#NVSummit2021

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

NORDIC — VIRTUAL SUMMIT —

Where and when did MDM start?

NORDIC
– VIRTUAL SUMMIT –

- 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?

NORDIC
– VIRTUAL SUMMIT –

Can do:	Can't 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)	• Installation of Win32 apps (beyond Office and single-file MSIs) • Win32 app inventory • Remote control • Script execution

Windows 10 MDM: Two choices

NORDIC
– VIRTUAL SUMMIT –

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?

NORDIC
– VIRTUAL SUMMIT –

- 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

Authenticate with Azure AD

- Put in your e-mail, password
- Complete MFA
- Azure AD returns URLs

Terms of use

- Azure AD loads the specified web page, which can do what it wants (separate from CA terms of use)

Discovery

- The device asks the MDM service for a list of additional URLs

Enrollment

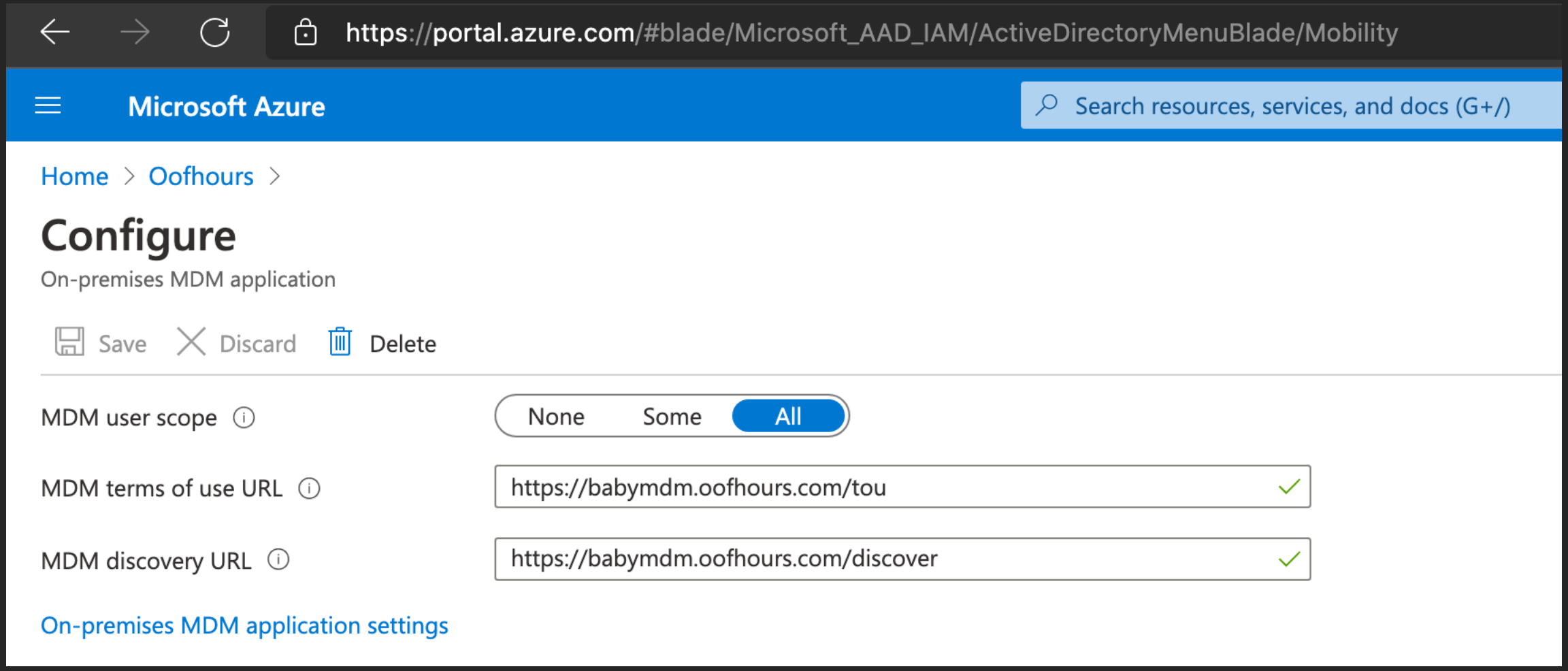
- The device asks for enrollment policy details
- The device requests enrollment
- The MDM service returns a certificate for the device to use, as well as an initial "WAP" payload

