Security Controls 2019.2

Upgrade Guide

Welcome

Purpose of this Guide

Welcome to Ivanti Security Controls 2019.2. This document describes how to upgrade from Security Controls 2019.1.1, Security Controls 2019.1 or Patch for Windows® 9.3 Update 1. It also applies to Security Controls 2018.3 users who are NOT using the Application Control feature. If you are using the Preview version of Application Control that was available in Security Controls 2018.3, you must uninstall the program and all agents and perform a fresh installation.

In addition to describing the upgrade procedure, this document lists a number of functional differences you should be aware of when upgrading to Security Controls 2019.2. It also highlights the areas in the user interface that have changed significantly.

New System Requirements and Prerequisites

Customers upgrading from Ivanti Security Controls 2019.1.1 or earlier should note the following new console requirement:

- Microsoft Visual C++ Redistributable for Visual Studio 2015-2019

Customers upgrading from 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 4.7.2 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

All missing software prerequisites will be automatically installed during the upgrade process. See the Help for the complete list of system requirements.

User Account Requirements for Performing an Upgrade

In order to perform an upgrade your user account must meet the following requirements:

- The user performing the database upgrade must be a member of the db_owner role.
- If you have multiple consoles that share a database and are linking an additional console to a database that is already upgraded, the user account you use must be a member of the following database roles: db_datareader, db_datawriter, STExec, and STCatalogupdate. In addition, the service account used for background operations must be a member the db_owner role. If your account is a member of the db_securityadmin and db_accessAdmin roles, the database upgrade tool will automatically attempt to map and configure the required roles for you.

Upgrade Procedure

Overview

This section describes how to upgrade from Security Controls 2019.1.1, 2019.1, 2018.3 (non-AC users only) or Patch for Windows® 9.3 to Security Controls 2019.2. If you are taking this opportunity to move the console to a new machine and you want to perform the migration using the Migration Tool, see the *Migration Tool User's Guide* before performing the upgrade.

Before performing the upgrade, be sure to read the *New Features* sections at the end of this document so you are aware of how the upgrade will affect your system. You also may want to make a note of all your current custom user settings as some are not preserved during the upgrade.

Note: Be aware that after the upgrade of the console is complete, any agents that are installed on your target machines will be automatically upgraded the next time they check in with the console.

Performing the Upgrade

1. Free up unused space in the database that is used to store scan results and patch deployment results.

   You can do this in SQL Server Management Studio by right-clicking the Protect database and selecting **Tasks > Shrink > Database**.

2. Create a backup of your current database using SQL Server Management Studio.

   The database contains results from program operations and it also contains configuration information. Backing up your database is an important step.

3. Close all programs running on the console machine, including Patch for Windows or Security Controls.
4. Download the Ivanti Security Controls 2019.2 executable file to your console machine using the following link:

   https://go.ivanti.com/Web-Download-Security-Controls.html

5. Begin the installation process using one of the following methods:

Note: If your console machine resides in a disconnected network, there are a few extra steps you must take in order to (a) download and install any missing prerequisite software and (b) download the product core files. For complete instructions, see the Performing a New Installation topic in the ISeC Help.

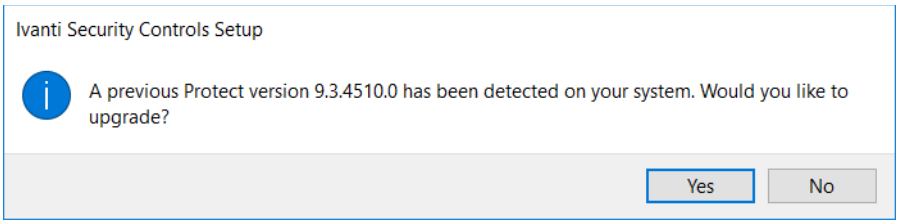
- Double-click the file named **IvantiSecurityControls.exe.**
- Type the file name at a command prompt. Doing so enables you to use one or more command-line options. You should consider this method if you are upgrading a very large database. The DBCOMMANDTIMEOUT option is used to specify the SQL command timeout value during installation. The default value is 15 minutes per GB. The minimum timeout value is the greater of 15 minutes per GB or 1800 seconds (30 minutes). You should override the default value only if you expect the upgrade to take an exceptionally long time due to constrained resources.

