MDM Migration Analysis Tool (MMAT)

Executive Summary

What is this thing called MMAT?

More and more organizations want to move to MDM to manage their devices. For Windows 10 Creators Update, Microsoft is adding functionality to the Operating System itself to make transitioning to MDM easier. See additional documentation for more background.

Transitioning from Group Policy to MDM can be challenging. Some organizations have Group Policies that have been in place for over a decade and which may not be fully inventoried, never mind understood. Furthermore, MDM does not have a 1-1 mapping for all legacy Group Policies. While it is possible for an IT administrator to manually inventory Group Policy and cross reference MDM documentation on MSDN to determine the support level, this would be labor intensive and error prone.

Microsoft created the **MDM Migration Analysis Tool** – aka MMAT[1] - to help. MMAT will determine which Group Policies have been set for a target user/computer and cross-reference against its built-in list of supported MDM policies. MMAT will then generate both XML and HTML reports indicating the level of support for each Group Policy in terms of MDM equivalents.

If you have a Group Policy targeting Minimum Password Length, for instance, MMAT will detect this and tell you that MDM also support this policy. If you are using start up scripts, MMAT will report which ones you are using and indicate they are not supported by MDM.

The easiest way to get started with MMAT is to get started. Install MMAT's prerequisites, run it, and then examine the HTML report.

What MMAT can greatly speed your migration to MDM, please be aware…

> MMAT ONLY DOES A BEST-EFFORT ANALYSIS OF YOUR DOMAIN CONFIGURATION. MIGRATION TO MDM REQUIRES ADDITIONAL TECHNICAL, BUSINESS, AND POLICY CONSIDERATIONS BEYOND WHAT ANY AUTOMATED TOOL CAN PROVIDE. PLEASE READ THE CAVEATS BELOW BEFORE ACTUALLY TRANSITIONING.

Reach out to Microsoft!

Microsoft is releasing MMAT prior to the next Windows release because we want early feedback. We can use this to improve MMAT itself as well as the Operating System. Please contact us at mmathelp@microsoft.com to let us know about your good and bad experiences using MMAT. We want all feedback, but in particular:

- Are there any policies that MDM does not support that are critical for your migration? Please let us know what they are, why they are critical, and what substitutes (if any) you would want.
- Your experiences using MMAT itself, both good and bad:
    - Does the report "just make sense?" Or were there parts that could have been presented more clearly?

[1] Pronounced M-Mat. Not MMMat and certainly not MMMBop.

- Is there missing data that the report should add?
- Please carefully review MMAT's caveats. Do they make sense? Are any particularly concerning to you?

The more information you can provide Microsoft in your report, the better. We will take all output of MMAT, including HTML, XML, logs, and Get-GPOReport* intermediate files. This will be the most useful since we can get a good idea of how Group Policy and MDM transitions will happen in practice.

If you are not comfortable sharing this much data with Microsoft, please share as much as you can. Even a single sentence "Policy <Foo> is critical but not in your MDM supported list, please add it because <…>" is helpful.

MMAT Invocation

MMAT runs in two phases. In the first phase, you invoke the included PowerShell script which will query the target user and computer and cache these results. In the second phase, an EXE is invoked which compares the cached domain query against the built-in allow list.

Usage

MMAT by default runs against the currently logged on user/machine but can be configured to target a different user/machine via PowerShell arguments.

To have MMAT use Group Policies applied to the currently logged on user and on the current computer as the basis for comparing against MDM, you should:

- Install Remote Server Administration Tools.[2]
- Copy the contents of installation directories that contain the PowerShell script, EXE, and XML and XSLT files to your PC.
- Open a PowerShell Window running as an Admin.
- Enable script execution if needed, e.g. <<Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope Process>>
- Recommended, increase verbosity by <<Set $VerbosePreference="Continue">>
  - Invoke-MdmMigrationAnalysisTool.ps1 may take a few minutes. Increasing verbosity will allow you to better monitor progress.
- Invoke-MdmMigrationAnalysisTool.ps1 -collectGPOReports –runAnalysisTool

When Invoke-MdmMigrationAnalysisTool.ps1 is through, it will generate:

- MDMMigrationAnalysis.xml: XML report containing information about policies for the target user and computer and how they map, if at all, to MDM.
- MDMMigrationAnalysis.html: HTML representation of the XML report.
- MdmMigrationAnalysisTool.log: A log file with more details about the MMAT run.