Sync sessions

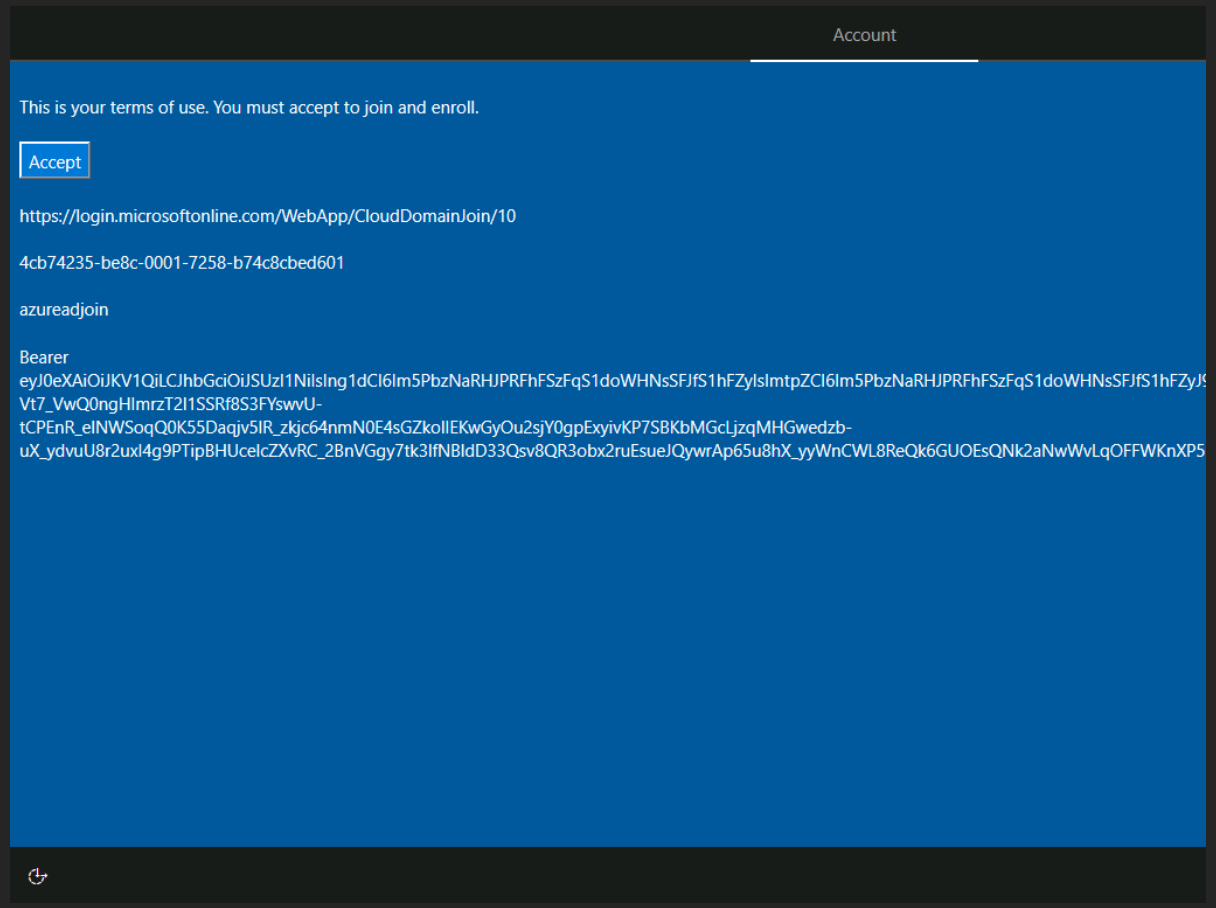
- Normal, scheduled MDM service polling
- Sessions triggered via Windows Notification Services (WNS)

