This article describes how to configure certificate based authentication using Microsoft Certificate Services (PKI) for WorxMail 10.0.3, XenMobile 10 and Microsoft Exchange Server.

For this article, the following Citrix and Microsoft components were used:

- XenMobile Server 10
- NetScaler 10.5 build 55.8
- WorxMail 10.0.3 for iOS, Android and Windows Phone 8.1
- Microsoft Windows Server 2008 R2 with Microsoft Certificate Services acting as Root Certificate Authority (CA)
- Microsoft Exchange Server 2010 SP3*

For this scenario, we are assuming that users once enrolled, they will no longer enter domain credentials. Instead, a Worx PIN would be prompted to log on to XenMobile.

*Note: Microsoft Exchange Server 2010 was not load balanced.
# Table of Contents

Prerequisites .................................................................................................................. 1

Configuration from XenMobile Server 10........................................................................ 2
  PKI Configuration ........................................................................................................ 2

Setup WorxMail for iOS, Android and Windows Phone 8.1 ........................................ 7
  Network Access section (for iOS/Android only)............................................................ 8
  Application Settings (for iOS/Android/Windows Phone 8.1)........................................ 8

Setup NetScaler Gateway Settings .................................................................................. 9

Create Enterprise Hub policy for Windows Phone 8.1 .................................................. 10

Configuration from NetScaler 10.5 ................................................................................. 12

Testing ............................................................................................................................ 15

Troubleshooting FAQ ..................................................................................................... 16
Prerequisites

- Ensure to check the article CTX200105 - FAQ: Windows Phone 8.1 and XenMobile to wrap Windows Phone 8.1 Worx apps correctly using the latest MDX Toolkit for Windows Phone 8.1 available at the download site.
- Follow the instructions in the article CTX141541 - Worx Home Setup Fails when trying to Enroll Windows Phone 8.1 Devices to disable Session Reuse on NetScaler if you are using Windows Phone 8.1 devices.
- Check the article CTX200463 - How to Integrate XenMobile MDM with Microsoft Certificate Services and follow the steps to configure the Microsoft Certificate Services role on the Windows Server and test Certificate Based Authentication (PKI) against the Windows Server acting as Root Certificate Authority.
- When the Certificate Based authentication has been validated on the Root Certification Authority server, go to the step to Configure XenMobile Server 10 and NetScaler Gateway for Certificate Based authentication.
- If you are using private server certificates to secure the ActiveSync traffic to the Exchange Server, ensure to have all the Root/Intermediate certificates on the mobile devices. Otherwise, certificate based authentication will fail during the mailbox setup in WorxMail.
Configuration from XenMobile Server 10

PKI Configuration

On XenMobile Server 10, log on to the Web admin console (for example, https://XenMobileServer-IP-or-FQDN:4443).

1. Upload the XenMobile Client Certificate (PFX) generated as mentioned in the article CTX200463 - How to Integrate XenMobile MDM with Microsoft Certificate Services, section “Generate the XenMobile Client Certificate”. Ensure that the PFX certificate does include the private key and all certificates in the chain.
2. In the XenMobile Server 10 console, go to Configure > Settings > Certificates > select Import.
3. Set the following parameters:
   - Import: Keystore
   - Keystore type: PKCS#12
   - Use as: Server
   - Keystore file: Your XenMobile ClientCertificate.pfx
   - Password: Type the PrivateKey Passphrase

4. Click Import.
5. When imported, verify the certificate was installed correctly. It would be displayed as a “Users” certificate.
6. Create the PKI entity for certificate based authentication.

8. In the **PKI Entities**, click Add > select **Microsoft Certificate Services Entity**.
9. Under General, enter the following parameters:
   - Name: *Type any name for the entity*
   - Web enrollment service root URL: [https://RootCA-URL/certsrv/](https://RootCA-URL/certsrv/)
     **Note:** Ensure to add the last slash “/” in the URL path.
   - certnew.cer page name: *certnew.cer (default value)*
   - certfnsh.asp: *certfnsh.asp (default value)*
   - Authentication Type: **Client certificate**
   - SSL Client Certificate: *Select the RootCA who signed the XenMobile Client Certificate.*
Example:

10. Under Templates, add the template that you created when following the article CTX200463 - How to Integrate XenMobile MDM with Microsoft Certificate Services, section “Create a Certificate Template for XenMobile Certificate Requests”.

