This document explains the required steps to configure the RAP as a Service for System Center Configuration Manager (SCCM).

There are two scenarios available to configure the assessment. Determine which scenario fits best for your organization.

1. Data collection machine does not have Internet access
2. Data collection machine has Internet access

**Data collection machine does not have Internet access**

In this scenario, the data collection machine has no Internet connection and connects to either an OMS Gateway or a SCOM server (with or w/o OMS Gateway) to upload the data to log analytics. The OMS Gateway must have Internet access. This scenario is recommended for environments where the Internet connection is restricted from the data collection machine or where security is a concern due to this schedule task requirement.

In the scenario where you use an OMS Gateway, we require two computers. One will be designated as the data collection machine, and the second machine will be the OMS Gateway.

For information about the OMS Gateway, go to https://go.microsoft.com/fwlink/?linkid=830157.

The data collection machine must be a member of the domain containing the Management Server being assessed. In this scenario, the data collection machine will contact one Management Server (chosen by you during the installation) in the SCCM Hierarchy to collect data. After the data is collected, the data collection machine will analyze the information, and for increased security, will forward the data to an OMS Gateway to upload it to log analytics.

The following path shows the relationship between your Windows computers and log analytics after you have installed and configured the OMS Gateway and data collection machine.

Data Collection Machine → Query the designated Management Server in the Hierarchy → Forward collected data to OMS Gateway → Submit data to log analytics Workspace

**Data collection machine has Internet access**

This scenario can be used when the data collection machine can contact log analytics directly. It requires one computer that will be designated as the data collection machine which has to be able to access the Internet to upload data to log analytics. This scenario can be used in environments where the Internet connection is not restricted.

The data collection machine must be a member of the domain containing the Management Server being assessed. It will collect data from one Management Server (chosen by you during the installation) in the SCCM Hierarchy. After the data is collected, the data collection machine will analyze the information and then upload the data to log analytics directly, which will require HTTPS connectivity to your log analytics workspace. The following path shows the relationship between your Windows computers and log analytics after you have installed and configured the data collection machine:

Data collection machine → Query the designated Management Server in the Hierarchy → Submit data to the log analytics workspace.

**Detailed information on these configurations and requirements are listed later in this document.**

*This document was last updated on November 11, 2018. To ensure you have the latest version of this document, check here: https://www.microsoft.com/en-us/download/details.aspx?id=34698*
Table of Contents

System Requirements and Configuration at Glance................................................................. 3
  Supported Versions.................................................................................................................. 3
  Common to Both Scenarios.................................................................................................... 3
  Data Collection Machine....................................................................................................... 3
  OMS Gateway (required in the Data Collection Machine does not have Internet access scenario) ................................................................. 4

Appendix A – Setting up the Environment............................................................................. 5
  Enable the assessment in Services Hub portal ....................................................................... 5
  1. Log Analytics OMS Gateway Setup .................................................................................. 5
  2. Data Collection Machine Setup ....................................................................................... 7
  3. Setup and configure log analytics using SCOM .................................................................. 13

Appendix B - Setting up the SCCM Assessment .................................................................... 18

Appendix – C Data Collection Methods.................................................................................. 21
System Requirements and Configuration at Glance

According to the scenario you want to use, review the following details to ensure that you meet the necessary requirements.

Supported Versions

- Your SCCM environment must run on System Center Configuration Manager 2007/R2/R3, System Center 2012/2012 R2 Configuration Manager, System Center Configuration Manager 1610/1702/1706/1710 with site systems including Windows Server 2008/R2, and Windows Server 2012 or latest.

Common to Both Scenarios

- You will need a log analytics workspace
- User account rights:
  - A domain account with the following rights:
    - Admin access to every server (Site System) in the Configuration Manager hierarchy. Single user account if Site Systems are in Multi-Domain Environment
    - Unrestricted network access to every server (Site System) in the Configuration Manager hierarchy
    - Administrator permissions to all SQL servers used by the Configuration Manager Sites or Software Update Points
    - Full access rights to all the Configuration Manager Site objects in all Primary Sites
    - SysAdmin permission to all SQL Instances used by Configuration Manager Sites or Software Update Points.