Azure AD MDM settings

NORDIC
– VIRTUAL SUMMIT –

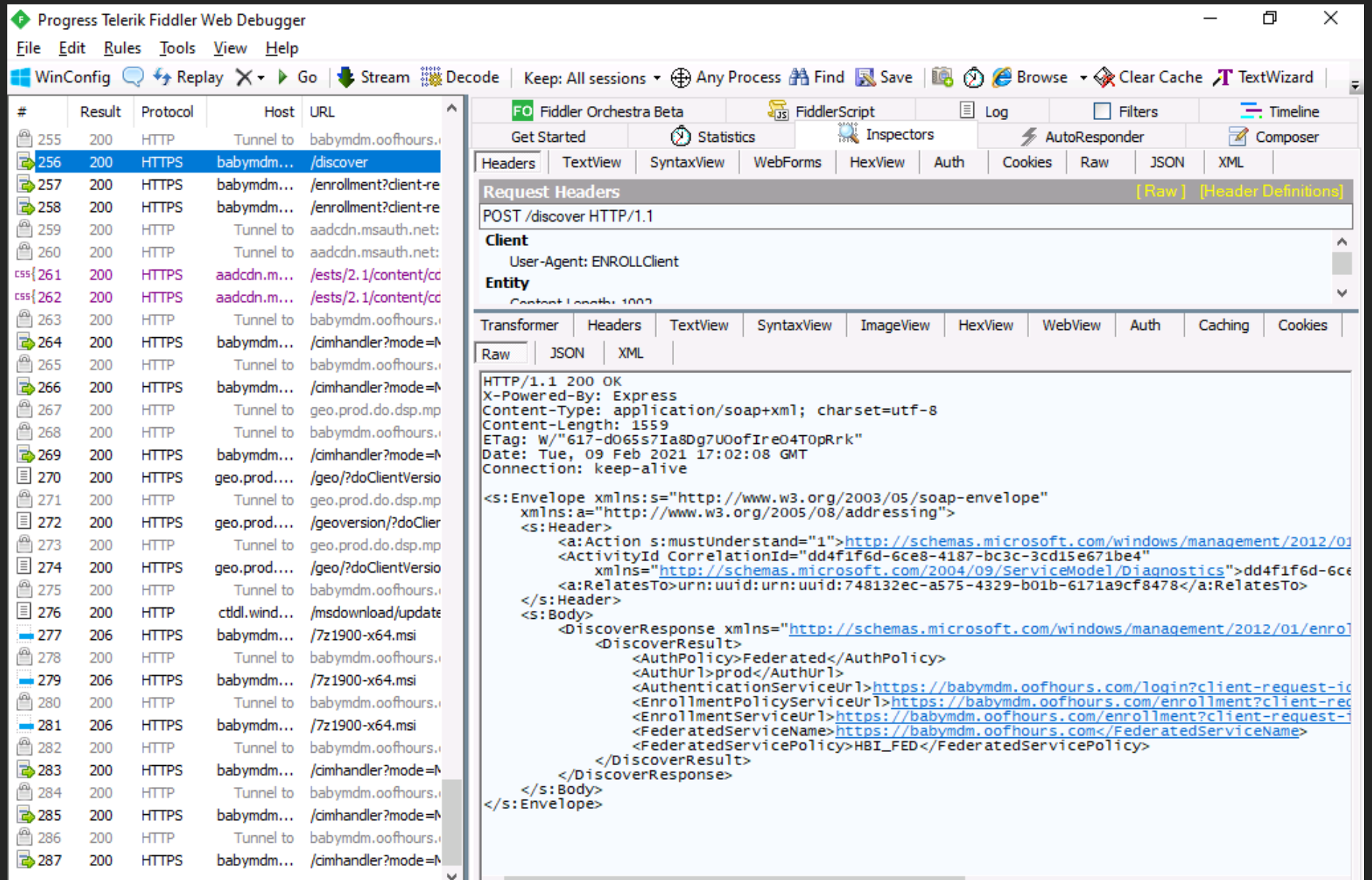


MDM terms of use

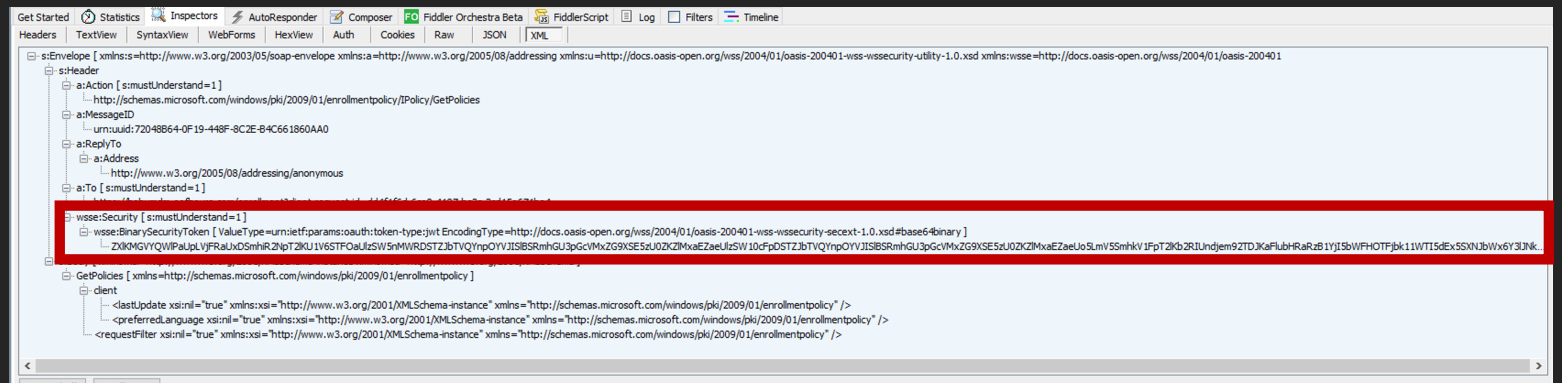



```
{
  aud: 'https://babymdm.oofhours.com/',
  iss: 'https://sts.windows.net/f28cef80-3f9b-49d7-921e-81b2bf
  iat: 1612889828,
  nbf: 1612889828,
  exp: 1612893728,
  acr: '1',
  aio: 'AUQAu/8TAAAAMFv3RzQhl6TTihVLLqhgjkqEwe5WpzJgjEA1yX6qic
  amr: [ 'pwd', 'rsa', 'mfa' ],
  appid: '29d9ed98-a469-4536-ade2-f981bc1d605e',
  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.AAAAgO-M8ps_10mSHoGyv2D9bJjt2SlppDZFreL5gbwdYF52AC8.'
  scp: 'mdm_delegation',
  sub: 'r_hyIr6NMuFwIiPeePJr-L7vWMryiZTqB5VdYVpjoD0',
  tid: 'f28cef80-3f9b-49d7-921e-81b2bf60fd6c',
  unique_name: 'Michael@oofhours.com',
  upn: 'Michael@oofhours.com',
  uti: 'zd7-N3jlPkiGs4O8bbEbAA',
  ver: '1.0'
}
```

