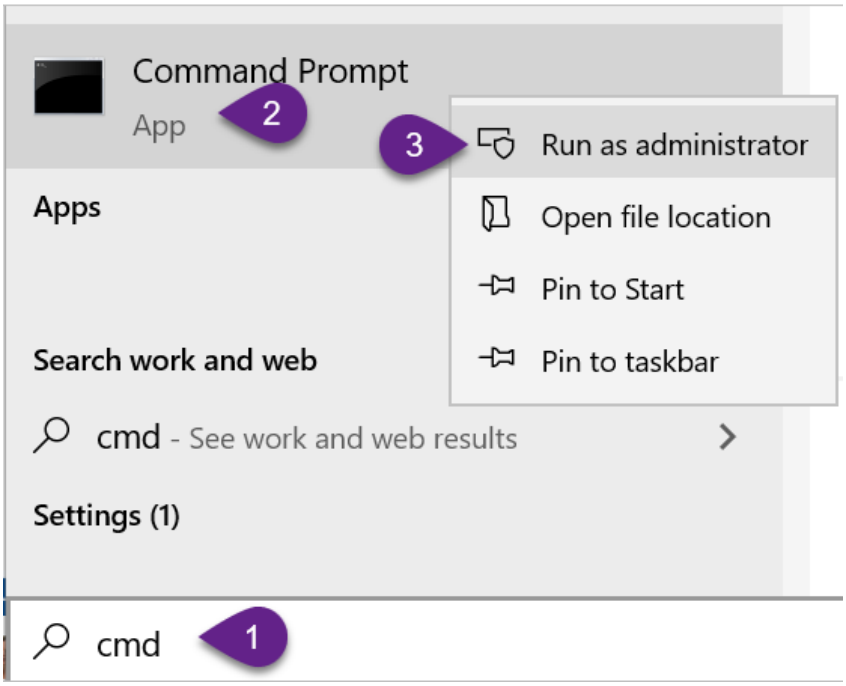
How To Troubleshoot Offline Agents

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 Behavioural 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, we will use the Windows command prompt with **Run as Administrator**.

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



NETWORK CONNECTIVITY TEST

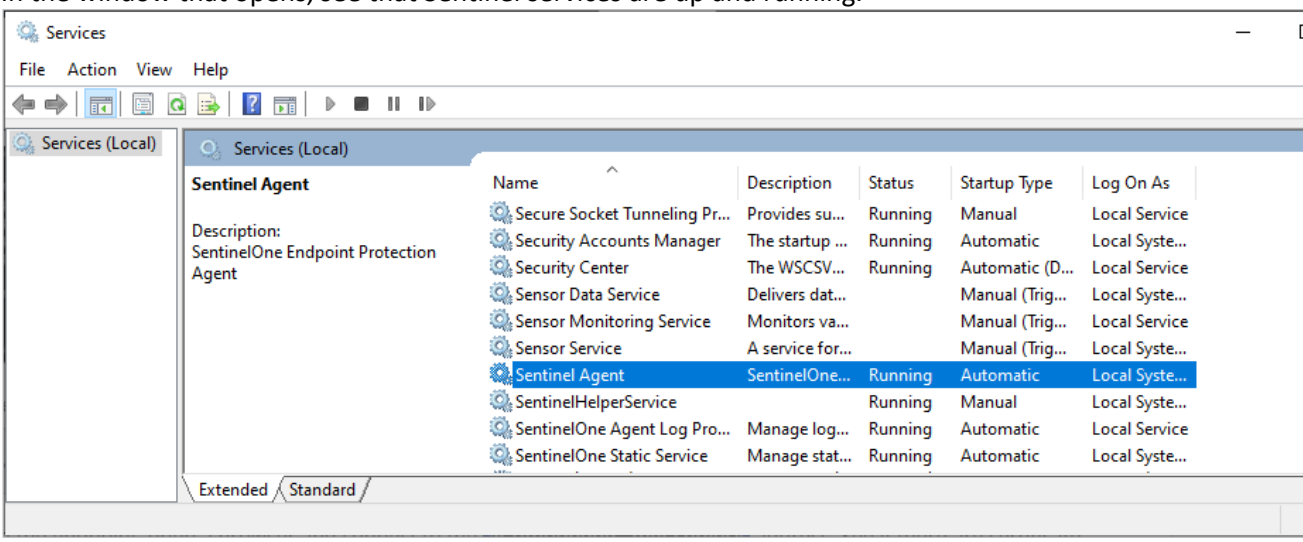
1. From an endpoint, ping our Management URL and see that it resolves.
2. If the ping times out, but resolves to an IP address, the ping is successful.

