Authentication in XenMobile 8.6 with a Focus on Client Certificate Authentication

Authentication is about security and user experience and balancing the two goals. This document describes the authentication options available for the XenMobile 8.6 solution, highlighting the configuration that provides the best experience, client certificates.

Users perceive authentication as an inconvenience to getting their work done. But to the organization, authentication is a means with which they can secure their organizational data and intellectual property. The authentication options within XenMobile allow the organization to balance security and usability to provide an optimal user experience.

Components associated with authentication for XenMobile include the Device Manager, NetScaler Gateway, App Controller, and optionally StoreFront. These components work together to provide access to XenMobile resources. All capabilities are available on iOS and Android.

- **Device Manager** – Authentication options center on the enrollment process for the device.
- **NetScaler Gateway** – Provides authentication in front of the App Controller and optionally StoreFront to broker the authentication and provide a secure tunnel.
- **App Controller** – Provides authentication to provision and control single sign-on (SSO) to web, SaaS, iOS and Android mobile apps.
- **StoreFront** – Access to Windows-based apps from XenApp and virtual desktops from XenDesktop.

**User Authentication Options**

Device Manager, App Controller, and NetScaler Gateway represent the authentication points. The authentication process for Device Manager is to validate device enrollment. The device can be registered with the Active Directory UserName/UPN or an invitation URL. UserName options use the auto-discovery system, whereas the URL is a direct connection to the
environment. Two-factor and high security options are available for organizations that require higher levels of authentication. The following figure shows the various authentication combinations that you can configure for device enrollment:

<table>
<thead>
<tr>
<th>Device Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username (UPN) + Password</td>
</tr>
<tr>
<td>Username (UPN) + One Time PIN (OTP)</td>
</tr>
<tr>
<td>Invitation URL + PIN or Password</td>
</tr>
<tr>
<td>Invitation URL</td>
</tr>
<tr>
<td>Two Factor</td>
</tr>
<tr>
<td>High Security</td>
</tr>
</tbody>
</table>

The App Controller and NetScaler Gateway authentication process is used for authentication to enable single sign-on (SSO) to web, SaaS, iOS and Android mobile apps, and pass-through authentication to StoreFront.

The user certificate authentication method is a new addition in XenMobile 8.6. Certificates allow an authentication option that improves the user experience during revalidation periods. The certificate can be used on its own or in combination with other authentication methods. In combination with Worx PIN, for example, the user certificate improves the usability of XenMobile greatly. The following figure shows the options for authentication through NetScaler Gateway and App Controller.

<table>
<thead>
<tr>
<th>NetScaler Gateway/App Controller</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Certificate</td>
</tr>
<tr>
<td>Username + Password</td>
</tr>
<tr>
<td>Username + User Certificate</td>
</tr>
</tbody>
</table>
Understanding the Worx PIN

The Worx PIN simplifies the user authentication experience. Worx PIN is used to secure a client certificate or save Active Directory credentials locally on the device.

When administrators configure Worx PIN settings in App Controller, when users start Worx Home for the first time, they receive a prompt to enter a PIN, as shown in the following figure, which caches the Active Directory credentials. When users subsequently start Worx Home, WorxMail, or WorxWeb, they enter the PIN and log on. This simplifies the logon process on the mobile device.

You configure Worx PIN settings on the Settings > Support Options page in App Controller. You can configure the following settings:

- Enabling Worx PIN. The default is false.
- Enabling password caching. The default is false.
- Configuring the PIN complexity to require alphanumeric or numeric characters. The default is numeric.
- Configuring the length of the PIN. The default is 6 characters.
- Configuring the length of time before users need to change their PIN. The default is 0.

You can configure the following combinations for the PIN:

- Numeric that are numbers only
- Alphanumeric that contain at least one letter with numbers
- Complex that contain at least one letter, number, and a symbol

After you configure a Worx PIN, each of these settings appears on the Support Options page as shown in the following figure.

You can click the pencil icon for each item to edit the settings to match your requirements. The steps to edit a Worx PIN in App Controller are as follows:

1. In the App Controller management console, click **Settings**.
2. In the navigation pane, under **System Configuration**, click **Support options**.
3. In the details pane, select an item and then click the pencil icon.
4. In the **Add Property** dialog box, do the following:
   a) In **Value**, type the value for the item.
   b) In **Description**, type a description for the item.
Citrix Recommended Authentication Configuration

The client certificate option in XenMobile offers high security for the organization and ease of use for users. Citrix recommends the following configuration:

- Device Manager - Enable auto-discovery of email address or UserName (UPN)/Password or OTP.
- NetScaler Gateway and App Controller - Enable the user certificate
- StoreFront - Enable the user certificate.