MDM discovery



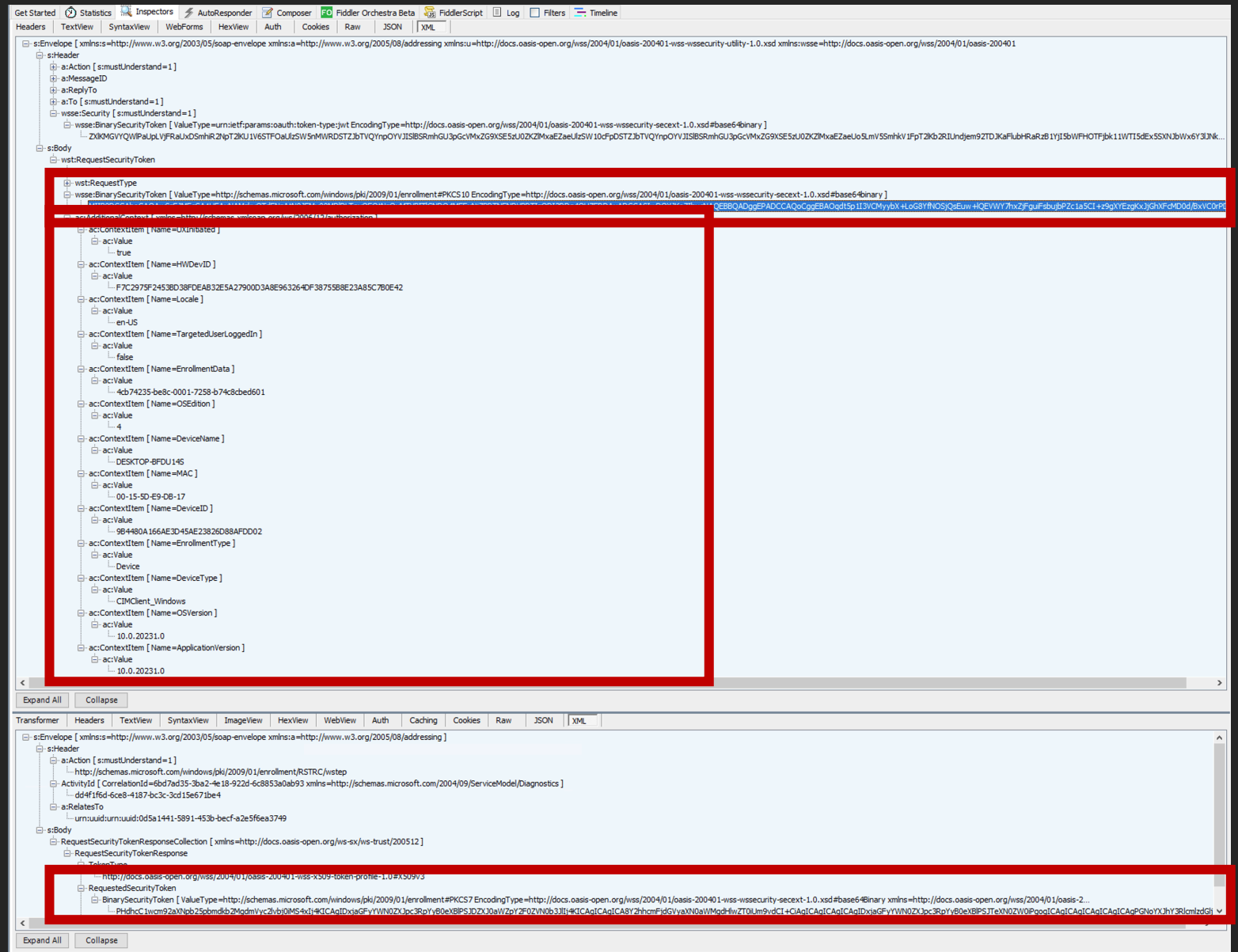
MDM enrollment policy



JWT bearer token

Certificate requirements

MDM enrollment

