VMware AirWatch Certificate Authentication for EAS with ADCS

For VMware AirWatch

Have documentation feedback? Submit a Documentation Feedback support ticket using the Support Wizard on support.air-watch.com.

Table of Contents

Chapter 1:
Workspace ONE UEM Certificate Authentication for EAS with ADCS

Workspace ONE UEM may be configured to allow a user's device to connect to Microsoft Exchange ActiveSync using a certificate for authentication.

For those who are using an email server other than Exchange ActiveSync, there is an explanation of the methodology and concepts enabling you to implement it on a different email server.

System Requirements, EAS with ADCS

The following tasks must be completed before proceeding with the steps outlined in this document.

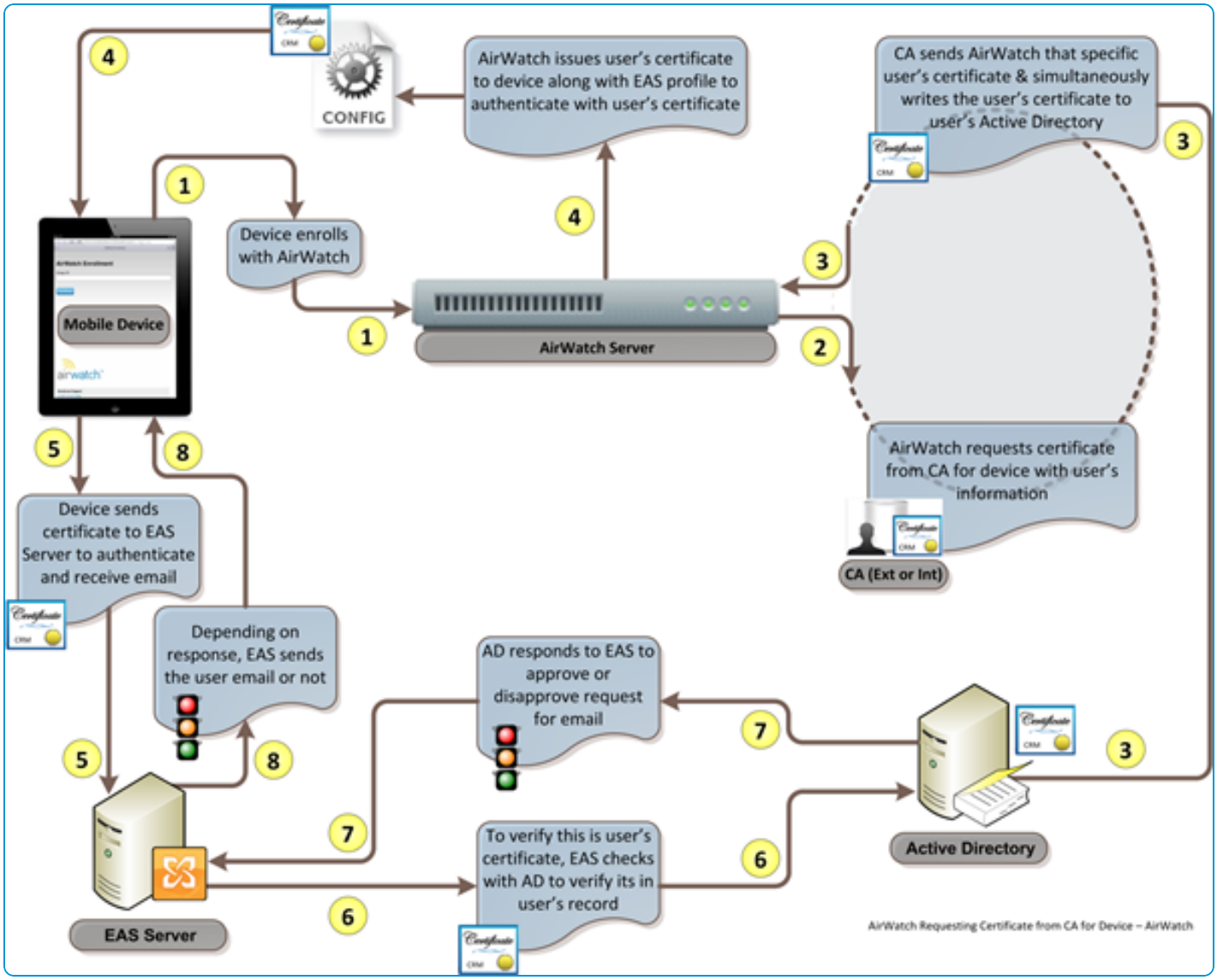
- A certificate authority server must be set up and configured. If you want guidance as to the methodology of setting up a certificate authority, refer to Setting Up a Microsoft Certificate Authority for Use with Workspace ONE UEM. The certificate authority must be an enterprise certificate authority as opposed to a standalone certificate authority (standalone does not allow for the configuration and customization of templates).