[2] Windows 7 and Windows Server 2008 - https://www.microsoft.com/en-us/download/details.aspx?id=7887
Windows 8 and Windows Server 2012 - https://www.microsoft.com/en-us/download/details.aspx?id=28972
Windows 10 - https://www.microsoft.com/en-us/download/details.aspx?id=45520

Output Directory Related Switches

You can optionally pass Invoke-MdmMigrationAnalysisTool.ps1 the following flags.

-gpoReportOutputDirectory: Stores the intermediate GPOReport-*.xml in specified directory.
-analysisToolOutputDirectory: Stores the generated reports and log in specified directory.

Targeting a specific user or computer

You may want to target a remote computer or user, not the one currently logged in. Use these flags to the PowerShell script to do this:

- -targetUser: Name of the user to target
- -targetComputer: Name of the computer to target

Note that the user who calls Invoke-MDMMigrationAnalysisTool must have required privileges on the remote computer. The target user must have logged on at least once to the target computer, though they do not need to be logged on at the time the script is invoked against the target.

Targeting an entire domain

To query ALL GPO's on a domain, analogous to *Get-GPOReport -all*, do:

- -targetDomain: fully qualified domain name of domain to query

Note that -targetDomain is mutually exclusive with the -user/-computer options and if not set. If no parameters are set, MMAT will query the current user on the current machine.

Because -targetDomain queries all GPO's, you may end up getting a report on GPO's that are not used by any users / computers that you want to migrate to MDM – or any users at all if the GPO has been forgotten! The tradeoff of all this extra data is of course that there are no policies for a given domain that will not be turned up just because you selected the wrong mix of users / computers to query.

Interpreting the reports

In general, the HTML should be self-explanatory and not require further documentation. If there are elements that are confusing, please **Reach out to Microsoft**.

Running MMAT on non-English systems

MMAT currently only supports mapping English policy names between GP ⇔ MDM. This means if GP policies are returned in French – as they will on a French system – MMAT is going to be confused.

There is a workaround. On your system where you are invoking the MMAT script, install the English language pack. You do not have to uninstall existing languages. Set English to default and reboot. MMAT's policy query will now return English results and its policy table will work. You do **not** have to install the English language packs on all target systems. Just install it on the PC running MMAT and use -targetUser/-targetComputer to query other devices.

Caveats and Warnings

MMAT is a pre-release software for pre-release version of Windows

For Windows 10 Creators Update, Microsoft is adding the ability to more easily transition from Group Policy to MDM's in the OS itself. This is explained in the accompanying documentation. This feature and the policies that it will natively support in the OS are not yet released and may change prior to release.

MMAT itself is being released in a pre-release version. We are doing this to get into the hands of our IT partners and MDM vendor hands sooner than later. If you hit issues, please **Reach out to Microsoft.**

MMAT is a best effort reporting tool

While MMAT has been tested internally prior to release, it has not been tested on all possible combinations of domains, forests, OU's, etc. MMAT will learn as much about your domain as it can and translate that into MDM readiness. But there may be cases it cannot handle. You still need to do some level of manual validation that your domain is ready.

MMAT reports policy conflicts but does not resolve them

Suppose that two different GPO's set MinimumPasswordLength. Because MMAT queries the GPO's themselves, not the RSOP, MMAT will contain values for both MinimumPasswordLength in its reports. In general the fact that a given policy is being used and whether or not it's supported on MDM should be the most important piece of data for your migration. Those few cases where policies conflict will need to be addressed during MDM ingestion time.

Choose your Target User / Machine Carefully – Especially WMI Filtering Considerations

The target users and computers that you run MMAT against should be chosen with care. They should obviously represent the population(s) that you intend to migrate to MDM.

Just as importantly is understanding MMAT's interaction with WMI filtering. GPO's may be disabled for given machines with WMI filtering. For instance, a GPO may apply to all computers in the Accounting OU *except* computers from Contoso-Manufacturer that are running Windows 7. When MMAT queries which GPO's to build up its mapping table from, it ignores any GPO's that are filtered out for the targeted user and computer.

This means that if you building up an MDM Migration plan for the Accounting OU, but you use as your MDM comparison a Windows 7 Contoso-Manufacturer PC, then you will not take into account any GPO's that were associated with it even though these may have made sense to carry over to MDM for the general population.