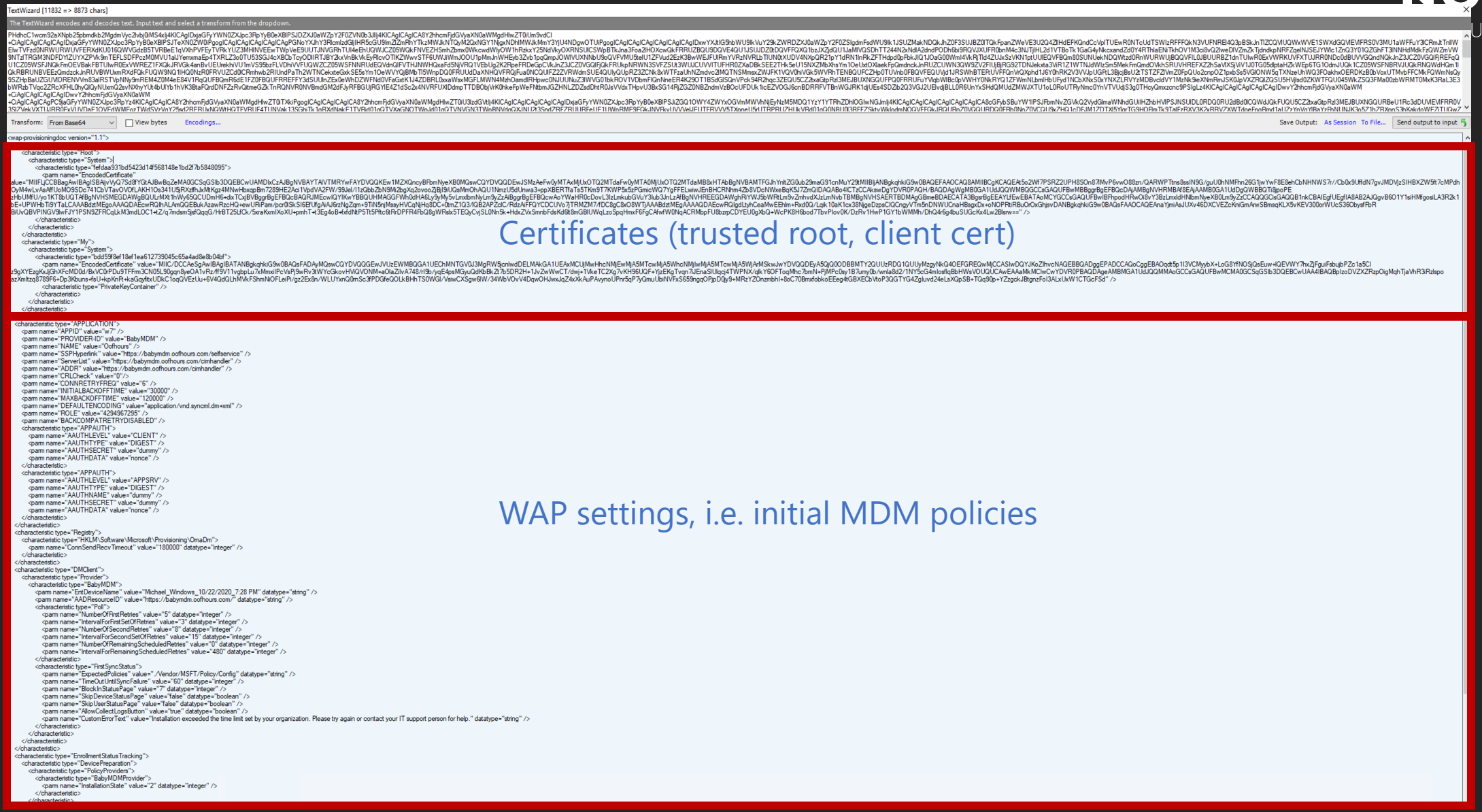


Certificate request

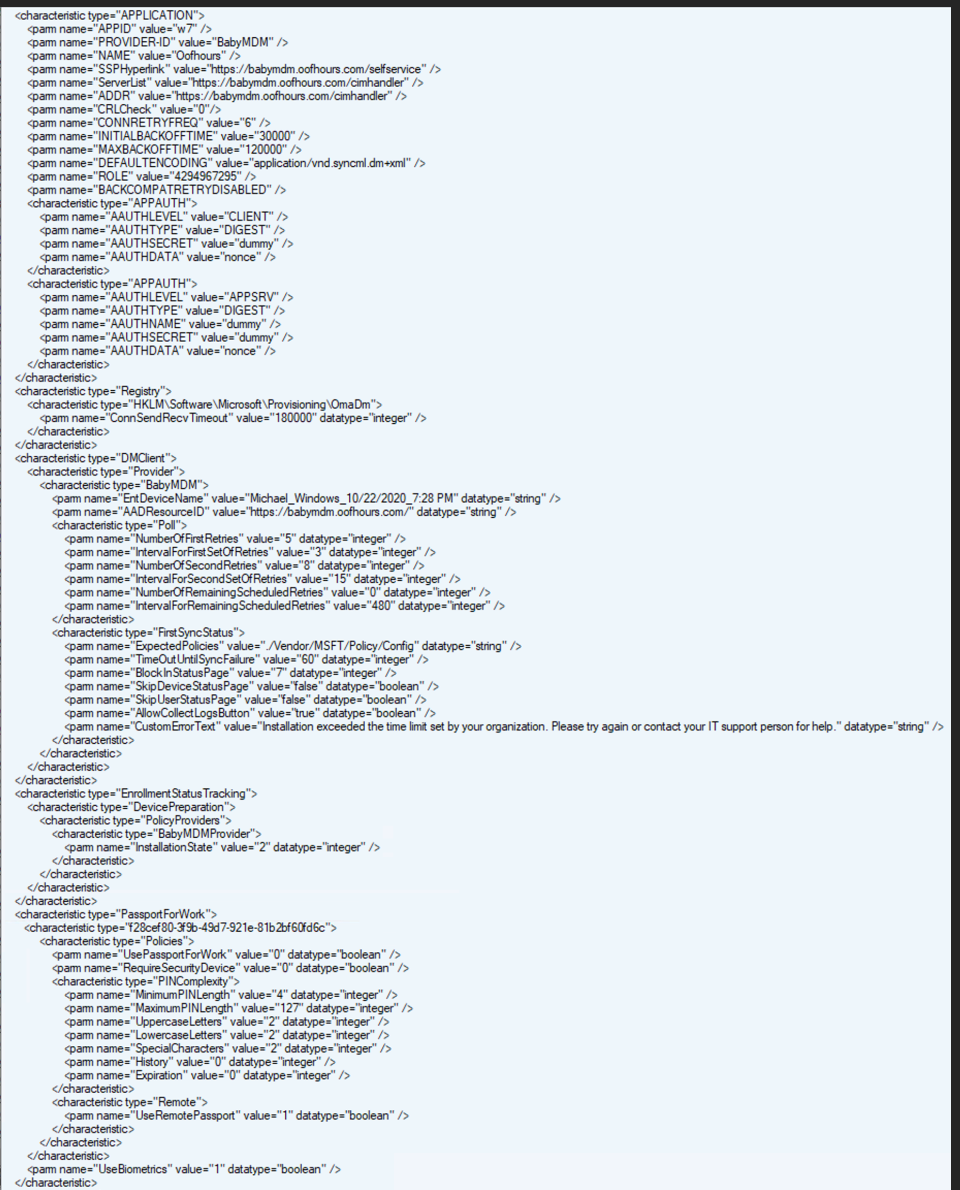
Device details

Certificate and "other stuff"

