This article describes how to configure S/MIME (Secure/Multipurpose Internet Mail Extensions) for WorxMail iOS.

**Note:** This feature works with WorxMail 10.0.3 for iOS and later versions.

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
- Microsoft Windows Server 2008 R2 with Microsoft Certificate Services acting as Root Certificate Authority (CA)
- Microsoft Exchange Server 2010 SP3

To generate the user certificates for signing and encryption, manual enrollment is used through the Web enrollment site (example, [https://ad.domain.com/certsrv/](https://ad.domain.com/certsrv/)) on Microsoft Certificate Services. An alternative for IT Admins is to configure “auto enrollment” through Group Policy for the group of users that would use this feature. For more information, refer to the Microsoft TechNet article - [Configure User Certificate Autoenrollment](https://docs.microsoft.com/en-us/windows-server/security/certificates/auto-enrollment).


# Table of Contents

Prerequisites .......................................................................................................................... 1  
Create New Certificate Templates .......................................................................................... 2  
Request User Certificates ..................................................................................................... 8  
Validate Published Certificates ............................................................................................. 12  
Exporting the User Certificates ............................................................................................ 14  
Send Certificates through Email ........................................................................................... 16  
Enabling S/MIME on WorxMail ............................................................................................. 17  
Testing .................................................................................................................................. 23  
Troubleshooting FAQ .......................................................................................................... 24
Prerequisites

- Refer 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.
  
  **Note:** We will create two new certificate templates for signing and encryption purposes.

- Ensure the Web enrollment site (example, https://ad.domain.com/certsrv/) to request user certificates is secured (HTTPS) with a server certificate (private or public).
  
  **Note:** This site must be accessed through HTTPS.

- Ensure to deliver the Root/Intermediate certificates to the mobile devices (iOS) either manually or through a XenMobile Device Policy > Certificates policy. For more information, click here.

**Example:**

![Policy Information](image)

- Ensure to wrap WorxMail 10.0.3 or later for iOS with the latest MDX Toolkit available in the Citrix downloads site.

- Ensure to download, install, and configure WorxMail (iOS) on your device.
  
  **Note:** No special policy configuration is needed on XenMobile Server 10 for the WorxMail (MDX) app.

- If you are using private server certificates to secure the ActiveSync traffic to the Exchange Server, ensure to have all the Root/Intermediate certificates installed on the mobile devices (iOS).
Create New Certificate Templates

For the purpose of signing and encrypting email messages, it is recommended to create new certificates on the Microsoft Active Directory Certificate Services. In the event of using the same certificate for both purposes and archive the encryption certificate, then, it is possible to recover a signing certificate and allow impersonation.

The following procedure will duplicate the certificate templates on the CA (Certificate Authority) server:

- Exchange Signature Only (for Signing)
- Exchange User (for Encryption)

1. Go to the Certificate Authority snap-in.
2. Expand the CA and go to the Certificate Templates.
3. Right-click and select Manage.
4. Search for “Exchange Signature Only” template, right-click and select Duplicate Template.
5. Assign any name.
6. Select the checkbox “Publish certificate in Active Directory”.

**Note:** If you do not select “Publish certificate in Active Directory”, then, end-users will have to publish the user certificates (for signing and encryption) manually through Outlook mail client > Trust Center > E-mail Security > Publish to GAL (Global Address List). For more information, click here.

7. Go to Request Handling tab and ensure these parameters are set:
   - Purpose = *Signature*
   - Minimum key size: **2048**
   - Allow private key to be exported = **checked**
   - Enroll subject without requiring any user input = **selected**
8. Under Security tab, ensure that Authenticated Users (or any desired Domain Security Group) is added and has the permissions to Read and Enroll.
9. For all other tabs and settings, leave them as default.
10. Repeat the same procedure to duplicate the certificate template but now for Exchange User.

For the new Exchange User template, we will use the same default settings as the original template.

Example:
11. Go to **Request Handling** tab and ensure these parameters are set:

- **Purpose** = *Encryption*
- **Minimum key size**: 2048
- Allow private key to be exported = **checked**
- Enroll subject without requiring any user input = **selected**

![XM Exchange User Properties](image)

<table>
<thead>
<tr>
<th>Purpose: Encryption</th>
<th>Delete revoked or expired certificates (do not archive)</th>
<th>Include symmetric algorithms allowed by the subject</th>
<th>Archive subject's encryption private key</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
</tbody>
</table>

Minimum key size: 2048

- Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

- Enroll subject without requiring any user input
- Prompt the user during enrollment
- Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs...
12. When both templates are created, ensure to issue both certificate templates.
Request User Certificates

In this procedure, we will use “user1” to navigate to the Web enrollment page (example, https://ad.domain.com/certsrv/) and request two new user certificates for secure email: one certificate for signing and the other for encryption.

The same procedure can be repeated for other domain users that require to use S/MIME through WorxMail (iOS).

1. From a Windows workstation, open Internet Explorer and go to the Web enrollment site to request a new user certificate.

   **Note:** Ensure to log on with the correct domain user to request the certificate.

   **Example:**

   ![Connect to ad.training.lab](image)

   ![Microsoft Active Directory Certificate Services](image)

   2. When logged in, click **Request a certificate**.
3. Select **advanced certificate request**.

4. Select **Create and Submit a request to this CA**.

First, we will generate the user certificate for signing purposes.

