

Custom Policy Cheat Sheet

OMA-Goodness there's a lot of acronyms to know for custom policies.

- **OMA-DM**

The OMA Device Management Protocol (OMA DM) defines how SyncML is used for various management procedures.

<https://aka.ms/oma-dm>

<https://omaspecworks.org/membership/current-members/>

- **SyncML**

The OMA DM client communicates with the server over HTTPS and uses SyncML (**S**ynchronous **M**arkUp **L**anguage) as the message payload.

Response codes can be found in Windows event logs.

<https://aka.ms/syncml>

- **CSP**

A configuration service provider (CSP) is an interface to read, set, modify, or delete configuration settings on a broad set of devices. Microsoft started using CSPs with Windows Mobile 5.0. Open standard—unlike WMI.

Think, GPO client-side extensions.

<https://aka.ms/oma-uri>

- **OMA-URI**

Windows 10 can use Open Mobile Alliance Uniform Resource Identifier (OMA-URI) settings to configure different features. Mobile device management is built-in.

OMA-URI paths are used to create custom Intune policies.

Custom Policy Cheat Sheet

Policy CSP OMA-URI Path

- **Scope**

./Device

- **Sub-Category**

./Vendor/MSFT/Policy/Config/

- **AreaName**

RestrictedGroups

- **PolicyName**

ConfigureGroupMembership

Custom Policy Cheat Sheet

Policy CSP Custom Policy Definition

OMA-URI path

./Vendor/MSFT/Policy/Config/RestrictedGroups/ConfigureGroupMembership

Data type

XML


Custom XML

```
<?xml version="1.0"?>
- <groupmembership>
  - <accessgroup desc="Administrators">
    <member name="Administrator"/>
    <member name="S-1-12-1-2000207915-1299385509-563920268-1234567890"/>
    <member name="S-1-12-1-2337914333-1124758123-909008569-1234567890"/>
    <member name="AzureAD\User-1@domain.com"/>
    <member name="AzureAD\User-2@domain.com"/>
  </accessgroup>
</groupmembership>
```

Custom Policy Cheat Sheet

Policy CSP Custom Policy Definition

OMA-URI Settings

Name *	Local Administrators
Description	Based on Policy CSP - RestrictedGroups
OMA-URI *	./Vendor/MSFT/Policy/Config/RestrictedGroup...
Data type	String (XML file) 

Custom XML *

Custom XML *	Not configured
--------------	----------------

```
"localAdmins.xml"
```



```
1 <groupmembership>
2   <accessgroup desc = "Administrators">
3     <member name = "Administrator"/>
4     <member name = "S-1-12-1-2000207915-1299385509-5639202
5     <member name = "S-1-12-1-2337914333-1124758123-9090085
6     <member name = "AzureAD\User-1@domain.com"/>
7     <member name = "AzureAD\User-2@domain.com"/>
8   </accessgroup>
9 </groupmembership>
```

Custom Policy Cheat Sheet

Other Interesting Custom Policies

- MDMWinsOverGP
 - ./Vendor/MSFT/Policy/Config/ControlPolicyConflict/MDMWinsOverGP
 - Data type: Int
 - Value = 1
- SSPR (adds to **G**raphical Identification and **A**uthentication)
 - ./Vendor/MSFT/Policy/Config/Authentication/AllowAadPasswordReset
 - Data type: Int\
 - Value = 1