MDM enrollment



MDM enrollment WAP settings



```
<characteristic type="APPLICATION">
  <parm name="APPID" value="w7" />
  <parm name="PROVIDER-ID" value="BabyMDM" />
  <parm name="NAME" value="Oofhours" />
  <parm name="SSPHyperlink" value="https://babymdm.oofhours.com/selfservice" />
  <parm name="ServerList" value="https://babymdm.oofhours.com/cimhandler" />
  <parm name="ADDR" value="https://babymdm.oofhours.com/cimhandler" />
  <parm name="CRLCheck" value="0" />
  <parm name="CONNRETRYFREQ" value="6" />
  <parm name="INITIALBACKOFFTIME" value="30000" />
  <parm name="MAXBACKOFFTIME" value="120000" />
  <parm name="DEFAULTENCODING" value="application/vnd.syncml.dm+xml" />
  <parm name="ROLE" value="4294967295" />
  <parm name="BACKCOMPATRETRYDISABLED" />
  <characteristic type="APPAUTH">
    <parm name="AAUTHLEVEL" value="CLIENT" />
    <parm name="AAUTHTYPE" value="DIGEST" />
    <parm name="AAUTHSECRET" value="dummy" />
    <parm name="AAUTHDATA" value="nonce" />
  </characteristic>
  <characteristic type="APPAUTH">
    <parm name="AAUTHLEVEL" value="APPSRV" />
    <parm name="AAUTHTYPE" value="DIGEST" />
    <parm name="AAUTHNAME" value="dummy" />
    <parm name="AAUTHSECRET" value="dummy" />
    <parm name="AAUTHDATA" value="nonce" />
  </characteristic>
</characteristic>
<characteristic type="Registry">
  <characteristic type="HKLM\Software\Microsoft\Provisioning\OmaDm">
    <parm name="ConnSendRecvTimeout" value="180000" datatype="integer" />
  </characteristic>
</characteristic>
<characteristic type="DMClient">
  <characteristic type="Provider">
    <characteristic type="BabyMDM">
      <parm name="EntDeviceName" value="Michael_Windows_10/22/2020_7:28 PM" datatype="string" />
      <parm name="AADResourceID" value="https://babymdm.oofhours.com/" datatype="string" />
      <characteristic type="Poll">
        <parm name="NumberOfFirstRetries" value="5" datatype="integer" />
        <parm name="IntervalForFirstSetOfRetries" value="3" datatype="integer" />
        <parm name="NumberOfSecondRetries" value="8" datatype="integer" />
        <parm name="IntervalForSecondSetOfRetries" value="15" datatype="integer" />
        <parm name="NumberOfRemainingScheduledRetries" value="0" datatype="integer" />
        <parm name="IntervalForRemainingScheduledRetries" value="480" datatype="integer" />
      </characteristic>
      <characteristic type="FirstSyncStatus">
        <parm name="ExpectedPolicies" value="./Vendor/MSFT/Policy/Config" datatype="string" />
        <parm name="TimeOutUntilSyncFailure" value="60" datatype="integer" />
        <parm name="BlockInStatusPage" value="7" datatype="integer" />
        <parm name="SkipDeviceStatusPage" value="false" datatype="boolean" />