3. From the endpoint, open a browser and connect to the Management address. See if there are certificate errors.
4. 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.
5. See if there is a proxy and if it is configured correctly.

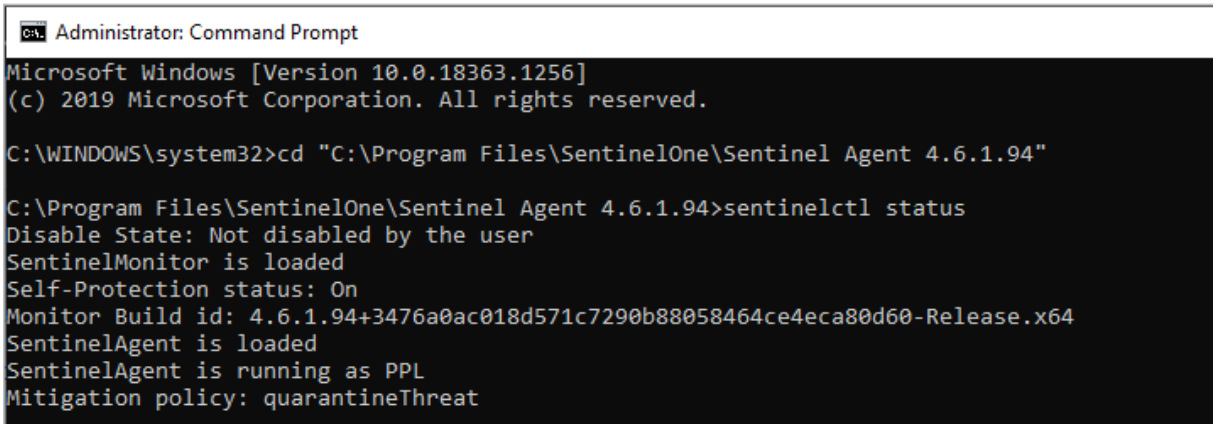
AGENT SERVICES TEST

1. See if Agent services are up and running. On an endpoint, run: services.msc

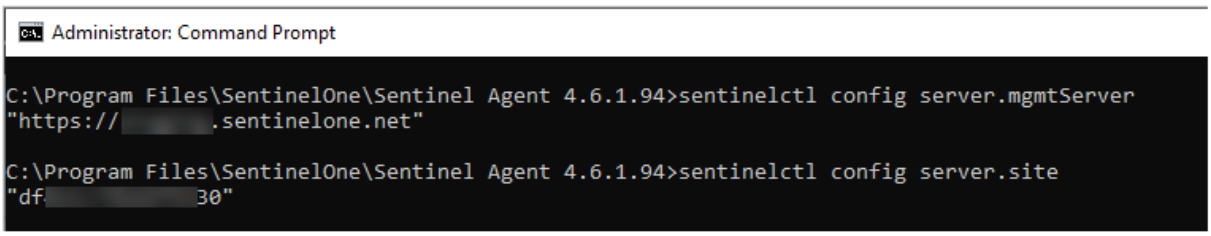
In the window that opens, see that Sentinel services are up and running.