  > **Important:** Certificate Authorities can be set up on servers running a variety of operating systems, including Windows®2000 Server, Windows Server® 2003, and Windows Server 2008. However, not all operating systems support all features or design requirements, and creating an optimal design requires careful planning and lab testing before you deploy a client access server (e.g., ADCS) in a production environment.

- Microsoft Exchange with ActiveSync enabled.
- Internet Information Services (IIS) on the Exchange ActiveSync server must have the option Client Certificate Mapping Authentication installed.

High Level Design, EAS with ADCS

This diagram shows how certificate authentication is handled from the point where the user device enrolls into Workspace ONE UEM to when the user begins to receive email.



Implementation Approach, EAS with ADCS

Before your enterprise email server can securely pass email to the user's device, you need to configure your email server to recognize the user's device and trust it is the authorized user of that device.

This is accomplished by authenticating the user and their device using a certificate. Regardless of the enterprise email server or client access server being used, the methodology is basically the same. If you understand the methodology, have the technical expertise, and have a strong understanding of the hardware and software required, then it is much easier to configure and ensures enterprise email is pushed securely to your user's device.

Chapter 2:
Install, Set Up, Configure Certificate

This section provides instructions to configure the certificate authority (CA) of your choice to work with the Workspace ONE ™ UEM console. Take the following steps and procedures to integrate the certificate.

Configure Email Server, EAS with ADCS

Before your enterprise email server can securely pass email to the user's device, you need to configure your email server to recognize the user's device and trust it is the authorized user of that device.

Set up a Trust Relationship between Directory Services and the Certificate Authority

Establish trust between the certificate authority (CA) and directory services such that it can authenticate the certificate stored in the user's directory account.

For instance, establishing such a trust for Microsoft Active Directory would entail these steps.

- Open your system administrator software tool's console (e.g., MMC)
- Add the particular snap-ins (e.g., Enterprise PKI)
- Associate the snap-in with the desired certificate authority.

Next, complete each following step in sequence.

Configure the Exchange ActiveSync server for Certificate-based Authentication

Set up permissions for your users to be able to access your enterprise email server using certificate authentication. For example, in order to accomplish this on a Microsoft Exchange server.

1. Open the tool you use (e.g., IIS) to choose the authentication method being used by your enterprise email server.
2. Choose to only allow authentication through identity certificates (e.g., Active Directory Client Certificates)
3. Configure your email server to require Secure Socket Layer (SSL).
4. Increase the cache memory of your internet server (e.g., IIS) to accommodate the increased demands of using certificate authentication.

Configure Certificate Authority and Certificate Template in Workspace ONE UEM

Once you have configured certificate authentication to your email infrastructure, enable Workspace ONE UEM to request the end-user identity certificates used for authentication from your certificate authority.

1. Navigate to **Devices > Certificates > Certificate Authorities** and configure the certificate authority that was used to generate the user's certificate.
2. Choose the Authority Type used by your enterprise.
3. Add the certificate authority to the Workspace ONE UEM console.
4. Add a certificate template that associates the certificate authority used to generate the user's certificate.
5. Transfer the certificate to the Workspace ONE UEM console.
6. Assign the certificate to a particular user or organization group.

For more information, see **Step 3: Configure Certificate Authority and Certificate Template in Workspace ONE UEM**.

Create a Profile for Exchange ActiveSync

The final step is to configure the Workspace ONE UEM console to create and deploy the user's profile to push email to the user's device.

1. Navigate to **Devices > Profiles**.
2. Configure the Credentials screen to define the certificate authority that created the user's certificate and the certificate template associated to that certificate authority's certificate.
3. Configure the Exchange ActiveSync screen to publish the user's profile to the device by configuring your enterprise email server and security protocol (e.g., SSL) with the user's email address and payload certificate.
4. Push the user's profile and certificate to the user's device.
5. Have the user authenticate and connect to your enterprise email server and begin receiving email.

