Using the Barracuda RMM WsusClientDiagnostic tool

https://campus.barracuda.com/doc/93200626/

This article was developed to complement the use of the WsusClientDiagnostic tool.

- The target system must have Microsoft .NET Framework 4.0 or higher installed
- A standalone zip package containing an exe that can be run manually or via command line
  - The download can be found here.
    - *Users that cannot access the tool via the hyperlink, please right-click and select Save As.*

Read this article all the way through as it has useful information about the results in the tool but also steps on how to troubleshoot/resolve issues the tool highlights.

OS Information

This section provides basic information about the system in question.

A warning will be displayed if the system is missing a major update which may prevent it from receiving future windows updates, or if the operating system is unsupported.

Windows Update Agent (WUA) Client Information

This section will provide information about the Windows update client.

A warning is displayed if certain older versions of Windows update are detected on some operating systems which have been known to be problematic.

- In these cases, we recommend manually installing the latest windows update agent.

A warning is displayed if the SusClientId is detected as being malformed or otherwise invalid.

WUA Registry Settings

This section will provide information on the Windows update policy registry key settings. These settings are best described in Microsoft's documentation on the topic Configure Automatic Updates using Registry Editor.

This information may be used to help validate the configuration on the client machine against what is configured in Service Center.

> When a patch policy using a monthly schedule, or multiple days of the week is applied, the settings displayed here may not match what is seen in the policy. This is because these scheduling options are not native to Windows update, and, in order to achieve these schedules, Barracuda RMM updates the scheduled time on the system periodically until the correct scheduled date and time are reached.

Windows Server Update Services (WSUS) Connectivity

This section will provide results for basic connectivity tests to the Onsite Managers patch service, or your Service Center Patch service in the case of a Device Manager. DNS lookups are also performed which can be useful in identifying DNS resolution issues.

> A successful test does not guarantee that a system can check for updates successfully, only that it can successfully reach the patch service.

Group Policy Conflicts

This section will report any potential group policies applied to the device which may conflict with Patch Management through Barracuda RMM.

If any group policies are detected they should be reviewed and any Windows Update-specific settings contained within them should be set to "Not Configure" as documented in the latest version of the Domain Configuration Guide.

Dual Scan

Additionally, Dual Scan can be an issue with Windows 10 Kernel-based systems. Please see this Knowledge Base article on that behavior.

> Dual Scan does not show up in the WSUSClientDiagnostic tool, but should be check by end devices as well as an Onsite Manager when patching is failing

Windows Service Configurations

This section displays the status of the Windows Update (wuauserv) and Background Intelligent Transfer (bits) services.

> A warning will be displayed if either service is disabled.

Reboot Status

This section checks if there is a pending reboot for previous windows update operations.

> If the system is in a pending reboot state due to patch installation, it may prevent the system from checking into Patch Management to find new updates or report new update status information. If there is a pending reboot, a warning will be presented.

BITS Queue

This section will check the Background Intelligent Transfer Service job queue which is used by windows update to download updates.

If jobs are stuck in an error or suspended state, this could prevent Windows from downloading updates until the BITS queue is reset.

Update History

The console output will report the number of installed updates collected via the Windows Update API. The details of each individual updates are logged in the WsusClientDiagnostic.txt log file in the utilities folder when executed.

This log may be requested by support in troubleshooting patch issues.

Check Updates

This section will perform a check for updates using the default source of updates on the system. If a policy is applied through Barracuda RMM, then the device will check for updates through an Onsite Manager or Barracuda RMM Update Service. The number of installed and needed updates will be reported, along with a number of warnings, if any, as well as the result code for the check for updates.

The details of each individual updates are logged in the WsusClientDiagnostic.txt log file in the utilities folder when executed.

If an error occurs, the error code will be reported here.

Microsoft Update

This section will perform a check for updates using Microsoft Update. This can be used to verify that the Windows update agent does function and detect updates however, this cannot be used as a 1:1 comparison due to variations in update availability between Microsoft update and WSUS that Barracuda RMM depends on for patch metadata. The results may sometimes provide hints to review

Products and Categories synchronized in Service Center, as well as verifying that patches that are expected to be installed, are in fact approved. The number of installed and needed updates will be reported, along with a number of warnings, if any, as well as the result code for the check for updates.

The details of each individual updates are logged in the WsusClientDiagnostic.txt log file in the utilities folder when executed.

If an error occurs, the error code will be reported here.