Getting Started with

Application Whitelist Monitor

Version 10.2.0.1

Contents

Chapter 1: Introduction

Workspace Control Application Whitelist Monitor is a companion tool to Workspace Control. It simplifies security whitelisting if you deploy new applications via a third-party tool such as Microsoft System Center or IBM BigFix, or if you deploy them manually by storing them on a file share.

The Application Whitelist Monitor eliminates the need to manually configure file hashes and file certificates for Authorized Files, as it allows you to automatically import and update these in your Workspace Control environment.

This document guides you through the installation of the Workspace Control Application Whitelist Monitor and explains how to configure it.

Chapter 2: Installation

2.1 Prerequisites

	Prerequisites
Software (Ivanti)	• Workspace Control version 10.2 or higher Management Console • Workspace Control Application Whitelist Monitor installation file (`Ivanti Workspace Control Application Whitelist Monitor 10.2.0.1.msi`) • *Optional* - only necessary when using **File Certificates security**: • Workspace Control Management Portal version 10.2 or higher
Software (general)	• Microsoft .NET Framework 4 or higher • *Optional* - only necessary when using archive files: • Program that can handle the extracting of archive files. It is recommended to use a program that can handle different file extensions, for example, 7-Zip.
Account	Administrator rights to install software on the target computer
Service Account	Account with access to the Management Console (defined using an Workspace Control **Administrative Role**). Go to the Workspace Control Application Whitelist Monitor service (`RESFHM`), select **This account** and specify the credentials of the Service Account.

2.2 Installing Workspace Control Application Whitelist Monitor

To start using the Workspace Control Application Whitelist Monitor, install the MSI file `Ivanti Workspace Control Application Whitelist Monitor 10.2.0.1.msi` on the machine on which the Workspace Control Console is installed.

When installing the Workspace Control Application Whitelist Monitor, the **Setup Wizard** will guide you through the installation process. During the installation, you also configure the Workspace Control Application Whitelist Monitor in the **Configuration** window.

Chapter 3: Configuration

In the **Configuration** window, four tabs are available:

- **Configuration tab** (on page 3)
- **Directories tab** (on page 3)
- **Extraction tab** (on page 4)
- **Scan tab** (on page 4)

3.1 Configuration tab

Specify the **Import interval**. At this interval, the following steps occur:

1. The **Directories to scan** (specified on the **Directories** tab) are scanned for new files that need to be processed.
2. For new or modified files, the **Info to retrieve** (specified on the **Scan** tab) is collected.
3. The new data is imported into the Datastore, using the Management Console (`pwrtech.exe`).

The **Working temp directory** is used when calculating file hashes (SHA-256).
If **Enable extracting of archive files** is selected (on the **Extraction** tab), archive files that are found in the **Directories to scan** are also extracted to the **Working temp directory**.

The **Output file** is where the Application Whitelist Monitor stores retrieved hash and/or certificate information. By default, if **Info to retrieve** is set to **Hash** (on the **Scan** tab), the file will be in CSV format. For **Certificates** or **Hash and Certificates**, the file will be in XML format.
Please note, that the full path to the **Output file** must be specified.

The output file is imported using the Management Console whenever it contains new data (after a scan of the directories for new files).

3.2 Directories tab

Specify the credentials (**Username** and **Password**) of an account that has access to the location where the **Directories to scan** are located (network share). If no credentials are specified here, the credentials of the Service Account that is specified for the Workspace Control Application Whitelist Monitor service will be used.

The full path to the **Directories to scan** must be specified.
Any subdirectories in the specified **Directories to scan** will also be scanned.

3.3 Extraction tab

Select **Enable extracting of archive files** if files are stored in archive files. If this option is selected, make sure a program is available that can handle the extracting of archive files. It is recommended to use a program that can handle different file extensions, for instance, 7-Zip.

Add any additional or remove existing **Archive file extensions to extract**. By default, the file extensions `.cab`, `.exe`, `.msi`, `.msp`, `.rar`, `.zip` are filled in. Please note that not all extracting programs can handle all these file extensions.

At **Path to executable**, specify the extraction program you want to use. When using 7-Zip, the entry for **Parameters** (below **Path to executable**), is filled in automatically.

