MDM Product 360 - Azure Key Vault Encryption Accelerator

Informatica MDM - Product 360
Table of Contents

1  Prerequisites ......................................................................................................................... 4

2  Azure Encryption Accelerator Configuration ................................................................. 4
    2.1 Required programs ........................................................................................................ 4
    2.2 Certificate creation ........................................................................................................ 4
    2.3 Azure Key Vault configuration ..................................................................................... 5
    2.4 Product 360 configuration ........................................................................................... 9
        2.4.1 Azure Key Vault properties (keyvault.properties) ................................................... 9

3  Azure Encryption Accelerator installation ......................................................................... 10
    3.1 Certificate installation .................................................................................................. 10
    3.2 Accelerator installation ................................................................................................ 11
        3.2.1 General information .............................................................................................. 11
        3.2.2 Product 360 server ................................................................................................. 12
        3.2.3 Product 360 Database setup .................................................................................. 12
        3.2.4 Product 360 Audit Trail .......................................................................................... 12
        3.2.5 Product 360 Control Center ................................................................................... 13
        3.2.6 Product 360 Web Search ........................................................................................ 14
    3.3 Product 360 Supplier Portal .......................................................................................... 14
        3.3.1 Supplier Portal database ........................................................................................ 14
        3.3.2 Supplier Portal service .......................................................................................... 15
        3.3.3 Product 360 Media Manager Web (since 8.0.6.01) ............................................... 16
            3.3.3.1 Media Manager Rest Service for Supplier Portal ................................................ 16

4  Azure Encryption Accelerator Setup .................................................................................... 17
    4.1 Using the Azure Encryption Accelerator to encrypt/decrypt configuration files .......... 17
    4.2 Changing the key for the encryption/decryption process .............................................. 17

5  Azure Encryption Trouble Shooting ................................................................................... 17
    5.1 Installation Encryption Troubleshooting ...................................................................... 17
        5.1.1 I cannot see "Azure Key Vault" in the list of APIs when adding a new required permission ...................................................... 17
        5.1.2 It is not possible to save the delegated permission of Azure Key Vault from the Azure Application ........................................ 18
    5.2 Installation Troubleshooting .......................................................................................... 19
        5.2.1 There is an error while loading the class like in the screenshot ................................ 19
        5.2.2 Invalid memory access while trying to start the service or application .................. 19
5.2.3 The Product 360 component does not start with the error "Invalid OAEP-Padding"
The Azure Key Vault Encryption Accelerator is used to enhance the security by using Azure Key Vault to encrypt and decrypt the passwords of your Product 360 config files. Azure Key Vault handles the keys which are used for encrypting and decrypting in the Microsoft Cloud where they are safe from attackers who got access to the local system.

This accelerator can currently be used for the following Product 360 components:

- Product 360 Server
- Product 360 Audit trail
- Product 360 Supplier Portal
- Product 360 Database setup

Until 8.1

- Product 360 Web search

To use the Azure Key Vault Encryption Accelerator start the configuration of Key Vault (see page 4).

1 Prerequisites

To use Azure Key Vault it is necessary to have an active subscription on the Azure platform.

2 Azure Encryption Accelerator Configuration

2.1 Required programs

- Powershell on the local system to create the certificate and read information from the certificate

2.2 Certificate creation

To use the Azure Encryption Accelerator a certificate to authenticate the machine against Azure Key Vault is needed.

To create a certificate with Powershell see the following snippet.
Power Shell example

```
makecert -r -pe -n "CN=<CertificateName>" -ss My -len 2048 certificateFileName.cer -sv privateKeyFileName.pvk
```

2.3 Azure Key Vault configuration

Before using Azure Key Vault encryption the following configuration for Key Vault is needed:

1. Create a new Azure Key Vault or use an existing one.
2. Register a new Azure application in the Azure Active Directory with the following settings:
   a. Type: Web
   b. URL of your choice (can be any URL, it is not used anywhere)

3. In your created application go to settings and set the required permission to have full access to Key Vault, depending on the Azure version you are using.
   When using the Classic Portal, go to the created application and set the permissions to other applications:
   "Azure Key Vault" -> "Delegated Permissions" -> "Have full access to Key Vault"
   When using the Resource Manager, go to the created application, then "Required permissions" -> "Azure Key
Download the manifest of the created application and create a backup on the local system.

