

How does MDM work in Windows 10?

- Michael Niehaus
- Global Technology Specialist @ Tanium
- Twitter @mniehaus
- Ex-MVP, ex-Microsoft, ex-IT Pro
- Michael@oofhours.com

Where and when did MDM start?



- Started by mobile phone providers in 2000
 - SyncML Initiative, with companies like Palm, Nokia, Ericsson, Motorola
 - Initially implemented over WAP, not HTTP
- Shifted to Open Mobile Alliance (OMA) in 2002
 - Open Mobile Alliance – Device Management (OMA-DM)
 - Version 1.2 was most popular, but 2.0 is the current version
- Microsoft adopted the protocol for Windows Phone and Windows 8.1/Windows RT 8.1 in 2013
 - Based on OMA-DM 1.2.1 from 2008
 - Remember »Bring Your Own Device»? Design decisions were based on that.
 - Can be implemented by anyone

What can MDM do and not do?



Can do:

- Setting policies (native MDM and ADMX-backed)
- Installing Office, single-file MSIs, UWP/Appx/MSIX apps
- Inventory of basic hardware, UWP apps
- Simple remote actions (reboot, reset)

Can't do:

- Installation of Win32 apps (beyond Office and single-file MSIs)
- Win32 app inventory
- Remote control
- Script execution

Windows 10 MDM: Two choices



Azure AD automatic enrollment

- Easiest option, but requires Azure AD Premium (or equivalent)
- Discovery based on Azure AD MDM settings (specifying URLs for the MDM service)
- Authentication is (obviously) based on Azure AD

