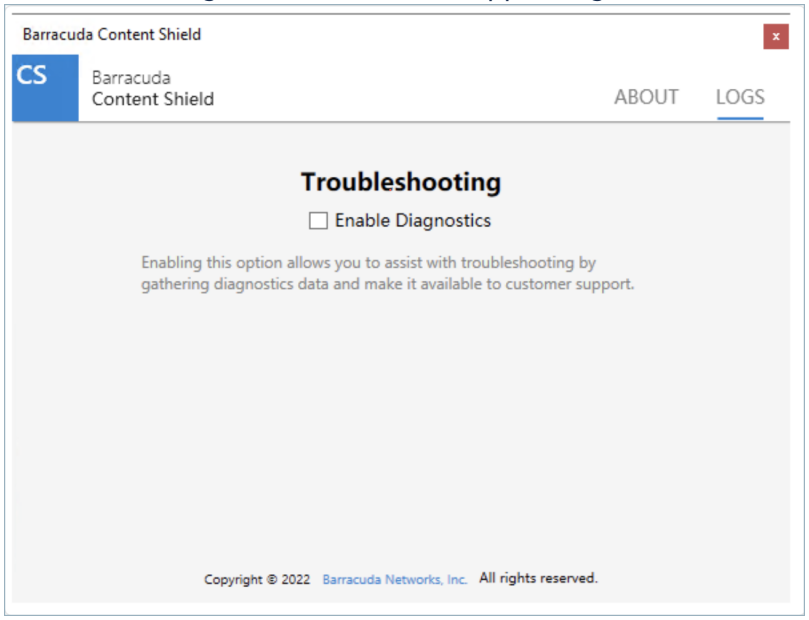
Agent Settings

https://campus.barracuda.com/doc/93201092/

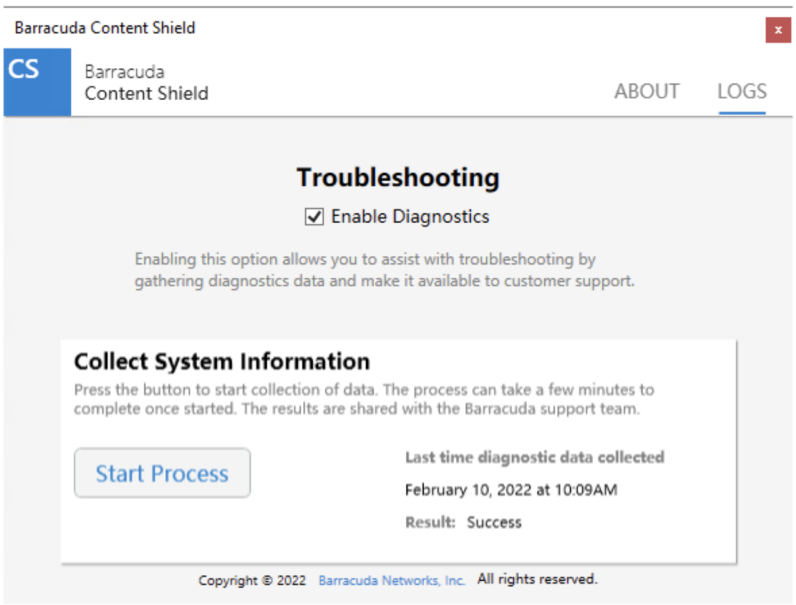
These settings apply to the Barracuda Content Shield (BCS) Suite, if you have it deployed on endpoint machines.

Agent Security and Utilization

- **Allow Log Collection (*Windows only*):** If set to *ON*, the user can enable a feature on the agent to collect and send log diagnostics data to Barracuda Networks Support. When this feature is enabled on the **Agent Settings** page, a **LOGS** tab appears in the upper right in the agent UI after the next successful configuration sync on the endpoint. To collection support log data:
  1. The user clicks the **LOGS** tab, and then checks **Enable Diagnostics** on the Troubleshooting screen to enable support log collection:



  2. Next, the user can trigger log collection by clicking **Start Process**. Log collection can take several minutes to complete.



3. After log collection has completed, the last diagnostics collection date and the Result (e.g. "Success") are displayed to the right of **Start Process**.
   ***Note**: This functionality is blocked for 5 minutes after the log collection is triggered in order to maintain system performance.*
4. The log data is sent from the agent to Barracuda Networks Support.

- **Tamper Proof**: When set to *ON*, this feature prevents the user from removing the BCS agent from the endpoint. This requires creating an **Agent Password,** which must be used when uninstalling the agent at the endpoint. **You will not be able to uninstall the agent on the endpoint if you set this feature to** *ON* **and do not have the password.** However, by setting this option to *OFF*, you can bypass the Tamper Proof feature and uninstall the agent on the endpoint without the password. See Preventing Users from Uninstalling the Barracuda Content Shield Suite for details on how to use this feature.
- **Max CPU Usage**: Configure the maximum CPU resource you want to allow the BCS agent to use on the endpoint.

Agent Update

Click **Apply Agent Updates** to select how you want to apply updates to the BCS Suite on endpoint machines. **Note that *Automatic* updates only apply to Windows machines**.

- **Manually**
- **Automatically When Devices Reboot**
- **Automatically at a Specific Time** – When you select this option, additional fields are presented for specifying the time at which agent updates will be initiated. The selection applies to the device's local time zone.

Define All Local Domains

Best Practice: If you are using the BCS agent with a DNS proxy solution, do the following:

I n the **LOCAL DOMAINS** text box, add any local (internal) domains/hostnames that should be resolved by the DNS server configured on the endpoint computer, instead of the DNS server selected by BCS Plus.

Figures

1. Troubleshooting1.png
2. DiagnosticsComplete.png