At **Parameters**, the markers `<file-path>` and `<folder-path>` must be used along with the parameters of the extraction program specified at **Path to executable** (for 7-Zip this line is filled in automatically). The marker `<file-path>` will automatically be replaced by the archive file path that was identified when scanning the directories and their subdirectories (the **Directories to scan** are specified on the **Directories** tab). For the marker `<folder-path>`, the location that is specified for **Working temp directory** on the **Configuration** tab will be used and the File Hash Monitor will add some additional information that is needed.
The following command-line options are specified by default to optimize performance when using 7-Zip:

- `-y` (assume `Yes` on all queries): prevents, for example, overwrite messages during extraction.
- `-p` (assume a blank password): prevents a 15 second timeout when encountering a password-protected file for which the password is not provided. Because the file cannot be extracted, its hash will not be calculated.

Please refer to the documentation of your extracting program of choice for similar or additional command-line options.

3.4 Scan tab

Add any additional or remove existing **Extensions to be scanned**. By default, the file extension `.exe` is filled in.

At **Info to retrieve**, select the file information that the Application Whitelist Monitor should retrieve for the files:

- **Hash**
- **Certificates**
- **Hash and Certificates**

When you click **OK**, you return to the **Setup Wizard**, which you can then close by clicking **Finish**.

To access the Application Whitelist Monitor **Configuration** Window after installation has finished, you can use the command-line option `/config`.
Example:

```
C:\Program Files (x86)\Ivanti\Workspace Control Application Whitelist Monitor\FileHashMonitor.exe /config
```

Chapter 4: After importing

In the Workspace Control Management Portal, you can configure application security based on file hashes *and* file certificates on their dedicated pages under **Security > Applications**.

In the Management Console, you can *only* configure application security based on file hashes. This is located at **Security > Data > Authorized Files**.

The following applies when importing file hashes for Authorized files:

- For each imported rule, the system checks if there are existing Authorized Files (global and application-level) that match the imported combination of authorized executable and additional process.
- If one or more matches are found, then:
  - If the imported file hash is not yet listed in the matching Authorized Files, it is added to them. The file hash will be imported with the Mode “Allow”.
- Rules in the import file are processed top-down, so if the import file contains multiple rules that update the same Authorized File or file hash, the end result depends on the order in which the rules appear in the file.

Chapter 5: Ivanti Support

At Ivanti, our core business is to help heighten productivity in your organization. Ivanti Support helps us to achieve this goal, and has been embedded in the core principles of our company since it was founded. Ivanti is dedicated to supporting everyone who uses or wants to use its proven products with Ivanti Support, which elevates our enterprise solutions above and beyond technology.

Support - If you are experiencing difficulties with any of our products, you may find the solution in our Knowledge Base (**Success Center > Support**) or you can contact Ivanti Support directly (**Success Center >** Click **Contact Us**).

Product Upgrades and Service Releases - To upgrade your product to the latest standard, you can install Product Upgrade Packs and Service Releases from the **Success Center > Downloads**.

Solution Assurance - To protect your investment, it is mandatory that you purchase one initial year of Solution Assurance with each license purchase. Solution Assurance unlocks access to Technical Support, Product Updates and Upgrades and the Knowledge Base. Solution Assurance is extended automatically, unless you specify otherwise. For more information: http://res.com/support.

Early Adopter Program - Participants of the Early Adopter Program are actively involved in taking Ivanti solutions to the next level. The Early Adopter Program unlocks access to interim releases of our products. These releases are production-ready and allow you to test drive and explore new functionality.

Community - Ivanti invites you to become part of our community to share best practices and tips with fellow IT professionals, find solutions and more (**Success Center > Q&A**).

Please visit the Success Center (http://success.res.com) for more information on Support.

Chapter 6: Ivanti Training

Ivanti has developed a mix of learning materials to help our customers and channel partners get the most out of our products. Our goal is to give you a choice in how you learn; whether that is in the classroom, online tutorials and virtual workshops, or downloading our self-study kits. Please visit the Academy at the Success Center (http://success.res.com) or go to http://res.com/support/training to find more information on Training.

Ivanti Academy - Ivanti Academy provides an engaging way to learn about Ivanti products and technologies. It consists of short video tutorials, including practice questions, informative links and more. These tutorials cover a broad range of subjects: from planning, installing and configuring an environment to using the functionality of the Ivanti product.

Workshops - For customers and partners Ivanti organizes free interactive online workshops. These one-hour events are intended for experienced users of our software and deal with specific use cases and troubleshooting. Due to the interactive nature of these workshops, the number of seats per session is limited.

Training Classes - For partners and customers, Ivanti has developed several technical courses that deal with the installation and configuration of Workspace Control, Automation and Identity Director. These technical courses are offered by RES Authorized Learning Centers (RALCs).

Certification - Ivanti offers a certification program designed to validate IT professionals with the technical capabilities and expertise needed to effectively use the Ivanti product portfolio, giving companies the confidence that their IT employees have the skills and experience needed to be successful.