ABSOLUTE APPLICATION PERSISTENCE TECHNICAL GUIDE

TECHNOTE

ABSTRACT

This document serves as a technical guide for administrators to learn how Absolute® Application Persistence® can be used to monitor and remediate critical security applications through the Absolute console. It details the functionality and architecture behind Application Persistence and lists the processes involved in configuring the self-healing capabilities for an application and viewing related application remediation reports.

SECURITY CHALLENGES AT THE APPLICATION LAYER

Organizations deploy a set suite of security applications to maintain the compliance and protection of their device fleet against ever-increasing cyber threats in today's digital environment. Despite this, applications are easily tampered with through the reimaging of machines, disabling of running services by negligent users or malicious intruders and the corruption of registry files. This vulnerability at the endpoint application layer can leave organizations susceptible to cyber threats, fleet non-compliance and ultimately large financial penalties. IT administrators universally agree that the only solution to this pressing issue is automation. Absolute Application Persistence offers zero-touch automated security through the health monitoring of critical applications and remediation of running services, operational directories or registry files in cases of non-compliance.

APPLICATION PERSISTENCE

Absolute's Application Persistence product offering enables organizations to monitor and remediate the health of critical applications to ensure the security posture of their corporate network. Application Persistence leverages Absolute's patented Persistence technology, embedded in the BIOS of over 1 billion devices worldwide, to maintain a direct two-way connection between the Absolute console and the endpoint device, enabling the monitoring and remediation of critical applications.

Application Persistence runs periodic health checks on critical applications across the device fleet and seamlessly remediates applications that are either not installed, not running appropriately (e.g. services disabled) or are missing critical operational files, registry files or directories.

Additionally, Application Persistence sends regular updates on the compliance status of applications across all managed devices to a secure Absolute web server. Through this, the administrator has the ability to actively monitor application compliance at the fleet level, without having to worry about individual instances of non-compliance on specific endpoints whenever they occur.

COMPATIBILITY

Application Persistence is supported on all devices having the following configuration:

- Absolute console.
- Operating System: Windows 7 or higher.

FUNCTIONALITY

Remediation Action Overview

The specific remediation actions that the Application Persistence (AP) engine takes in cases of application non-compliance can be summarized by the three following phases:

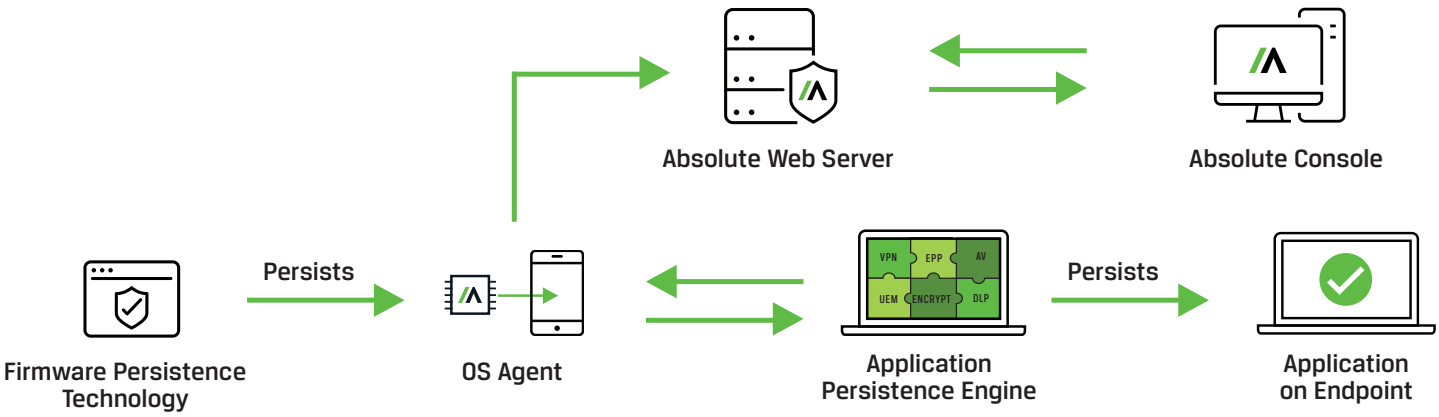
- **Report only:** Every 6 hours, the AP engine runs health checks on the endpoint to deduce whether the application is

installed and running correctly. This includes, but is not limited to, checking if the application is listed in the Windows registry, if the application folder has all critical files and operational subdirectories intact and if the application's services are running smoothly. The AP engine send the compliance status back to the Absolute web server.