MMAT is not an automated process

As stated above, MMAT helps with only the initial, inventory phase of Group Policy => MDM Migration. Additional stages in the migration include but are not limited to:

- Mitigating policies that MDM does not support.
- Doing legal/security/business analysis of MDM in general and policies specifically.
- Understanding which policies, even if supported by MDM, are vestigial and should not be carried forward in any event.

- Pre-testing deployments to MDM

Current MMAT does not consider per SKU

There may be MDM policies that are only available on Windows Enterprise, Windows Pro, or other specific SKU's. The MMAT tool does not currently have a "targetSku" support but instead shows which MDM policies are available on any SKU, which may or may not be your ultimate target.

No Local GPO Integration

MMAT does not consider any policy configured in the Local GPO in its reports.

Group Policy Only, No Other Management Systems

Group Policy is one many technologies available to manage Windows devices. Windows can also be configured with SCCM, MDM, WMI, PowerShell, third party management solutions, or even custom software created by the IT department.

MMAT only queries Group Policies. If you are using other management technologies to configure your target machine and wish to migrate this logic to MDM as well, MMAT will not be able to help you.

HTML report show whether policies are enabled or disabled, not more complex policies

Most Group Policies are simple enabled/disabled/not configured tri-states. Some policies, however, need more complex configuration. In the generated HTML reports, MMAT will not include the more specific, complex policies being used. Instead it will simply report the enabled/disabled state. It does this for brevity. Knowing a policy is set and whether MDM supports it is often enough.

To see such a policy, open gpedit.msc. Go to Computer Configuration->Administrative Templates->Printers, then select Point and Print Restrictions. There are Options beyond enable/disable to set.

The actual values set are recorded in the XML report if you need to analyze them.

Reporting ALL registry values as configurable via ADMX

When MMAT encounters registry backed policies, it will indicate that these are supported if the IT or MDM vendor creates a custom ADMX to describe that registry and applies that ADMX to the OS. This ADMX ingestion is a coming, built-in Windows feature and a critical component to help to migrate to MDM.

MMAT will list **all** registry values it encounters as eligible to be configured via custom ADMX. However, i**f the policy is a Windows setting, do not try to use custom ADMX on MDM to configure it.** Even if it works, it would not be supported and may break in future releases.

Future versions of MMAT may have more knowledge about which registry settings are Windows specific and should be listed in "Not supported by MDM". Until MMAT is upgraded, caution must be used. Microsoft's policy about which Windows settings will be explicitly blocked by MDM during the OS runtime itself is still subject to change.

Do not modify MDMPolicyMapping.xml

MDMPolicyMapping.xml is the list of policies that MDM's can support, as well metadata about which version/SKU/partial support level is included.

MDMPolicyMapping.xml ships as a separate file, not an embedded resource in MdmMigrationAnalysisTool.exe, to help you understand which policies are supported. That said, **do not modify MDMPolicyMapping.xml** – especially to add additional policies you believe MDM should support.

Your MDM vendor and/or the Operating System itself have checks that limit which policies shall be supported. Hacking the mapping XML will only create a report that lies to you about what is supported and causes problems during your deployment.

If you think a policy is critical that is missing from MDM, please **Reach out to Microsoft** and let us know. There may be technical limitations that prevent us from adding the policy you request, so while we can't make commitments we want to understand what the MDM migration pain points are in any event.

How MMAT Works

You don't have to understand how MMAT works to take advantage of it. *For the curious…*

MMAT works in three stages:

- Determine which Group Policy Object (GPO's) have been applied to the target user/computer. It does this via invocation of WMI's RSOP (Resultant Set of Operations) and in particular RSOP_GPO. It will then filter out GPO's that are marked as not enabled, access denied, or to be filtered out.
- For each GPO from the initial stage, query the Remote Server Administration Tools 'Get-GPOReport' PowerShell helper to get the GPO XML from the server. These are stored in GPOReport-{GPOGuid}.txt either in the current directory or else "-gpoReportOutputDirectory."
- Invoke MdmMigrationAnalysisTool.exe. MdmMigrationAnalysisTool.exe consumes the GPOReport-* files and compares them against its policy mapping table, MDMPolicyMapping.xml. MdmMigrationAnalysisTool.exe then generates the final reports.

You are free to read and modify the PowerShell script as you see fit, though be aware you may be getting yourself into unsupported scenarios doing this as the underlying MdmMigrationAnalysisTool.exe was only tested with the released PS1. Feel free to Reach out to Microsoft with any modifications you'd like to see in the next script release (either bug fixes or new features). We'll consider taking them, though we can't commit to doing so.