Open powershell and import the certificate created earlier. Use the following snippet to import the certificate and extract the following 3 values from powershell: $base64Value, $base64Thumbprint, $keyid

Delegate permissions
If it is not possible to select or save delegated permissions for Azure Key Vault have a look at the troubleshooting page (see page 17).
certificate extraction

```powershell
$cer.Import("YourCertificateName.cer")
$cer.GetRawCertData()
$bin = $cer.GetCertHash()
$base64Value = [System.Convert]::ToBase64String($bin)
$base64Thumbprint = [System.Convert]::ToBase64String($bin)
$keyid = [System.Guid]::NewGuid().ToString()
```

6. Edit the manifest of your application to use the certification as credentials of the application. Adjust the `keyCredentials` section of the manifest of the application with your certificate information from above.

```json
manifest

 [...]"keyCredentials": [
  {
    "customKeyIdentifier": "$base64Thumbprint",
    "keyId": "$keyid",
    "type": "AsymmetricX509Cert",
    "usage": "Verify",
    "value": "$base64Value"
  }
], [...]
```

value property
The "value" property in the key credentials has to be one string without carriage return or line feed.

7. Save the manifest of the application

value property
The "value" property is not visible after saving (stated as null) for security reasons.
8. Create a new key in Azure Key Vault with a preferred name and key type.

9. In Azure Key Vault add the newly created application (done in Step 2) as principal with full access rights to the Key Vault.

10. Save the access policies of the principals

The Azure Key Vault is now configured to be used with the Azure Encryption Service.
2.4 Product 360 configuration

To configure the Product 360 components you have to add the corresponding Key Vault settings to the keyvault.properties file.

2.4.1 Azure Key Vault properties (keyvault.properties)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>keyvault.encryptionMethod</td>
<td>Encryption method which the Azure Key Vault should use. Currently supported methods of Key Vault are: RSA1_5, RSA-OAEP</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The keyvault.encryptionMethod has to be compatible with the keyvault.keyType. More information about the encryption method and keytype can be found at <a href="https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys-secrets-and-certificates#BKMK_KeyTypes">https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys-secrets-and-certificates#BKMK_KeyTypes</a></td>
</tr>
<tr>
<td>keyvault.keyVaultURL</td>
<td>URL to the Azure Key Vault which should be used. The URL can be found at the configured Key Vault as &quot;DNS Name&quot; (Example: <a href="https://INFAKEYVAULT.vault.azure.net">https://INFAKEYVAULT.vault.azure.net</a>)</td>
</tr>
<tr>
<td>keyvault.certificationName</td>
<td>Name of the certificate that is seen in the Microsoft Management Console (mmc.exe) as &quot;Issued To&quot;.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Has to be the certificate which was used as a key in the Azure Application, see &quot;Azure Key Vault Configuration&quot; section above.</td>
</tr>
<tr>
<td>keyvault.clientID</td>
<td>ClientID (when using manage.windowsazure.com) or ApplicationID (when using portal.azure.com) of the application created in the &quot;Azure Key Vault Configuration&quot; section above. Is used to identify if the application has access to Key Vault and its functions.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>keyvault.keyName</td>
<td>Name of the key which should be used by Key Vault for encryption/decryption. If no key with the given name exists in Key Vault, a new one will be created.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>This is the key which will be used to encrypt and decrypt. To change the key after you have already encrypted something please look at the setup section</td>
</tr>
<tr>
<td>keyvault.keyType</td>
<td>Type of key which is used to encrypt/decrypt. Currenty supported values are: RSA</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>The keyvault.encryptionMethod has to be compatible with the keyvault.keyType. More information about the encryption method and keytype can be found at <a href="https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys-secrets-and-certificates#BKMK_KeyTypes">https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys-secrets-and-certificates#BKMK_KeyTypes</a></td>
</tr>
</tbody>
</table>

After the configuration of Product 360 you can start with installing the Azure Encryption Accelerator.

## 3 Azure Encryption Accelerator installation

### Configuration

Note: Before installing the Azure Encryption Accelerator please make sure that you have configured your Key Vault on the Azure Website like described in the "Azure Encryption Accelerator configuration" section.

### 3.1 Certificate installation

Open the program "Microsoft Management Console" on the machine and add the certificates as a "Snap-in" for the "computer account".