For more information, see **Step 4: Create a Profile for Exchange ActiveSync**.

Step 1: Set Up a Trust between Active Directory and the CA, EAS with ADCS

In order for Microsoft Exchange ActiveSync to authenticate a user from a certificate, it must first trust the source of the certificate.

1. On the Certificate Authority server, select **Start > Run**.
2. Type MMC in the dialog box and press **Enter** to launch the Microsoft Management Console (MMC).
3. Click **File > Add/Remove Snap-in…** from the MMC main menu.
4. Select **Enterprise PKI** from the list of Available snap-ins and then select **Add**.
5. Click **OK**.
6. Right-click **Enterprise PKI** and select **Manage AD Containers**.

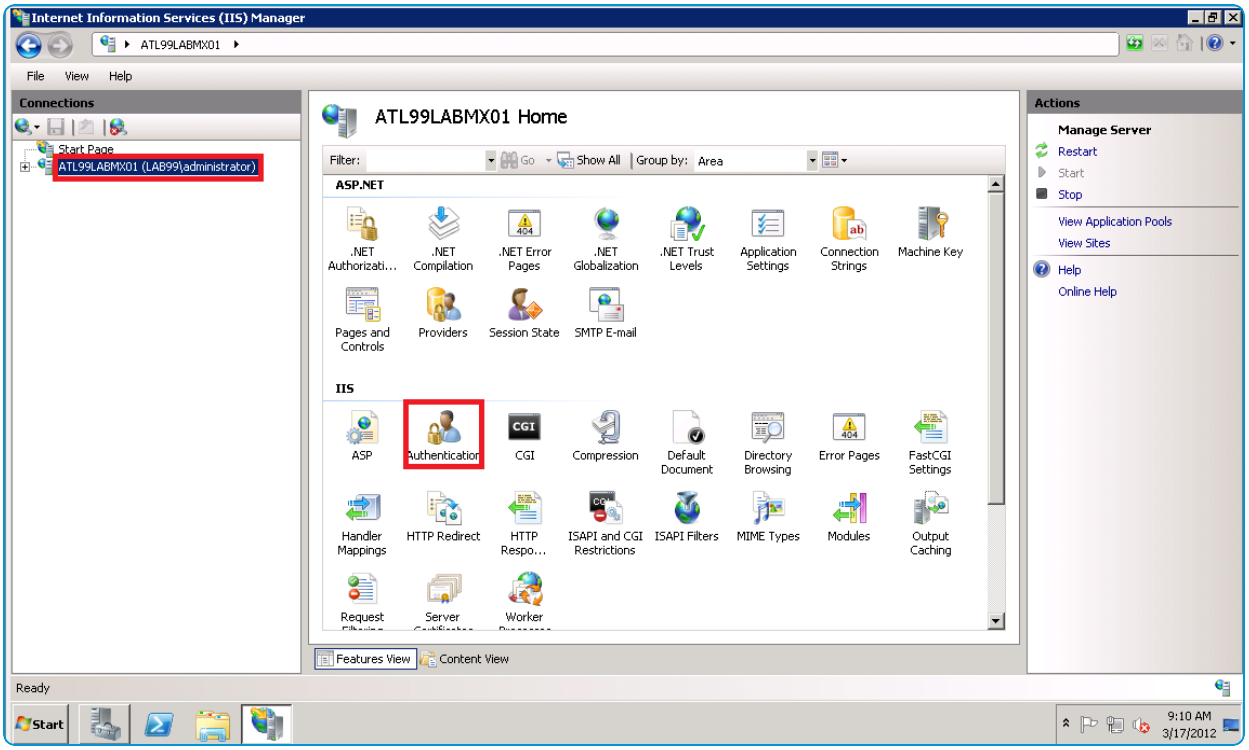
7. Select the **NT AuthCertificates** tab and verify the Certificate Authority is listed. If not, select **Add** to add the Certificate Authority to the group.
8. Click **OK**.

Step 2: Set Permissions on Exchange Server

In order for devices to authenticate with Microsoft Exchange ActiveSync, you must configure several changes on the Exchange Server.

Certificate Authentication

1. On the Exchange server, select **Start > Run**.
2. Type `inetmgr` in the dialog box to launch **Internet Information Services (IIS)**.
3. Select the server in the left-hand **Connections** pane.
4. Under IIS, double-click the **Authentication** icon.