  For example, if you have a 4 GB database, to double the default timeout value from 3600 seconds (60 minutes) to 7200 seconds (120 minutes) you would type the following command:

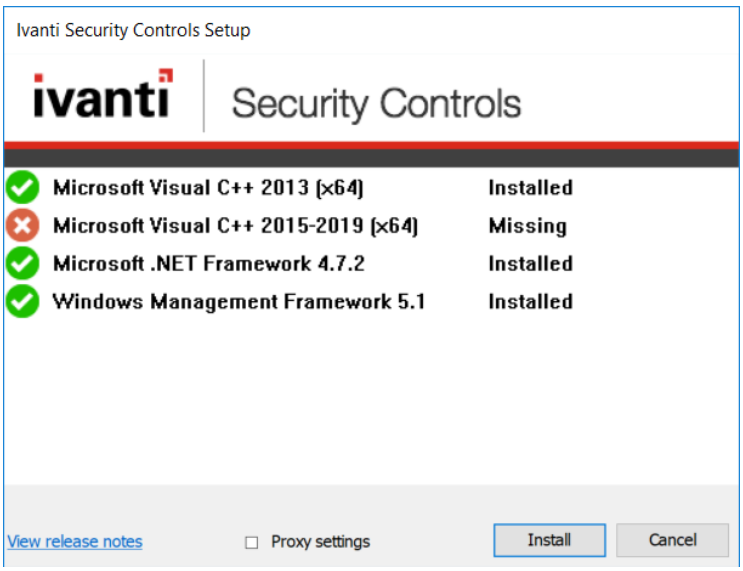
  ```
  IvantiSecurityControls /wi:"DBCOMMANDTIMEOUT =7200"
  ```

Note: If you receive a prompt indicating that a restart is required, click **OK** and the installation process will automatically resume after the restart.

6. Respond to the dialog that asks if you want to continue with the upgrade.



If you click **Yes** and your console machine is missing one or more prerequisites, a dialog similar to the following is displayed. If you are not missing any prerequisites, skip the following step and proceed with the **Welcome** dialog.



7. Click **Install** to install any missing prerequisites.

   The Setup Wizard may need to perform a reboot during this portion of the installation process. If a reboot is required, when the machine is restarted the Setup dialog will reappear. Simply click **Install** again to proceed with the upgrade.

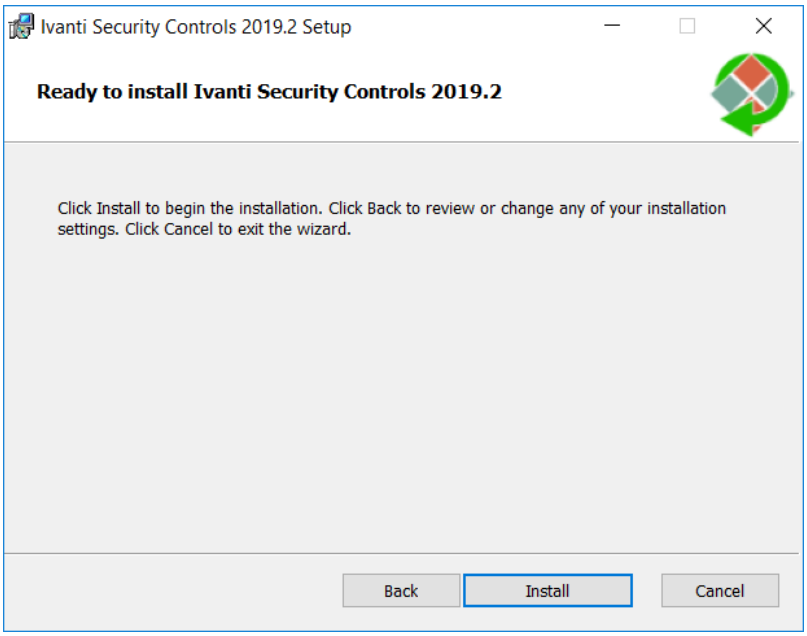
   The **Welcome** dialog is displayed.