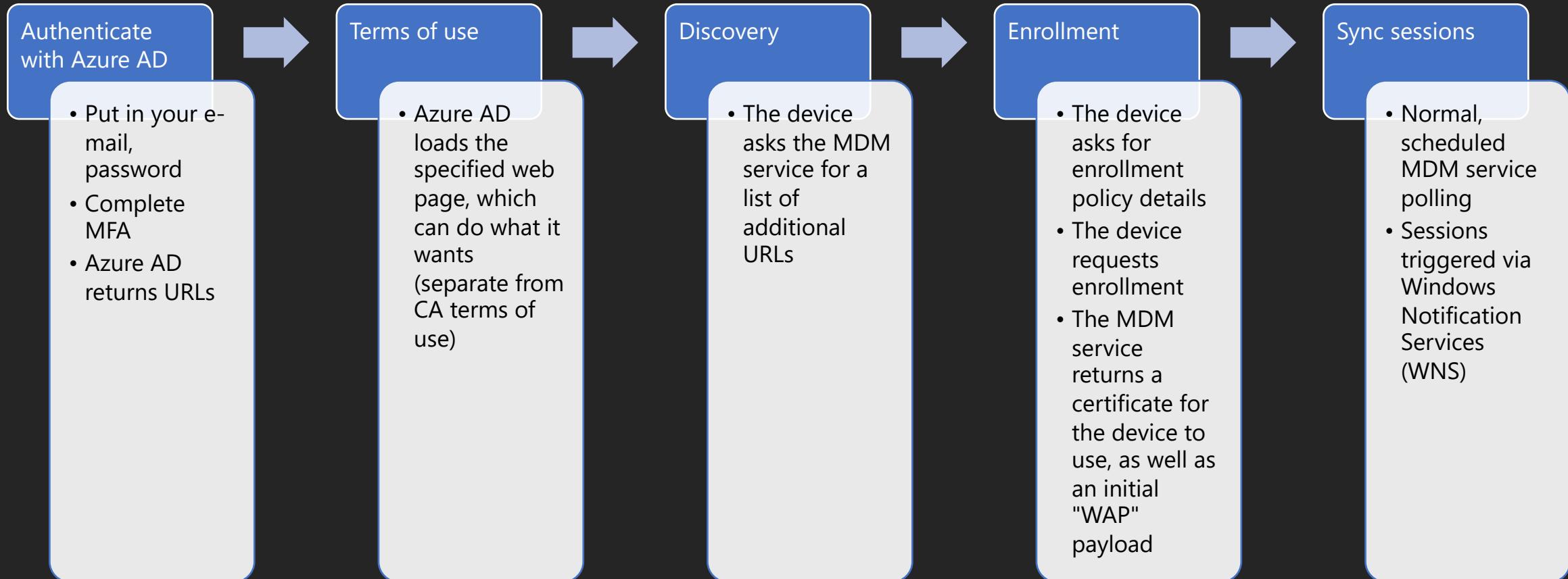
MDM-only enrollment

- Does not require Azure AD, but may still use it (depends on implementation)
- Leverages "enterpriseenrollment.domain.com" DNS entry to find the MDM service
- After discovery from that (redirected) URL, it works mostly the same

Want to watch?

- Communication uses HTTPS (TLS), so it's all encrypted
 - Leverage Fiddler to decrypt and capture the traffic
 - See [my blog](#) for more information on how to do this
 - Export the MDM client cert to see actual policies after the enrollment completes
- Even decrypted, it might still look like gibberish
 - SyncML can be tokenized using [WBXML](#), to reduce overhead in the protocol (based on XML/SOAP)
 - Some information can be Base64-encoded (e.g. to nest XML/SOAP payloads inside of XML/SOAP payloads)
 - Fiddler is very good at decoding payloads, even when nested

Azure AD automatic enrollment



Azure AD MDM settings



The screenshot shows the Microsoft Azure portal interface for configuring an On-premises MDM application. The URL in the address bar is https://portal.azure.com/#blade/Microsoft_AAD_IAM/ActiveDirectoryMenuBlade/Mobility. The page title is "Microsoft Azure". A search bar at the top right contains the placeholder "Search resources, services, and docs (G+/-)". The breadcrumb navigation shows "Home > Oofhours > Configure". The main heading is "Configure" followed by "On-premises MDM application". Below this, there are three buttons: "Save" (with a disk icon), "Discard" (with a cross icon), and "Delete" (with a trash bin icon). A horizontal line separates this from the configuration section. The first setting is "MDM user scope" with options "None", "Some", and "All", where "All" is selected. The second setting is "MDM terms of use URL" with the value <https://babymdm.oofhours.com/tou>, which has a green checkmark to its right. The third setting is "MDM discovery URL" with the value <https://babymdm.oofhours.com/discover>, also with a green checkmark. At the bottom, there is a link "On-premises MDM application settings".

MDM terms of use

This is your terms of use. You must accept to join and enroll.

<https://login.microsoftonline.com/WebApp/CloudDomainJoin/10>

4cb74235-be8c-0001-7258-b74c8cbed601

azureadjoin

Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6Im5PbzNaRHJPRFhFsFqS1doWHNsSFJS1hFZylsImtpZCI6Im5PbzNaRHJPRFhFsFqS1doWHNsSFJS1hFZyJSVt7_VwQ0ngHlmrzT21SSRF8S3FYswU-tCPEnR_elNWSoqQ0K55Daqjv5IR_zkjc64nmN0E4sGZkollEKwGyOu2sjY0gpExyivKP7SBKbMGclJzqMHGwedzb-uX_ydvyu8r2uxl4g9PtipBHUCelcZXvRC_2BnVGgy7tk3lfNBldD33Qsv8QR3obx2ruEsueJQywrAp65u8hX_yyWnCWL8ReQk6GUOEsQNk2aNwWvLqOFFWKnXP5