5. Select **Active Directory Client Certificate Authentication** and then select **Enable**.

Configuration Editor

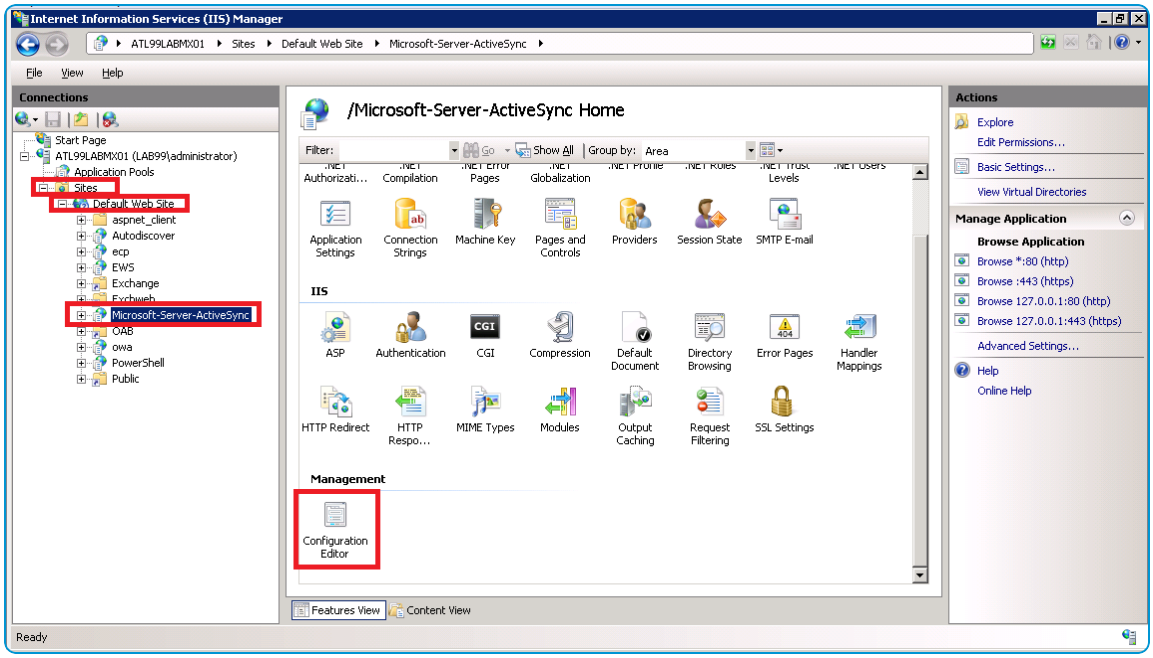
1. Click **+** to expand **Site** and then **Default Web Site** to display all available configuration editors.
   a. If you are using MS Server 2008 R2 or later, the **Configuration Editor** icon appears as shown below; Select **Microsoft-Server-ActiveSync** and double-click on the **Configuration Editor** icon. Skip steps 1. b & 1. c, and go directly to step 2.

b. If you are using Exchange servers older than 2008 R2, you need to be familiar with the use of **appcmd.exe** and run it from the command prompt.

c. Open a command prompt by selecting **Start > Run**. In the dialog box type cmd and select OK. In the command prompt, type the following command:

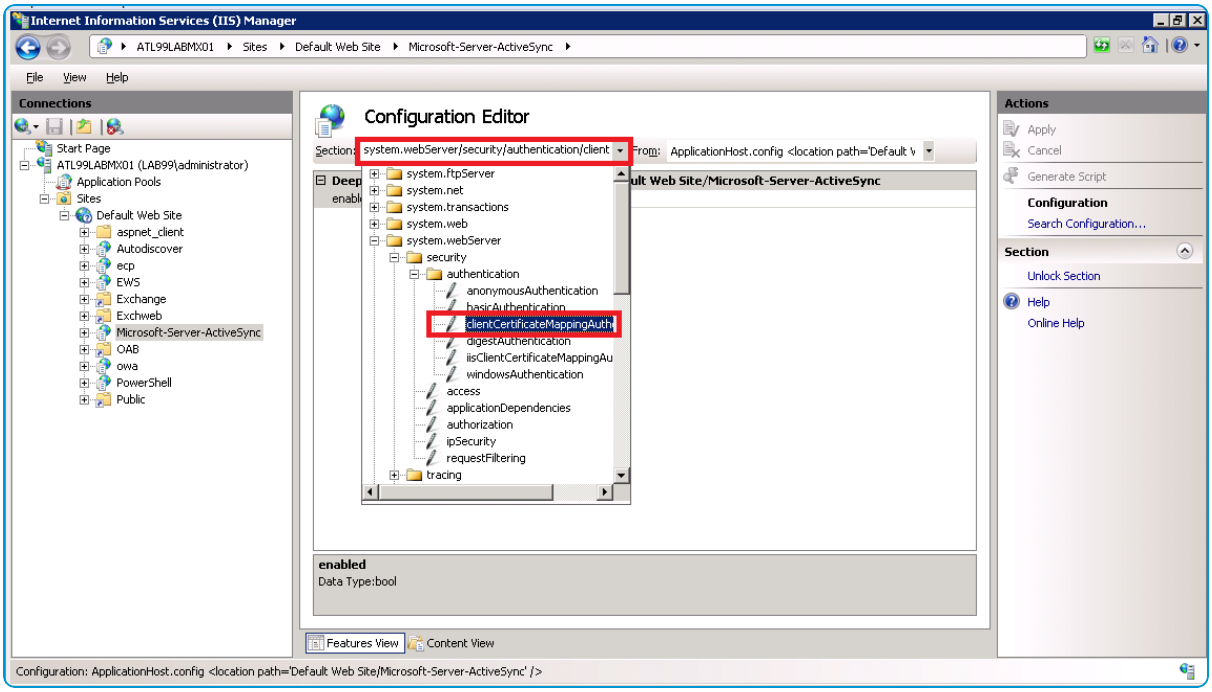
```
appcmd.exe set config "Microsoft-Server-ActiveSync" -
section:system.webServer/security/authentication/clientCertificateMappingA
uthentication /enabled:"True" /commit:apphost
```

If you performed this step, then skip the remaining steps and advance to Setting up Secure Socket Layer (SSL).