8. Read the information on the **Welcome** dialog and then click **Next**.

   The license agreement is displayed. You must accept the terms of the license agreement in order to install the program.

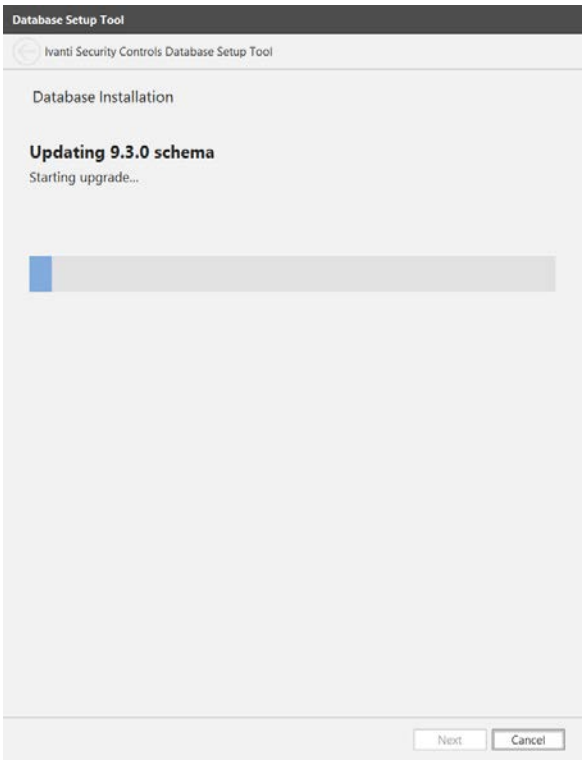
9. Enable the **I accept the terms in the License Agreement** check box and then click **Next**.

   The **Ready to Install** dialog is displayed.

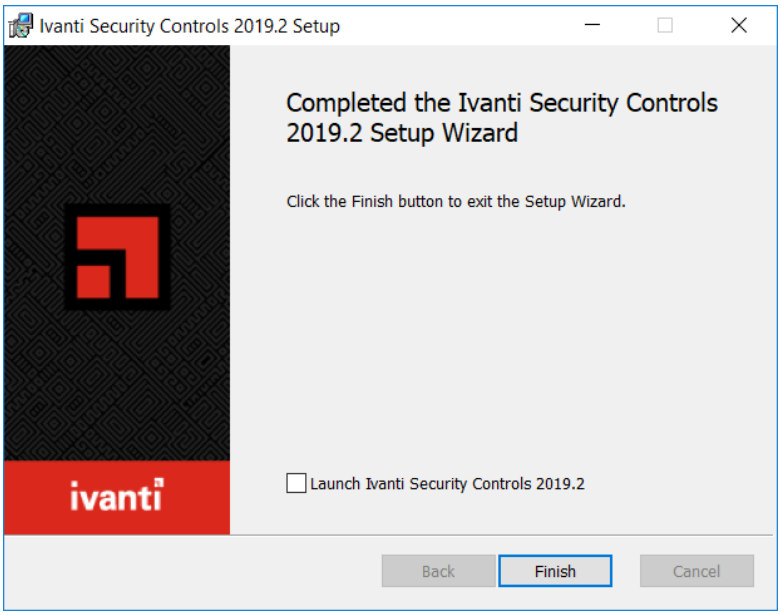


10. To begin the installation, click **Install**.

    Your existing database is automatically upgraded.



11. On the **Completed the Ivanti Security Controls 2019.2 Setup Wizard** dialog, enable the **Launch Ivanti Security Controls 2019.2** check box and then click **Finish**.



The core engines and definitions files are updated and Security Controls is started.

