Security Controls 2020.1

Release Notes

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2020.1.
The GA version can be downloaded from this link:

https://application.ivanti.com/isec/v9.4/installers/IvantiSecurityControls_2020.1.2.exe

The GA build is 9.4.34717.0.

You can upgrade to Security Controls 2020.1 from Security Controls 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 2020.1 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

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

Shared Credentials

You can now share credentials with one or more users. This is especially useful in multi-admin environments, as it enables a senior administrator to delegate operations to junior administrators. The junior administrators can interact with endpoints using a secure credential without knowing the password for that credential. In addition, when a password needs updating, it can be updated from a single location.

For more details, see Shared Credentials in the Security Controls help.

Grouping of Machines in Machine View and Scan View

The new **Assigned Groups** column in Machine View and Scan View enables you to group related machines, making it easier to perform agentless operations and generate reports on the machines. This column is particularly useful for machines such as Cloud agents, as those machines do not belong to a machine group. With the Assigned Group feature, you can now group those machines with other machines that share similar attributes, such as the same physical location or agent policy.

For more details, see the Assigned Group column description in the Security Controls help.

Improved Product Licensing Process

A new credentials-based activation method is now available that enables you to specify exactly how many of your available license seats you want to consume on a specific entitlement. This method will be used by new customers who have an internet connection from the console. The legacy key-based activation method is still supported for existing customers who are upgrading and for customers who need to activate from within a disconnected network.

For more details, see Activating Security Controls in the Security Controls help.

Additional REST API Functionality

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

- Cloud Sync
- Machines
- Users

The ability to share credentials and assign a machine to a group has also been added. For complete information, see the REST API help.

Minor Features and Enhancements

Deep Rebrand

References to outdated company and product names have been scrubbed. Directory paths and other items that contain company and/or product names are now current.

Software Distribution Notification

A notification dialog is now provided whenever you add a software distribution patch to a patch group or initiate a scan for third-party applications. This warning will help prevent the inadvertent installation of third-party applications on your endpoints.

Improved List of Port Requirements

The **Port Requirements** table in the System Requirements help topic now contains much greater detail.

Patch Breakdown Column Renamed to Health

Within Machine View and Scan View, the **Patch breakdown** column has been renamed to **Health**. The new name better reflects the purpose of the column, which is to indicate the "health" of a machine by providing a visual representation of the percentage of installed patches vs missing patches.

Carry Original Scan name into the Associated Deployment Name

When a patch scan is followed by an automatic patch deployment, the scan name is now associated with the corresponding deployment operation.

Deprecated Features

Features That Have Been 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 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.

Resolved Issues

The following customer support issues have been resolved in 2020.1.

General Availability Release (September 2020, Build 9.4.34633.0)

Problem ID	Title
633023	Resolved an issue where hosted VMs were being removed from machine groups.
635139	Resolved an issue where it was unclear that scheduling a recurring agent patch task would occur based on the time of the target machine, not the local time of the console.
640217	Resolved an issue where setting the scan connection timeout value to 0 prevented patch scans from finding machines; 1 second is the new minimum.
641413	Resolved an issue where an error message would be displayed at the conclusion of a distribution server sync if a patch file contained a name with more than 100 characters.
641969	Resolved an issue where the Last agent check-in time in Machine View would incorrectly be red at the start of a new month.
642032	Resolved an issue where changes to an ITScripts template were not being saved.
642731	Resolved an issue where recipients were not being added to the “To:” field of a scheduled report.
647088	Resolved an issue where scheduling a Machines/OS Listing report filtered by machine group would result in no report being generated.
649743	Resolved an issue where the OS column in Machine View would incorrectly be red if a Windows 7 machine with an agent was upgraded to Windows 10.
654172	Resolved an issue where updating a credential via the REST API did not update the corresponding service credential.
654684	Resolved an issue where the console would crash when selecting a hypervisor bulletin due to a null value.
654926	Resolved an issue where a failure would occur when unregistering a Security Controls Cloud console.
658593	Resolved an issue where agents without an installed patch engine or content triggered a failure when processing status updates from Security Controls Cloud.
663209	Resolved an issue where the installation of the .NET and SQL Server prerequisite software would fail when the OS culture and region settings did not match.
663825	Resolved an issue where information landing page content was being automatically downloaded and substituted for an ISO when a patch was set to be acquired from the vendor.
668703	Resolved an issue when selecting the All Languages option in the Custom Patch Editor.
670862	Resolved an issue where the console would crash when connecting to a vCenter Server with custom or atypical certificates.

