an issue where the Application Control engine would fail due to an incorrect file type. |
| 607723 | Resolved an issue where the console would fail when accessing Protect Cloud due to improperly handling an unsupported media type. |
| 608287 | Resolved an issue where a SQL database error would occur during an upgrade from Patch for Windows 9.3 to ISeC 2019.2. |
| 608533 | Resolved an issue where trace logging around hypervisor download and proxy configuration was lacking. |
| 612113 | Resolved an issue where performing a REST API GET request on a machine group failed due to an issue with the runAsCredential parameter. |
| 620112 | Resolved an issue where the location of the Next link in the Patches function of the REST API was inconsistent with other functions. |
| 624963 | Resolved an issue where patch scans would incorrectly time out due to an issue with the Connection timeout parameter. |
| 625374 | Resolved an issue where enabling User Role Assignments incorrectly prevented the user from generating a report. |
| 625404 | Resolved an issue where the console failed when attempting to deploy service packs that did not have a valid download source. |
| 625656 | Resolved an issue where Predictive Patch automatic downloads got stuck in an In Progress state and failed to finish. |

| Problem ID | Title |
|---|---|
| 625801 | Resolved an issue where the Help did not properly disclose that an active user session was required in order to use the “If a user is logged on” options. |
| 626092 | Resolved an issue where the console displayed an incorrect product level ISO name. |
| 628412 | Resolved an issue where the REST API was missing support for RSA/AES session key encryption when using a session credential. |
| 629349 | Resolved an issue where, due to a proxy credential error, one of the users at a site could not access the console following an upgrade from Patch for Windows 9.3 to ISeC. |
| 629387 | Resolved an issue where a SmartFilter configuration was not preserved when upgrading from Patch for Windows 9.3 to ISeC. |
| 629562 | Resolved an issue where attempting to generate an Executive Summary report for all operating system platforms failed due to a SQL Server 2008 R2 backward compatibility problem. |
| 630807 | Resolved an issue where the data versions displayed on the home page were not properly updated. |

## General Availability Release (December 2019)

| Problem ID | Title |
|---|---|
| 631119 | Resolved an issue where Linux deployment history was not being updated after a deployment task was run on a Linux 7.x machine. |
| 631508 | Resolved an issue where database maintenance operations would fail due to excessive amounts of asset scan data. |
| 636710 | Resolved an issue where performing an agentless scan on a machine group that contains a nested group would report that no machines were found. |
| 637008 | Resolved an issue where a SQL deadlock would occur when deleting machines at the same time that results were being imported. |
| 637031 | Resolved an issue where a user with an assigned role that did not include Application Control was presented with an AC trial offer even though the console was already licensed for AC. |
| 640167 | Resolved an issue where agents were not able to be deployed to non-English Linux machines. |

## General Availability Refresh (January 2020)

| Problem ID | Title |
|---|---|
| 647088 | Resolved an issue where filtering the Machine OS Listing report failed when filtering by machine group. |
| 647117 | Resolved an issue where upgrading from 2019.3 EA (Build 9.4.34511) to 2019.3 GA (Build 9.4.34534) failed on non-English operating systems. |

## General Availability Refresh 2 (April 2020)

| Problem ID | Title |
|---|---|
| 654674 | Resolved an issue where access errors were not being properly handled when enumerating child OUs or security groups, both in the OU browser and while scanning. |
| 664613 | Resolved an issue where scheduled report filtering by machine group resulted in no filter being applied. |
| 666443 | Resolved an issue where large numbers of tasks prevented the Scheduled Console Tasks Manager from loading. |

## General Availability Refresh 3 (June 2020)

| Problem ID | Title |
|---|---|
| 609697 | Resolved an issue where kernel patches would continue to be reported as missing when the system was up to date. |
| 683655 | Resolved an issue where a VMware VDDK driver bug caused access failures to virtual machine template disks. |