- **Report and Repair:** If the AP engine deduces non-compliance during the Report phase, it will attempt to remediate the application through steps taken within the confines of the endpoint device. This includes, but is not limited to, restarting the application's services as well as running the cached MSI package to install (if the application is missing) or reinstall the application (if critical application files are missing).
- **Report, Repair and Reinstall:** If the Repair phase fails to remediate the application, the AP engine will attempt to download the application's installer from a preset URI on a customer hosted web server. It will then perform a hash check to authenticate the binary contents of the downloaded installer and run a fresh installation on the endpoint device.
- Note: The ability to Report Only is available with an Absolute Visibility or Control license, while Report, Repair and Reinstall is available with an Absolute Resilience license.

TECHNICAL ARCHITECTURE

The architecture behind Application Persistence's functionality is described in the diagram and process listed below.

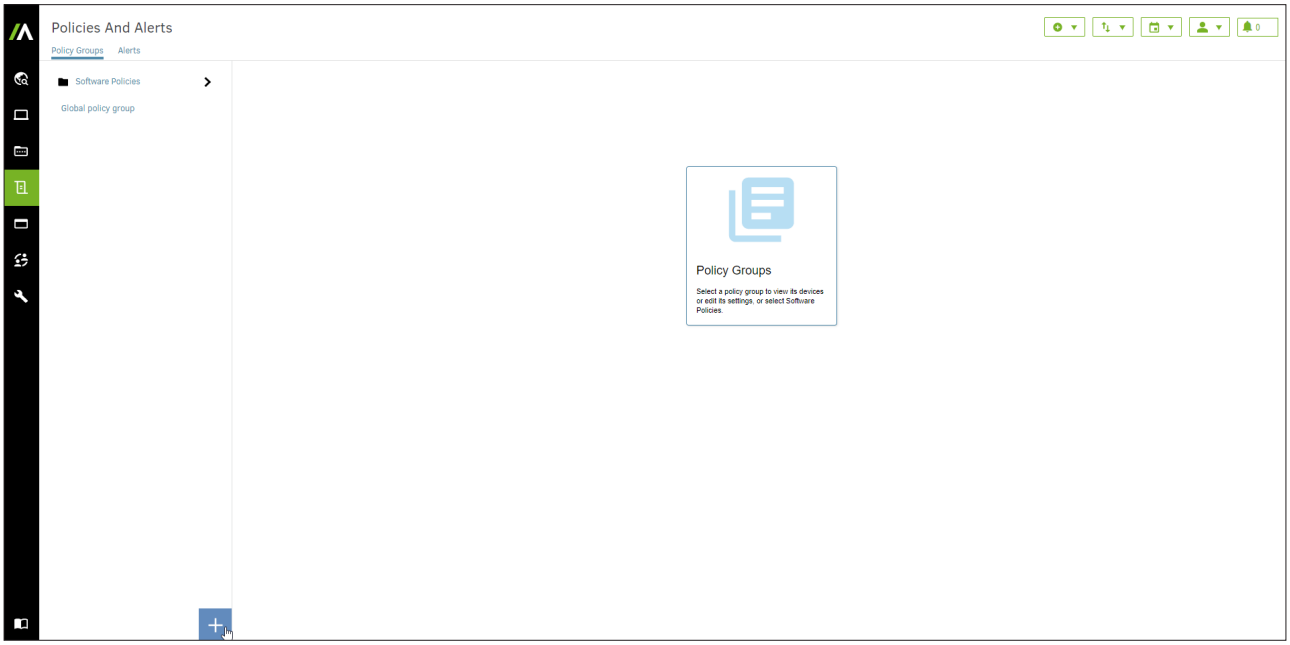


1. Upon device boot-up, Absolute Firmware Persistence, embedded in the BIOS of the endpoint device, ensures the OS agent is healthy; if not, it initiates the recovery of the agent.
2. The administrator sets Application Persistence (AP) configuration instructions and creates a device policy group for assigned machines through the Absolute console. The Absolute console then lays this information to the OS agent via the Absolute web server.
3. The OS agent periodically monitors the health of AP configured applications on the endpoint by running the Application Persistence engine.
4. The Application Persistence engine remediates the AP configured application(s) in cases of non-compliance on any of the assigned machines.
5. The Application Persistence engine then sends compliance and remediation activity information back to the Absolute web server via the OS agent. This information is then used to provide reporting capabilities to the administrator through the Absolute console.

DEVICE POLICY GROUP CREATION

Prior to configuring persistence for an application, a policy group needs to be created. A policy group is assigned to a subset of machines within an organization's device fleet. Functionality available through the Absolute console including Hardware and Software monitoring, Endpoint Data Discovery as well as Application Persistence to name a few, can all be configured and assigned to specific policy groups. Policy groups can be created by selecting the "Policies and Alerts –

Data Collection and notification" button on the left hand vertical pane. Once the "Policies and Alerts" page appears, click on the blue "+" sign on the bottom left side of the page, as shown in the image below.