Upgrade Tasks Performed on the Console

In order to complete the upgrade, the following tasks must be performed on the Ivanti Security Controls console.

Refresh Your License (Offline Consoles Only)

If your console is offline (if it does not have an Internet connection), in order to view and use the new features in Security Controls 2019.2 you must manually refresh your license. For information on activating a disconnected console, see Activating the Program in the Help.

If the console is online the license will be automatically refreshed during the upgrade process.

Enter Any New Add-On License Keys

If you purchased additional add-on license keys for the Application Control feature and/or the Power Management feature, now is the time to activate those features using the **Help > Enter/refresh license key** menu. For complete information, see Activating the Program in the Help.

Assign Aliases to the Console

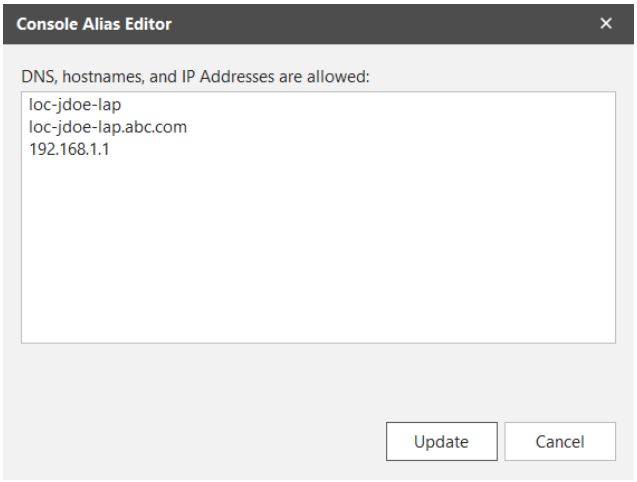
This task is necessary if one or more of the following conditions apply:

- You have assigned the console machine to a new domain
- You have given the console a new common name or IP address
- You manually installed agents and they use an IP address to communicate with the console

Under these conditions you must use the **Console Alias Editor** tool to identify the old console names or addresses as trusted aliases. If you don't, when an agent checks in with the Security Controls console or when an agentless machine attempts to send patch deployment status messages to the console, they will not be able to verify that the machine they contacted is a trusted machine.

1. Select **Tools > Console alias editor**.

   The **Console Alias Editor** dialog is displayed. It will contain the names and IP addresses currently used to identify the console machine. For example:

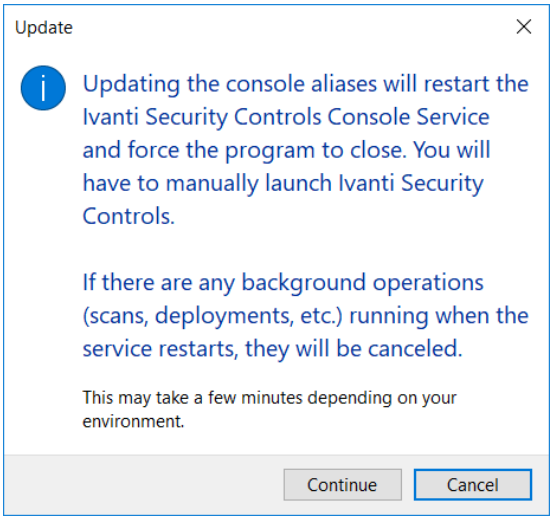


2. Type the names and/or IP addresses that you want to use as an alias for the console machine.

   You can specify IP addresses using either an IPv4 or IPv6 format.

3. Click **Update**.

   The following dialog is displayed:



4. Click either **Continue** or **Cancel**.

   If you click **Continue**, both the console service and the Security Controls program will be automatically restarted; this is necessary in order to update the console aliases list. If you click **Cancel**, the console aliases list will not be updated.

IMPORTANT! The agents will not recognize a new alias until after they check in with the restarted console. The check-in must be initiated by an agent either manually using the agent client program or via a scheduled check in; a check-in command issued from the console to an agent will not update the console certificate on the agent machine.