Note: Ensure not to add any spaces.

Example:

11. Skip the HTTP Parameters and go to the CA Certificates section.

Ensure to select the Root CA name that correspond to your environment. This Root CA is part of the chain imported from the XenMobile Client Certificate.

Example:

12. Click Save.
13. Next, configure the Credentials Providers.
15. Click Add.
16. Under General section, enter the following parameters:
   - Name: Type any name for the credentials providers.
   - Description: Type any description desired for the credential providers.
   - Issuing entity: Select the PKI entity created earlier.
   - Issuing method: SIGN.
   - Templates: Select the template added under PKI entity.

Example:

17. Under Certificate Signing Request, enter the following parameters:
   - Key algorithm: RSA
   - Key size: 2048
   - Signature algorithm: SHA1withRSA
   - Subject name: cn=$user.username

18. For Subject Alternative Names, click Add and enter the following parameters:
   - Type: User Principal name
   - Value: $user.userprincipalname
Example:

**Credentia Providers**

<table>
<thead>
<tr>
<th>1 General</th>
<th>2 Certificate Signing Request</th>
<th>3 Distribution</th>
<th>4 Revocation XenMobile</th>
<th>5 Revocation PKI</th>
<th>6 Renewal</th>
</tr>
</thead>
</table>

**Credentia Providers: Certificate Signing Request**

- **Key algorithm**: RSA
- **Key size**: 2048
- **Signature algorithm**: SHA1withRSA
- **Subject name**: Gw.<User name>

**Subject alternative names**

<table>
<thead>
<tr>
<th>Type</th>
<th>Value*</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Principal name</td>
<td>$user.userprincipalname</td>
</tr>
</tbody>
</table>

19. **Under the Distribution section**, type the following parameters:
   - **Issuing CA certificate**: *Select the Root CA who signed the XenMobile Client Certificate*.
   - **Select distribution mode**: *Prefer centralized: Server-side key generation*.

**Example:**

**Credentia Providers**

**Credentia Providers: Distribution**

- **Issuing CA certificate**: ON:training-AD-CA, Serial 148401655602712119558...
- **Select distribution mode**:
  - Prefer centralized: Server-side key generation
  - Prefer distributed: Device-side key generation
  - Only distributed: Device-side key generation

**Note**: For the next two sections, Revocation XenMobile and Revocation PKI, set the parameters as required. For the purpose of this article, both options are skipped.

20. **Under the Renewal section**, type the following parameters:
   - **Renew certificates when they expire**: **ON**.
   - **Leave all other settings as default or change them as required**.

**Example:**

**Credentia Providers**

**Credentia Providers: Renewal**

- **Renew certificates when they expire**: **ON**
- **Notify when the certificate comes within**: 30 days
- **Send notification**: **OFF**
- **Notify when the certificate nears expiration**: **OFF**

21. **Click Save**.
Setup WorxMail for iOS, Android and Windows Phone 8.1

Before uploading to XenMobile, ensure to wrap WorxMail with the latest MDX Toolkit available at the download site.

1. On the XenMobile Server 10 Web console, go to Configure > Apps.
2. Click Add and select MDX to upload WorxMail.

3. Configure the name, description and app category as required.

   Example:

4. Under MDX Policies, enter the following parameters:
Network Access section (for iOS/Android only)

Network access: Tunneled to the internal network

Example:

![Network Access](image)

Application Settings (for iOS/Android/Windows Phone 8.1)

- WorxMail Exchange Server: *Exchange Server FQDN* (for example, mail.domain.com)
- WorxMail user domain: *domain suffix* (for example, .domain.com)
- Background network services: *Exchange Server FQDN:443* (e.g. mail.domain.com:443)
- Background services ticket expiration: **168 hours (default)**.
  