Data Collection Machine

- Microsoft Monitoring Agent requires computers running Windows Server 2008 SP1 or later (or Windows 7 SP1 or later – Important: The option of installing the Microsoft Monitoring Agent on client operating systems is strongly discouraged due to the risk of exposing privileged domain account credentials to lower trust workstations.
- The data collection machine must be a member server of the Active Directory domain in which the SCCM Hierarchy resides that you wish to be assessed.
- Data collection machine hardware: Minimum 8 gigabytes (GB) of RAM, 2 gigahertz (GHz dual-core processor, minimum 10 GB of free disk space.
- The data collection machine is used to connect to your SCCM Hierarchy and retrieve information from it, communicating over Remote Procedure Call (RPC), Server Message Block (SMB), WMI, remote registry, SQL Database, Lightweight Directory Access Protocol (LDAP) and Distributed Component Object Model (DCOM).
- Microsoft .NET Framework 4.0 or newer installed.
- The data collection machine must be able to connect to the Internet using HTTPS to submit the collected data to your log analytics workspace. This connection can be direct, via a proxy.
- For the Microsoft Monitoring Agent to connect to and register with the log analytics service, it must have access to the Internet. If you use a proxy server for communication between the agent and the log analytics service, you will need to ensure that the appropriate resources are accessible. If you use a firewall to restrict access to the Internet, you need to configure your firewall to permit access to log analytics. To ensure data can be submitted follow the steps in Configure Proxy and Firewall Settings in Log Analytics at https://azure.microsoft.com/en-in/documentation/articles/log-analytics-proxy-firewall/.
OMS Gateway (required in the **Data Collection Machine does not have Internet access scenario**)

- The **OMS Gateway** must be able to connect to the Internet using HTTPS to submit the collected data to your log analytics workspace. This connection can be direct, via a proxy.
- **OMS Gateway hardware**: Minimum 4 GB of RAM and 2 GHz processor.
- **OMS Gateway services**: When the Windows Firewall service is disabled the installation of the OMS Gateway fails.
- **OMS Gateway user account rights**: None required.

**Click the link to download the “Setup Assessment” documentation to install the OMS Gateway and Microsoft Monitoring Agent.**

[https://go.microsoft.com/fwlink/?linkid=860142](https://go.microsoft.com/fwlink/?linkid=860142)

After you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway, continue with the next section to set up the assessment.

A PFE will assist with the setup, configure both machines and scheduling the SCCM assessment during the scoping call.
If you do not have an Azure Log Analytics workspace, the PFE assists you creating one and link that workspace with our Services Hub portal where you enable the assessment.
Depending on the scenario you have chosen, have one or two machines installed and account ready according to the requirements mentioned above. These machines can be VMs.

The appendix has the information how to setup the data collection machine and assessment.
Appendix A – Setting up the Environment

Enable the assessment in Services Hub portal

1. To ensure the Microsoft Monitoring Agent knows what assessments can be run, you need to add the assessment you want to run.
   If you have not added the Microsoft Unified Support Solution you are setting up, do this now. In https://serviceshub.microsoft.com go to Health -> Assessments, select an assessment and click on Add Assessment.

2. Click Add on the Assessment you want to setup

The option changes from Add to View in Azure Log Analytics. You are now all set for the next steps.

Determine the steps to follow to successfully setup the environment for your scenario:

**Data collection machine has Internet access**

- Follow Step 2. Data Collection Machine Setup, then Appendix B – Setup Assessment

**Data Collection machine has no Internet access**

- Using OMS Gateway
  - Start with Step 1, then Step 2 and next Appendix B - Setup Assessment
- Using SCOM
  - Start with Step 3

1. Log Analytics OMS Gateway Setup

If your scenario includes the installation of an OMS Gateway, follow this section. If not, move to the step 2. On the designated OMS Gateway machine, you must install both the OMS Gateway and the Microsoft Monitoring Agent. Follow the instructions in the sections below to set up both components.

Download and install the OMS Gateway
On the designated OMS Gateway server, complete the following:

1. Download the Setup file from https://go.microsoft.com/fwlink/?linkid=837444
2. On the Welcome page, click Next.
3. On the License Agreement page, select I accept the terms in the License Agreement to agree to the EULA, and then click Next.
4. On the Port and Proxy Address page, do the following:
   - Type the TCP port number to be used for the OMS Gateway. Setup opens this port number from Windows firewall. The default value is 8080.
   - [Optional] If the server on which the OMS Gateway resides needs to go through a proxy, input the proxy address where the OMS Gateway needs to connect. For example, myorgname.corp.contoso.com:80. This is an optional value. If it is blank, the OMS Gateway will try to connect to the Internet directly. Otherwise, the OMS Gateway will connect through your internal proxy. If your proxy requires authentication, you can provide a username (domain\user) and password. (NOTE: If you do not provide a domain for the user, it will not work).
   - Click Next.
5. On the Destination Folder page, either retain the default folder location of %ProgramFiles%\OMS Gateway, or type the location where you want to install, and then click Next.
6. On the Ready to install page, select Install. A User Account Control dialog box might appear requesting permission to install. If so, click OK.
7. After Setup completes, click Finish. You can verify that the service is running by opening the Services.msc snap-in and checking the status of the service called OMS Gateway.
8. Download and install the Microsoft Monitoring Agent setup file from log analytics.

Note. It is required to install the Microsoft Monitoring Agent on the OMS Gateway and configure it to with the log analytics workspace that you configure on the data collection machine. Follow the instructions in the next section in this document, Data Collection Machine Setup.
2. Data Collection Machine Setup
Download and install the Microsoft Monitoring Agent setup file from Azure Log Analytics

On the designated data collection machine or OMS Gateway server complete the following:

**Note.** If the collection machine does not have an Internet connection, perform the first 3 steps from an Internet Connected machine.

1. In the Azure portal, go to log analytics, select your workspace and click the **Advanced Settings** Icon.

2. **Click** **Connected Sources**, and then select **Windows Servers**.

3. **Click the Download Windows Agent** link that is applicable to your computer processor type to download the setup file. If the agent is downloaded on another machine, copy the Setup file over to the data collection machine or OMS Gateway server.

**Note.** If a monitoring client was installed for System Center Operations Manager (SCOM), the setup only offers to Upgrade the agent, preserving existing settings. The upgrade does not include any of the configuration steps below.

The next steps apply to installations where no monitoring client was installed for SCOM. Refer to the **Microsoft Monitoring Agent Upgrade** section in this document when you are performing an upgrade of the Monitoring Agent for SCOM.
4. Run Setup to install the agent.
5. On the Welcome page, click Next.
6. On the License Terms page, read the license and then click I Agree
7. On the Destination Folder page, change or keep the default installation folder and then click Next.
8. On the Agent Setup Options page, choose the Connect the agent to Azure Log Analytics (OMS) option. Click Next.

9. On the Overview, Settings Dashboard page, click Connected Sources, and then copy and paste the Workspace ID and Workspace Key (Primary Key) from the log analytics portal. (Hint: Click the copy button then paste in the corresponding Agent Setup field).
Select Azure Commercial or if you are using an Azure US Government cloud select Azure US Government from the Azure Cloud drop down menu and click OK.

10. If you are currently installing the agent on the data collection machine and using an OMS Gateway as part of the OMS Gateway and Data Collection Machine scenario, or if your company requires access through a proxy server, click the Advanced button to provide HTTP proxy configuration. If you do not use any of the above, click Next and go to step 12.

11. Specify the fully qualified domain name (FQDN) or the IP address and port of the OMS Gateway.
If you use a proxy server instead of an OMS Gateway, add the information for your proxy server and if required, authentication credentials (not required for the OMS Gateway), then click Next twice.

12. On the Microsoft Update page, optionally select Use Microsoft Update when I check for updates (recommended), then click Next.
13. On the Ready to Install page, review your choices, and then click Install.

15. When complete, the Microsoft Monitoring Agent appears in Control Panel. You can review your configuration there and verify that the agent is connected to log analytics. When connected to log analytics, the agent displays a message stating: The Microsoft Monitoring Agent has successfully connected to the log analytics service.
Note. If you have been installing the Microsoft Monitoring Agent on the OMS Gateway, you need to repeat the installation on the data collection machine.

After setting up the data collection machine, continue with the setup of the Assessment as outlined in the prerequisites and configuration documentation for each technology.
Microsoft Monitoring Agent Upgrade

If a monitoring agent is already installed, the Microsoft Monitoring Agent setup will only display the upgrade option. The upgrade will keep the existing configuration and adds a new option to configure a log analytics workspace.

Follow the steps below to perform an upgrade and configure the agent for the log analytics Workspace.

1. Run Setup to install the agent.
2. On the Welcome page, click Next.
3. On the License Terms page, read the license and then click I Agree
4. On the begin Upgrade page, click Upgrade.
5. On the Completion page, click Finish.
6. Once the agent installation completed, go to the Control Panel.