Import the certificate with private key (.pfx file) you created in the "Azure Encryption Accelerator configuration" section into the "Personal" certificate store.
3.2 Accelerator installation

Extract all files from the Azure Encryption Accelerator to a directory. It should contain these files

```
dll_dependencies
plugins
keyvault.properties
```

3.2.1 General information

All Product 360 components can be installed separately.

It is recommended to copy the `keyvault.properties` file to a location where it can be referenced by all Product 360 components like `<PATH_TO_P360SERVER>/configuration/HPM/`

The tag `<PATH_TO_KEYVAULT_PROPERTIES>` is the absolute path to the location of the `keyvault.properties` file.

For example: `ppm.encryptionService.configPath=C:/Product360/server/configuration/HPM`
3.2.2 Product 360 server

1. Copy the azure encryption service plugin to `<PATH_TO_P360SERVER>/plugins`
2. In the server configuration directory `<PATH_TO_P360SERVER>/configuration` include the following lines before the end of file marker in the `config.ini` file

```
config.ini

ppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService
ppm.encryptionService.configPath=<PATH_TO_KEYVAULT>.PROPERTIES>
```

3. Include all dlls from the `dll_dependencies` folder to the java bin directory of Product 360 server, `<PATH_TO_P360SERVER>\jre\bin`

3.2.3 Product 360 Database setup

1. Copy the azure encryption service plugin to `<PATH_TO_DBCLIENT>/plugins`
2. In the database client configuration directory, `<PATH_TO_DBCLIENT>/configuration`, include the following lines in the `config.ini` file

```
config.ini

ppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService
ppm.encryptionService.configPath=<PATH_TO_KEYVAULT>.PROPERTIES>
```

Also include the reference to the encryption service in the `config.ini` at the `osgi.bundles` property

```
config.ini

osgi.bundles=[...],reference\:file\:com.heiler.ppm.encryption.azure_1.0.0.jar@4
```

3. Include all dlls from the `dll_dependencies` folder to the Product 360 database client directory where the `Database.exe` is located
4. Include all dlls from the `dll_dependencies` folder to the java bin directory of Product 360 database setup, `<PATH_TO_DBCLIENT>\jre\bin`

3.2.4 Product 360 Audit Trail

1. Copy the azure encryption service plugin to `<PATH_TO_AUDIT_TRAIL>/plugins`
2. In the audit trail configuration directory `<PATH_TO_AUDIT_TRAIL>/configuration` include the following lines in the `config.ini` file
Also include the reference to the encryption service in the config.ini at the osgi.bundles property

3. Include all dlls from the dll_dependencies folder to the Product 360 audit trail directory where the atserver.exe is located

4. Include all dlls from the dll_dependencies folder to the java bin directory of Product 360 audit trail, <PATH_TO_AUDIT_TRAIL>\jre\bin

When starting the application as a service also add the following lines to the configuration of the wrapper located at <PATH_TO_AUDIT_TRAIL>/bin/conf

```
wrapper.conf
```

```
wrapper.java.additional.13=-Dppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService
wrapper.java.additional.14=-Dppm.encryptionService.configPath=<PATH_TO_KEYVAULT>.PROPERTIES
```

3.2.5 Product 360 Control Center

1. Copy the azure encryption service plugin to <PATH_TO_CONTROL_CENTER>/plugins

2. In the control center configuration directory <PATH_TO_CONTROL_CENTER>/configuration include the following lines in the config.ini file

```
config.ini
```

```
ppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService
ppm.encryptionService.configPath=<PATH_TO_KEYVAULT>.PROPERTIES
```

3. Add all dlls from the dll_dependencies folder to the java bin directory of Product 360 Control Center located at <PATH_TO_CONTROL_CENTER>\jre\bin

When starting the application as a service also add the following lines to the configuration of the wrapper located at <PATH_TO_CONTROL_CENTER>/service
Informatica MDM - Product 360 - MDM Product 360 - Azure Key Vault Encryption Accelerator

wrapper.conf

wrapper.java.additional.13=-Dppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService
wrapper.java.additional.14=-Dppm.encryptionService.configPath=<PATH_TO_KEYVAULT>.PROPERTIES>