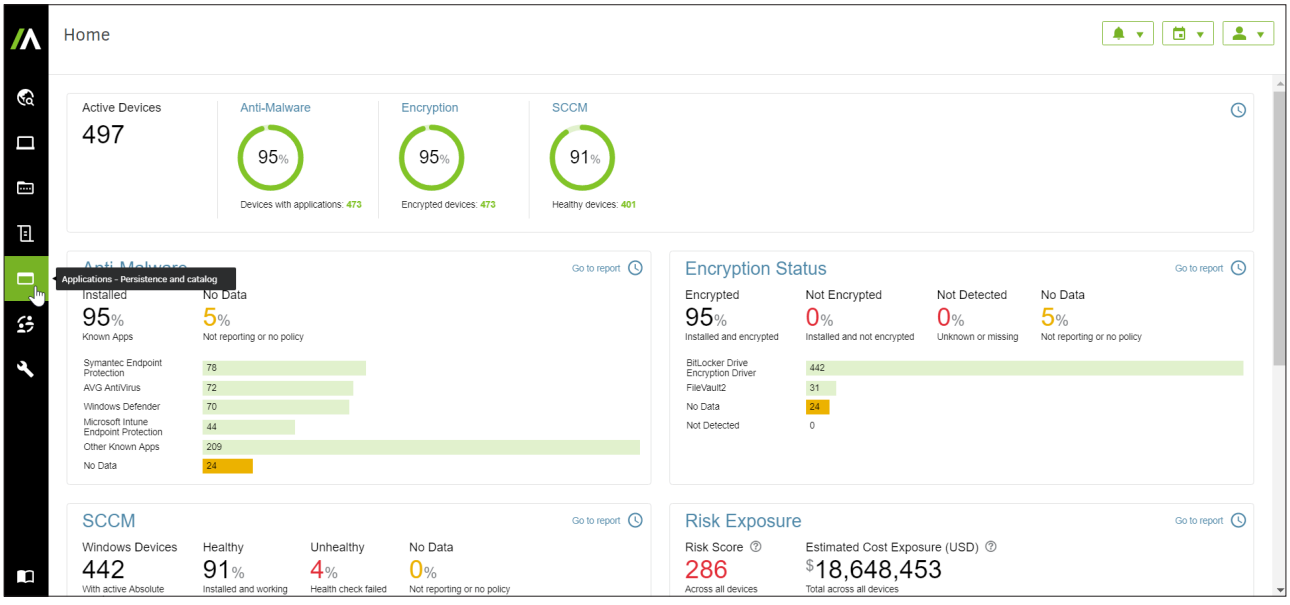
Next, follow the "create a policy group" wizard to create the policy name, select machines to assign to the policy group and confirm the policy group's creation.

APPLICATION PERSISTENCE CONFIGURATION:

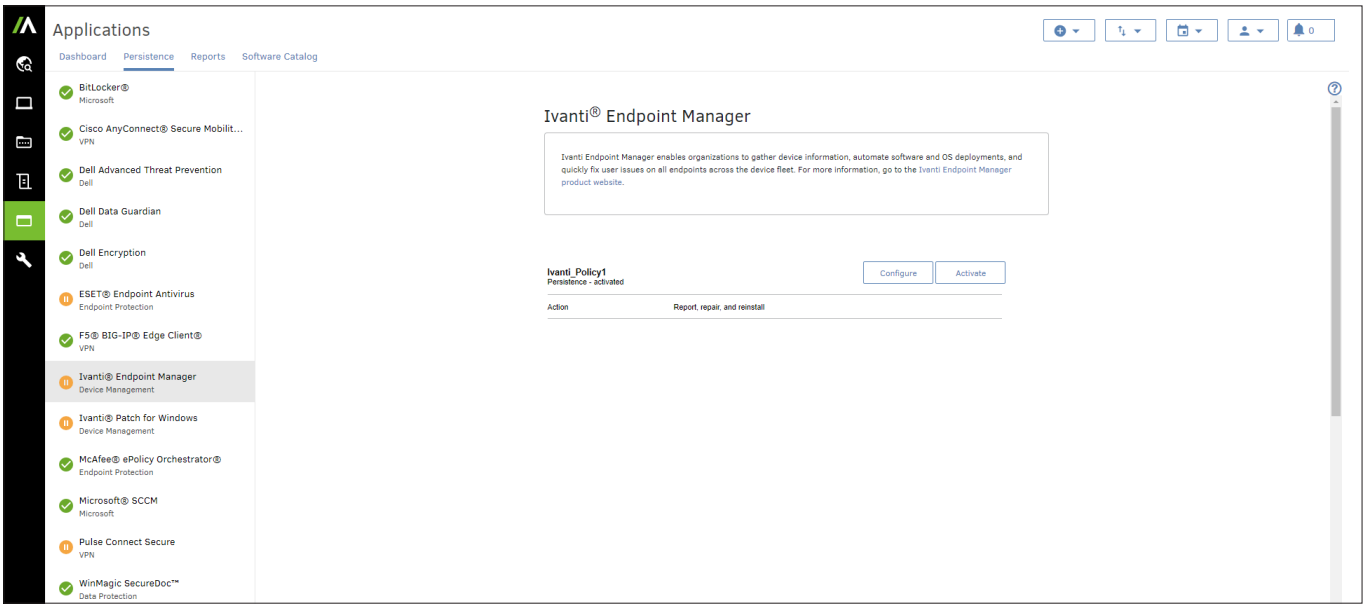
Having created a device policy group and subscribed to one or more Application Persistence modules, the persistence of a listed application can be configured using any one of the two following processes.