⊕

{
aud: 'https://babymdm.oofhours.com/',
iss: 'https://sts.windows.net/f28cef80-3f9b-49d7-921e-81b2bf60fd6c',
iat: 1612889828,
nbf: 1612889828,
exp: 1612893728,
acr: '1',
aio: 'AUQAu/8TAAAAMFv3RzQhl6TTihVLLqhgjkqEwe5WpzJgjEA1yX6qic',
amr: ['pwd', 'rsa', 'mfa'],
appid: '29d9ed98-a469-4536-ade2-f981bc1d605e',
appidacr: '0',
deviceid: 'f7b84542-ef9b-4eca-b739-35fd4e2178a4',
family_name: 'Niehaus',
given_name: 'Michael',
ipaddr: '73.42.162.199',
name: 'Michael Niehaus',
oid: '781a9aed-f357-48e9-9f06-1d5e42feea2c',
pwd_exp: '6005524',
pwd_url: 'https://portal.microsoftonline.com/ChangePassword.',
rh: '0.AAAAG0-M8ps_10mSHoGyv2D9bJjt2SlppDZFreL5gbwdYF52AC8.',
scp: 'mdm_delegation',
sub: 'r_hyIr6NMuFwIiPeePJr-L7vWMryiTqB5VdYVpjD0',
tid: 'f28cef80-3f9b-49d7-921e-81b2bf60fd6c',
unique_name: 'Michael@oofhours.com',
upn: 'Michael@oofhours.com',
uti: 'zd7-N3jlPkIGs408bbEbAA',
ver: '1.0'
}

MDM discovery

Progress Telerik Fiddler Web Debugger

File Edit Rules Tools View Help

WinConfig Replay Go Stream Decode | Keep: All sessions Any Process Find Save | Browse Clear Cache TextWizard |

#	Result	Protocol	Host	URL
255	200	HTTP	Tunnel to	babymdm.oofhours.com
256	200	HTTPS	babymdm...	/discover
257	200	HTTPS	babymdm...	/enrollment?client-re
258	200	HTTPS	babymdm...	/enrollment?client-re
259	200	HTTP	Tunnel to	aadcdn.msauth.net
260	200	HTTP	Tunnel to	aadcdn.msauth.net
261	200	HTTPS	aadcdn.m...	/ests/2.1/content/cc
262	200	HTTPS	aadcdn.m...	/ests/2.1/content/cc
263	200	HTTP	Tunnel to	babymdm.oofhours.com
264	200	HTTPS	babymdm...	/cimhandler?mode=N
265	200	HTTP	Tunnel to	babymdm.oofhours.com
266	200	HTTPS	babymdm...	/cimhandler?mode=N
267	200	HTTP	Tunnel to	geo.prod.do.dsp.mp
268	200	HTTP	Tunnel to	babymdm.oofhours.com
269	200	HTTPS	babymdm...	/cimhandler?mode=N
270	200	HTTPS	geo.prod....	/geo/?doClientVersio
271	200	HTTP	Tunnel to	geo.prod.do.dsp.mp
272	200	HTTPS	geo.prod....	/geoversion/?doClien
273	200	HTTP	Tunnel to	geo.prod.do.dsp.mp
274	200	HTTPS	geo.prod....	/geo/?doClientVersio
275	200	HTTP	Tunnel to	babymdm.oofhours.com
276	200	HTTP	ctldl.wind...	/msdownload/update
277	206	HTTPS	babymdm...	/7z1900-x64.msi
278	200	HTTP	Tunnel to	babymdm.oofhours.com
279	206	HTTPS	babymdm...	/7z1900-x64.msi
280	200	HTTP	Tunnel to	babymdm.oofhours.com
281	206	HTTPS	babymdm...	/7z1900-x64.msi
282	200	HTTP	Tunnel to	babymdm.oofhours.com
283	200	HTTPS	babymdm...	/cimhandler?mode=N
284	200	HTTP	Tunnel to	babymdm.oofhours.com
285	200	HTTPS	babymdm...	/cimhandler?mode=N
286	200	HTTP	Tunnel to	babymdm.oofhours.com
287	200	HTTPS	babymdm...	/cimhandler?mode=N

F Fiddler Orchestra Beta FiddlerScript Log Filters Timeline

Get Started Statistics Inspectors AutoResponder Composer

Request Headers [Raw] [Header Definitions]