2. Navigate to **system.webserver/security/authentication** in the Section drop-down menu.

3. Select **clientCertificateMappingAuthentication**.

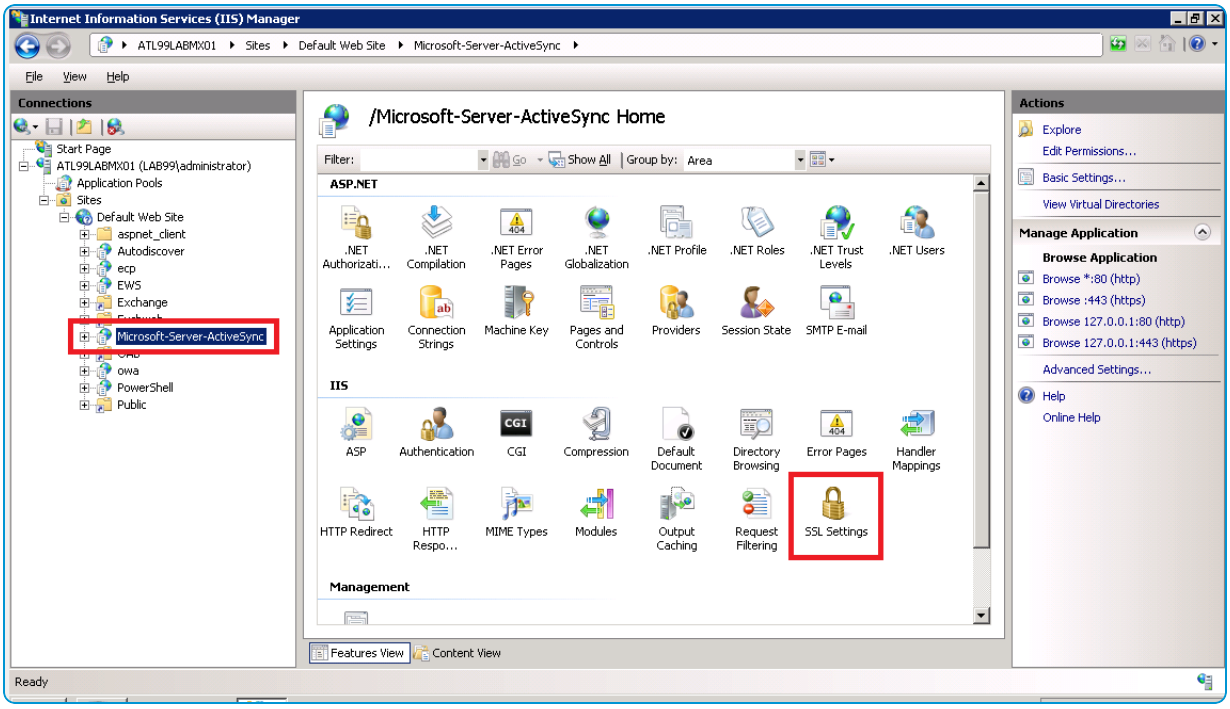


4. Select True from the drop-down menu on the Enabled option.

Set Up Secure Socket Layer (SSL)

If only certificate authentication is being used, then you must configure Secure Socket Layer (SSL).

1. Select **Microsoft-Server-ActiveSync**, and then double-click the **SSL Settings** icon.



2. Select **Accept** if other types of authentication are allowed. If only certificate authentication is allowed, then select the **Require SSL** checkbox and then select **Required**.

Adjust uploadReadAheadSize Memory Size

Since certificate based authentication uses a larger amount of data during the authentication process, some adjustments must be made in IIS configuration to account for the increased amount of data. This is accomplished by increasing the value of the uploadReadAheadSize. The following steps guide you through the configuration:

1. Open a command prompt by selecting **Start > Run**.
2. Type cmd in the dialog box and select OK.
3. Enter the following commands to increase the value of the uploadReadAheadSize from the default of 48KB to 10MB:

```
C:\Windows\System32\inetsrv\appcmd.exe set config -section:system.webServer/serverRuntime
/uploadReadAheadSize:"10485760" /commit:apphost
```

```
C:\Windows\System32\inetsrv\appcmd.exe set config "Default Web Site" -
section:system.webServer/serverRuntime /uploadReadAheadSize:"10485760" /commit:apphost
```

   "Default Web Site" is used. If the name of the site has been changed in IIS then the new name needs to replace "Default Web Site" in the second command.

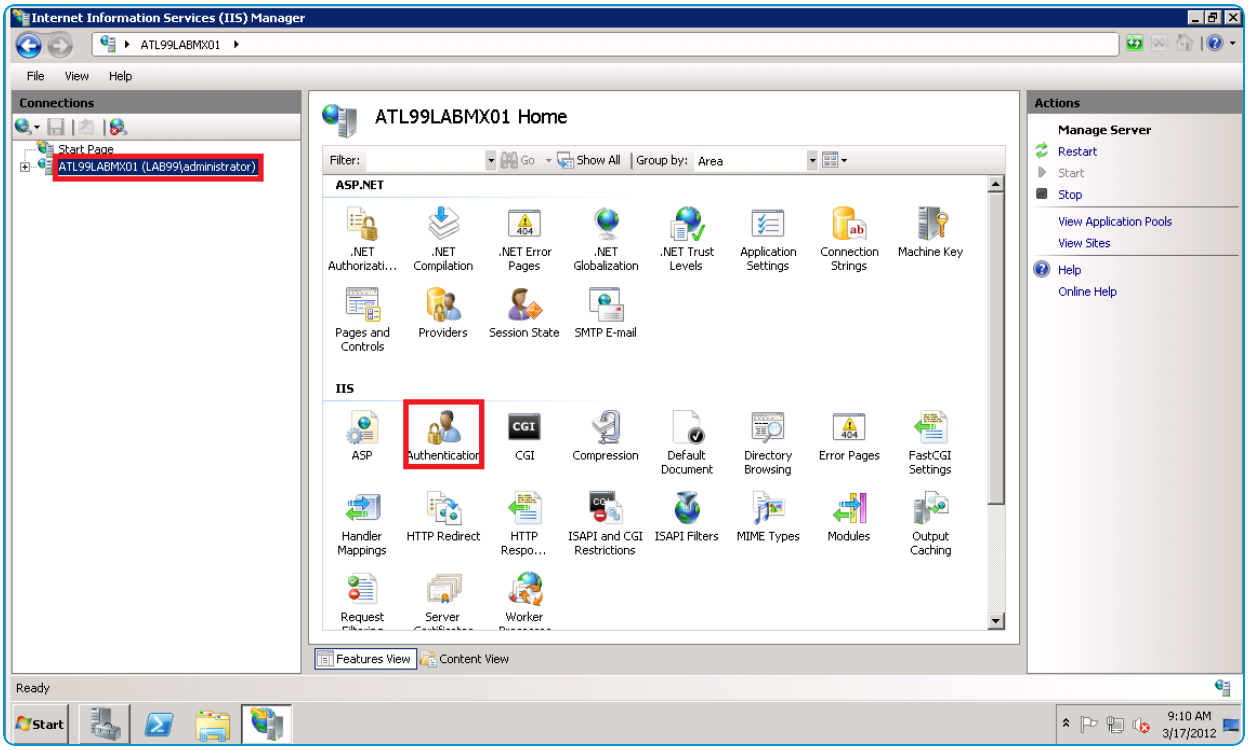
4. Enter the IIS Reset command to perform an IIS reset by entering the following command:
   `iisreset`

