Security Controls 2021.1

Upgrade Guide

Welcome

Upgrade Procedure

Upgrade Tasks Performed on the Console

New Features Introduced in Security Controls 2021.1

New Features Introduced in Security Controls 2020.1

New Features Introduced in Security Controls 2019.3

Welcome

Purpose of this Guide

Welcome to Ivanti Security Controls 2021.1. This document describes how to upgrade from Security Controls 2020.1, 2019.3 or 2019.2. 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 2021.1. It also highlights the areas in the user interface that have changed significantly.

New System Requirements

As of 2020.1, the following operating systems are no longer supported for use by the Security Controls console:

- Windows 7 SP1
- Windows Server 2008 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 upgrade 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 Security Controls help.

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 2020.1, 2019.3 or 2019.2 to Security Controls 2021.1. 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.

Before You 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. If your database is in a SQL Server high availability group, it must be removed prior to upgrading.

   The upgrade process will fail if the database is in a high availability group.

4. If your current console resides on a virtual machine, you should take a snapshot prior to the upgrade.

   This is simply a precaution in the event there is a problem during the upgrade and you want to revert to your original environment.

Performing the Upgrade

1. Close all programs running on the console machine, including Security Controls.
2. Download the Ivanti Security Controls 2021.1 executable file to your console machine using the following link:

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

   - Double-click the file named **IvantiSecurityControls.exe**

     -OR-

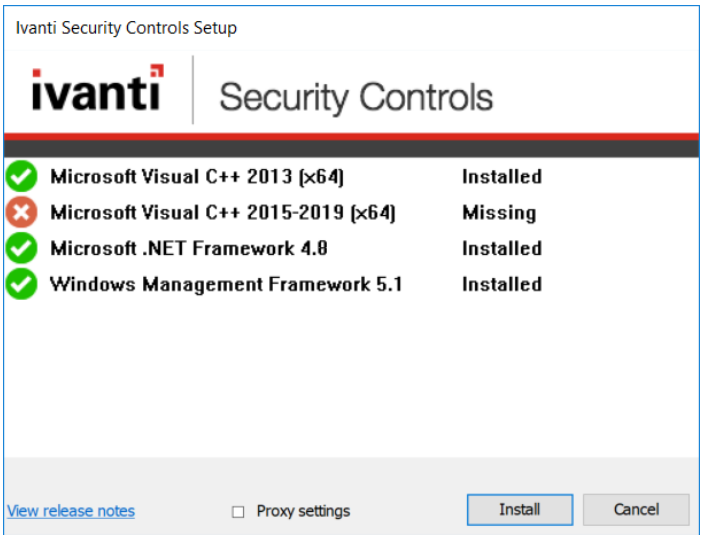
   - Type the file name at a command prompt. Doing so enables you to use one or more command-line options. You should consider this method if you are upgrading a very large database. The DBCOMMANDTIMEOUT option is used to specify the SQL command timeout value during installation. The default value is 15 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.
4. 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.



5. 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.

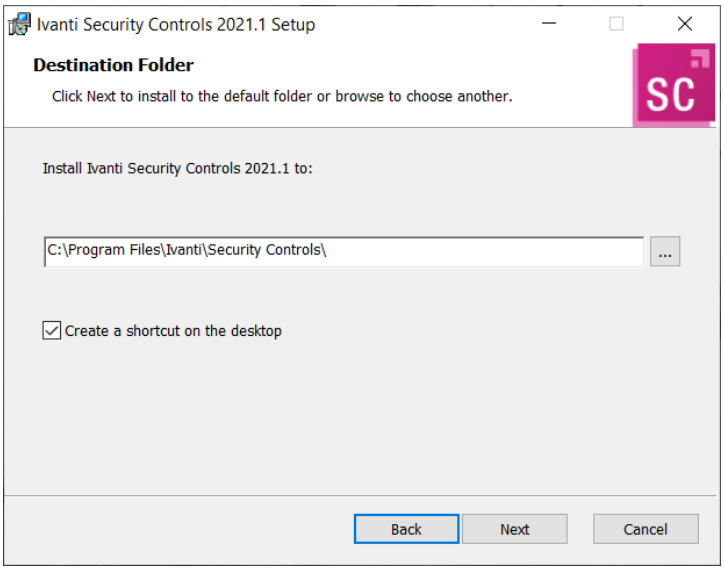
   The **Welcome** dialog is displayed.

