Absolute Application Persistence™ FAQ

GENERAL INFORMATION

What is Absolute Application Persistence™?
Absolute Application Persistence is a unique self-healing capability for third-party applications that is part of **Absolute's product offerings**. Application Persistence leverages Absolute **Persistence**® technology already in embedded in over 500 million devices, to remotely remediate an application, making it resilient whether it is uninstalled, disabled, or corrupted.

As a result, mission-critical applications running on the endpoint self-heal to maintain the endpoint's security posture. 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, as well as other security and business applications.

How does Application Persistence work?
The Absolute Agent must be installed on each endpoint to activate Application 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 remediation. Once setup is completed, Application Persistence will repair or reinstall the software agent and other critical application components whenever they are removed or tampered with on a device. Here is how it works:

1. The device calls into the Absolute Monitoring Center every 15 minutes.
2. A custom agent script is retrieved and executed on the device.
3. Whenever an Application Persistence policy is activated or updated through the Absolute Console, 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 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 15 minutes, the Application Persistence 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, as well as if the application's services are running smoothly. The Application Persistence engine sends the application's health status back to the Absolute Monitoring Center. Payloads are sent whenever application health changes occur between scans or at a minimum once every 6 hours whenever no changes take place.
- **Report and Repair:** If the Application Persistence 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, primary agent and remediating corrupted registry files.

- **Report, Repair, and Reinstall:** If the Repair phase fails to remediate the application, the Application Persistence engine will attempt to download the application's installer from a pre-set URI on a customer-hosted web server, or from Absolute's cloud servers, if a customer chooses for Absolute to host the installer on their behalf as part of the Application Persistence configuration. 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.

PRODUCT

What platforms are supported?
Currently, Application Persistence is supported on devices running Windows 7 and higher. 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 Absolute 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 the following **Application Persistence product page**.

What if my organization needs to self-heal an application that is currently not supported?
Absolute is continuously adding to its library of supported applications. If you have a particular application that you would like to persist, contact **Absolute Sales** to make a request.

How is the self-healing feature configured for an application?
The administrator can configure the capability for an application directly through the Absolute Console by configuring an Application Persistence policy.

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 capabilities 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 if 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 if this new version is supported through Application Persistence. 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.

How are application version upgrades to respond to a discovered vulnerability handled?
If the specific application version is supported you can select this version through the Application Persistence Configuration window for the application through the Absolute console. If the version is not supported yet, get in touch with your Absolute Sales Account Executive to request support for it.

How does Absolute support the release of newer version of applications?
Absolute engages in Application Persistence partnerships with independent software vendors (ISV) to ensure the latest versions of their applications are supported via Application Persistence soon after they are released by the ISV. If you have a specific version of an app you'd like to persist, reach out to your Absolute Sales Account Executive.

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 can 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.

Alternatively, for certain supported applications, customers can choose to let Absolute host the application's installer on their behalf by uploading the installer file through the Application Persistence configuration window via the Absolute Console. View the **Absolute Help** for details regarding the applications on which installer hosting via Absolute is supported.

What security processes does Absolute have in place with respect to hosting application installers and other components as part of the Application Persistence reinstall function?
Absolute's products are developed through comprehensive security processes and a robust architecture. An Application Persistence Report, Repair and Reinstall policy includes the following security practices as part of the offering:

- The download URL of where the application is hosted is encrypted on the XML Application Persistence policy file.
- The download URL is protected by a signature
- The SHA 256 hash code is compared at download against the hash code referenced when the installer is uploaded.

What is the authentication method between the agent communication and the customer 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. In addition, the administrator must specify a SHA-256 hash 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 includes, but is not limited to, restarting relevant application services, the application's primary agent and fixing corrupted registry files. Reinstalling an application will silently download the application's installer from the customer's or Absolute's web server,

authenticate the installer, and perform a silent install on the endpoint device.

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 Reports section through the Absolute Console. This report shows the current health status of configured applications across different policy groups, as well as specific information on remediation activity on any assigned device. The administrator also has the option of configuring and saving a custom report to include columns most relevant to their persistence configuration.

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