7. Click Microsoft Monitoring Agent
8. If the OMS Gateway scenario is chosen or a Proxy server is in place go to the Proxy Settings tab

When this scenario is not used go to step 9.
Select **Use a proxy server** and specify the fully qualified domain name (FQDN) or the IP address and port of the OMS Gateway.

If you use a proxy server instead of an OMS Gateway, add the information for your proxy server and if required, authentication credentials (not required for the OMS Gateway), then Select **Apply**

9. Select the **Azure Log Analytics (OMS)** tab and click **Add...**

![Image of Azure Log Analytics (OMS) tab](image1)

10. Copy and paste the **Workspace ID** and **Workspace Key (Primary Key)** from the log analytics portal. (Hint: Click the copy button then paste in the corresponding **Agent Setup** field). Select **Azure Commercial** or, if you are using an Azure US Government cloud select **Azure US Government** from the **Azure Cloud** drop down menu and click **OK**.

11. An exclamation mark will be visible in the Workspaces pane. Click **Apply**. This will stop and start the agent, and the Workspaces pane should look like the following example after a few seconds.

![Image of Microsoft Monitoring Agent Properties](image2)

12. Click **OK** to finish the Microsoft Monitoring Agent upgrade for log analytics.
3. Setup and configure log analytics using SCOM

If SCOM is already in use and you want to use SCOM and the already installed agents, follow the steps in this section. In this configuration SCOM will either act as the gateway or it leverages the OMS Gateway itself to send data to log analytics.

**Pre-requisites**

The SCOM 2012 SP1 UR6 (UR7 for proxy/gateway support) or SCOM 2012 R2 UR2 (UR3 for proxy/gateway support) agent is the minimum version required to fully support log analytics functionality.

If you are using multi homing of log analytics workspaces, we would suggest that you not use the agent that comes with SCOM but use the Microsoft Monitoring Agent from Microsoft Update/log analytics workspace instead. The current Microsoft Monitoring Agent version is backwards compatible and supported with all SCOM 2012 R2/2016 management groups.

1. On the SCOM Administration Console go to **Administration -> Operations Management Suite -> Connection**

2. Click on **Register to Operations Management Suite**

   A login window will appear. Log in with an account that has administrative rights to connect to the log analytics workspace. Select the proper workspace (if there is more than one) and click **Next**. In the **Confirm the settings** window click on **Create**.
3. Go to the log analytics workspace.

4. From the log analytics workspace, to confirm that the Management Group is connected, go to **Advanced Settings -> Connected Sources -> System Center**:

   Back in the SCOM Administration Console you need to opt-in the agents for log analytics/OMS:

   1. Go to **Administration -> Operations Management Suite -> Connection**
   2. In the right pane, click on **Add a Computer/Group** below Actions:
3. Select the **object type** *(Windows Computer or Groups)* and optionally leave the **Filter** field empty to return all objects of the type selected.

Verify the solution is downloaded on the data collection machine.

Every agent opted-in will receive Management Packs (MPs) from the log analytics workspace. The MPs will depend on which solutions are added. For the Microsoft Unified Support Assessment, the MPs are named:

```
Microsoft.IntelligencePacks.<technology>.Assessment
```

The Microsoft Unified Support assessments MPs will be downloaded as soon as the solution is added to the log analytics workspace. The MPs are downloaded into the Management Pack folder of the agent (this is true regardless of the setup – direct, through GW, or through SCOM):

![Management Packs](image)

You can also look at the OperationsManager event log (it’s the same for the SCOM agent or the stand alone MMA agent) for the events indicating the MPs have been downloaded:
Below picture shows how the Management Packs flow from the OMS Workspace

1. Add Microsoft Unified Support Solution Pack & solution assessment

2. MP is distributed to agents

3. Every agent now has the PowerShell modules and can be a collection agent

4. Agent(s) will send back collection data
Collected data from any agent that is running the scheduled task is sent back to the SCOM Management Server which in turn will upload to the log analytics/OMS Workspace

**Note:** the SCOM Management Group might connect directly to the log analytics service or through the OMS Gateway. The OMS Gateway in the picture above is used for certain solutions that cannot leverage SCOM.

Appendix B - Setting up the SCCM Assessment

After you have finished the installation of the Microsoft Monitoring Agent/OMS Gateway/SCOM, you are ready to setup the SCCM Assessment.