POST /discover HTTP/1.1

Client

User-Agent: ENROLLClient

Entity

Content-Length: 1007

Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies

Raw JSON XML

```

HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: application/soap+xml; charset=utf-8
Content-Length: 1559
ETag: W/"617-d065s7Ia8Dg7UoofIreO4T0pRrk"
Date: Tue, 09 Feb 2021 17:02:08 GMT
Connection: keep-alive

<s:Envelope xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">http://schemas.microsoft.com/windows/management/2012/01/enrollment?client-request-id</a:Action>
    <ActivityId CorrelationId="dd4f1f6d-6ce8-4187-bc3c-3cd15e671be4" xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics">dd4f1f6d-6ce8-4187-bc3c-3cd15e671be4</ActivityId>
    <a:RelatesTo>urn:uuid:urn:uuid:748132ec-a575-4329-b01b-6171a9cf8478</a:RelatesTo>
  </s:Header>
  <s:Body>
    <DiscoverResponse xmlns="http://schemas.microsoft.com/windows/management/2012/01/enrollment?client-request-id">
      <DiscoverResult>
        <AuthPolicy>Federated</AuthPolicy>
        <AuthUrl>prod</AuthUrl>
        <AuthenticationServiceUrl>https://babymdm.oofhours.com/login?client-request-id=dd4f1f6d-6ce8-4187-bc3c-3cd15e671be4</AuthenticationServiceUrl>
        <EnrollmentPolicyServiceUrl>https://babymdm.oofhours.com/enrollment?client-request-id=dd4f1f6d-6ce8-4187-bc3c-3cd15e671be4</EnrollmentPolicyServiceUrl>
        <EnrollmentServiceUrl>https://babymdm.oofhours.com/enrollment?client-request-id=dd4f1f6d-6ce8-4187-bc3c-3cd15e671be4</EnrollmentServiceUrl>
        <FederatedServiceName>https://babymdm.oofhours.com/FederatedServiceName</FederatedServiceName>
        <FederatedServicePolicy>HBI_FED</FederatedServicePolicy>
      </DiscoverResult>
    </DiscoverResponse>
  </s:Body>
</s:Envelope>

```

MDM enrollment policy

Fiddler Orchestra Beta

Get Started Statistics Inspectors AutoResponder Composer FiddlerScript Log Filters Timeline

Headers TextView SyntaxView WebForms HexView Auth Cookies Raw JSON XML

s:Envelope [xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-username-token-1.0.xsd"]

 a:Action [\$mustUnderstand=1]
 http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy/IPolicy/GetPolicies

 a:MessageID
 a:UUID:72048864-0F19-448F-8C2E-B4C661860AA0
 a:ReplyTo
 a:Address
 http://www.w3.org/2005/08/addressing/anonymous
 a:To [\$mustUnderstand=1]
 wsse:Security [\$mustUnderstand=1]
 wsse:BinarySecurityToken [ValueType="urn:ietf:params:oauth:token-type:jwt" EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd#base64binary"]
 ZXIMGYYTQPaUpVPrRaUxSmhRZhpT2kU16STFoUz5W5nMRDSTZj6TVQYrp0YVJISBSmGU3pGcVmzG9XSE5zU0Zk2MxaEzaeUo5LnV5SmhkV1PpT2kb2RIundjem92TDJKaFlubHrRzB1YJ5WFHOTFjbk1WTI5dEx55XNbWx6Y3lNk...
 GetPolicies [xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy"]
 client
 <lastUpdate xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <preferredLanguage xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <requestFilter xsi:nil="true" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />

Expand All Collapse

Transformer Headers TextView SyntaxView ImageView HexView WebView Auth Caching Cookies Raw JSON XML