The following figure shows the deployment and the consecutive steps users take when you configure the XenMobile environment with client certificate authentication.

1. Users install Worx Home from the App Store or Google Play.
2. Worx Home opens. Users enter UserName/UPN/OTP and the system validates the credentials with the XenMobile auto-discovery service.
③ Worx Home enrolls with Device Manager using Username/Password and the user certificate is installed to the device.
④ Worx Home authenticates with NetScaler Gateway by using the user certificate.
⑤ Authentication is passed to App Controller.
⑥ NetScaler Gateway passes authentication to StoreFront.

The configuration of the XenMobile environment for client certificate authentication occurs as follows:

**First Step:** Set up a Certificate Authority (CA) if the organization does not currently have a CA. The XenMobile infrastructure was tested with the Microsoft Certificate Services. Instructions to install and configure the Microsoft CA are located at the end of this document in Appendix A.

**Second Step:** Create a certificate template for XenMobile certificate requests. Configuration of the template occurs on the Microsoft CA server as follows:

1. Open the MMC Console on the Microsoft CA server.
2. Add a Snap-In for **Certificate Templates**.
3. Open **Certificate Templates**.
4. Right-click the **User template** and then click **Duplicate Template**.
5. Select **Windows 2003 Server** for the template type and then click **OK**.

6. Enter a certificate **Template display name**.
   **Note:** Save the following actual **Template name** because you need it later in the configuration.

7. Click the **Request Handling** tab and then specify **Signature and Encryption**.
8. (Optionally) enable or disable **Allow private key to be exported**.
9. Select **Enroll subject without requiring any user input**.
10. Click **Supply in the request**.

11. In the notification dialog box, select **OK**.
12. Click the **Security** tab and then select to allow **Enroll** permissions to a user account that will be making the certificate requests from Device Manager.

![Security tab with permissions settings](image)

13. Open MMC and add a Snap-In for **Certification Authority**.
14. Expand the CA server and then right-click **Certificate Templates**.
15. Click **New** and then click **Certificate Template to Issue**. Select the certificate template you created in the preceding steps.

![Certificate Templates menu](image)

**Third Step:** Generate the XenMobile client certificate. You can request a certificate from any system in the domain. The domain account must have
local administrator rights to the system requesting a certificate from the Certificate Server.

1. Click **Start** and then click **Run**.

2. Type **MMC**.

3. Click **File->Add/Remove Snap-in**.
4. In the **Snap-in list**, click **Certificates**.

5. Click **Add** and then click **OK**.

6. Click **Finish**.

7. Expand the **Certificates – Current User** option in the left window pane.
8. Expand the **Personal** folder.
9. Right-click **Certificates** and then click **All Tasks**.

10. Click **Request New Certificate**.

12. Click Next again.

13. Scroll to the bottom of the Request Certificates list and then select the User check box in the lower left-hand corner.
14. Click **Enroll**.

15. Click **Finish**.

16. The certificate is now created. Next, you need to import the certificate into the Device Manager server. Right-click **Certificate**.

17. Select **All Tasks** and then click **Export**.
The Certificate Export wizard opens.

18. Click **Yes, export the private key** and then click **Next**.

19. Click **Personal Information Exchange – PKCS #12 (.PFX)**.
20. Select **Include all certificates in the certification path if possible**.
21. Select **Export all extended properties** and then click **Next**.
22. To protect the security of the private key for the certificate, enter a **password** and then click **Next**.

![Certificate Export Wizard](image)

23. Browse to a location where you want to save the certificate with the extension .pfx and then click **Next**.

![Certificate Export Wizard](image)

24. Click **Finish**.

![Certificate Export Wizard](image)

25. Click **OK**.
Fourth step: Create the XenMobile Microsoft CA payload configuration on the Device Management server.

1. Open the XenMobile admin console. Browse to XenMobile Server Options.

2. Expand the PKI section and then click Server certificates.
3. Click Upload a certificate.

4. On the Upload a Certificate Type page, enter the following:
a) **Certificate Type**: Keystore.
b) **Keystore type**: PKCS#12.
c) **Keystore file**: Upload a .pfx or .p12 certificate that was exported to the server.
d) **Password**: The password created with the certificate

5. Click **Upload**.

6. The certificate is now loaded into the XenMobile server.

7. Under **PKI**, click **Entities**.
8. Click **New -> MS CertSrv entity**.
9. The wizard menu loads. Enter the following:
   a. **Entity name**: CA Server name
   b. **Authentication type**: Client certificate
   c. **SSL client certificate**: Select the client certificate that was uploaded

10. Click the **Templates** tab.

11. Enter template name from the Microsoft CA server.

12. Click the **CA Certificates** tab.
13. Click **Add** and then select the certificate. Use intermediate if available; if not, choose default CA and then click **Add**.