6. 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.

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

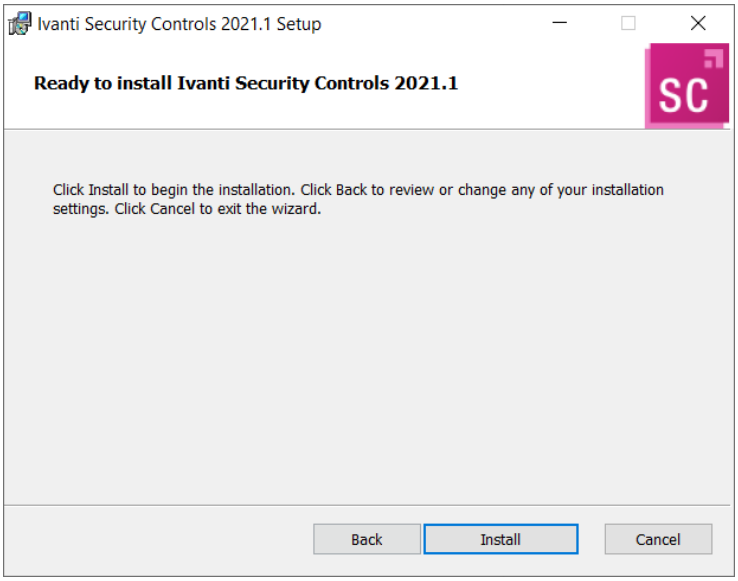
   The **Destination Folder** dialog is displayed.



8. If you want to change the default location, click the browse button and choose a new location.

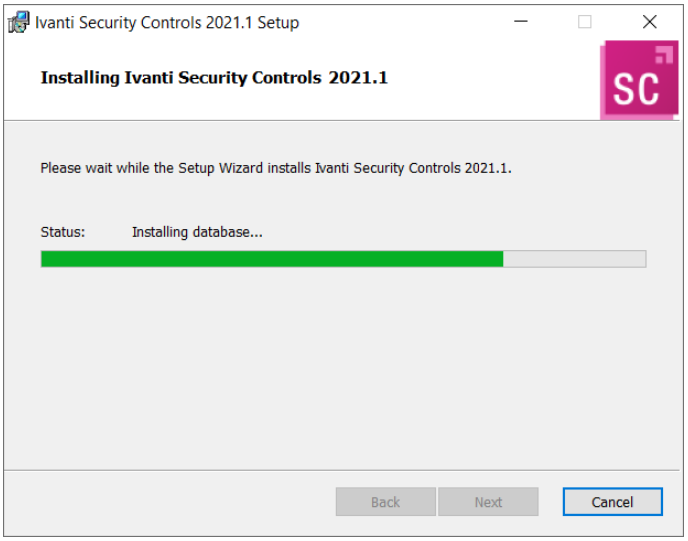
9. Click **Next**.

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



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

    Your existing database is automatically upgraded.

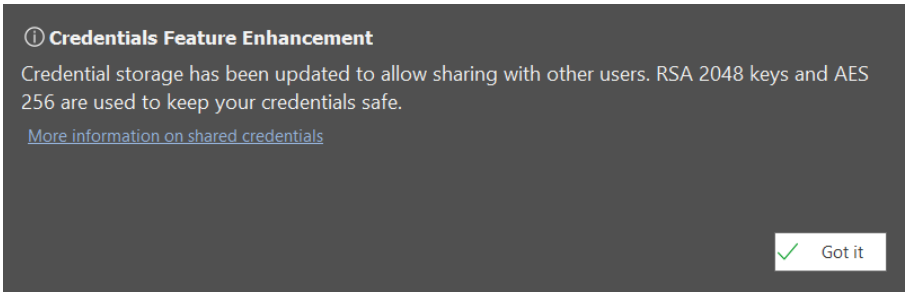


11. On the **Completed the Ivanti Security Controls 2021.1 Setup Wizard** dialog, enable the **Launch Ivanti Security Controls 2021.1** check box and then click **Finish**.

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

What You May See the First Time Security Controls 2021.1 is Started

One of the most important new features introduced in Security Controls 2020.1 is the Shared Credentials feature. This feature enables you to share credentials with one or more users. If you are upgrading from Security Controls 2019.3 or 2019.2, the first time you launch Security Controls 2021.1, a one-time notification is displayed that informs you about the new feature and briefly describes the security precautions that are in place to keep all credentials safe. You can click the embedded help link for more information.