s:Envelope [xmlns:s="http://www.w3.org/2003/05/soap-envelope" xmlns:a="http://www.w3.org/2005/08/addressing"]
 s:Header
 a:Action [\$mustUnderstand=1]
 http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy/IPolicy/GetPoliciesResponse
 ActivityId [CorrelationId=4550ff25-0de4-49c8-71f998ba5af xmlns="http://schemas.microsoft.com/2004/09/ServiceModel/Diagnostics"]
 d4f1fd-ec8e-4187-bc3c-3cd15e67be4
 a:RelatesTo
 a:UUID:uuid:72048864-0F19-448F-8C2E-B4C661860AA0
 s:Body
 GetPoliciesResponse [xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy"]
 response
 <policyFriendlyName p6:nil="true" xmlns:p6="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <nextUpdateHours p6:nil="true" xmlns:p6="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <policesNotChanged p6:nil="true" xmlns:p6="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 policies
 policy
 policyOIDReference
 0
 attributes
 policySchema
 3
 privateKeyAttributes
 <minKeyLength
 2048
 <keySpec p10:nil="true" xmlns:p10="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <keyUsageProperty p10:nil="true" xmlns:p10="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <permissions p10:nil="true" xmlns:p10="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <algorithmOIDReference p10:nil="true" xmlns:p10="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <cryptoProviders p10:nil="true" xmlns:p10="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 useTPM
 false
 <supersededPolicies p9:nil="true" xmlns:p9="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <privateKeyFlags p9:nil="true" xmlns:p9="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <subjectNameFlags p9:nil="true" xmlns:p9="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <enrollmentFlags p9:nil="true" xmlns:p9="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <generalFlags p9:nil="true" xmlns:p9="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 hashAlgorithmOIDReference
 0
 <ARRequirements p9:nil="true" xmlns:p9="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <keyArchivalAttributes p9:nil="true" xmlns:p9="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 <extensions p9:nil="true" xmlns:p9="http://www.w3.org/2001/XMLSchema-instance" xmlns="http://schemas.microsoft.com/windows/pki/2009/01/enrollmentpolicy" />
 oIDs
 oID
 value
 2.16.840.1.101.3.4.2.1
 group
 2
 oIDReferenceID
 0

Expand All Collapse

JWT bearer token

Certificate requirements

MDM enrollment

The screenshot shows an MDM enrollment request message captured by the Fiddler tool. The message is structured as follows:

- s:header**: Contains standard SOAP headers.
- s:body**: Contains the main body of the message.
- s:body wst:RequestSecurityToken**: This section is highlighted with a red box and contains a large amount of XML data. It includes:
 - wst:RequestType**
 - wsse:BinarySecurityToken** [ValueType=http://schemas.microsoft.com/windows/pk/2009/01/enrollment#PKCS10 EncodingType=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd #base64binary]

A blue arrow points from the highlighted section to the text "Certificate request".

Below this, another blue arrow points to the "Device details" section, which is also highlighted with a red box. This section contains detailed information about the device being enrolled, such as device name, MAC address, and various context items.

The bottom part of the screenshot shows the response message, also with a red box highlighting the certificate-related XML.

→ Certificate request

→ Device details

→ Certificate and "other stuff"