2. 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



3. See that the output shows **loaded** and **running**, similar to the example.
   > sentinelctl config server.mgmtServer
   > sentinelctl config server.site



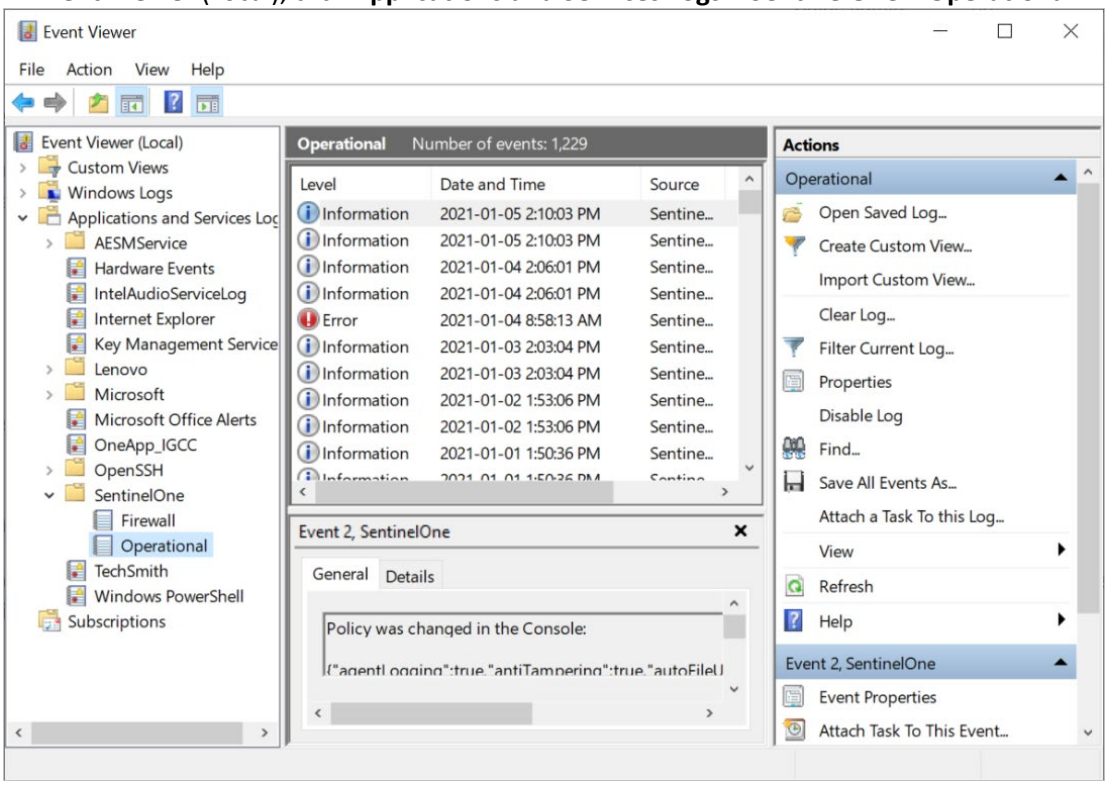
4. Make sure the output is not empty.

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.

1. 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**.



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

4. If the endpoint can resolve the ping or reach the management console login page, there is likely not a firewall/network issue.
5. 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: The WMI repository is corrupt. If you ever see the below or similar error(s), it indicates the repository is corrupt:

Solution: Reset the WMI repository.