Process 1:

After logging into the Absolute console, click on the "Applications – Persistence and catalog" button on the left hand vertical pane, as shown below.

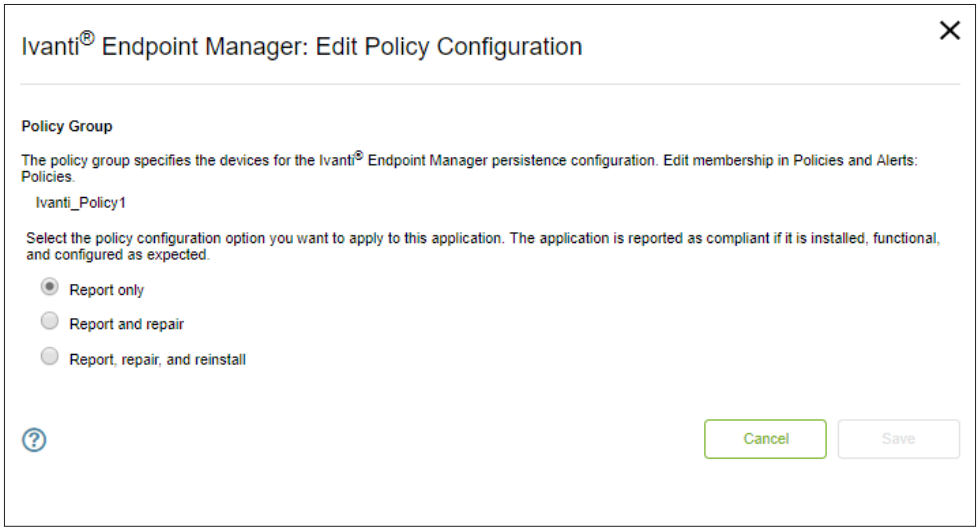


1. After reaching the Application Persistence landing page, click on the application you wish to configure in the list on the left hand side, below the "Persistence" tab. As an example, the images below illustrate how to configure the persistence for the Ivanti® Endpoint Manager, which is available through the Application Persistence for Device Management module. Click on the "Configure" button next to the device policy for which the application's persistence will be assigned.

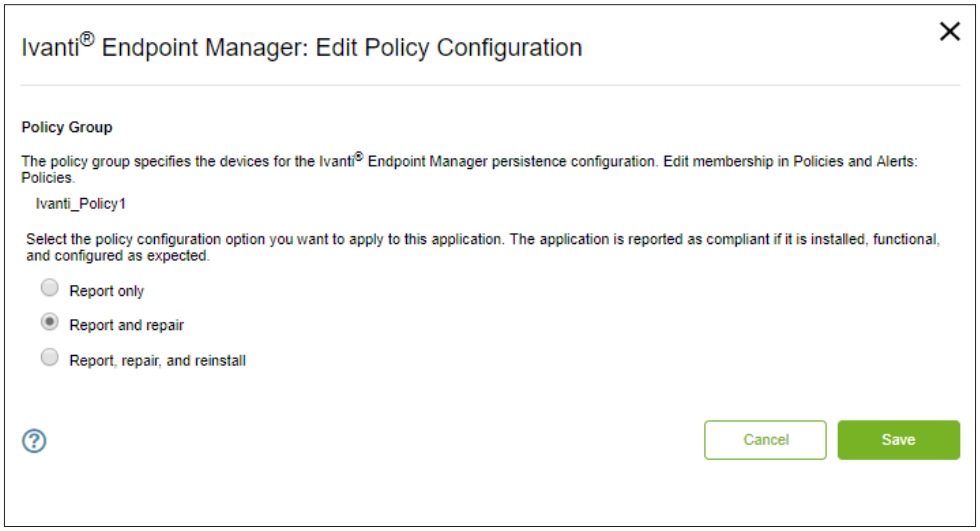


2. Once the "Edit Policy Configuration" window appears, select one of "Report", "Report and Repair" or "Report, Repair and Reinstall" based on the necessary depth of the application remediation in cases of non-compliance.

