APPLICATION PERSISTENCE

FREQUENTLY ASKED QUESTIONS

This FAQ provides answers to questions you may have regarding Application Persistence.

GENERAL INFORMATION

What is Application Persistence?
Application Persistence is a unique self-healing capability for third party applications that is part of the **Absolute platform**. Application Persistence leverages Absolute **Persistence**®, technology already in embedded in over 1 Billion devices, to remotely remediate an application, making it resilient whether it is uninstalled, disabled or corrupted.

As a result, the endpoint becomes self-healing. Application Persistence is currently available to the security industry ecosystem, including enterprises, security vendors and OEMs worldwide. Organizations of all sizes have already taken advantage of this technology to self-heal critical applications such as VPN, endpoint protection, device management, data protection and other internal business-critical applications.

How does Application Persistence work?
In order for this solution to be implemented, the Absolute agent must be installed on each endpoint to activate Persistence. Based on the specific software application to be persisted and the policy determined by the administrator, the Absolute solution deploys policy files to the device to support the automatic, zero-touch reinstallation. Once setup is complete, Persistence will reinstall the software application agent whenever it is removed from a device or tampered with. Here is how it works:

1. The device calls into the Absolute Monitoring Center on a regular basis.
2. A custom agent script is retrieved and executed on the device.
3. An XML policy file, configured specifically, is downloaded to the device.
4. This policy file validates specified pre-deployment conditions (e.g. device type, operating system, device group):
    a. If conditions are met, the correct application is already present on the device.
    b. If conditions are not met, the application components are downloaded and installed as per policy file.

What actions does Application Persistence take to remediate a non-compliant application?
The remediation actions that the Application Persistence (AP) engine takes in cases of application non-compliance can be summarized by the three following options. The administrator can choose any one of the three options when configuring the application policies within the Absolute console.

- **Report only:** Every 6 hours, the AP engine runs health checks on the endpoint to determine 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 sends the compliance status back to the Absolute Monitoring Center.

- **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. For a detailed explanation on Application Persistence in action, view the **Application Persistence Technote**

PRODUCT

What platforms are supported?
Currently, Application Persistence is supported on devices running Windows 7 and higher. Android devices, including those with Persistence technology embedded, are not currently supported. The Absolute team continues to investigate methods to extend this capability to other desktop, laptop and mobile platforms.

How is Application Persistence offered?
Application Persistence is available for all supported applications through an Absolute subscription. Application health reporting is available through Absolute Visibility or Control, while application remediation is available with Resilience.

Is there a list of supported applications?
The list of supported applications available can be obtained from an Absolute Sales representative. The Absolute team continues to add new applications to the list on a quarterly basis. For a list of vendors, please visit: **absolute.com/application-persistence**

What if my organization needs to self-heal an application that is currently not supported?
If your organization is interested in self-healing an application that is currently not listed in any of the modules, Absolute's Professional Services team can implement its persistence as a custom SLA offering. The team can configure the self-healing of any application, including custom or internal apps with any specific requirements you may have.

How is the self-healing capabilites of an application configured?
The administrator can configure the the applications directly within the Absolute console. This process is described in detail in the Application Persistence Technote.

What happens when a Windows device is wiped? Does it automatically reinstall the application?
If the firmware is flashed, the device is re-imaged or the hard-drive is replaced the application will automatically reinstall as soon as the device has an internet connection.

Can Application Persistence be limited to selected machines?
Yes, the administrator can assign selected machines to a custom policy group and configure the application self-healing capabilites specifically for that policy group. Once configured, an XML configuration file will be downloaded to the assigned endpoint devices to ensure Application Persistence is run only on those machines.

Does Application Persistence support virtual machines?
Application Persistence can install an application to a virtual machine as long as the virtual machine has access to the internet and has Windows 7 or higher deployed.

How are application version updates/upgrades managed?
Anytime a new version of an application is available, the administrator has the option of upgrading the application across the device fleet as long as this new version is supported through Application Persistence or after an engagement with Absolute's Professional Services team. This can be done by assigning selected (or all) devices to a new policy group, specific to the new version.

If an endpoint user manually upgrades the application on their device to a version that is not currently configured by the IT administrator, Application Persistence will not decrement the application's version to the previous, supported version. It will simply notify the administrator that the specific endpoint has a newer version of the application installed. It is then up to the administrator to manually take action, if necessary.

Can Application Persistence be used in reverse? For example, can it help recognize unwanted apps and persist their de-installation?
Yes, Application Persistence can be used to 'persistently uninstall' unwanted software. This use case is a separate and distinct custom service offering available only through an engagement with Absolute's Professional Services team. Contact the **Absolute Professional Service team** for more information on customized services.

INFRASTRUCTURE

Where can the application's installer or specific components be hosted?
As part of the Repair remediation action, a cached MSI package of the application's installer is downloaded to the endpoint device from Absolute's data centers.

To configure the Reinstall action, the administrator must provide a URI link to a customer hosted data center from which the Application Persistence engine will download a copy of the application's installer and subsequently install the application on the endpoint device.

Specifically for engagements with Absolute's Professional Services team, the application components can be installed on a private network or within the Absolute data centers in the US or Canada. For components hosted within the Absolute data centers, Absolute will be responsible for ensuring that the hosted infrastructure is available and the correct application/version is deployed to each device.

What is the authentication method between the agent communication and the public web server?
Whilst configuring the Reinstall action, the administrator has the option of adding in user authentication to the chosen URI link and listing the set "username" and "password" to ensure the Application Persistence engine specifies this information whenever it attempts to download the installer from the URI link. Additionally, the administrator must specify a HASH-256 code for the Application Persistence engine to authenticate the downloaded installer.

What is the end-user experience when an application is installing/reinstalling?
All remediation actions are performed silently. Repairing an application will initiate the restarting of relevant application services or silently running the cached MSI installer package. Reinstalling an application will silently download the application's installer from an external source, authenticate the installer and perform a silent install on the endpoint device.

For engagements with Absolute's Professional Services team, customers have the option of changing the user experience during installation/reinstallation to suit their needs.

What level of reporting is included with Application Persistence?
Administrators can view Application Persistence related reports through the Absolute console. A default "Application Persistence" report can be viewed from the "Find devices" page through the Absolute console. This report shows the current compliance status of configured applications across different policy groups as well as specific information on remediation activity on any assigned machine.

The administrator also has the option of configuring and saving a custom report to include columns most relevant to their persistence configuration. Detailed information on Application Persistence reporting through the Absolute console can be found in the **Application Persistence Technote**.

SUBSCRIPTION & SUPPORT

What Application Persistence functionality is available with an Absolute subscription?
The following functionality is available with any Absolute license (Visibility, Control or Resilience):

- The ability to report on the health of supported applications.
- Ability to view standard or custom Application Persistence related reports listing the compliance status of all configured applications across the device fleet and detailing any application remediation activity that occurs on specific machines.

The following is available with an Absolute Resilience license only:

- The ability to remediate critical supported applications.

For engagements with Absolute's Professional Services team, the annual subscription fee includes the following:

- Business requirements definition, technical design, development, testing, deployment
- Maintenance:
  - Forward compatibility with Absolute agent updates during subscription term.
  - Up to one application version upgrade per year. If Application Persistence is used across multiple apps, this applies to one upgrade per application. Additional upgrades will require a Services engagement.
- Reports: automated daily and monthly reports
- Defects: remediation of reported issues

For more information on Application Persistence, visit: **absolute.com/application-persistence**