How To Solve an Invalid Signature Error

Found in: Windows 21.7.6

Problem:

Invalid signature error.

Background:

Windows certificate updates needed.

Possible causes:

- This group policy setting[https://admx.help/?
 Category=Windows_10_2016&Policy=Microsoft.Policies.InternetCommunicationManagement::
 CertMgr_DisableAutoRootUpdates] blocks auth root updates.
- Access to the auth root update URL is blocked by the corporate firewall. Access to *ctldl.windowsupdate.com* must be unblocked for the facility to work.

Required Certificates:

Currently, the Agent requires these root certificates:

- Microsoft Azure Code Signing (ACS) root To install, we recommend you have patches newer than those mentioned here[https://support.microsoft.com/engb/topic/kb5022661-windows-support-for-the-azure-code-signing-program-4b505a31-fa1e-4ea6-85dd-6630229e8ef4],
- **DigiCert root** To install, ensure you are synchronized with the latest certificate trust lists and certificate revocation lists.

Configure a network share to grab certificate updates in firewalled and offline scenarios (see Microsoft instructions[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/dn265983(v=ws.11)]).

Alternate Solution:

Update certificates from the auth root update site on Windows 10. Run:

certutil -verifyCTL -f AuthRootWU
certutil -verifyCTL -f DisallowedWU
certutil -verifyCTL -f PinRulesWU

If these commands do not work due to a firewall, create an SST file on one computer:

```
certutil -generateSSTFromWU C:\roots.sst
```

and then in PowerShell, import this file on the firewalled computer:

Import-Certificate -FilePath C:\roots.sst -CertStoreLocation Cert:\LocalMachine\Root

To manually install digital certificates:

If you cannot update the certificates explained in the previous methods, you can manually import them from the signed files to your local endpoint's trusted root certificate authority store.

Important

A

Installing the root certificates manually only addresses signing issues with the Agent and its installer. The Agent relies on the OS having populated roots for signature validation on software the user runs. If you do not deploy Microsoft's CTL updates, known-malicious certificates that were revoked are not revoked on your system.

1 Right click SentinelAgent.exe.

ß

ß

ß

- 2 Open Properties.
- 3 Click the **Digital Signatures** tab.

🛑 SentinelAgent Prop	erties		×
Security General	Details Compatibility	Previous Versions Digital Signatures	
Signature list]	
Name of signer:	Digest algorithm	Timestamp	
Sentinelone, Inc.	sha256	Tuesday, March 14, 2023	
SentinelOne Inc.	sha256	Tuesday, March 14, 2023	
		Details	
	ОК	Cancel Apply	

4 Select each one of the two signatures it currently has, and click **Details > View Certificate**.

)igital Signature Deta	ils 🔓	? >
General Advanced		
Digital Sig	nature Informatio signature is OK.	n
Signer information		
Name:	Sentinelone, Inc.	
E-mail:	Not available	
Signing time:	Tuesday, March 14	ł, 2023 10:30:52 PM
		View Certificate
Countersignatures		
Name of signer:	E-mail address:	Timestamp
Name of signer.		
DigiCert Timesta.	Not available	Tuesday, March 14,
DigiCert Timesta.	Not available	Tuesday, March 14,
DigiCert Timesta.	Not available	Tuesday, March 14, Details
DigiCert Timesta.	Not available	Tuesday, March 14, Details

5 Click the **Certification Path** tab to see the exact chain of certificates that is used.

Certificate	×
General Details Certification Path	
Certification path	
Sentinelone, Inc.	
View Certificate	
Certificate status:	
This certificate is OK.	
ОК	

6 Click the General tab and Install certificate.



7 Select Local Machine as the location.

🔶 🛿 🐉 Certificate Import Wizard	×
Welcome to the Certificate	e Import Wizard
This wizard helps you copy certificates, co lists from your disk to a certificate store.	ertificate trust lists, and certificate revocation
A certificate, which is issued by a certifica and contains information used to protect connections. A certificate store is the sys	ation authority, is a confirmation of your identity data or to establish secure network tem area where certificates are kept.
Store Location	
Current User	
To continue, click Next.	
	Vext Cancel

8 Select Please all certificates in the following store and click Browse.

		×
\leftarrow	F Certificate Import Wizard	
	Certificate Store	
	Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	O Automatically select the certificate store based on the type of certificate	
	Place all certificates in the following store	
	Certificate store:	
	Browse	
	Next Canc	el

9 Select Trusted Root Certification Authorities as the location for the certificate, and click OK.

Select Certificate Store	×
Select the certificate store you want to use.	
ersonal	
Trusted Root Certification Authorities	
Intermediate Certification Authorities	
Intrusted Certificates	
Show physical stores	
OK Cancel	

←	🛃 Certificate Import Wizard	×
	Certificate Store Certificate stores are system areas where certificates are kept.	
	Windows can automatically select a certificate store, or you can specify a location for the certificate.	
	Automatically select the certificate store based on the type of certificate	
	Place all certificates in the following store	
	Trusted Root Certification Authorities Browse	
	Next Cance	e

10 Click Finish.

🗧 🖉 Certificate Import Wizard	×
Completing the Certificate Import Wizard	
The certificate will be imported after you click Finish.	
You have specified the following settings:	
Certificate Store Selected by User Trusted Root Certification Authorities Content Certificate	
Finish Cance	el
Was this helpful?	



No

© SentinelOne Last modified: 10 April 2023