**To install the Agent on a Windows endpoint:**

1. Get the site or group token. For more information, see [Getting a Site or Group Token](https://apse1-2001.sentinelone.net/docs/en/getting-a-site-or-group-token.html).
2. In the **Sentinels** toolbar, click **Packages**.



1. Download the applicable Windows Installer package.

A hand cursor and a button

Description automatically generated

Make sure the **Access Level**  of the package includes the Site that the Agent will go to.

A screenshot of a computer

Description automatically generated

1. Run the installer package and follow the instructions.

* To install with the interactive GUI wizard:

Run the installation package and enter the Site or Group Token when prompted in the installation wizard.

A screenshot of a computer error

Description automatically generated

* To install silently without user interaction:

In a command prompt run as administrator, run the installer with switches for the token and silent installation. Example for EXE packages: C:\Users\S1\Desktop\Sentinel\SentinelInstaller.exe /SITE\_TOKEN=<site\_Token or group\_Token> /quiet

Example for MSI packages: C:\Users\S1\Desktop\Sentinel\SentinelInstaller.msi SITE\_TOKEN=<site\_Token or group\_Token> /QUIET

Tip: Add /NORESTART to prevent a forced reboot

1. Complete the installation:

In Windows Agent 22.1 and later, most Agent functionality is operational after installation, even if you do not reboot the endpoint. This includes Static AI detection, Deep Visibility™, all Agent menu actions, and all response functions. The Behavioral AI detection and mitigation capability requires a reboot. For earlier Agent versions, most Agent functionality cannot be guaranteed without a reboot.

 The Behavioral AI mode becomes active after you or the end user restart the endpoint. In the Management Console, the endpoint status remains **Pending Reboot** until it restarts.

**Important for all endpoints:**  We recommend that you enhance endpoint security with protection against physical theft and hacking (such as unauthorized disk mount modification). Enable full disk encryption, apply OS patches, and maintain measures according to your vendor recommendations and corporate policies.