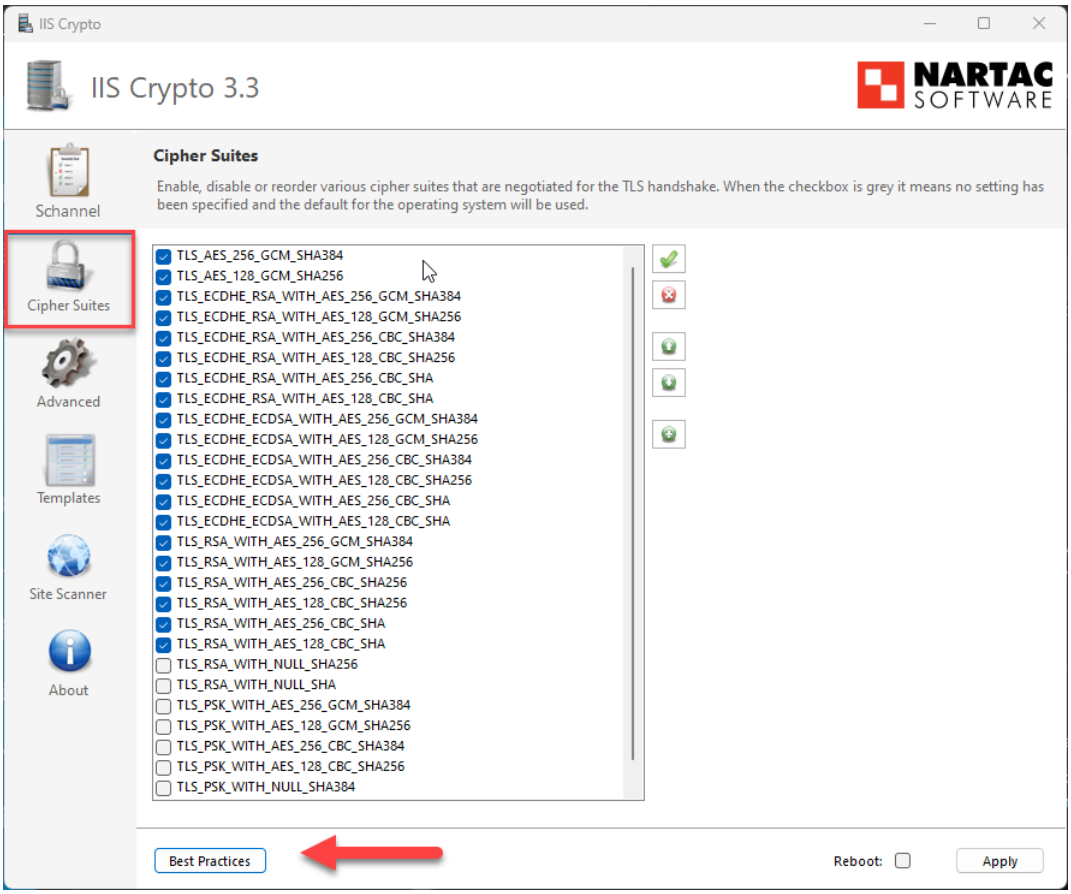
1. Open CMD as Administrator on the affected endpoint and run the below commands. Press enter after each entry.
    - **net stop winmgmt**
    - **winmgmt /resetrepository**
2. Reboot the endpoint. Wait a few minutes after startup to see if the agent connects. If it does not, reinstall the Agent.

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 will not be able to communicate with the management console.

Solution:

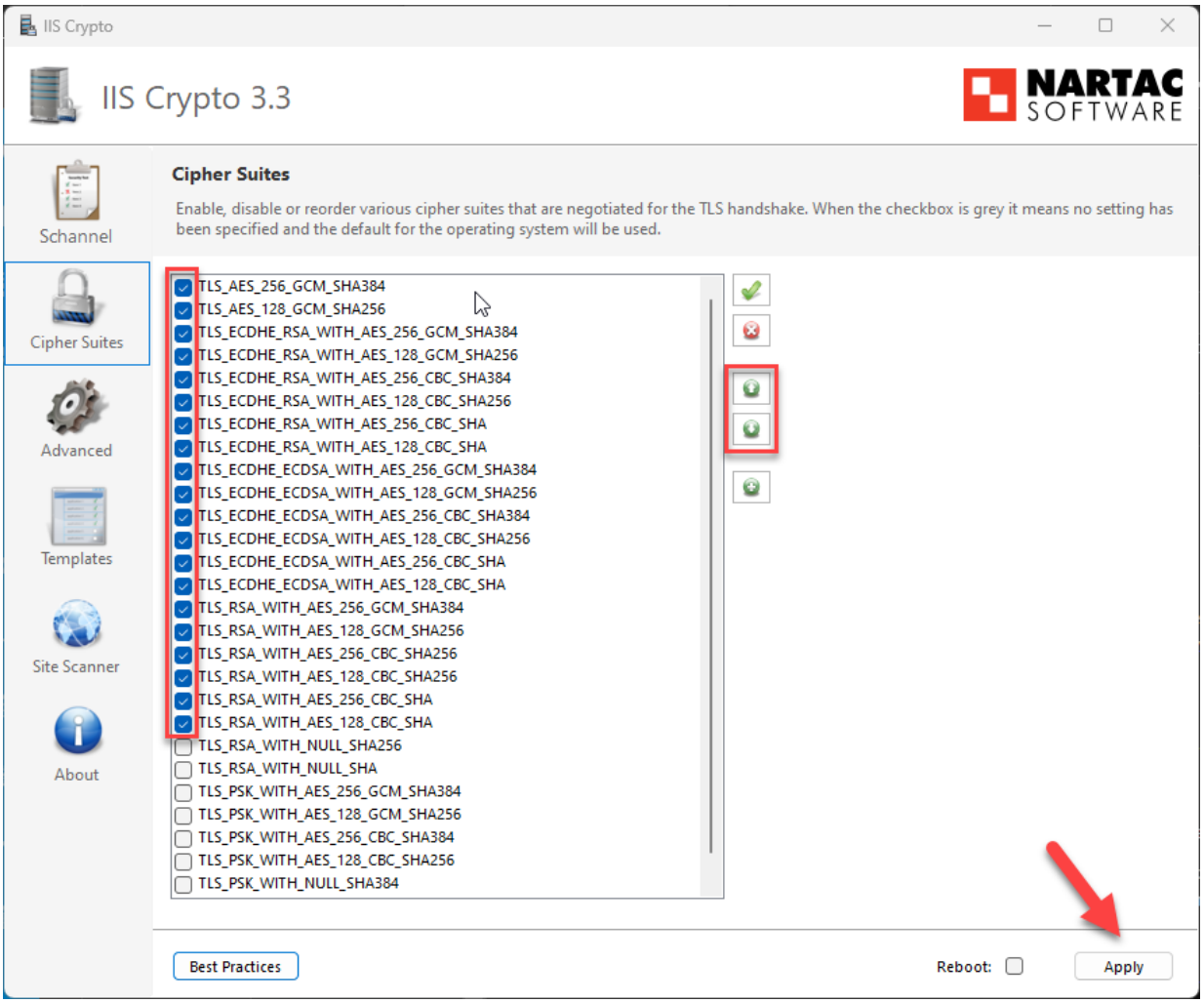
1. Check OS version to ensure there are no pending security patches or Windows Updates.
2. Check that the required cipher suites are enabled on the host.
    a. Endpoints occasionally have an issue where they do not have the correct ciphers enabled for communication with the management console. To enable the necessary cipher suites and get the device connected to the console, please follow the below steps:
1. Download the GUI IIS Crypto Program on to the affected endpoint: https://www.nartac.com/Products/IISCrypto/Download
2. Launch the program. On the left side of the GUI, click "Cipher Suites".

3. Click “Best Practices” to apply the most secure TLS settings for the device. Continue to step 4.



4. In this cipher suites list, you will need to reorder the cipher suites so that the following ciphers are **enabled** and **moved to the top of the list**. You can 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, you must add them using the plus (+) button on the right-hand side, underneath the arrow keys. Simply copy/paste any missing ciphers one at a time. After they are added, ensure they are enabled by checking the box and continue to the next step.
   To re-order the cipher suites, use the arrow keys on the right.



5. 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.
6. 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 are experiencing this issue with multiple endpoints, consider using Group Policy to push out this change instead. You can use this Microsoft article to create the GPO. - https://learn.microsoft.com/en-us/windows-server/security/tls/manage-tls

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