5. Select the appropriate template name and type your user settings. Ensure to select **PKCS10** for **Request Format**.
6. The request has been submitted. Click **Install this certificate**.

7. Verify the certificate was installed successfully.
8. Repeat the same procedure but now for encrypting email messages. With the same user logged on to the Web enrollment site, go to the **Home** link to request a new certificate.

9. This time, ensure to select the new template for encryption and type the same user settings entered previously.

10. Ensure to install the certificate successfully.

11. Repeat the same procedure to generate a pair of user certificates for another domain user. In our use case, we followed the same procedure and generated a pair of certificates for “User2”. **Note:** For the purpose of this article, we used the same Windows workstation to request the second pair of certificates for “User2”.
Validate Published Certificates

1. To ensure the certificates were properly installed in the domain user profile, go to Active Directory Users and Computers > click View > select “Advanced Features”.

2. Go to the properties of your user (example, User1 for our example) > click Published Certificates tab. Ensure both certificates are available.

You can verify that each certificate has a specific usage.
Example:

*Certificate to encryption email messages*

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority Key Identifier</td>
<td>KeyID=f3 c1 57 6a 5d 77 b7 c...</td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>[1]CRL Distribution Point: Distrib...</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>[1]Authority Info Access: Acc...</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Secure Email (1.3.6.1.5.7.3.4)</td>
</tr>
<tr>
<td><strong>Key Usage</strong></td>
<td>Key Encipherment (20)</td>
</tr>
</tbody>
</table>

Key Encipherment (20)

*Certificate to sign email messages*

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authority Key Identifier</td>
<td>KeyID=f3 c1 57 6a 5d 77 b7 c...</td>
</tr>
<tr>
<td>CRL Distribution Points</td>
<td>[1]CRL Distribution Point: Distrib...</td>
</tr>
<tr>
<td>Authority Information Access</td>
<td>[1]Authority Info Access: Acc...</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>Secure Email (1.3.6.1.5.7.3.4)</td>
</tr>
<tr>
<td><strong>Key Usage</strong></td>
<td>Digital Signature (80)</td>
</tr>
</tbody>
</table>

Digital Signature (80)
Exporting the User Certificates

In this procedure, we will export both “User1” and “User2” pair certificates in .PFX (PKCS#12) format with the private key. When exported, we will send these certificates through email to the user using Outlook Web Access (OWA).

1. Open the MMC console and go to the Certificates snap-in > My Current User.

You should see both “User1” and User2” pair of certificates.

2. Next, right-click on the certificate > click All Tasks > Export.

3. Ensure to export the private key.
4. Ensure to select “Include all certificates in the certification path if possible” and “Export all extended properties”.

![Certificate Export Wizard]

5. When you export the first certificate, repeat the same procedure for the remaining certificates for your users.

**Note:** Ensure to clearly label which one is the “signing” certificate and “encryption” certificate. In the example, we labeled them as “userX-sign.pfx” and “userX-enc.pfx”.

**Example:**

![Certificate Examples]
Send Certificates through Email

When all certificates are exported in PFX format, we will use Outlook Web Access (OWA) to send them through email.

For this example, we are logged on as “User1” and send myself an email with both certificates.

Repeat the same procedure for “User2” or other users in your domain.
Enabling S/MIME on WorxMail

When the email has been delivered, the next step is to open the message using WorxMail and enable S/MIME with the appropriate certificates for signing and encryption.

1. On WorxMail, open the email message.

2. Download the first certificate (for signing) and select “Import certificate for Signing”.

3. Type the passphrase assigned to the private key when the certificate was exported.
4. Go to Settings to enable signing on WorxMail.

5. Turn ON S/MIME > tap Signing > tap “OFF”.
6. In Signing, enable and verify the correct signing certificate is selected.

![Signing Certificate](image)

7. Go back to the email message to download and import the certificate for encryption.

![Certificate Import](image)

8. Type the passphrase assigned to the private key.

![Certificate Password](image)

9. Go to Settings to enable encryption on WorxMail. Tap Encrypt by default “Off”.
10. Enable encryption and ensure the correct user certificate is selected for encryption.

11. Repeat the same procedure to install the pair of user certificates to the other domain users.

For this exercise, we repeat the same procedure for “User2”. It should look similar to the following screen shots.
Example:

S/MIME enabled with signing and encryption.

Signing enabled with user certificate (for signing).
Encryption enabled with user certificate (for encryption).
Testing

If everything has been performed correctly, when “User1” or “User2” sends an email signed and encrypted, whoever is the recipient should be able to decrypt and read the message in clear text.

Encrypted message read by recipient.

Verification of signer trusted certificate
Troubleshooting FAQ

Q: I am unable to send an encrypted message to another domain user through WorxMail. What is wrong?

A: Ensure that the user has the correct encrypted certificate assigned to the user. You can verify this under Active Directory Users and Computers > user properties.
The way WorxMail works is by checking the “userCertificate” user object attribute via LDAP queries.

This value can also be read by IT Admins under the Attribute Editor tab. If this field is empty or has the incorrect user certificate for encryption, then, WorxMail cannot encrypt (or also decrypt) a message.

Q: Why can’t I see any user certificates installed in the iOS profile for S/MIME?

A: The user certificates for signing and encryption are installed in the secured MDX sandbox. The certificates can only be accessed by WorxMail’s security framework.