MDM enrollment WAP settings

```
<characteristic type="APPLICATION">
<pam name="APID" value="w7" />
<pam name="PROVIDER-ID" value="BabyMDM" />
<pam name="NAME" value="Oofhours" />
<pam name="SSPHyperlink" value="https://babymdm.oofhours.com/selfservice" />
<pam name="ServerList" value="https://babymdm.oofhours.com/cimhandler" />
<pam name="ADPR" value="https://babymdm.oofhours.com/cimhandler" />
<pam name="CRLcheck" value="0" />
<pam name="CONNTRYFREQ" value="6" />
<pam name="INITIALBACKOFFTIME" value="30000" />
<pam name="MAXBACKOFFTIME" value="120000" />
<pam name="DEFAULTENCODING" value="application/vnd.syncml.dm+xml" />
<pam name="ROLE" value="http://schemas.microsoft.com/2009/06/7295" />
<pam name="BACKCOMPATTRYDISABLED" />
<characteristic type="APPAUTH">
<pam name="AAUTHLEVEL" value="APPSRV" />
<pam name="AAUTHTYPE" value="DIGEST" />
<pam name="AAUTHNAME" value="dummy" />
<pam name="AAUTHSECRET" value="dummy" />
<pam name="AAUTHDATA" value="nonce" />
</characteristic>
<characteristic type="Registry">
<characteristic type="HKLM\Software\Microsoft\Provisioning\OmaDm">
<pam name="ConnSendRecvTimeout" value="180000" datatype="integer" />
</characteristic>
<characteristic type="DMClient">
<characteristic type="Provider">
<characteristic type="BabyMDM">
<pam name="EntDeviceName" value="Michael_Windows_10/22/2020_7:28 PM" datatype="string" />
<pam name="AADResourceId" value="https://babymdm.oofhours.com/" datatype="string" />
<characteristic type="Poll">
<pam name="NumberOfFirstRetries" value="5" datatype="integer" />
<pam name="IntervalForFirstSetOfRetries" value="3" datatype="integer" />
<pam name="NumberOfSecondRetries" value="8" datatype="integer" />
<pam name="IntervalForSecondSetOfRetries" value="15" datatype="integer" />
<pam name="NumberOfRemainingScheduledRetries" value="0" datatype="integer" />
<pam name="IntervalForRemainingScheduledRetries" value="480" datatype="integer" />
</characteristic>
<characteristic type="FirstSyncStatus">
<pam name="ExpectedPolicies" value=".\\Vendor\\MSFT\\Policy\\Config" datatype="string" />
<pam name="TimeOutUntilSyncFailure" value="60" datatype="integer" />
<pam name="BlockInStatusPage" value="7" datatype="integer" />
<pam name="SkipDeviceStatusPage" value="false" datatype="boolean" />
<pam name="SkipUserStatusPage" value="false" datatype="boolean" />
<pam name="AllowCollectLogsButton" value="true" datatype="boolean" />
<pam name="CustomErrorText" value="Installation exceeded the time limit set by your organization. Please try again or contact your IT support person for help." datatype="string" />
</characteristic>
</characteristic>
<characteristic type="EnrollmentStatusTracking">
<characteristic type="DevicePreparation">
<characteristic type="PolicyProviders">
<characteristic type="BabyMDMProvider">
<pam name="InstallationState" value="2" datatype="integer" />
</characteristic>
</characteristic>
</characteristic>
<characteristic type="PassportForWork">
<characteristic type="128c80-39b-49d7-921e-81b2bf60fd6c">
<characteristic type="Policies">
<pam name="UsePassportForWork" value="0" datatype="boolean" />
<pam name="RequireSecurityDevice" value="0" datatype="boolean" />
<characteristic type="PINComplexity">
<pam name="MinimumLength" value="4" datatype="integer" />
<pam name="MaximumPINLength" value="16" datatype="integer" />
<pam name="UppercaseLetters" value="2" datatype="integer" />
<pam name="LowercaseLetters" value="2" datatype="integer" />
<pam name="SpecialCharacters" value="2" datatype="integer" />
<pam name="History" value="0" datatype="integer" />
<pam name="Expiration" value="0" datatype="integer" />
</characteristic>
<characteristic type="Remote">
<pam name="UseRemotePassport" value="1" datatype="boolean" />
</characteristic>
</characteristic>
<pam name="UseBiometrics" value="1" datatype="boolean" />
</characteristic>
```

- ➡ w7 Application CSP
 - Sets the “default encoding” (in this case, making SyncML as XML instead of WBXML)
- ➡ Registry CSP
 - Pokes in random values
- ➡ DMClient CSP
 - Specifies sync intervals, enables enrollment status page
- ➡ Enrollment status page CSP
 - Enables additional “policy providers”
- ➡ Passport for Work CSP
 - Configures (e.g. disables) Windows Hello for Business

MDM sync schedules

- The service specifies how often devices should sync
- Typical setup:
 - Every three minutes for the first 15 minutes after enrollment
 - Every 15 minutes for the next two hours after enrollment
 - Every 8 hours from that point forward
- Scheduled tasks are used to perform the syncs
- You can override the sync settings using a custom OMA-URI policy (see DMClient CSP)
 - Recreates the scheduled tasks when the new policy is received
 - Want to drive an MDM service crazy? Configure all clients to poll very frequently...
- The service can leverage Windows Notification Services (WNS) to trigger sync sessions on demand

