Security Controls 2021.1

Release Notes

About this Release

Build Information

These release notes support the General Availability (GA) version of Ivanti Security Controls 2021.1.
The GA version can be downloaded from these links:

- Existing customers: https://forums.ivanti.com/s/article/Ivanti-Security-Controls-Download
- New customers: https://preview.ivanti.com/ty/security/trial/security-controls

The GA build is 9.4.34771.0.

You can upgrade to Security Controls 2021.1 from Security Controls 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 2021.1 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 2020.1, 2019.3 or 2019.2 customer, you should perform an upgrade to Security Controls 2021.1. 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

Support for Red Hat Enterprise Linux 8

All vendor-supported Server, Workstation, Client and Computer Node variants of RHEL 8 (64-bit-only) are now able to be scanned and patched using agents.

Note: Support for RHEL 8 is made possible through an update to the dynamic data content that is provided by Ivanti. This means that the two previous versions of Security Controls, 2019.3 and 2020.1, are now also able to support RHEL 8.

Connect to Machines by Fully Qualified Domain Name (FQDN)

Prior to this release, Security Controls made connections with clients using the IP address of the machines. Some networks, however, have begun to operate in stricter environments that employ the use of additional Kerberos security measures. In particular, if the client machines in your environment establish a connection with servers using the Server Message Block (SMB) protocol, a certain level of validation may be required to be performed on the client's Service Principal Name (SPN). For these networks, you now have the option to choose **Fully Qualified Domain Name (FQDN)** as your connection method. Doing so will satisfy the additional validation requirements and enable successful connections to your client machines.

Copy Usages Button

For a shared credential, this new button enables you to add any credential usage that is not already being used by your user account. You might do this if the credential owner, or another user who is sharing the credential, has added one or more new usages since the credential was initially shared with you and you want to keep in sync with those changes..

REST API Enhancements

Several new capabilities have been added to the following functional areas in the REST API:

- **Patch Metadata:** Support has been added for IAVA IDs, and you can now sort and paginate the results of queries. This is implemented with the introduction of three new query URL parameters: **iavaIds**, **orderBy** and **sortOrder**. In addition, nine new output fields are now available: **affectedProducts**, **bulletinTitle**, **familyId**, **familyName**, **fileSize**, **iava**, **summary**, **vendorId** and **vendorName**.
- **Machine Groups:** The **connectionMethod** property has been added to the input and output models. This is being done in conjunction with the *Connect to Machines by Fully Qualified Domain Name (FQDN)* feature (see above).
- **Patch Scans:** You are now able to specify the connection method in conjunction with the endpoint names specified for scanning. This is being done in conjunction with the *Connect to Machines by Fully Qualified Domain Name (FQDN)* feature (see above).

- **Agent Deployments:** The connectionMethod property has been added to the input model. This is being done in conjunction with the *Connect to Machines by Fully Qualified Domain Name (FQDN)* feature (see above).
- **Patch Deployments:** You now have the ability to deploy specific patches to specific machines using a designated deployment template. This provides an integrated patching solution for Ivanti Neurons customers, and it is useful for existing on-premise customers who wish to tailor their patch deployment. The following input parameters are now available: **deployWhat**, **machines**, and **runAsDefault**.

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 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.
- Support for CentOS 6 Linux clients will end in a future release. This will be done because Red Hat has stopped providing maintenance support for CentOS 6.

Resolved Issues

2021.1 Early Availability

Problem ID	Title
749008	Resolved an issue where, if a Security Controls Cloud credential's usage got removed from the credentials manager while the machine was still registered with the Cloud, Security Controls was unable to use and save a new credential in the Security Controls Cloud options.
749264	Resolved an issue where the DownloadDisconnectedData.ps1 script did not honor binary prerequisite refences in the manifest, leaving an incomplete set of downloaded data.
760363	Resolved an issue where test deployments could not be successfully deleted using the database maintenance tool.
760564	Resolved an issue where selecting an ITScripts template in the agentless operation window crashed the application.
766887	Resolved an issue where Security Controls consoles that had agent records for outdated agent versions could not successfully synchronize with the Security Controls Cloud.
768959	Resolved an issue where the agent check in process needed to be optimized in order to allow agents with policies using distribution servers assigned by IP range to successfully check in.
769864	Resolved an issue with the Security Controls Operations Monitor so that agent listening commands could correctly validate when Linux patch data has been updated.
770150	Resolved an issue with notifying users when agents have not succeeded in fully checking in by adding an additional "Policy update failed" state to the Agent State in Machine View.
772022 & 777116	Resolved an issue where it was not clear when the agent policy reboot options would be used.
772464	Resolved an issue where a race condition occurred when creating the user certificates that are used for encrypting credentials.
774450	Resolved an issue where the copy smart filter functionality did not work properly in Patch View, Scan View and Machine View.
779957	Resolved an issue with data returned from a Patch Metadata REST API query; the data was not being sorted consistently if sorting in ascending or descending order.
784901	Resolved an issue where setting credentials after upgrading to the original EA release (9.4.34758) caused the Security Controls console to crash.

2021.1 General Availability

Problem ID	Title
788439	Resolved an issue where telemetry switches did not disable operational event logging.
789345	Resolved an issue where the console would crash after an upgrade due to a duplicate shared service credential.
792917	Resolved an issue where the console would crash if extra null terminator characters were returned by the Win32 API on Windows Server 2016 in certain customer environments.