Recast

# Validate Authenticode Signature with PowerShell

Last Modified on 02.03.26

You can verify the authenticity of downloaded Recast Software installation files by running a PowerShell command that checks that the Windows installer (for example, .msi) is signed by a trusted publisher and shows no signs of tampering. The command compares the signed SHA256 against the SHA256 of the file to ensure that it was signed by a valid certificate authority.

To validate the Authenticode Signature, run the following PowerShell command against the file: `Get-AuthenticodeSignature '<Path_To_Downloaded_File`. The Recast Software Certificate Thumbprint is `5F503B4667889944234BDD808AE38689A892F1F4`. All installer files will be signed with this certificate thumbprint.

Example:

```
$sig = Get-AuthenticodeSignature '.\Recast Console Extension.msi'
If ($sig.status -eq 'Valid' -and $sig.SignerCertificate.Thumbprint -eq "5F503B4667889944234BDD808AE38689A892F1F4") {
    Return $true
} else {
    Return $false
}
```

PowerShell will return the Status and the SignerCertificate thumbprint:

- If the **Status** is **Valid**, the file's signature is intact and chains to a trusted root.
- If you see **NotSigned**, **UnknownError**, or **HashMismatch**, do not deploy the file.

You can cross-check the validity of the installer files in File Explorer by right-clicking the file and selecting **Properties**. On the **Digital Signatures** tab, ensure the publisher and timestamp look correct then open the **Details** tab if you need the certificate chain.