3.2.6 Product 360 Web Search

1. Copy the azure encryption service plugin to <PATH_TO_WEB_SEARCH_ROOT>/internal/buildFiles/lib and <PATH_TO_WEB_SEARCH_ROOT>/apache-tomcat-X.X.XX/webapps/hps-web/WEB-INF/lib
2. In the web search configuration file <PATH_TO_WEB_SEARCH_ROOT>/configuration.properties fill the following lines:

configuration.properties

ppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService
ppm.encryptionService.configPath=<PATH_TO_KEYVAULT>.PROPERTIES>

3. Go to the java directory which is configured at the jdk.home property in configuration.properties. Copy all dlls from the dll_dependencies to the following paths: <PATH_TO_JAVA_JDK>/jre/bin and <PATH_TO_JAVA_JDK>/bin

Before starting the application add all dlls from the dll_dependencies folder to the Apache Tomcat bin directory where tomcat.exe is located at <PATH_TO_WEB_SEARCH_ROOT>/apache-tomcat-X.X.XX/bin.

The scripts to start the Web Search Server Service (service_HPS_install.cmd) or the Web Search Server (start_HPS_tomcat.cmd) have to be started as Administrator, best practice is here from a console (cmd) which runs as Administrator.

3.3 Product 360 Supplier Portal

3.3.1 Supplier Portal database

1. Copy the azure encryption service plugin to <PATH_TO_SUPPLIER_PORTAL_ROOT>/database/lib
2. In the Supplier Portal configuration directory <PATH_TO_SUPPLIER_PORTAL_ROOT>/configuration include the following lines in the configuration.properties file:
3. Go to the java directory which is configured as JAVA_HOME property. Copy all dlls from the dll_dependencies to the following paths: <PATH_TO_JAVA_JDK>/jre/bin and <PATH_TO_JAVA_JDK>/bin

The scripts to install the Supplier Portal database (setup.cmd) has to be started as administrator, best practice is here from a console (cmd) which runs as administrator.

3.3.2 Supplier Portal service

1. Open the command line as administrator and install the Supplier Portal service (install.cmd). Make sure that the same JAVA_HOME property like in the Supplier portal database installation is used.
2. Execute the configure.bat in the same command line window.
3. In the configuration pop-up select "Java" and add the following lines in the "Java Options" area:

   Java Options

   -Dppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService
   -Dppm.encryptionService.configPath=<PATH_TO_KEYVAULT.PROPERTIES>

   It is now possible to start the service with the encrypted passwords.
3.3.3 Product 360 Media Manager Web (since 8.0.6.01)

1. Copy the azure encryption service plugin 'com.heiler.ppm.encryption.azure_1.0.0.jar' to OpasGWebServer/Tomcat/lib and OpasGWebServer/Tomcat/webapps/opas/WEB-INF/lib
2. Copy all dlls from the dll_dependencies to the following paths: OpasGWebServer/java/jre/bin and OpasGWebServer/Tomcat/bin
3. Copy keyvault.properties file to OpasGWebServer/ and adjust values to your needing
4. Edit file startup.bat and add 2 new JAVA_OPTS values

```batch
:: old line
set JAVA_OPTS=-server -Xms%APP_XMS% -Xmx%APP_XMX%
-Dcom.sun.management.jmxremote -Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8

:: new line with absolute path to parent folder of keyvault.properties
set JAVA_OPTS=-server -Xms%APP_XMS% -Xmx%APP_XMX%
-Dcom.sun.management.jmxremote -Dfile.encoding=UTF-8 -Dsun.jnu.encoding=UTF-8
-Dppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService
-Dppm.encryptionService.configPath=C:/OpasGWebServer
```

5. Edit file installService.bat and add 2 new JAVA_OPTS values

```batch
:: old line
%TOMCAT_HOME%\bin\tomcat8 //US//Tomcat8 --DisplayName "Informatica Media Manager Apache Tomcat"

:: new line with absolute path to parent folder of keyvault.properties
%TOMCAT_HOME%\bin\tomcat8 //US//Tomcat8 --DisplayName "Informatica Media Manager Apache Tomcat" ++JvmOptions "-Dppm.encryptionService=com.heiler.ppm.encryption.azure.AzureKeyVaultEncryptionService;-Dppm.encryptionService.configPath=C:/OpasGWebServer"
```

If you have already installed the Tomcat Windows service you need to reinstall (removeService.bat and installService.bat) the service to apply the new JAVA_OPTS.