MDM sync session

Fiddler screenshot showing an MDM sync session. The request header shows a POST to https://babymdm.oofhours.com/cimhandler?mode=Maintenance&Platform=wOA. The response body is a large XML document representing the sync session.

```

POST https://babymdm.oofhours.com/cimhandler?mode=Maintenance&Platform=wOA HTTP/1.1
Connection: Keep-Alive
Content-Type: application/vnd.syncml.dmxml
Accept: application/vnd.syncml.dmxml, application/vnd.syncml.dmxml+xml, application/octet-stream
Accept-Charset: UTF-8
User-Agent: MSFT OMA DM Client/1.2.0.1
Content-Length: 1159
Host: babymdm.oofhours.com

<SyncML xmlns="SYNCML:SYNCML1.2"><SyncHdr><VerDTD>1.2.</VerDTD><VerProto>DM/1.2.</VerProto><SessionID>1</SessionID><MsgID>1</MsgID><Target><LocURI>https://babymdm.oofhours.com/cimhandler</LocURI></Target><Source><LocURI>984480A166AE3D45AE23B26D88AFDD02</LocURI></Source></SyncHdr><SyncBody><Status><CmdID>1</CmdID><MsgRef></MsgRef><CmdRef></CmdRef><SyncHdr><Cmds><Data>200</Data></Status><Status><CmdID>2</CmdID><MsgRef></MsgRef><CmdRef>2</CmdRef><CmdAlert></CmdAlert><Data>200</Data></Status><Status><CmdID>3</CmdID><MsgRef></MsgRef><CmdRef>3</CmdRef><CmdAlert></CmdAlert><Data>200</Data></Status><Status><CmdID>4</CmdID><MsgRef></MsgRef><CmdRef>4</CmdRef><CmdAlert></CmdAlert><Data>200</Data></Status><Status><CmdID>5</CmdID><MsgRef></MsgRef><CmdRef>5</CmdRef><CmdReplace></CmdReplace><Data>200</Data></Status><Replace><CmdID>6</CmdID><Item><Target><LocURI>./Vendor/MSFT/DMClient/Provider/BabyMDM/Poll/PollOnLogin</LocURI></Target><Data><Format xmlns="syncml:metinf">bool</Format><Type xmlns="syncml:metinf">text/plain</Type><Meta><true></Data></Item><Replace><CmdID>7</CmdID><Item><Target><LocURI>./Vendor/MSFT/DMClient/Provider/BabyMDM/Push/PFN</LocURI></Target><Data>1728karoshiware.BabyMDM</Data></Item><Replace><CmdID>7</CmdID><Item><Target><LocURI>./Vendor/MSFT/PassportForWork/f28cef80-3f9b-49d7-921e-81b2bf60fd6c/Policies/UsePassportForWork</LocURI></Target><Data><Format xmlns="syncml:metinf">bool</Format>
  
```

→ Client initiates the sync session (always)

→ Service first acknowledges requests from client

→ Service then sends any new policies

MDM sync session

```
<Replace>
  <CmdID>7</CmdID>
  <Item>
    <Target>
      <LocURI>./Vendor/MSFT/PassportForWork/f28cef80-3f9b-49d7-921e-81b2bf60fd6c/Policies/UsePassportForWork</LocURI>
    </Target>
    <Meta>
      <Format xmlns="syncml:metinf">bool</Format>
      <Type xmlns="syncml:metinf">text/plain</Type>
    </Meta>
    <Data>false</Data>
  </Item>
</Replace>
<Replace>
  <CmdID>7</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/Policy/Config/WindowsLogon/EnableFirstLogonAnimation</LocURI>
    </Target>
    <Meta>
      <Format xmlns="syncml:metinf">int</Format>
      <Type xmlns="syncml:metinf">text/plain</Type>
    </Meta>
    <Data>0</Data>
  </Item>
</Replace>
<Get>
  <CmdID>8</CmdID>
  <Item>
    <Target>
      <LocURI>./DevDetail/Ext/Microsoft/ProcessorArchitecture</LocURI>
    </Target>
  </Item>
</Get>
<Get>
  <CmdID>9</CmdID>
  <Item>
    <Target>
      <LocURI>./Vendor/MSFT/DMClient/Provider/BabyMDM/AADDeviceID</LocURI>
    </Target>
  </Item>
</Get>
<Get>
  <CmdID>10</CmdID>
  <Item>
    <Target>
      <LocURI>./DevDetail/Ext/DeviceHardwareData</LocURI>
    </Target>
  </Item>
</Get>
```

