

## **Troubleshooting SentinelOne Agent Offline**

#### https://campus.barracuda.com/doc/35982/

Occasionally, a SentinelOne agent will read as "Offline" in the Agent UI and fail to connect to our management console. When this happens, the SOC loses visibility to any threats detected during the loss of connectivity. The endpoint will still be fully protected by the Static and Behavioral engines. However, our proprietary STAR custom rules will not be in effect.

This article covers self-troubleshooting options for communication issues between your Agents and Management.

In these tests, use the Windows command prompt with **Run as Administrator**.

- 1. Press the **Windows Start** key and type cmd.
- 2. Right-click **Command Prompt** and select **Run as administrator**.

Command Prompt	_	
App 2 3	5	Run as administrator
Apps	D	Open file location
	ᅯ	Pin to Start
Search work and web	ᅯ	Pin to taskbar
✓ cmd - See work and web r	>	
Settings (1)		
🔎 cmd < 🚺		

#### **Network Connectivity Test**

1. From an endpoint, ping the Management URL and see that it resolves. If the ping times out, but resolves to an IP address, the ping is successful.



Command Prompt

```
C:\>ping .sentinelone.net
Pinging .sentinelone.net [ ..: . . ] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Ping statistics for :
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\>
```

- 2. From the endpoint, open a browser and connect to the Management address. See if there are certificate errors.
- 3. If there are third-party anti-virus applications on the endpoint, make sure the SentinelOne Agent (specifically, the C:\Program Files\SentinelOne\ folder and all its contents) is excluded from the AV.
- 4. See if there is a proxy and if it is configured correctly.

#### **Agent Services Test**

- 1. See if Agent services are up and running. On an endpoint, run services.msc
- 2. In the window that opens, see that Sentinel services are up and running.

File Action View	Help							
Þ 🔿 📊 🔛 🛛	a 🖦 🛛 🖬 🕨 🖛 💷 🕪							
Services (Local)	Services (Local)	-						
	Sentinel Agent	Name	Description	Status	Startup Type	Log On As		
	Description: SentinelOne Endpoint Protection Agent	Secure Socket Tunneling Pr     Security Accounts Manager     Security Center     Sensor Data Service     Sensor Monitoring Service     Sensor Service	Provides su The startup The WSCSV Delivers dat Monitors va A service for	Running Running Running	Manual Automatic Automatic (D Manual (Trig Manual (Trig Manual (Trig	Local Service Local Syste Local Service Local Syste Local Service Local Syste		
		C. Sentinel Agent C. SentinelHelperService C. SentinelOne Agent Log Pro SentinelOne Static Service	SentinelOne Manage log Manage stat	Running Running	Automatic Manual Automatic Automatic	Local Syste Local Syste Local Service Local Syste		

3. See if the Agent and Monitor are running. Run these commands: > cd "C:\Program Files\SentinelOne\Sentinel Agent <latest installed version>"

(Tip: Use TAB to auto-complete the pathnames.)
> sentinelctl status





Make sure the output is not empty.

5. If one or both of these values are empty, please contact our Global SOC for further assistance.

#### SentinelOne Event Viewer

SentinelOne Agent logs are available in Windows Event Viewer on endpoints. These logs show you the SentinelOne activities on the endpoint.

- On an endpoint with a supported SentinelOne Agent, open Event Viewer (Windows key + "event").
- 2. In Event Viewer (Local), click Applications and Services Logs > SentinelOne > Operational.