Review Your Scheduled Tasks

Scheduled tasks are monitored and managed from two separate areas. You should review both scheduled tasks managers to verify that your existing tasks were properly ported.

- The **Scheduled Console Tasks Manager** provides one location to view tasks currently scheduled on the console such as patch scans, asset scans, patch deployments to the console machine, script execution and scheduled reports. To access this dialog, select **Manage > Scheduled Console Tasks**.
- The **Scheduled Remote Tasks Manager** provides one location from which to view power tasks and patch deployments tasks currently scheduled on your remote target machines. You access the Scheduled Remote Tasks Manager from Machine View by right-clicking on a machine and then selecting **View scheduled tasks**.

Synchronize Your Distribution Servers

You must update your distribution servers with the latest patches and/or scan engines and XML definition files contained on the console. This is particularly important if your agents use distribution servers to download these files. The distribution servers must be synchronized with the updated console files **prior** to the agents performing their check-in.

To synchronize your distribution servers:

1. Select **Help > Refresh files** to make sure the console contains all the latest files.
2. Select **Tools > Options > Distribution Servers**.
3. In the top pane, select which distribution server you want to synchronize with the console.
4. In the **Add scheduled sync** box in the top pane, select the component you want to synchronize.
5. Click **Add scheduled sync**.
6. Specify when you want the synchronization to occur and then click **Save**.
7. In the **Schedule automatic synchronization** pane, select the scheduled synchronization entry.
8. Click **Run now**.

Don't worry if the agents happen to check in before you have finished synchronizing the distribution servers. The agents will be updated the next time a scheduled task is run or the agent updates its binaries.

Check Your Custom User Settings

The following custom user settings are not preserved during the upgrade.

- Tools > Options > Display tab:
    - Recent item (days)
    - Show only items created by me
    - Show patch content updates on main page
    - Show informational items in patch scan results
    - Show product levels in View -> Windows Patches
- Tools > Options > Notifications and Warnings tab:
    - Warn before scheduling deployments
    - Close Refresh Files when finished
    - Warn if Protect Cloud sync is not enabled on this console
    - Warn before opening 7 or more bulletins
- Tools > Options > Logging tab:
    - Diagnostic patch scanning

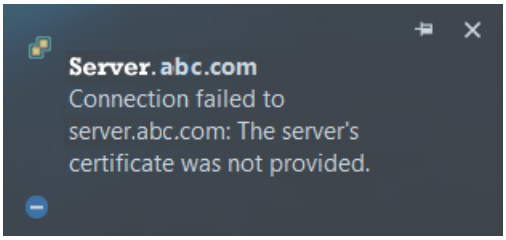
- Deployment Tracker:
  - Update speed
  - Days to show
  - Show failures
  - Show in progress
  - Show successfully completed
- ESXi Hypervisor Bulletins tab:
  - Only show latest
- Event History
  - Limit results to previous (days)
- ITScripts Results View
  - Results since

If You Use an Agent on the Console

If you have an agent installed on the Security Controls console, you should manually reinstall that agent. This should be done in order to ensure that the console agent is properly upgraded with the new agent certificate. No actions are required for agents that are installed on target machines.

Verify Certificate When Connecting to a Virtual Server

A security feature added in v2019.1 requires you to verify a virtual server's certificate information before the program will allow you to connect to the server. If you refresh the view of a vCenter Server following the upgrade, it will fail and you will receive a notification similar to the following:



The solution is to right-click on the server in the navigation pane and select **Edit/Refresh certificate**. A prompt will be issued that asks if you want to accept the certificate. Once accepted, the server's certificate thumbprint will be stored and you will not have to repeat the verification process.

For more information, see Adding, Editing or Removing vCenter Servers in the Help.

If You Use the CHM Version of the Help

Beginning in Security Controls 2018.3, the CHM version of the Help is no longer included with the installation package. If you use the CHM file, you will need to follow the instructions for downloading and configuring the 2019.2 version of the file.