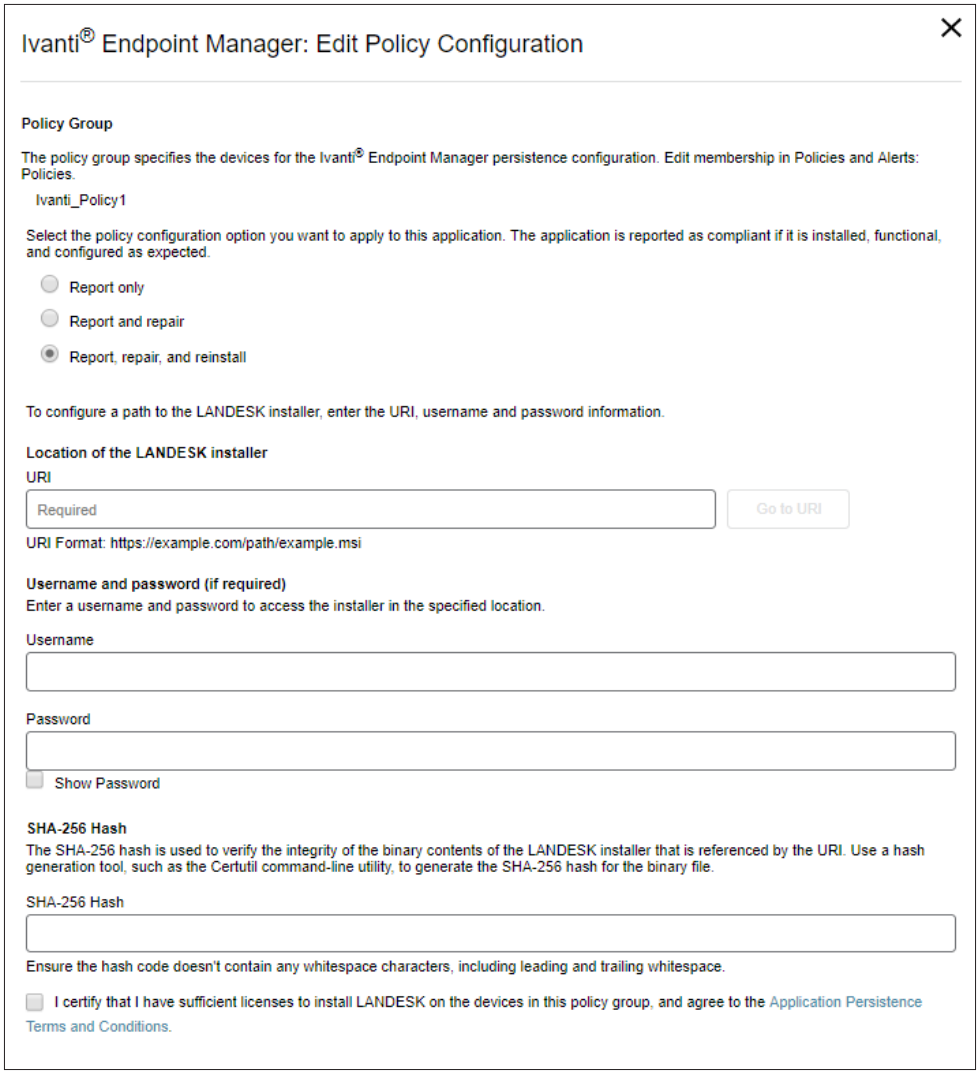
   a. Report Only



b. Report and Repair



c. Report, Repair and Reinstall

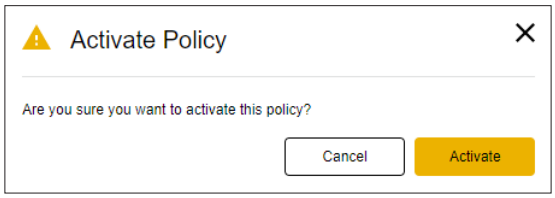


If "Report, Repair and Reinstall" is selected, provide a URI path from where the AP engine would download the application's installer. The administrator has the option of securing the path through authentication and specifying a username and password for the AP engine to access the installer. Additionally, the administrator has to provide a SHA-256 hash corresponding to the binary components of the installer for the AP engine to confirm the installer's identity.