File Action View Help								_
Event Viewer (Local)	Operational N	umber of events: 1,229			Acti	ions		
Custom Views Windows Logs	Level	Date and Time	Source	^	Ope	erational		-
Applications and Services Loc	(i) Information	2021-01-05 2:10:03 PM	Sentine		a	Open Saved Log		
Applications and services Loc     AESMService	(i) Information	2021-01-05 2:10:03 PM	Sentine		17	Create Custom Vie		
Hardware Events	(i) Information	2021-01-04 2:06:01 PM	Sentine		T T			
IntelAudioServiceLog	(i) Information	2021-01-04 2:06:01 PM	Sentine		I	Import Custom Vie	ew	
Internet Explorer	Error	2021-01-04 8:58:13 AM	Sentine		L	Clear Log		
Key Management Service	(i) Information	2021-01-03 2:03:04 PM	Sentine		7	Filter Current Log.	_	
> 🧮 Lenovo	(i) Information	2021-01-03 2:03:04 PM	Sentine				-	
> 🧮 Microsoft	(i) Information	2021-01-02 1:53:06 PM	Sentine			Properties		
Microsoft Office Alerts	(i) Information	2021-01-02 1:53:06 PM	Sentine			Disable Log		
OneApp_IGCC	(i) Information	2021-01-01 1:50:36 PM	Sentine		00	Find		
> 🦲 OpenSSH	Information	2021 01 01 1-50-26 DM	Contino	~		Save All Events As		
✓ SentinelOne	<		1	,	1 ° ° °		_	
Firewall	Event 2, Sentinel	One		×		Attach a Task To th	his Log	
Operational					L	View		)
TechSmith	General Detail	s			a	Refresh		
Subscriptions				^	2	Help		
Subscriptions	Policy was ch	anged in the Console:			Ľ.	нер		
	("agentl oggi	ng":true."antiTampering":tr	ue."autoFileU		Eve	nt 2, SentinelOne		-
				~		Event Properties		
	<		>		1	Attach Task To Thi		

Search for Error ID 5, error in registration due to invalid certificate or other connection issues.

- 1. If the endpoint can resolve the ping or reach the management console login page, there is likely not a firewall/network issue.
- 2. If the agent services are all running/operational, the installation is clean and not the issue.

# If the above steps do not point to any errors/resolve the issue, see below for more potential causes and their fixes:

#### **Potential Cause: Corrupt WMI repository**

If you ever see the below or similar error(s), it indicates the repository is corrupt:

**Solution:** Reset the WMI repository.

- Open CMD as Administrator on the affected endpoint and run the below commands. Press enter after each entry. net stop winmgmt
  - winmgmt /resetrepository
- 2. Reboot the endpoint. Wait a few minutes after startup to see if the agent connects. If it does not, reinstall the Agent.



### Potential Cause: Missing cipher suites or outdated OS security patches

The S1 management console requires updated TLS ciphers for communication. These are often included in Windows updates/security patches. If an endpoint lacks the required cipher suites, it can't communicate with the management console.

#### Solutions:

- 1. Check OS version to ensure there are no pending security patches or Windows Updates.
- 2. Check that the required cipher suites are enabled on the host.
  - Endpoints occasionally have an issue where they don't have the correct ciphers enabled for communication with the management console. To enable the necessary cipher suites and get the device connected to the console, follow the below steps:
- Download the GUI IIS Crypto Program on to the affected endpoint: <u>https://www.nartac.com/Products/IISCrypto/Download</u>
- 4. Launch the program. On the left side of the GUI, click **Cipher Suites**.
- 5. Click **Best Practices** to apply the most secure TLS settings for the device. Continue to step 6.



- 6. In this cipher suites list, you reorder the cipher suites so the following ciphers are **enabled** and **moved to the top of the list**. Enable the ciphers by checking the box to the left of each one. The order required is in the list below:
  - TLS DHE RSA WITH AES 256 GCM SHA384
  - TLS DHE RSA WITH AES 128 GCM SHA256
  - TLS DHE RSA WITH AES 256 CBC SHA
  - TLS DHE RSA WITH AES 128 CBC SHA

IMPORTANT: If any of the above cipher suites are missing from the list, add them using the plus (+) button on the right-hand side, underneath the arrow



keys. Copy and paste any missing ciphers one at a time. After you add them, ensure they are enabled by checking the box, then continue to the next step. To re-order the cipher suites, use the arrow keys on the right.



- 7. Once the cipher suites are in the correct order according to the table above, hit Apply. A reboot is necessary for the changes to take effect.
- 8. After a reboot, you can verify connectivity by right clicking the SentinelOne Agent system tray icon. Alternatively, wait 5 to 10 minutes and check for the device on your Barracuda Dashboard.

If you experience this issue with multiple endpoints, consider using Group Policy to push out this change instead. Use this Microsoft article to create the GPO: <a href="https://learn.microsoft.com/en-us/windows-server/security/tls/manage-tls">https://learn.microsoft.com/en-us/windows-server/security/tls/manage-tls</a>

If you encounter any further issues, contact our Global SOC.

#### Barracuda XDR



#### Figures

- 1. Picture11.png
- 2. Picture12.png
- 3. Picture13.png
- 4. Picture14.png
- 5. Picture15.png
- 6. Picture16.png
- 7. Picture17.png
- 8. Picture18.png

© Barracuda Networks Inc., 2025 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.