Tasks That are Performed Automatically

When you upgrade from Patch for Windows 9.3 to Security Controls 2019.2, the following tasks will happen automatically behind the scenes.

- The console certificate is reissued. This will happen approximately 20 minutes after you finish the upgrade process. You can use Event History to verify that this PKI maintenance task has been successfully completed. The console certificate must be successfully reissued before you can push-install an agent policy to a Linux machine.
- If you use listening agents, each agent must check in and be upgraded before it will become an actual listening agent again. This has to do with changes that were made to the agent API protocols.

New Features Introduced in Security Controls 2019.2

Major New Features

Patch Management Support for CentOS

Patch management functionality is now available for CentOS systems. You can manage all vendor-supported Server, Workstation, Client and Computer Node variants of the following systems.

- CentOS 6, x64 (the libicu package is required)
- CentOS 7, x64 (the libicu package is required)

Linux Reporting

The reporting tool user interface has been reworked to organize the available reports into logical categories. In addition, several of the reports have been updated to provide information for all supported operating system platforms (Windows, Linux, etc.). New database views have also been added for use with custom reports.

Machine View Improvements

Machine View has been modified to provide a couple of important improvements:

- The tabs have moved from the top pane to the middle pane. This provides a more logical separation of the available patch and asset information and allows you to quickly and easily drill down and locate the information you want to find.
- Windows and Linux deployment history information is now available in the middle pane.
- Assigned AC () configuration information is now available in the top pane.

Import CVEs Improvements

Several improvements have been made to the Import CVEs feature:

- The CVE extraction process now occurs automatically as soon as you select the file containing the CVE file.
- Two tabs have been added to separate and display the associated Windows patches and Linux patches.
- An option has been added that enables you to view only security-related patches.

Minor New Features

Import Ivanti Application Control Configuration

An Ivanti Application Control configuration can now be imported to Security Controls in the .aamp format. For further details on configurations refer to the Configuration section of the Application Control Overview topic in the Help.

Application Control Configuration Enhancements

- New functionality added to the Configuration Editor so that a text search can be carried out. This helps you to quickly identify which rule collection, or rule set, a configured item belongs to.
- New Network Shares are Accessible by default option in the Executable Control Configuration Settings.
- Folders and Rule Collections can now be added to a parent Process Rule along with files and file hashes.

Extension to the Add delay (days) Scheduling Option

The Add delay (days) option that is used in several areas has been extended to allow delays of up to 31 days (was previously a 20 day maximum).

Patch File Size

A new File size column has been added to Scan View, Machine View and Patch View. This shows the patch file size and will be helpful when testing or planning patch deployments.

Agent Installation PowerShell Script

When manually installing agents, it is now a requirement to provide a secure connection between the remote machine and the console by importing the issuing certificate to the remote machine. A custom PowerShell script is provided to automatically perform these steps for you. For more information, see Agent Options.

Deployment Confirmation Dialog

The Deployment Configuration dialog has been updated to present deployment information is a much more useful manner.

Power Pack License Key

The Power Management and advanced ITScripts features are now available with a standard license key. The requirement for a separate add-on license key for these features has been removed.

New Features Introduced in Security Controls 2019.1

Major New Features

Application Control (now Generally Available)

The ability to prevent unauthorized code execution on your corporate machines, and thus protect these machines from ransomware and other malware attacks, is now available via the Application Control feature. Using techniques such as Executable Control, Privilege Management and Browser Control, Application Control reduces risk, helps achieve compliance and delivers security, all with minimal performance impact to your end users.

In addition, the Application Control Event Viewer is being introduced in Security Controls 2019.1. This view enables you to run a large number of customizable queries that show events that have occurred during a specified time period.

Finally, you can now perform daily maintenance on the AC events in your database by using the Database Maintenance tool.

Minor Features and Enhancements

Modified Home Page

The new home page design that was introduced in 2018.3 has been updated. It now has a cleaner and more graphical appearance.

