ABSOLUTE REACH FAQ

FREQUENTLY ASKED QUESTIONS

This FAQ provides answers to questions regarding **Absolute Reach**.

The Absolute platform features the innovative new capabilities of Reach, providing the incredible flexibility to see, manage and secure every endpoint, everywhere with the power to assess and take remedial action across 100% of your Windows and Mac devices in just a few clicks, regardless of user or location.

Reach leverages Persistence® technology, already embedded in the firmware of over a billion popular endpoint devices, for highly assured IT asset management, self-healing endpoint security and data visibility and protection. With Reach, no endpoint device under your management will ever go dark.

Gather precise insights or execute custom workflow and task automation commands to remediate dark endpoints, ransomware attacks, and other endpoint vulnerabilities and receive confirmation that the action has been performed successfully. With virtually endless query and remediation options, this powerful tool allows asset managers and security professionals to proactively expand emerging endpoint management and security use cases.

GENERAL INFORMATION

Absolute Reach is a powerful new custom query and remediation feature of the **Absolute platform.** Available with **Absolute Resilience** (formerly Premium), Reach gives you the power to detect, understand, and remediate vulnerabilities across 100% of your endpoints on-demand, even if your endpoints are off the corporate network.

Initially, Absolute Reach will allow you to upload and execute custom scripts to achieve deep visibility and control over any device, on or off network.

Query a device to gather and retrieve custom data points. These would include data points that are not traditionally collected by the Absolute agent, but are of unique importance to each organization. Data points collected can then be incorporated into custom reports as part of regular reporting capabilities.

Remediate and take immediate action on at-risk or suspicious devices. Remediation commands can be used for any number of asset management or security use cases, from minor tasks to mission-critical remediation of device vulnerabilities.

In subsequent releases, Absolute will add libraries from which users can select **prebuilt scripts** and **schedule script executions**. As the number of customers using Absolute Reach grows, Absolute will launch the **Absolute Script Community**, where users can share and reference scripts created by their peers, and stringently verified by Absolute, to solve common query and remediation use cases.

Why is Absolute Reach such a significant new capability?

This firmly places Absolute as the standard for Endpoint Visibility & Control. These innovative new capabilities give you an endless number of options when it comes to managing and securing your endpoints. IT professionals can reach out to any device, at any time, and execute a script, receiving confirmation that the action has been performed successfully.

For example, if a new threat appears, IT professionals can quickly develop or leverage an existing script, and rapidly deploy it to critical devices. No longer do organizations have to wait for vendors to develop a feature to address this

new threat. Leverage the power of Absolute's Persistence technology to reach out to any device and perform a specific action. This varies from something mundane such as changing a screensaver or desktop background, to more critical actions such as stopping malicious processes or closing vulnerable ports.

PRODUCT INFORMATION

What are the key capabilities of Absolute Reach?
Absolute Reach offers an unbreakable connection to every device for real-time visibility you can act on to rapidly remediate new vulnerabilities and regain compliance anytime, anywhere, on any endpoint. With Reach, you can execute any script across any of your devices with a script once, deploy anywhere model.

Quickly upload any script, and target specific devices to execute a command. Include with this specific conditions for the script to be performed (e.g. the script could run silently on the device or be set with a maximum run time of 30 minutes, which is important when executing scripts over a large population of devices). Each query or remediation command is supported by these customizable guardrails to ensure every script is executed under the conditions you determine.

Finally, validate that the script was successfully delivered and executed in scenarios where proof of compliance is critical.

What IT and security problems does this solve?
This solves a number of problems and use cases:

- Unlock device port
- Re-enable processes/services
- Rejoin device to domain
- Software audit
- Run Windows update
- Install MSI
- Add/Remove printer
- Get event log
- Contain/Isolate device
- Remove admin privileges
- Reset local admin password
- Restart computer
- Disable services
- List installed Windows hotfixes
- Run local tools (Disk Cleanup Wizard)
- Identify devices with a faulty driver installed

What are examples of significant security vulnerabilities that Reach can help address?
Following are two real-life security use cases that Absolute Reach can help address:

Problem: Devices in fleet susceptible to Shadow Brokers vulnerabilities or WannaCry
Solution: Identify the exact patch level of the Windows OS for each device in the fleet and determine vulnerability
Identify devices susceptible to **vulnerabilities** in the Microsoft SMB Service and turn off service if not patched
Identify vulnerable devices also out of hard drive space causing the security patch installation to fail

Problem: Devices in fleet susceptible to Intel AMT Critical Firmware Vulnerability
Solution: Run Intel utility on the client, "scrape" the resulting information from the screen and store as attributes to determine device vulnerability

What platforms and scripting languages does Absolute Reach support (Windows, Mac and Linux)?
Absolute Reach supports both Windows and Mac devices, with the popular Powershell and Bash scripting languages. Linux is not currently supported.

What happens when a script execution fails?
Absolute can ensure the script 'reaches' the device with a status confirmation of both successful and failed attempts.

Does Absolute Reach require connection to the corporate network to be effective?
No, Absolute Reach does not have any dependencies on the corporate network. All that is required is an internet connection. In some exceptional cases (e.g. downloading an MSI from a network location), a network connection will be required.

How is Absolute Reach different from existing scripting solutions?
Generally, existing solutions on the market are limited to devices that are accessible (generally on network and healthy agent), but this is often not the case when a vulnerability has occurred. By contrast. Absolute is firmware-embedded, self-healing and always-connected to endpoints with an efficient and direct, point-to-point tether to every device, on and off the network.

Solutions such as Microsoft Active Directory Group Policies (GPO) rely on a device being on network and are unable to return confirmation that a script has been executed, which is critical to prove compliance.

Other solutions offer off-network visibility to remediate, but this first requires customers to invest in additional on-premise infrastructure. Additionally, their visibility and off-network connection is challenged if their agent ever becomes compromised.

With Absolute, it doesn't matter where the device is, whether it is connected to the network or if attempts are made to remove the Absolute agent. We can automatically self-heal our agent to restore connectivity and return to a position of full visibility and control so no device is ever out of reach. Absolute can ensure the script 'reaches' the device and is executed, giving assurance in risk response or compliance scenarios. Finally, Absolute Reach requires no additional infrastructure.

How does Absolute ensure the script is not caught and blocked by an anti-virus/anti-malware client?
Before a script can be executed, customers can choose to sign it with their own certificate and register this certificate with their anti-virus/malware solution. This is highly recommended to prevent EDR solutions from blocking it. Once complete, the signed script can be uploaded and used to target specific devices.

How does Absolute ensure the validity, quality and safety of scripts shared in the Absolute Script Community?
Absolute inspects and scrutinizes every script before being published to the community and also performs sandbox testing before it receives the necessary approval for use by the wider community. In addition, we do not permit the use of scripts that pull/install from third-party URLs. Finally, all submissions are from verified Absolute customer accounts, ensuring only members familiar to Absolute are permitted to contribute to this community.

What controls exist to prevent someone with privileges to take advantage of this powerful scripting tool and execute a malicious attack on the organization?
As the saying goes, "with great power, comes great responsibility". Although this statement rings true for Absolute Reach, it is no different for comparable solutions like Microsoft Active Directory's Global Policies (GPO) or even a competing scripting solution.

Regardless of the tool, the current assignment of privileges to admin members of their organization would look almost identical to what would be assigned with Absolute Reach. They are simply different tools.
The most significant difference is that Absolute provides uncompromised visibility, control and an unbreakable connection with our self-healing capabilities to more successfully execute scripts to the same devices and confirm delivery.

That being said, Absolute recognizes the significance of this particular feature and offers **Role-based Access Control (RBAC)** to further protect the organization from unwanted privileged user actions, malicious or not. RBAC allows organizations to set granular permissions based on a user's role within the organization. This is to ensure that no user is provided controls above and beyond what their responsibilities would dictate they require. This also provides the organization with a degree of protection with a hierarchy of functions that map back to designated roles within the company.

In addition to role-based permissions, the flexibility of Absolute's RBAC supports granting users with admin privileges or a scope of control that limits them to only certain devices. Organizations may also invoke a separation of duties to ensure that no one person can perform all functions:

- Role A may create but not execute a script
- Role B may execute but not create scripts
- Role C may create and execute, but only on a group of devices

Visit www.absolute.com/reach for more information.