The removeService.bat and installService.bat have to been executed as Administrator.

3.3.3.1 Media Manager Rest Service for Supplier Portal

You can use the accelerator in the previous configured Tomcat beside the Media Manager Web application. In addition please
1. Copy the azure encryption service plugin 'com.heiler.ppm.encryption.azure_1.0.0.jar' to OpasGWebServer/Tomcat/webapps/rest/WEB-INF/lib

4 Azure Encryption Accelerator Setup

4.1 Using the Azure Encryption Accelerator to encrypt/decrypt configuration files

To use the Azure Encryption service add the tag 

```
sql.password = [_to_encrypt_]MyPassword[_to_encrypt_]
```

4.2 Changing the key for the encryption/decryption process

When you have encrypted the password with the key stated in the keyvault.properties do not change the key or else Azure will not be able to decrypt it again.

When you want to use a new key follow these steps:

1. Write the password in plain text with the encryption marker again.
2. Now change the keyName property of the keyvault.properties to the desired key.
3. Restart the Product 360 components.
4. The password will now be encrypted again with the new key.

5 Azure Encryption Trouble Shooting

5.1 Installation Troubleshooting

5.1.1 I cannot see "Azure Key Vault" in the list of APIs when adding a new required permission

This is a bug of the Azure system. "Azure Key Vault" can be selected when starting to type "Azure" in the search bar.
### 5.1.2 It is not possible to save the delegated permission of Azure Key Vault from the Azure Application

To fix this problem follow these steps:

1. Create a new Azure Application and use "Native" as type.
2. Delegate the permissions to Key Vault like in the web app.
3. Open the manifest of the Native app and copy the section like below to the appropriate manifest section of your web app. (Values can differ)

```json
"requiredResourceAccess": [
    {
        "resourceAppId": "cfa8b339-82a2-471a-a3c9-0fc0be7a4093",
        "resourceAccess": [
            {
                "id": "f53da476-18e3-4152-8e01-aec403e6edc0",
                "type": "Scope"
            }
        ]
    },
    {
        "resourceAppId": "00000002-0000-0000-c000-000000000000",
        "resourceAccess": [
            {"id": "311a71cc-e848-46a1-bdf8-97ff7156d8e6", "type": "Scope"}
        ]
    }
]
```
4. Save the manifest of the web app.
5. Check the permissions in the web app. It should now have the delegated rights.

If this step did not work create the needed web app though the classic portal and delegate the permission there.

5.2 Installation Troubleshooting

5.2.1 There is an error while loading the class like in the screenshot

![Error Screenshot]

This error occurs when the encryption service cannot be loaded. Please check the config.ini and wrapper.conf files if the encryption service plugin name is written correctly and check if the related plugin exists in the plugins directory of the Product 360 component.

If the error persists please check if the plugin is being loaded via console and check the config.ini if the encryption plugin is existent in the osgi.bundles property.

5.2.2 Invalid memory access while trying to start the service or application

Unfortunately this error is thrown by JNA when something happens to the connection to the Azure Key Vault and can have many causes.

Solutions:

- try starting the service or application with administrator rights.
- check that all dll files got copied to the corresponding Product 360 components and are at the right place.
  - if the error still persists please also copy all dll files to the machines jdk/jre directory which is labeled as JAVA_HOME system property.
- check the keyvault.properties file if the properties are set and have valid values.
- check if the Azure Key Vault is configured correctly and there is an application configured as principal with full access rights to the Azure Key Vault.
- check if the Azure Application is configured correctly and has the required permission to use the Azure Key Vault API.
- check if the certificate is created like described in the documentation and is installed correctly onto the machine under the "computer account" of the certification store.
- When using Product 360 Websearch make sure that the dll files are existent where the tomcat.exe file is located.
5.2.3 The Product 360 component does not start with the error "Invalid OAEP-Padding"

This error occurs when you have encrypted the password with a key and later changed the key in the keyvault.properties file.

Key Vault now tries to decrypt the password with the new key and fails, because it is not the key which was used to encrypt the password.

To fix the problem just redo the encryption process:

1. Enter the password surrounded by the encryption markers `[_to_encrypt_]MyPassword[_to_encrypt_]` again.
2. Restart the Product 360 component.