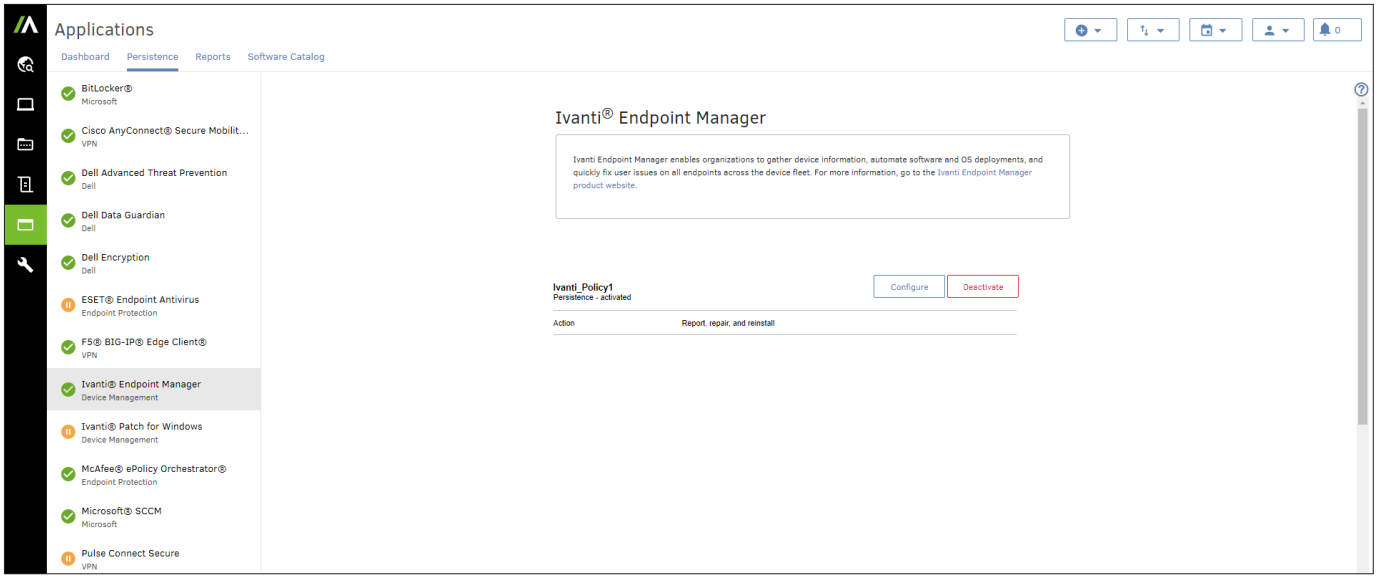
Once the URI, the username and password (if required) and the SHA-256 hash are specified, read through the "Application Persistence Terms and Conditions", click on the box next to the "I certify..." sentence on the bottom of the window to certify that you have read and agree with the terms and conditions, and click "Save".

Note: If the "Save" button is greyed out, make sure that you have specified the URI path and the SHA-256 hash in the correct format.

3. Once the "Activate Policy" window appears, click on the orange "Activate" button to activate the persistence of the application for the specific assigned policy group.



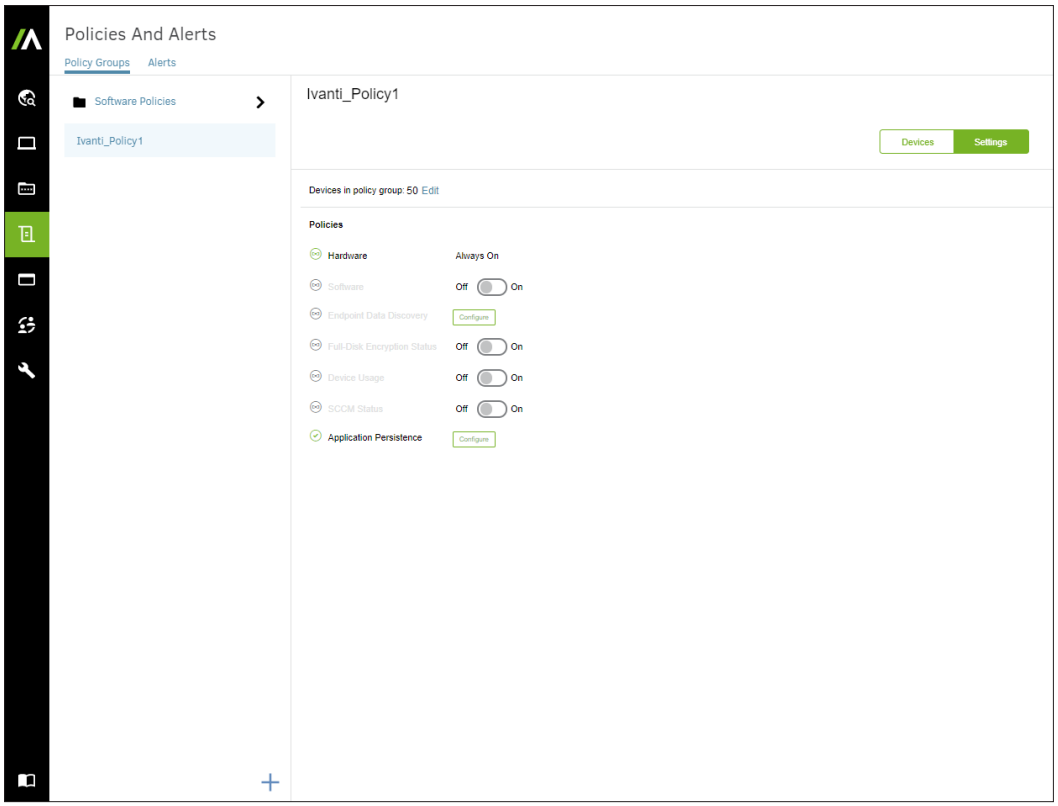
4. Once the persistence for the application is configured successfully, the appropriate policy group will be displayed as being "Activated" on the Application Persistence landing, as shown below. Additionally, in the list of applications below the "Persistence" tab, a green tick indicator will be displayed next to the name of the application whose persistence was configured (i.e. Ivanti® Endpoint Manager in the image below).