        <parm name="SkipUserStatusPage" value="false" datatype="boolean" />
        <parm name="AllowCollectLogsButton" value="true" datatype="boolean" />
        <parm 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>
</characteristic>
<characteristic type="EnrollmentStatusTracking">
  <characteristic type="DevicePreparation">
    <characteristic type="PolicyProviders">
      <characteristic type="BabyMDMProvider">
        <parm name="InstallationState" value="2" datatype="integer" />
      </characteristic>
    </characteristic>
  </characteristic>
</characteristic>
<characteristic type="PassportForWork">
  <characteristic type="f28cef80-3f9b-49d7-921e-81b2bf60fd6c">
    <characteristic type="Policies">
      <parm name="UsePassportForWork" value="0" datatype="boolean" />
      <parm name="RequireSecurityDevice" value="0" datatype="boolean" />
      <characteristic type="PINComplexity">
        <parm name="MinimumPINLength" value="4" datatype="integer" />
        <parm name="MaximumPINLength" value="127" datatype="integer" />
        <parm name="UppercaseLetters" value="2" datatype="integer" />
        <parm name="LowercaseLetters" value="2" datatype="integer" />
        <parm name="SpecialCharacters" value="2" datatype="integer" />
        <parm name="History" value="0" datatype="integer" />
        <parm name="Expiration" value="0" datatype="integer" />
      </characteristic>
      <characteristic type="Remote">
        <parm name="UseRemotePassport" value="1" datatype="boolean" />
      </characteristic>
    </characteristic>
  </characteristic>
  <parm 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

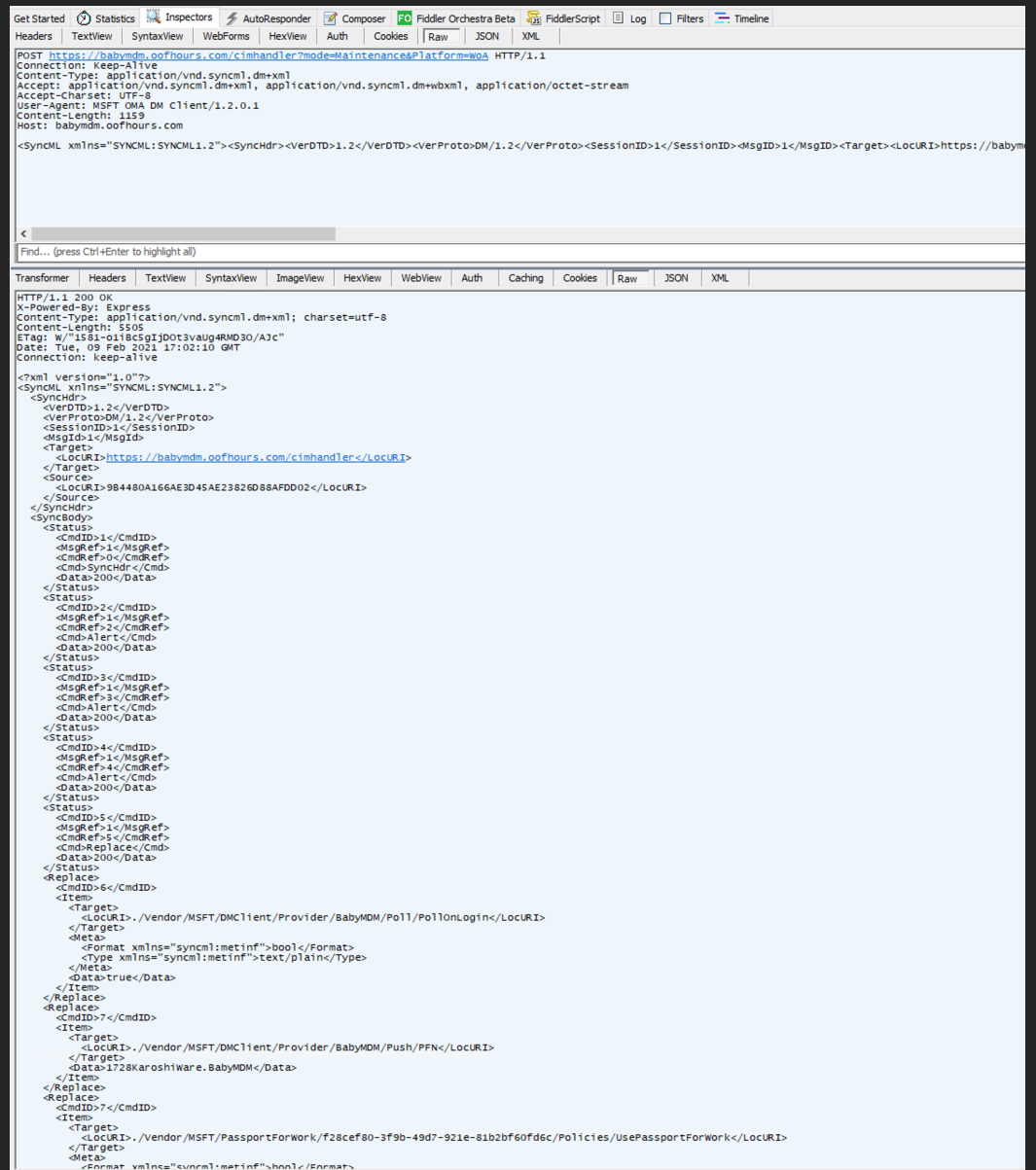
MDM sync schedules

- 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



- Client initiates the sync session (always)
- Service first acknowledges requests from client
- Service then sends any new policies

MDM sync session

NORDIC
– VIRTUAL SUMMIT –

```
<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

MDM sync session

NORDIC
— VIRTUAL SUMMIT —

```
<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>A7803233EEDB6A4B59B3024CCF9292A6FFFB94507DC998AA67C5B745D197A5DC</FileHash>
          </Validation>
          <Enforcement>
            <CommandLine>/qn</CommandLine>
            <RetryCount>3</RetryCount>
            <RetryInterval>5</RetryInterval>
          </Enforcement>
        </Product>
      </MsiInstallJob>
    </Data>
  </Item>
</Exec>
```

MDM sync session

NORDIC
– VIRTUAL SUMMIT –

```
<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

NORDIC
– VIRTUAL SUMMIT –

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

Thank you!

NORDIC
– VIRTUAL SUMMIT –

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