14. Click the **CA Certificates** tab again and then click **Update**. This opens the **XenMobile Server Options** screen for the **PKI entities** option.

15. Under **PKI**, click **Credential providers** and then click **New** credential provider.
16. Give your credential provider a name and description. Select the previously created Issuing entity. Select Issuing Method as Sign, and select the template you created with the entity.

17. Click the **CSR** tab and then complete the following settings:
   a) The **Key Size** must match the key length specified in the template that was created in the second step.
   b) In **Subject Name**, specify **CN=$user.username**
   c) In **Subject Alternate Names**, click **New alternative name** and then specify the **User Principal Name** and a value of **$user.userprincipalname**.
18. In **Issuer**, select the CA that is issuing the certificate and in **Distribution mode**, click ** Prefer centralized.**

19. Click the **Renewal tab.**

20. Select **Renew certificates when they expire.**

21. Enter the **number of days** within renewal before expiration and then click **Add.** The credential provider is now created.
**Step Five:** Configure Device Manager to provide a user certificate to App Controller.

1. Expand **Modules Configurations** and then click **App Controller**.
2. Complete the following settings:
   a. **Host Name** of App Controller.
   b. **Shared Key**.
   c. Select **Enable App Controller**.
   d. Select **Deliver user certificate for authentication**.
   e. In **Provider**, select the provider you created in Step four.
Fifth step: Configure NetScaler Gateway to accept client certificates

1. Open NetScaler -> Configuration.
2. Go to NetScaler Gateway -> Virtual Servers
3. Select the NetScaler Gateway virtual server from the list that you want to configure and then click Open.

4. To import the CA certificate, click the Certificates tab. A list of the certificates appears in the left-hand column.
5. Select the root certificate that was added to NetScaler Gateway from the third-party CA and then click Add -> As CA to add the CA to the Configured list on the right-hand side.
6. Click SSL Parameter.
7. In the **Configure SSL Params** dialog box, select **Client Authentication**.
8. In **Client Certificate**, select **Mandatory** and then click **OK**.

Next, configure a policy to use the client certificates.

9. Click **NetScaler Gateway -> Policies -> Authentication/Authorization -> Authentication -> CERT**.
10. Click **Add** to add the authentication server.
11. In **User Name Field**, make sure to use the `SubjectAltName:PrincipalName` to get the UPN delivered and then click **OK**.

12. Create a second authentication policy for Active Directory credentials with a lower priority. The following figure shows an example of the server and policy configuration.
The following figure shows an example of the entire configuration. **Note:** If you are using a NetScaler Gateway Callback (optionally, you can disable callback in newer builds), you will need to create a second virtual server that is not using client certificate authentication to handle the NetScaler Gateway Callback.
Seventh step: Configure App Controller

1. In the App Controller management console, click the **Settings** tab.
2. Under **System Configuration**, click **Deployment**.
3. In the details pane, under **NetScaler Gateway**, click **Edit**.
4. In **Configure authentication from NetScaler Gateway**, if devices need to access App Controller remotely, select **Yes** to allow remote users to connect.

**Note:** If this is the first NetScaler Gateway or virtual server you are configuring, this setting moves to **Yes** automatically. If this is not the first NetScaler Gateway or virtual server you are configuring, you must manually select **Yes**.

5. Click the plus (+) symbol to add an appliance. When you click the plus symbol, the fields in the following list appear. Enter the following:
   a) In **Alias**, type a name that is easily recognizable.
   b) In **Display name**, type the NetScaler Gateway name.
c) In **Callback URL** (optional) and **External URL**, enter the NetScaler Gateway Web address. For example, enter https://mynetscalergateway.com.

You can specify the port number in the web address, such as https://mynetscalergateway.com:443.

When you add the web address to Callback URL, App Controller appends the URL automatically with the NetScaler Gateway authentication service URL. For example, the URL appears as https://NetScalerGatewayFQDN/CitrixAuthService/AuthService.asmx.

d) In **Logon type**, select **Domain and Certificate**.
e) Select the **Set as default** check box.

6. Click **Save**.
7. In the left-hand menu, click **Certificates** and ensure that you import the root CA for your client certificates.

---

**Eighth step: Configure StoreFront**

To ensure a unified experience when you deploy StoreFront in conjunction with XenMobile, you need to configure an additional NetScaler Gateway virtual server for devices that run Citrix Receiver. NetScaler Gateway uses the STA token provided in the ICA file. No other authentication methods are necessary. You simply configure the appropriate authentication policies for the environment (such as LDAP and RADIUS) in the newly created virtual server. This implementation will allow the use of the second virtual server for additional items.
Requirements:
- An additional port is required through the firewall. This configuration uses port 8081. (You can also use an entirely different address depending on your environment.)
- StoreFront points at the virtual server configured for this purpose.
- StoreFront does not require knowledge of the certificate-enabled virtual server.
- You must configure STA servers on both virtual servers.
- This configuration assumes client certificate authentication is already configured on a separate virtual server.