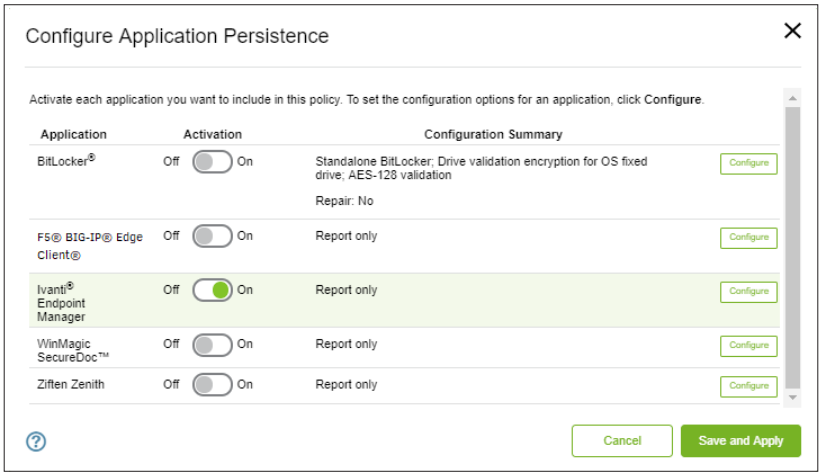
Note: Alternatively, the user can also configure the persistence of an application through the "Policies and Alerts" page, as described below.

Process 2:

1. Click on the "Policies and Alerts – Data Collection and notification" button on the left side vertical pane to get to the following "Policies and Alerts" page. Click on the "configure" button next to "Application Persistence" to select an application to configure.



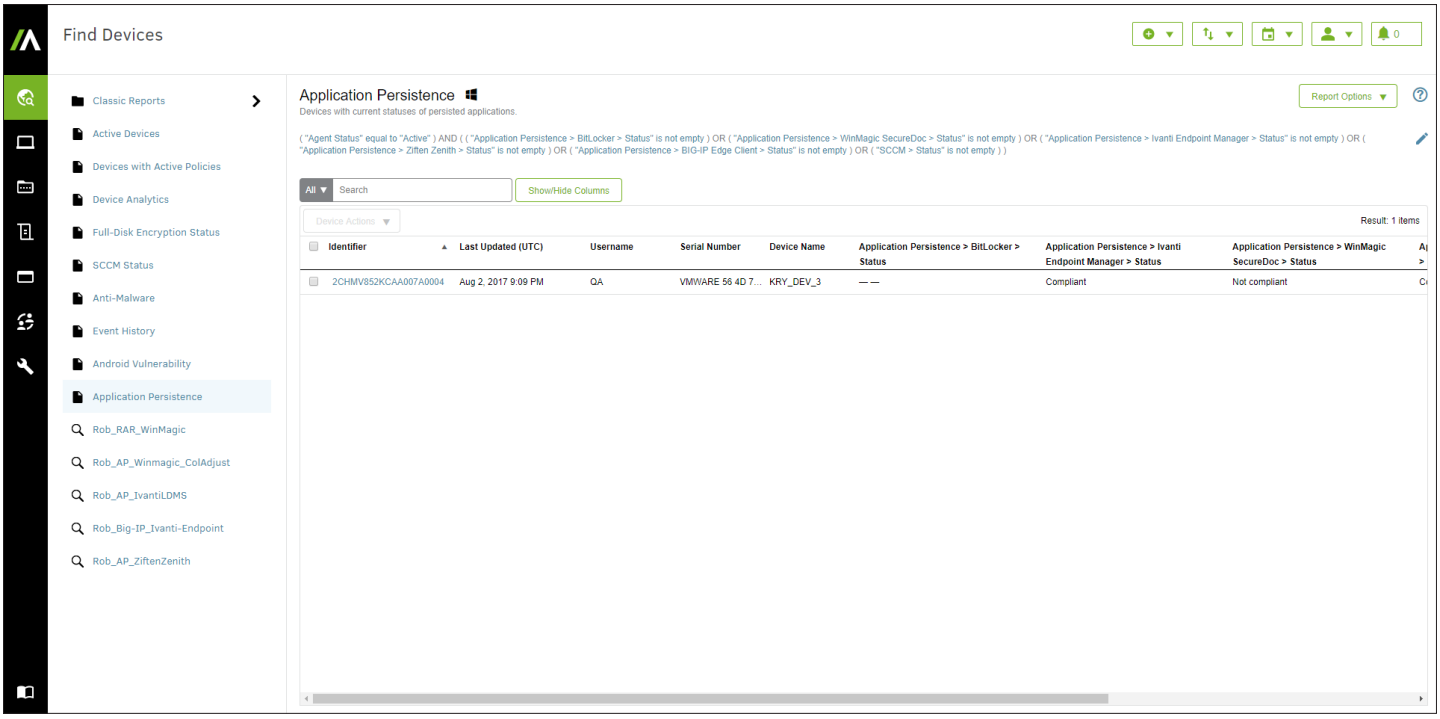
2. Click on the corresponding "configure" button next to the application you wish to configure in the window shown below.