→ Turn off Hello

→ Turn off first logon animation

→ Report hardware/OS details

- Processor architecture
- AAD device ID
- Hardware hash

```
<Add>
  <CmdID>11</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/EnterpriseDesktopAppManagement/MSI/%7B23170F69-40C1-2702-1900-000001000000%7D/DownloadInstall</LocURI>
    </Target>
  </Item>
</Add>
<Exec>
  <CmdID>12</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/EnterpriseDesktopAppManagement/MSI/%7B23170F69-40C1-2702-1900-000001000000%7D/DownloadInstall</LocURI>
    </Target>
    <Meta>
      <Format xmlns="syncml:metinf">xml</Format>
      <Type xmlns="syncml:metinf">text/plain</Type>
    </Meta>
    <Data>
      <MsiInstallJob id="{23170F69-40C1-2702-1900-000001000000}">
        <Product Version="7.8.9">
          <Download>
            <ContentURLList>
              <ContentURL>https://babymdm.oofhours.com/7z1900-x64.msi</ContentURL>
            </ContentURLList>
          </Download>
          <Validation>
            <FileHash>A7803233EEDB6A4B59B3024CCF9292A6FFF94507DC998AA67C5B745D197A5DC</FileHash>
          </Validation>
          <Enforcement>
            <CommandLine>/qn</CommandLine>
            <RetryCount>3</RetryCount>
            <RetryInterval>5</RetryInterval>
          </Enforcement>
        </Product>
      </MsiInstallJob>
    </Data>
  </Item>
</Exec>
```

MDM sync session

```
<Replace>
  <CmdID>13</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/DMClient/Provider/BabyMDM/FirstSyncStatus/ExpectedMSIAppPackages</LocURI>
    </Target>
    <Data>./Device/Vendor/MSFT/EnterpriseDesktopAppManagement/MSI/%7B23170F69-40C1-2702-1900-000001000000%7D/Status;1</Data>
  </Item>
</Replace>
<Replace>
  <CmdID>14</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/DMClient/Provider/BabyMDM/FirstSyncStatus/ExpectedPolicies</LocURI>
    </Target>
    <Data>./Device/Vendor/MSFT/DMClient/Provider/BabyMDM/EntDMID</Data>
  </Item>
</Replace>
<Replace>
  <CmdID>15</CmdID>
  <Item>
    <Target>
      <LocURI>./Device/Vendor/MSFT/DMClient/Provider/BabyMDM/FirstSyncStatus/ServerHasFinishedProvisioning</LocURI>
    </Target>
    <Meta>
      <Format xmlns="syncml:metinf">bool</Format>
      <Type xmlns="syncml:metinf">text/plain</Type>
    </Meta>
    <Data>true</Data>
  </Item>
</Replace>
```

Demo

What does the future look like?



- OS vendors are slowly taking control
 - Want to manage a Chromebook? Use Google's service.
 - Third-party MDM services then communicate indirectly to client devices
- ISVs depend on separate agents to extend functionality
 - They move faster than the OS vendors
 - This in effect defeats the idea of “agentless” management
 - Some OSes will prevent this...

Q&A



- Contact me at Michael@oofhours.com or via Twitter @mniehaus



Thank you!

MSEndPointMgr.com
#MSEndPointMgr

System Center User Group
Finland
#SCUGFI

System Center User Group
Denmark
#SCUGDK

System Center User Group
Sweden
#SCUGSE

Modern Management User Group
Norway
#MMUGNO