1. Log on to NetScaler Gateway by using Gateway Deployment type.
2. On the dashboard, click Create New NetScaler Gateway in the upper-right corner.

3. In Name, enter a name for the new virtual server.
4. In IP Address, enter a temporary placeholder. (In this example, the IP address is used when the configuration is done. If you are using a separate IP address for the virtual server, you can input the address here.)
5. In Port, enter the port number to be used in production for the virtual server.
6. Click Continue.
7. Click **Choose Certificate**, select a **certificate** for NetScaler Gateway and then click **Continue**.

![NetScaler Gateway Settings](image)

9. In **Primary Authentication** select an authentication type. In this case, we are unbinding this policy. Adjust the settings as appropriate for your environment. To allow only STA traffic, however, you can configure other policies for web traffic.

10. Click **Continue**.

![Certificate](image)

11. In **App Controller FQDN**, enter the fully qualified domain name (FQDN) from the XenMobile infrastructure and then click **Done**.
12. Click **Configure NetScaler Gateway Appliances** to edit the appliance settings.

13. In **IP Address**, modify the IP address of the new StoreFront virtual server to match the IP address of your client certificate virtual server, click **OK** and then click **Save**.

14. In **Single Sign on Domain**, modify your operating system session policy to match your SSO domain (for example, *Citrite*) and then click **OK**.
15. Click the **Intranet Applications** tab.
16. Add your intranet applications to match the originating virtual server. It is optional to offload traffic from the DNS server.

17. Click the **Published Applications** tab.
18. Under **Next Hop Servers**, click **Add** to add a STA server. This is the same as the StoreFront STA server.
19. Under **Secure Ticket Authority**, click **Activate all** and then click **OK**.
20. View the list of published applications and verify that servers show an **UP** state.
21. Click the **Authentication** tab.
22. Select the **Enable Authentication** check box.
23. Under **Authentication Policies**, select **Unbind Policy** for any primary or secondary policies and then click **OK**.

24. Open the **App Controller** management console.
25. Click **Apps & Docs** and then click **Windows Apps**.
26. Enter the **StoreFront** server information.
27. Open the management console for **StoreFront**.
28. Click **Change General Settings**.
29. Point the NetScaler Gateway URL to the Non-SSL virtual address just created (with port example) and then click **OK**.

---

**Appendix A**

Microsoft Certificate Services installation and configuration.

**Configuring Microsoft Certificate Services in Device Manager Prerequisites**

- Port 443 (default) open from XenMobile Device Manager to Microsoft Certificate Services server.
- Microsoft KB 980436 patch needs to be installed on Microsoft Certificate Services server.
- Microsoft KB 953461 patch needs to be installed on Microsoft Certificate. Services server on Windows 2008 Server Enterprise.
- Web enrollment for Microsoft Certificate Services needs to be enabled.
- SSL enabled on Microsoft Internet Information Services (IIS).
- IIS configured to accept client certificate authentication.
- The client certificate in .p12 format which is used to authenticate.

Enable Web Enrollment for Microsoft Certificate Services

1. Go to Administrative Tools and select Server Manager on the server to host the Certificate Authority.
2. Under Active Directory Certificate Services, check to see if Certificate Authority Web Enrollment is installed.
3. Select Add Role Services to install Certificate Authority Web Enrollment, if necessary.
4. Select Certificate Authority Web Enrollment and then click Next.
5. Click Close or Finish when the installation is complete.

![Add Role Services Wizard](image)

Configure Microsoft Internet Information Services

1. Go to Administrative Tools and click Server Manager.
2. Under **Web Server (IIS)**, look under **Role Services**. Verify that Client Certificate Mapping Authentication and IIS Client Certificate Mapping Authentication are installed. If not, install these role services.

3. Go to **Administrative Tools** and click **Internet Information Services (IIS) Manager**.

4. In the left-hand pane of the IIS Manager window, select the server running the IIS instance for web enrollment as shown in the following figure.

5. Click **Authentication**.

6. Make sure Active Directory Client Certificate Authentication shows the status of **Enabled**.
7. Click **Sites**.
8. Click **Bindings** in the right-hand pane.

9. Add a site binding of the type `https` if one does not exist.

10. Go to the **Default Web Site Home**.
11. Click **SSL Settings** and then click **Accept** for Client Certificates.