On the designated data collection machine, complete the following:

1. Open the Windows PowerShell command prompt as an Administrator

2. Run the `Add-SCCMAssessmentTask -ServerName <YourServerName> -WorkingDirectory <Directory>` command where `<YourServerName>` is the FQDN or NetBIOS name of one of the Management Servers that's topmost in the hierarchy (Central or Primary Site) and `<Directory>` is the path to an existing directory used to store the files created while collecting and analyzing the data from the environment.

   **NOTE:** If the directory does not exist, it must be created before you continue with the execution. If the command `Add-SCCMAssessmentTask` is not available, the module is not yet found. It can take some time after installing the agent before it to show up. Alternatively, run the following command to load the module manually: `Import-Module "C:\Program Files\Microsoft Monitoring Agent\Agent\PowerShell\Microsoft.PowerShell.Oms.Assessments"`

3. Provide the required user account credentials. These credentials are used to run the SCCM Assessment.

   **NOTE:** This domain account must have all the following rights:
   - Admin access to every server (Site System) in the Configuration Manager hierarchy. Single user account if Site Systems are in Multi-Domain Environment
   - Unrestricted network access to every server (Site System) in the Configuration Manager hierarchy
   - Administrator permissions to all SQL servers used by the Configuration Manager Sites or Software Update Points
   - Full access rights to all the Configuration Manager Site objects in all Primary Sites
4. The script will continue with the necessary configuration. It will create a scheduled task that will trigger the data collection.

5. Data collection is triggered by the scheduled task named “SCCMAssessment -ServerName <YourServerName>” within an hour of running the previous script and then every 7 days. The task can be modified to run on a different date/time or even forced to run immediately.

6. During collection and analysis, data is temporarily stored under the **WorkingDirectory** folder that was configured during setup, using the following structure:

```
This PC > OSDisk (C:) > OMS > SCCM > SCCMAssessment > asttest.redmond.corp.microsoft.com
```

7. After data collection and analysis is completed on the tools machine, it will be submitted to your log analytics workspace depending on the scenario you have chosen:
   - **Directly** if the Data Collection Machine is connected to the Internet and configured to submit directly.
   - **Through to the OMS Gateway Server** if this option is configured, which will then submit the data to your log analytics workspace.

8. After a few hours, your assessment results will be available on your log analytics Dashboard. Click the **System Center Configuration Manager Assessment** tile to review.
9. You will then be presented with findings grouped by the focus area.
Appendix – C Data Collection Methods

The SCCM Assessment in the log analytics workspace and Microsoft Unified Support Solution Pack uses multiple data collection methods to collect information from your environment. This section describes the methods used to collect data from your environment. No Microsoft Visual Basic (VB) scripts are used to collect data.

1. **Registry Collectors**
   Registry keys and values are read from the data collection machine and all domain controllers. They include items such as:
   - Service information from HKLM\SYSTEM\CurrentControlSet\Services.
     This allows you to determine where the Active Directory database and log files are located on each domain controller and get detailed information on each service relevant to the proper function of Active Directory. Microsoft does not collect information for all services, only the ones relevant to Active Directory.
   - Operating System information from HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion
     This allows you to determine operation system information such as Windows Server 2008 or Windows Server 2012.

2. **LDAP Collectors**
   LDAP queries are used to collect data for the domain, domain controllers, nTDSSiteSettings objects, partitions, and other components from AD itself. For a complete list of ports required by AD, see: [http://support.microsoft.com/kb/179442](http://support.microsoft.com/kb/179442).

3. **Windows PowerShell**
   Used to collect WMI information for installed updates and hotfixes on domain controllers.

4. **FileDataCollector**
   Enumerates files in a folder on a remote machine, and optionally retrieves those files.

5. **Windows Management Instrumentation (WMI) Collectors**
   WMI is used to collect various information such as:
   - **WIN32_Volume**
     Collects information on volume settings for each domain controller in the forest. For example, the information is used to determine the system volume and drive letter, which allows the assessment to collect information on files located on the system drive.
   - **Win32_Process**
     Collect information on the processes running on each DC in the forest. The information provides insight on processes that consume a large amount of threads, memory, or have a large page file usage.
   - **Win32_LogicalDisk**
     Used to collect information on the logical disks. We use the information to determine the amount of free space on the disk where the database or log files are located.

6. **SQL Data Collectors**
   SQL queries are used to collect information from Site Servers.