So your Onsite Manager is performing poorly

https://campus.barracuda.com/doc/98216966/

Over time an Onsite Manager can begin to use more and more resources, or the device the Onsite Manager is handled on is slowing down. There are a possible number of reasons for that. In this article, you will learn how to diagnose some of these and possibly mitigate them or at least better arm Support staff to be able to assist you. Some of the common symptoms we see in Support that indicate poor Onsite Manager performance might include:

- The device itself is slow.
- The site shows down in Barracuda RMM.
- MWExpertSystem service has stopped.
- The site is not Processing Commands.
- Service Center Receive Errors for the site.

Restart

The most common reason an Onsite Manager runs flat or slow is that it has been up and in service for a long time. Start by restarting the **MWExpertSystem** service to see if there are any improvements. If not, schedule a restart of the Onsite Manager device.

Underpowered Onsite Manager

A common issue Support runs into about Onsite Manager performance is that your device is underpowered. Refer to the Setup Guide for the ideal specs and supported operating systems for an Onsite Manager. If the Onsite Manager is a physical device, you may want to migrate it to something more robust. See the following:

- Barracuda Campus Barracuda RMM Documentation: Setup Guide and User Manual
- Migration KB

Also, remember that an Onsite Manager is best utilized when it is the only SQL-heavy item on the device. Support would also like to take this opportunity to caution against putting an Onsite Manager on a Domain Controller for security reasons.

The Onsite Manager is not scanning the local network on a new installation

This is standard behaviour from a brand new Onsite Manager installation. You will need to set the network you want to have scanned. Please note the below about overcanning a network or scanning over a peer-to-peer connection.

- In your Service Center, click **Site Management** > **Sites**.
- Click your Site.
- Click **Network Discovery**.
- Select **Modify**
- Then click on **Add**
- You can then add **Single** IP, **Range** or **Subnet Mask.**

Overscanning in Network Discovery

Another common issue with Onsite Managers is when a site is configured to scan far more IP addresses than truly needed to manage a site. Keep your scan range down to what you need, and do not overdo it, as the scan takes priority for an Onsite Manager. To determine your scan range, do the following:

- In your Service Center, click **Site Management** > **Sites**.
- Click your Site.
- Click **Network Discovery**.
- Remove any unnecessary scans.

If you are scanning a /16 subnet, this would be a non-ideal setup as the scans will not complete in a timely manner and cause issues. The Barracuda RMM Development and Support teams recommend scanning only that which is local and necessary for your Onsite Manager to manage properly.

Scanning over a Tunnel / VPN / IaaS Connection / Peer-to-Peer

The Barracuda RMM Support Team has noticed increased partners utilizing their Onsite Managers to scan over Tunnel / VPN / IaaS (or other non-direct and non-local) connections. While, in theory, this can work, it is unsupported by the Onsite Manager and strongly discouraged. We cannot reliably trust that a site will perform as expected when including devices not local to the OM in the scan range and can expect that other functionality would impact any device in the site scanned in by said OM. Instead, deploy an Onsite Manager at the physical location to handle the workload for those remote devices, or if you wish to have them all on the same site, deploy Device Managers to each remote device.

Incorrect or mismatched MWService Account Password

One of the easier things to ensure for your Site is that your MWService account password matches the Onsite Manager and within your environment. For a Domain within Active Directory and a workgroup, the password is set locally on the Onsite Manager. Follow these steps to ensure the password matches both in your environment and on the Onsite Manager.

- Within Active Directory, change the MWService Account Password
    - If the OM is in a workgroup, you would change it locally
- On the Onsite Manager, go to Start
- Type in Configure Onsite Manager
- When you get to the point where you set the MWService Account Password, match that to what you just changed it to
- Complete the registration

Incorrect SCMessaging URL

In some instances, the SCMessaging URL was not put incorrectly, or there was a change to the Service Center that was not reflected properly on the OM. To verify this, do the following:

1. In your Service Center, select **Configuration** > **System Settings**.
2. Select **Communication Settings**.
3. Take note of the Public SCMessaging URL.
4. Log into the Onsite Manager.
5. Click **Start**.
6. Find the **Level Platforms** folder.
7. Select **Configure Onsite Manager**.
8. Run through the configuration and ensure the SCMessaging URL matches what is in your Service Center.

If the Configure Onsite Manager executable is not found in the start menu, please refer to this KB for creating a shortcut to the file.

Devices scanning over WMI are using DCOM

Microsoft uses two conventions since an Onsite Manager communicates and manages through WMI. The first, DCOM, is an older standard with memory leak issues that cause an Onsite Manager to bleed resources slowly. Even one device showing as DCOM enabled will cause problems. There are two

methods to check whether DCOM is enabled on your site.

1. Check by hand by going to the device overview page and under status, and it will show WMI Enabled: Yes (DCOM)
2. Launch SQL Server Management Studio on the Onsite Manager and run this query.

```
use MWData
select * from device where WSManEnabled=0 and WmiEnabled=1
and deviceguid not in
(
select deviceguid from DiscoveryDevice where IsLocal=1
)
```

If devices are showing in the list, they are using DCOM. Note down the DNS name and if they are excluded (excluded devices may need to be reincluded for the following steps). To fix this, you install/enable Microsoft Windows Management Framework. Below are three different methods to accomplish this goal.

Install and enable Microsoft Windows Management Framework

- Click **Automation**.
- Click **Calendar**.
- Click **Run Now**.
- Select **Items from Library**.
- Select **Install Microsoft Windows Management Framework**.
- Target the devices on the site.
- Click **Run Now**.

Alternatively, you can also manually install WinRM by downloading it directly.

Run the Windows Prep Utility on end Devices

- Log into your **Service Center dashboard**
- Click on **Site Management**
- Then on **Sites**
- Select the Site with the device stated to be scanning under DCOM
- Click on **Resources**
- **Download the Windows Prep Utility** and run it on the end device

Set WinRM Manually on an End Device

- Log onto the End Device
- Open a Command Prompt as administrator
- type in ***winrm quickconfig***

This does not prompt for a reboot but requires one to take effect on each device.

Database Size

To check if your Database is maxing or near maxed out (10GB is the limit for SQL Express), do the following.

- Open SQL Server Management Studio.
- Log into **LPIMWOMEXPRESS** instance.
- Expand the **Databases**.
- Right-click **MWData**.
- Select **Properties**.

If this is close to or exceeds 10GB, contact Support.

Patch Metadata Bloat

Over time and upgrades, metadata can become bloated. This last step is informational for you but likely will help Support as you will want to call the team after this.

- Open SQL Server Management Studio
- Log into **LPIMWOMEXPRESS** instance.
- Expand the **Databases**.
- Right-click **MWData**.
- Select **Reports**.
- Select **Standard Reports**.
- Select **Disk Usage by Top Tables**.

When contacting support, please ensure you have screenshots and logs (Collecting logs for Barracuda RMM Support) to ensure we have a complete picture of the issue and can give quick assistance.