Problem ID	Title
685130	Resolved an issue where the note field was not being honoured when adding a machine to a machine group via the REST API.
690909	Resolved an issue where the console would crash if the LinuxScripts.zip file was missing when a file refresh was performed.
692539	Resolved an issue where an asset scan failed to return results due to non-printable characters in the input.
694878	Resolved an issue where an agent would continue to scan for a custom patch that had been removed from the console.
697975	Resolved an issue where the Safe Reboot pre-deployment message was slightly misleading because it was not providing context for the reboot.
698028	Resolved an issue where the installation of a Linux agent would fail due to a timeout error. The timeout value is now customizable via a registry key.
698679	Resolved an issue where an agent would not be updated during a check-in if there was an error with an engine installation.
699167	Resolved an issue where a synchronization attempt with Security Controls Cloud would fail due to an expired access token.
706030	Resolved an issue where a patch content error caused problems with the database. The issue was resolved by providing a database upgrade script.
707112	Resolved an issue where the console would not register with Security Controls Cloud due to a credential error.
719519	Resolved an issue where the console service would not start due to bad hypervisor scan results.
720317	Resolved an issue where a missing GO statement was causing unnecessary overhead when granting permission on a stored procedure in SQL Server.
727813	Resolved an issue where an offline scan of a virtual machine would fail due to a missing drive letter.
732034	Resolved an issue where patching Linux systems to zero (all patches deployed, including Kernel patches), the console would crash when viewing results in Machine View due to duplicate patch deployment entries.
732572	Resolved an issue where credentials that had been shared with background services would prevent an upgrade from 2019.3 to 2020.1 when the credentials were applied to a machine or a machine group.
732740	Resolved an issue where shared remote scheduler components were incompatible with previous releases (2019.2 and 2019.3) during patch deployment.

General Availability Refresh 1 (November 2020, Build 9.4.34705.0)

Problem ID	Title
731017	Resolved an issue where credentials assigned to a console fail testing when they are correct.
731897	Resolved an issue where attempting to deploy a detect-only patch (with no other patches in the deployment) didn't disable the deploy button or give an error message.
732291	Updated the software distribution warning to provide a clearer message.
733575	Resolved an issue where a report was sent in an email message as a .tmp file instead of a .pdf.
736209	Resolved an issue where setting deployment default credentials always indicated an invalid credential in the UI.
737568	Resolved an issue where a database exception was preventing the addition of Linux patches to an existing patch group.
740665	Resolved an issue where the PowerShell Get-PatchGroup did not display PatchGroupIDs.
740832	Resolved an issue where a console crash would occur when attempting to deploy product levels.
742607	Resolved an issue where the specific accounts could not open the console after upgrading to 2020.1 9.4.34633 (the GA release).
742688	Resolved an issue where the manifest download would start when the auto-update of definitions was disabled.
742745	Resolved an issue where the asset scan results failed to import.
742747	Resolved an issue where the console would crash when attempting to share a credential.
743024	Resolved an issue where the Dark/Black console skins did not render correctly after closing and reopening the console.
743470	Resolved an issue where selecting a report in the Tools > Create Report menu caused a crash after upgrading to 2020.1 9.4.34633 (the GA release).
744082	Resolved an issue where a scan could start, but shared access could be removed due to a timing issue.
751339	Resolved an issue where a foreign key constraint error occurred when trying to create a patch group.
754609	Resolved an issue where the file containing the patch KBs to scan for defaulted to C:\Program Files\Ivanti\Security Controls in the **Import from file** menu in a Windows patch group.
755701	Resolved an issue where the Windows Server Smart Filter in Machine View failed to display results.
756449	Resolved an issue where a credential error message was incorrectly displayed when initiating a patch deployment to multiple machines from Machine View or Scan View.
756464	Resolved an issue where a product-level deployment from Machine View or Scan View displayed an error message regarding non-deployable patches.

Problem ID	Title
757198	Resolved an issue where an error was generated during a REST API patch scan when two endpoints had the same credential and "usemachinecredential" was true.
757222	Resolved an issue where attempting to deploy a service pack to multiple machines presented the user with the wrong list of service pack options.
757273	Resolved an issue where the console would crash when attempting to deploy All Missing Patches for multiple machines.

General Availability Refresh 2 (December 2020, Build 9.4.34717.0)

Problem ID	Title
766353	Resolved an issue where Machine View took substantially longer to load when compared to previous versions if a large-scale deployment was performed.
766157	Resolved an issue where agentless operations were prevented from working when the workgroup contained only digits.