3. The remaining steps are the same as in Process 1. Hence, follow steps 3-5 in Process 1 to configure the persistence of an application to a policy group.

APPLICATION PERSISTENCE REPORTING:

The administrator can view Application Persistence related reports by selecting the "Find Devices – Find and report on hardware" button on the left hand vertical pane. Next, select the "Application Persistence" option on the "Find Devices" page, as shown in the image below.



The "Application Persistence" report provides a snapshot of the compliance status for all the applications available to be persisted. It includes the following default column fields.

COLUMN FIELD	DESCRIPTION	POSSIBLE VALUES
Identifier	The unique Electronic Serial Number (ESN) assigned to the Absolute agent that is installed on a device.	N/A
Last Updated (UTC)	The date and time (in UTC) a device's hardware information was last updated in the Absolute database.	E.g. Aug 2, 2017 9:09 PM
Username	The username associated with the user who was logged into the device when a connection between the Absolute agent and the device occurred.	N/A
Serial Number	The identification number assigned to the device by the device manufacturer.	N/A
Device Name	The name assigned to the device in the operating system.	N/A

COLUMN FIELD	DESCRIPTION	POSSIBLE VALUES
Application Persistence › [Application Name] › Status [**Note:** In the default "Application Persistence" report, there is a separate column for each application that can be persisted.]	The last detected compliance status of the application.	• **Compliant:** Application is functioning correctly. • **Non-compliant:** Application's configurations (e.g. services, registry files, etc.) do not comply with what is constituted as being healthy. • **Error:** An unexpected error occurred while the application status check was running on the device. Status information was not uploaded. • **Unknown:** unable to accurately detect the status of the application. • **Pending Scan Results:** Either the first AP scan is yet to take place or the scan results has not reached the Absolute server yet. • **Not Activated:** An AP policy for the application is no longer active on this device.

Additionally, the user has the option of creating and saving a custom report by clicking on the "Show/Hide Columns" button, selecting the necessary fields to be displayed for any application that is being persisted and selecting "Save As" under the "Report Options" drop down menu. For each application that can be persisted, users have the option of selecting one or more of the following Application Persistence specific column fields, listed in the table below.

COLUMN FIELD	DESCRIPTION	POSSIBLE VALUES
Application Persistence › [Application Name] › Last Updated (UTC)	The date and time (in UTC) the results of the application's status check were made available in the Absolute console. [**Note:** This is different from the "Last Updated (UTC)" column displayed in the default "Application Persistence" Report.]	E.g. Aug 2, 2017 9:09 PM
Application Persistence › [Application Name] › Repair Status	The status of any attempted repairs.	• **Success:** all attempted repairs were successful. • **Failure:** the device has a status of Non-compliant and the attempted repairs were unsuccessful. • **Repair disabled:** The Report only option is selected for the application, so no repairs were attempted. • **No repairs:** the device has a status of Compliant, so no repairs were attempted.
Application Persistence › [Application Name] › Status	The last detected compliance status of the application.	• **Compliant:** Application is functioning correctly. • **Non-compliant:** Application's configurations (e.g. services, registry files, etc.) do not comply with what is constituted as being healthy. • **Error:** An unexpected error occurred while the application status check was running on the device. Status information was not uploaded. • **Unknown:** unable to accurately detect the status of the application. • **Pending Scan Results:** Either the first AP scan is yet to take place or the scan results has not reached the Absolute server yet. • **Not Activated:** An AP policy for the application is no longer active on this device.

COLUMN FIELD	DESCRIPTION	POSSIBLE VALUES
Application Persistence › [Application Name] › Status Checked (UTC)	The date and time (in UTC), the AP engine checked the application's status on the device.	E.g. Aug 2, 2017 9:09 PM
Application Persistence › [Application Name] › Status Details	Lists additional details regarding the detected status of the application on the device.	• **For Compliant instances:** two emdashes (— —) denotes the application being compliant on the device. However, if the Absolute agent recently performed a repair or reinstall of the application, and the client is now Compliant as a result, the details of that status change will be listed in the column. • **For Non-compliant instances:** this column lists details about the specific components of the application that were checked. If either "Report and Repair" or "Report, Repair and Reinstall" was selected during activation, the column shows details about the repairs that were attempted.

To learn more about Application Persistence visit: **absolute.com/products/application-persistence**