Upgrade Tasks Performed on the Console

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

IMPORTANT! If you need to refresh your license or enter a new add-on license key, the legacy License Key Activation Method should be used. If for some reason you are using the new Credential Activation Method and you have agents deployed to your endpoints, you must wait for the agents to check in with the console and be upgraded to v2021.1 before you change licensing methods. All Linux agents, as well as Windows agents with Application Control tasks, will fail if you change licensing methods before the agents are upgraded.

Refresh Your License (Offline Consoles Only)

If your console is offline (it does not have an internet connection), in order to view and use the new features in Security Controls 2021.1, you must manually refresh your license. For information on activating a disconnected console, see Activating the Program in the Security Controls 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 an additional add-on license key for the Application Control feature, now is the time to activate that feature using the **Help > Enter/refresh license key** menu. For complete information, see Activating the Program in the Security Controls help.

Initialize Users for Credential Sharing

Each user in your organization will be assigned a user certificate and a public/private key pair the first time they launch Security Controls after the upgrade. The certificate and keys are required in order for the users to participate in the Shared Credentials feature. Encourage each Security Controls user to launch the program as soon as reasonably possible.

Note: The other option for getting users to be recognized by Security Controls is to issue a REST API request.

Review Credentials That are Shared with Background Services

Enabling a credential for use with background services is now performed on the new **Share Credential** dialog, rather than the **Define Credential** dialog. Any credential that was being shared with background tasks, agents and other features will be automatically converted to the new convention during the upgrade. You can access the **Share Credential** dialog by selecting **Manage > Credentials** and then clicking the **Share** button.

You should experience no interruption in service or scheduled background operations. If a background service is using credentials that for some reason cannot be decrypted, then the **Credential Reset** dialog will be displayed and that dialog can be used to recover from the situation.

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

Assign Groups in Machine View and Scan View

The new **Assigned Group** 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. The values in this column will be empty immediately following the upgrade. Values will be automatically assigned during future scan operations that involve machine groups, or you can manually assign values using the **Machine Properties** dialog. For more information, see the Assigned Group column description in the Security Controls help.

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.

Assign Aliases to the Console

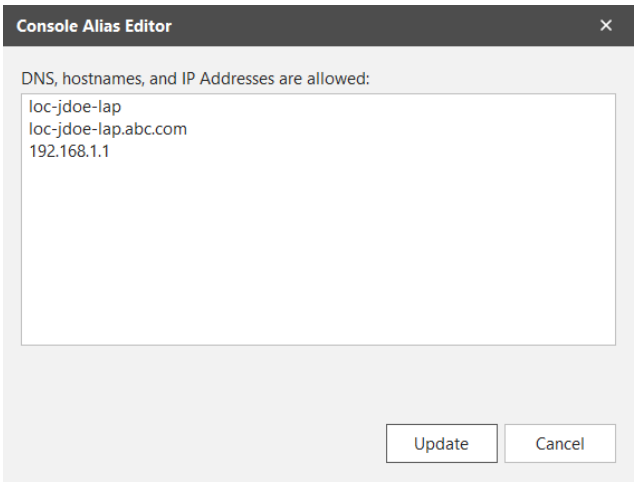
This task is necessary if one or more of the following conditions apply:

- 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:

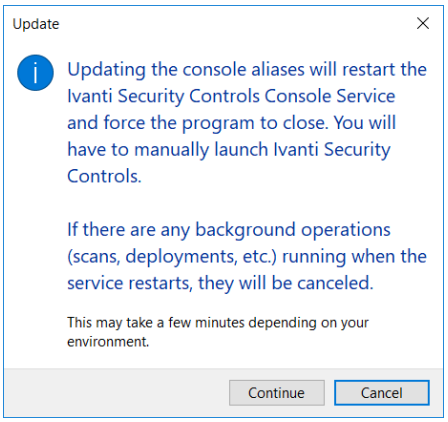


2. Type the names and/or IP addresses that you want to use as an alias for the console machine.

   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.

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 the CHM Version of the Help

The CHM version of the Security Controls 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 2021.1 version of the file.

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.

New Features Introduced in Security Controls 2021.1

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**.

New Features Introduced in Security Controls 2020.1

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 more details, see the REST API help.

Minor New 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.

New Features Introduced in Security Controls 2019.3

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. For details, see the REST API Help.

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

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 New Features

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.