Linux Deployment Results Reported to the Console

The results of Linux agent patch deployments are now reported to the console and can be found in the middle pane of Machine View. A history of prior deployments is also reported on the **Patch Deployment** tab of the **Database Maintenance** dialog.

Ability to Acknowledge Events in Event History

The Events History page now contains a new Acknowledge column that indicates whether each event has been seen and reviewed by an administrator. You can right-click an event to acknowledge it.

Review Certificate Before Connecting to a Virtual Server

The first time you connect to a vCenter Server, you may be prompted to review and verify the server's certificate. This security step ensures that you are not connecting to an untrusted server. Once the certificate is accepted, the certificate's thumbprint will be stored and you will not be asked to repeat the verification process. If a server’s certificate changes in the future, you will simply do a refresh to acknowledge the new certificate.

Agent Reboot Options Tab

A new Agent Reboot Options tab has been added to the Agent Policy Editor. This tab enables you to specify if and how an agent machine will be restarted after either an agent is upgraded or an engine component is installed or upgraded. These values have always been a part of the agent policy, but the addition of this tab enables you to fine-tune a number of reboot options.

New Import CVEs Button

A new Import CVEs button has been added to the Patch Group area of Windows Patch View. This provides a more intuitive location from which to initiate the import process.

New Database Views

A collection of new database views is now available for use in custom report queries. The new views begin with the term Reporting2.* and should be used in all new custom queries. The older collection of views, which begin with the term Reporting.*, is still available but should only be used by legacy queries.

Features That Have Been Removed

- The ITScripts WinRM Remoting target type has been removed. In conjunction with this change, the **Use SSL** check box and the **Port** option have been removed from the **ITScripts Template** dialog.
- Agents are no longer supported on Windows Vista, Windows Server 2008 and Windows Server 2008 R2 Gold operating systems. Agents are supported on Windows Server 2008 R2, SP1 or later but only if SHA-2 support is provided.

New Features Introduced in Security Controls 2018.3

Major New Features

REST API

The API feature provides a simple RESTful interface with lightweight JSON-formatted responses that enables you to read and write data to/from the program. The feature allows you to automate many of your day-to-day operations, saving you considerable time and effort. The REST API allows you to fully integrate Ivanti Security Controls into your orchestration and automation systems.

The list of available functions includes:

Asset Scan Templates	Patch Downloads	Patch Deployment Templates
Credentials	Patch Groups	Patch Metadata
Distribution Servers	Patch Scans	Vendor Family Product Metadata
Machine Groups	Patch Scan Templates	Virtual Infrastructure
Operation Controller	Patch Deployments	
Patches	Patch Deployment Status	

For complete details, see the REST API Help.

Patch Management Support for Linux

Patch management functionality is now available for Red Hat Enterprise Linux (RHEL) systems. The scan and deployment processes are nearly identical to that used by your Windows patch agents, so you can quickly begin managing your Linux systems.

You can manage all vendor-supported Server, Workstation, Client and Computer Node variants of the following systems.

- Red Hat Enterprise Linux 6, x64 (the libicu package is required)
- Red Hat Enterprise Linux 7, x64 (the libicu package is required)

To get started using this feature, refer to the Overview of Linux Patch Management topic in the Help.

Import CVEs Into a Patch Group

The Common Vulnerabilities and Exposures (CVE) List is a public reference of known cybersecurity vulnerabilities. This list, maintained by the MITRE Corporation (mitre.org), continually changes as new vulnerabilities are detected. If your organization uses the CVE list, it can be difficult to determine exactly which patches you need to deploy to protect your machines from the threats identified in the list.

Fortunately, Security Controls simplifies this process. You simply import a list of CVEs to Security Controls and then add them to a patch group. Security Controls will automatically determine which patches are related to each CVE and it will add those patches to the patch group. You then use the patch group in your scans and deployments.

To get started using this feature, refer to the Importing CVEs topic in the Help.

Application Control (Preview Only)

The Application Control feature was offered as a Community Technology Preview 2 (CTP 2) release in Security Controls 2018.3.

