

# How to Troubleshoot S1 Agent Installation Ended Prematurely

---

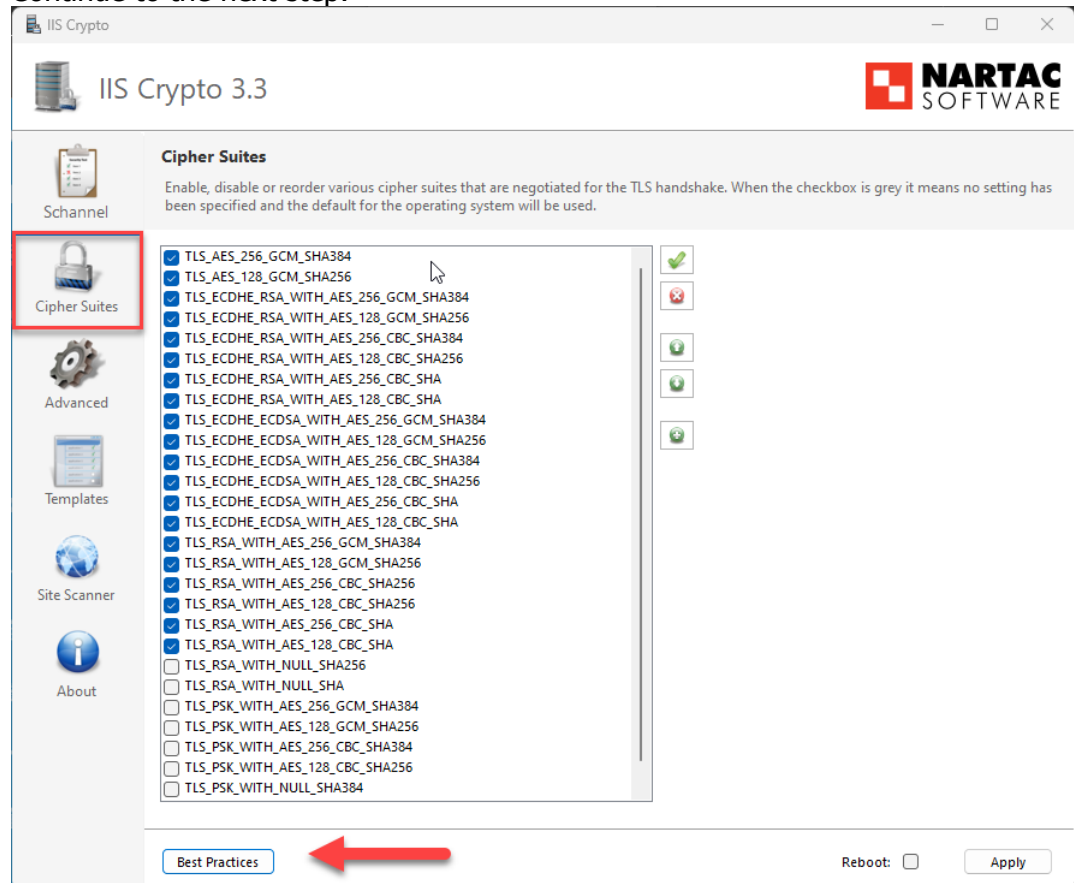
Occasionally, the SentinelOne agent will fail to install on an endpoint due to an error. You will receive a message stating: "Sentinel Agent Setup Wizard ended prematurely." There are a few steps you can follow to fix this error:

## SOLUTIONS

---

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

- Click "Best Practices" to apply the most secure TLS settings for the device. Continue to the next step.

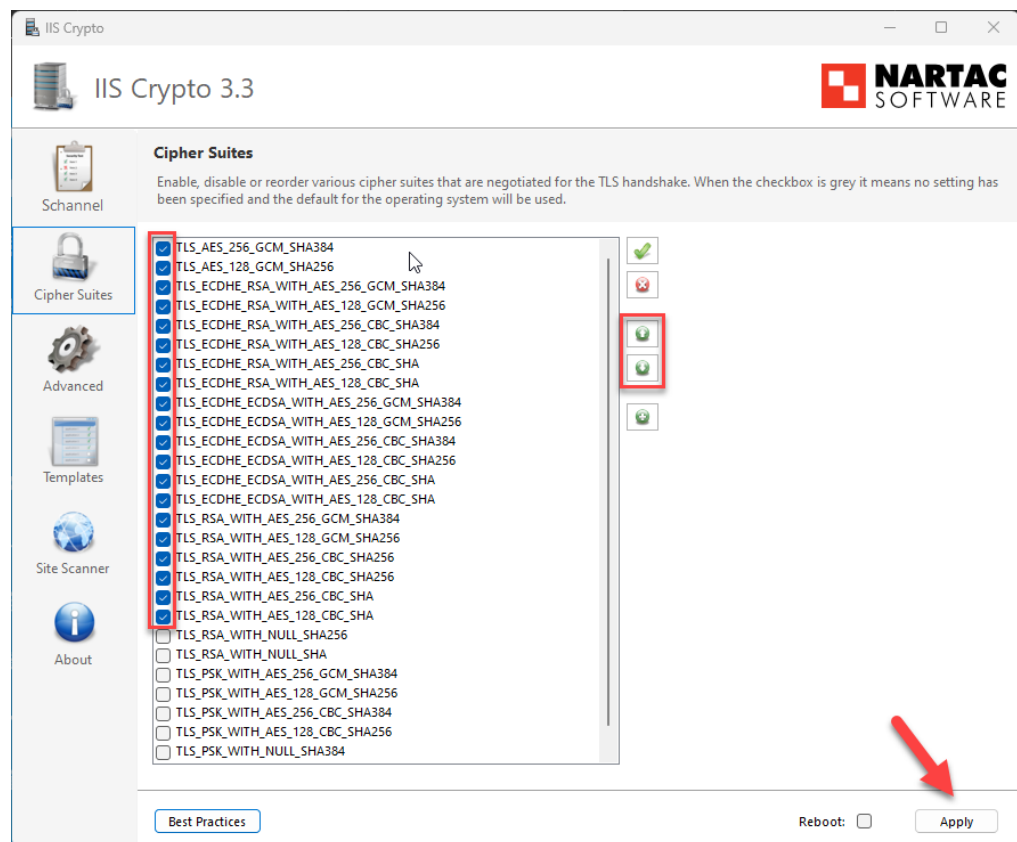


- In this cipher suites list, you will need to reorder the cipher suites so that the following ciphers are enabled and moved to the top of the list. You can enable the ciphers by checking the box to the left of each one. The order required is in the list below:

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.



- 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.
- 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, please contact our Global SOC.