  Note: This is the STA ticket lifetime. Once the ticket expires, then, Worx Home will prompt the user to log on through XenMobile. Once the user is validated, then, a new STA ticket is generated by XenMobile Server and sent to the user.
- Background network service gateway: *NetScaler Gateway FQDN:443* (for example, gateway.domain.com:443)

Example:

![Application Settings](image)

5. Click Save.
Setup NetScaler Gateway Settings

1. On XenMobile Server 10 Web console, go to Configure > Settings > More > select NetScaler Gateway.

![NetScaler Gateway Settings](image)

2. Click Add to add your NetScaler Gateway settings. Type the following parameters:
   - Name: *Type any name for the NetScaler Gateway*
   - External URL: [https://YourNetScalerGatewayURL](https://YourNetScalerGatewayURL)
   - Logon Type: *Certificate*
   - Password Required: *OFF*
   - Set as Default: *ON*

   **Example:**

   ![Add New NetScaler Gateway](image)

3. Next, set the following parameters for XenMobile Server to deliver the client certificate to the user using the credential provider created earlier.
   - Deliver user certificate for authentication: *ON*
   - Credential Provider: *Select the Credential Provider created earlier*
4. Click Save.

Create Enterprise Hub policy for Windows Phone 8.1

For Windows Phone 8.1 devices, an Enterprise Hub device policy should be created to deliver the AETX file and the Worx Home client.

**Note:** Ensure that both the AETX and Worx Home files were using the same enterprise certificate from Symantec and the same Publisher ID from the Windows Store developer account.

1. Click **Add** > **More** > **XenMobile Agent** > select **Enterprise Hub**.
2. Ensure to select the correct .AETX file and signed Worx Home app for the Enterprise Hub.

Example:

<table>
<thead>
<tr>
<th>Enterprise Hub Policy</th>
<th>Policy Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Policy Info</em></td>
<td>To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (AppSignTool.exe).</td>
</tr>
<tr>
<td><em>Platforms</em></td>
<td></td>
</tr>
<tr>
<td>Windows Phone 8.1</td>
<td></td>
</tr>
<tr>
<td><em>Assignment</em></td>
<td></td>
</tr>
</tbody>
</table>

Upload AETX file

Upload signed Enterprise Hub app

3. Set the assignment to the desired delivery groups.

Example:

<table>
<thead>
<tr>
<th>Enterprise Hub Policy</th>
<th>Enterprise Hub Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Policy Info</em></td>
<td>To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (AppSignTool.exe).</td>
</tr>
<tr>
<td><em>Platforms</em></td>
<td></td>
</tr>
<tr>
<td>Windows Phone 8.1</td>
<td></td>
</tr>
<tr>
<td><em>Assignment</em></td>
<td></td>
</tr>
</tbody>
</table>

Choose delivery groups

Search

Delivery groups to receive app assignment

4. Click **Save**.

5. Verify the Enterprise Hub device policy for Windows Phone 8.1 is created.

<table>
<thead>
<tr>
<th>Device Policies</th>
<th>Show filter</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Add</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Policy name</th>
<th>Type</th>
<th>Created on</th>
<th>Last updated on</th>
</tr>
</thead>
</table>
Configuration from NetScaler 10.5

1. Disable SSL Session Reuse on both load balancing virtual servers for XenMobile MDM traffic as mentioned in the article CTX141541 - Worx Home Setup Fails when trying to Enroll Windows Phone 8.1 Devices to avoid any issues with Windows Phone 8.1 devices.

   Example:

   ![Image: SSL Session Reuse Disabled]

2. Under Traffic Management > Load Balancing > Virtual Servers, go to each virtual server (both 443 and 8443), edit SSL Parameters and set SSL Session Reuse to disabled.