Minor Features and Enhancements

The Product Has Been Renamed to Ivanti Security Controls

The product name has been changed from Ivanti Patch for Windows to Ivanti Security Controls. The new name reflects the addition of functionality that was previously only available in two or more separate products.

New Home Page

The home page has been totally redesigned to provide status information and statistics, quick links to many of the most popular activities and notification of any possible issues that may require your attention.

The old home page functionality, from which patch, asset, power and ITScripts tasks can be quickly and easily performed, is still available and has simply been moved to the new Agentless Operation dialog. To access this dialog, select **New > Agentless operation** or press Ctrl + N.

Reorganized Menu Bar

The **New** menu has been reordered and Windows and Linux tasks have been consolidated into two **New > Windows patch** and **New > Linux patch** sub-menus. Import tasks have been removed from the **New** menu and are now located in the new **Import** menu. **Manage > Items** has been renamed to **Manage > Database Maintenance** and, in addition to enabling you to view a list of all prior scans and patch deployments, it now enables you to schedule database maintenance activities that were previously configured from the **Tools > Options > Database Maintenance** tab (which has been removed).

New Sections in the Navigation Pane

The sections in the navigation pane have been renamed and reordered to provide a smarter and easier to use organization. There are also two new sections:

- Linux Patch Configurations and Groups
- Application Control Configurations

Machine View Changes

- Three news tabs have been added to the top pane to help manage the presentation of machine information.
    - Windows patch & Application Control
    - Windows asset
    - Linux patch
- Several new columns are now available, including OS type, CVSS score and CVEs.
- Information in the bottom pane has been reorganized to increase usability.

Windows Patch View

The top pane in Patch View now contains new columns that show the CVSS score and the patch file name so that you can more clearly see affected products. The bottom pane has been reorganized so that the most commonly-used content is near the top.

Tools > Options Changes

- **Display** tab: Contains a new section that is used to define program startup defaults. The **Recent errors** check box controls the date range for the new Possible Issues area on the home page. A new **Select palette** button enables you to select the color swatch you prefer to use within the program.
- **Patch** tab: This has been renamed to **Scan**. A new **Patch scan results import timeout** option enables you to specify the maximum time to wait for the console to import scan results from all target machines.
- **Downloads** tab: A new **Open directory** button provides convenient access to Windows File Explorer.
- **Database Maintenance** tab: This tab has been removed from the **Options** dialog. The database maintenance functionality is now found by selecting **Manage > Database Maintenance**.
- **API** tab: This new tab provides access to a PowerShell script that helps establish a secure connection between remote REST API clients and the console

Agent Policy Editor Changes

To accommodate the new Linux and Application Control functionality, the **Agent Policy Editor** now supports defining one or more Linux patch tasks on the **Patch** tab and it contains a new **Application Control** tab. In addition, the interface used to add, edit and delete tasks has been updated on all tabs.

The CHM Help File is Now Only Available as a Separate Download

The CHM version of the Help is no longer included with the installation package. If you access the Help using the CHM file that is used when you choose the Local help viewer option, you will need to follow the instructions for downloading the file and configuring the system. This is a one-time process.

If you access the Help on the web, you are not affected.

Service Pack Groups are Now Called Product Levels

The term Product Level better reflects the terminology used by Microsoft Corporation to identify different versions or updates of their products, such as Windows 10. Some products may still use the older service pack terminology, and for these products you will still see the term SP1, SP2, etc. in the Product level column within Machine View and other areas of the product.

Manage > Items

This has been renamed to **Manage > Database Maintenance**. In addition to viewing and managing the list of prior scans, script executions and patch deployments, this dialog now contains the database maintenance functionality that was previously available on the old **Tools > Options > Database Maintenance** tab.

Help > About Dialog

The Version Info / App Info button has removed. This information is now presented on the new **Application** and **File versions** tabs. The columns on the **File versions** tab are now sortable. And the dialog now contains a link to a web page that shows the list of Ivanti patents that protect Ivanti software and cloud services.