Absolute Persistence

Absolute Persistence

FREQUENTLY ASKED QUESTIONS

Absolute Persistence® is factory-embedded into the core of most endpoint devices. Once activated, it gives you unrivalled visibility and control to confidently manage your endpoints, protect at-risk data, investigate and remediate potential threats. Persistence is the only firmware-embedded solution that will survive attempts to disable it, even if the device is reimaged, the hard drive is replaced or the firmware is flashed.

Through our partnership with device manufacturers (OEMs), the Persistence module is embedded in the firmware of endpoint devices at the factory. Persistence leverages Absolute's Secure Channel from the cloud-based console down to the firmware. In doing so, it maintains an undeleteable tether between device and console, ensuring two-way communication so you can reliably query information and run actions remotely.

Persistence remains dormant in the firmware until the Absolute agent is installed. Once the agent is installed, it initiates a call to the Absolute Monitoring Center and Persistence is activated. This means that the status of the software agent is monitored and if it is missing, a reinstallation will automatically occur.

NOTE: There is a vast array of form factors on the market today. In order to support this reality, the technical details of Persistence may vary based on operating system and device. The purpose of this FAQ is to provide a high level understanding of Persistence. For details about specific devices and operating systems, contact your Absolute sales representative.

What is the Persistence module?
The Persistence module is installed in the firmware of most endpoint devices at the factory. Each device leaves the factory with the Persistence module in place, waiting to be activated. Activation occurs when a customer purchases an Absolute product that supports Persistence and installs the necessary software agent.

Which Absolute products support Persistence?
All Absolute products support Persistence. The software agent is installed on computers in the operating system by running an installer or when the device is imaged. The software agent sends information from each device to the Absolute platform for IT administrators and security professionals to risk assess and to take appropriate action.

The Absolute agent makes regularly scheduled calls over the internet to the Absolute Monitoring Center, where customers access their account via the cloud-based Absolute console. Telemetry collected includes device, data, application and user information. Customers can define conditions and receive alerts if the conditions occur, allowing them to respond immediately to any potential security incident. The software agent also supports remote actions such as the running of scripts through **Absolute Reach** and self-healing of critical security applications through **Application Persistence**.

For more information about specific Absolute features, view the **Resources section** on the Absolute website.

NOTE: Features will vary based on the product version, form factor, and device operating system.

How does the Persistence module become embedded into the firmware of a device?
Through our partnership with leading hardware manufacturers, the Persistence module is embedded in most devices during assembly at the factory.

On which manufacturer devices is the Persistence module embedded?
A current list of all devices manufactured with Persistence embedded in the firmware is available on **absolute.com**.

If a device has the Persistence module embedded into the firmware, is it already protected?
No. Even though the Persistence module is built into the device, it still requires activation by installing the Absolute agent. Once installed, the first call from the software agent to the Absolute Monitoring Center will detect and enable the Persistence module. Once enabled, the self-healing feature of the Persistence module in the device will initiate the reinstallation of the software agent if it is removed.

What additional configurations are required for Absolute Persistence to work?
The Persistence module is embedded into the firmware of the device. Once the software agent is installed, there is no additional configuration needed for Persistence to work.

What is Application Persistence?
Application Persistence leverages Absolute Persistence® technology to remotely and instantly remediate an application, making it self-healing and resilient — whether it is uninstalled, disabled, or the registry file is 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 in the healthcare, financial services, pharmaceuticals and manufacturing industries have already integrated this technology into their applications, including VPN, anti-virus/anti-malware, endpoint protection, encryption, data loss prevention, device management, internal business-critical applications, etc.

What happens if the BIOS is flashed on a computer? Will the Absolute agent need to be reinstalled?
No. If the Persistence module has been enabled, the self-healing capability will repair the Absolute agent or any other applications supported by Application Persistence. The computer will still be protected. The enable/disable state of the Persistence module is stored in a part of the BIOS that cannot be flashed to remove it.

Will Persistence continue to work if the computer undergoes an IMAC (install/move/add/change) process such as replacing a hard drive?
Yes. The self-healing capability will survive IMAC procedures such as imaging, hard drive replacement or operating system changes.

ABSOLUTE PLATFORM AGENT

Since Persistence relies on the presence of the Absolute platform agent, how easily can it be detected?
The software agent is tamper-resistant and difficult to detect. It runs as a non-descript service and is not listed as an application, nor does it show up on the programs menu listing or as a system tray icon.

What type of protection is provided for communication between the Absolute agent and the Absolute Monitoring Center?
The communication between the software agent and the Absolute Monitoring Center is encrypted. Optionally, you can also enable FIPS-140 certified communication.

The Federal Information Processing Standard (FIPS) Publication 140-2 is a US government security standard that specifies the security requirements for cryptographic modules protecting sensitive information. The National Institutes of Standards and Technology (NIST) publishes the list of vendors with validated FIPS 140-1 and 140-2 cryptographic modules.

The Absolute Encryption Engine is validated FIPS 140-2 and the certificate can be viewed here: Certificate 1680.

What is the footprint, or size, of the Absolute agent?
The Absolute agent has a very small footprint, requiring less than 200Kb of disk space. It occupies a small amount of memory when idle, and when placing a call the software agent optimizes data transfer, which means a very low demand is placed on the network.

What if an unauthorized user still manages to remove the Absolute agent?
The Persistence module embedded in the device will simply trigger a reinstallation of the Absolute agent. This self-healing feature can repair the agent or other third-party applications supported by Application Persistence in newly formatted and installed operating systems as well as freshly imaged systems.

What if the Absolute agent needs to be removed from a device?
IT administrators that have been authorized to do so, may carry out this function themselves within the Absolute console.

For more information contact your **Absolute sales representative**.