   Example:

   ![Image: SSL Parameters Configuration]

3. Next, on the NetScaler Gateway virtual server, set Client Authentication to ENABLED and Mandatory.

   Example:

   ![Image: Client Authentication Configuration]

4. Create a new authentication Certificate policy so we can extract the User Principal Name from the client certificate provided by Worx Home to NetScaler Gateway.

5. Ensure to set the following parameters for the certificate profile:
   - Authentication Type: CERT
   - Two Factor: OFF
   - User Name Field: SubjectAltName:PrincipalName
6. Ensure to bind only the certificate authentication policy as the Primary Authentication in the NetScaler Gateway virtual server.

Example:

```
<table>
<thead>
<tr>
<th>Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Authentication</td>
</tr>
<tr>
<td>1 Cert Policy</td>
</tr>
</tbody>
</table>
```

7. Ensure to bind the Root CA certificate to validate the trust of the client certificate presented to NetScaler Gateway.

Example:

```
<table>
<thead>
<tr>
<th>SSL Virtual Server CA Certificate Binding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
</tr>
<tr>
<td>Root-CA-TrainingLab</td>
</tr>
</tbody>
</table>
```

CRL and OCSP Check | Skip CA | OCSP Optional | X
<table>
<thead>
<tr>
<th>Certificates</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Server Certificate</td>
</tr>
<tr>
<td>1 CA Certificate</td>
</tr>
</tbody>
</table>
**Testing**

If everything was configured correctly, users should be able to enroll their mobile device against XenMobile, get prompted to create a Worx PIN and be redirected to the Worx Store.

When users launch WorxMail for iOS, Android or Windows Phone 8.1, they should **not** get prompted for user credentials to configure their mailbox. Instead, WorxMail will request the client certificate from Worx Home and submit it to Microsoft Exchange Server for authentication automatically. No user intervention would be needed.

**Example of WorxMail configuring the mailbox during the first time launch:**

Users should be directed to their mailbox.
Troubleshooting FAQ

Q. I am able to download and install WorxMail on my mobile device, but during the mailbox configuration WorxMail fails to finish the configuration. What is wrong?

1. If Microsoft Exchange Server ActiveSync is using private SSL server certificates to secure the traffic, ensure to have the Root/Intermediate certificates installed on the mobile device.
2. Check the authentication type selected for ActiveSync. It should have “Require client certificates”.

3. On Microsoft Exchange Server, check the Microsoft-Server-ActiveSync site to have client certificate mapping authentication enabled (by default it is disabled). The option is under the Configuration Editor > Security > Authentication.
Note: After selecting “True”, ensure to click Apply for the changes take effect.

4. Check the NetScaler Gateway settings on XenMobile Server 10. Ensure that “Deliver user certificate for authentication” is turned ON and Credential provider has the correct profile selected.
Q. How can I see if the client certificate was generated/delivered to the mobile device?

This information is available under each managed mobile device enrolled on XenMobile 10.

To check the certificate details:

1. Go to the XenMobile Server 10 Web Management console > Manage > Devices.
2. Select one of the devices.
3. Click “Edit” or “Show More”.
4. Go to the Delivery Groups section, and search for this entry:

   **NetScaler Gateway Credentials : Requested credential, CertId=**
Q. I noticed that I cannot deliver Root/Intermediate certificates to my Windows Phone 8.1 device through XenMobile. How can I install these files in order to trust my Exchange Server?

You can send Root/Intermediate certificates (.cer) files through email to the Windows Phone 8.1 device and install them directly.
Q. I cannot get WorxMail installed successfully on my Windows Phone 8.1 device. What could cause this issue?

- Ensure the Application Enrollment Token (.AETX) file is delivered through XenMobile using the Enterprise Hub device policy.
- Ensure the Application Enrollment Token was created using the same Enterprise Certificate from Symantec used to wrap WorxMail and sign Worx Home apps.
- Ensure the same Publisher ID is being used to sign and wrap Worx Home, WorxMail, and the Application Enrollment Token.