Step 2: Set Permissions on Exchange Server

In order for devices to authenticate with Microsoft Exchange ActiveSync, you must configure several changes on the Exchange Server.

Certificate Authentication

1. On the Exchange server, select **Start > Run**.
2. Type `inetmgr` in the dialog box to run **Internet Information Services (IIS)**.
3. Select the server in the **Connections** pane.
4. Under IIS, double-click the **Authentication** icon.



5. Select **Active Directory Client Certificate Authentication** and then select **Enable**.

Configuration Editor

1. Click **+** to expand **Site** and then **Default website** to display all available configuration editors.

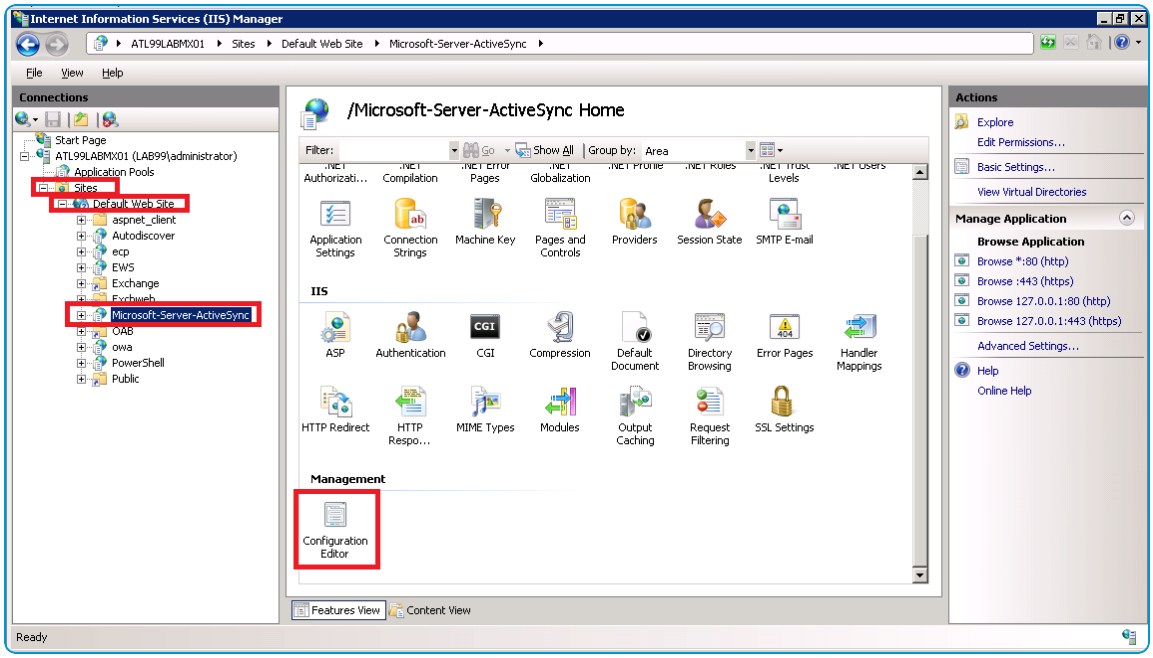
   a. **If you are using MS Server 2008 R2 or later, the Configuration Editor icon appears; Select Microsoft-Server-ActiveSync and double-click on the Configuration Editor icon. Skip steps 1b & 1c, and go directly to step 2.**

   b. If you are using Exchange servers older than 2008 R2, be familiar with the use of **appcmd.exe** and run it from the command prompt.

   c. Open a command prompt by selecting **Start > Run**. Type `cmd` in the dialog box and select **OK**. In the command prompt, type the following command:

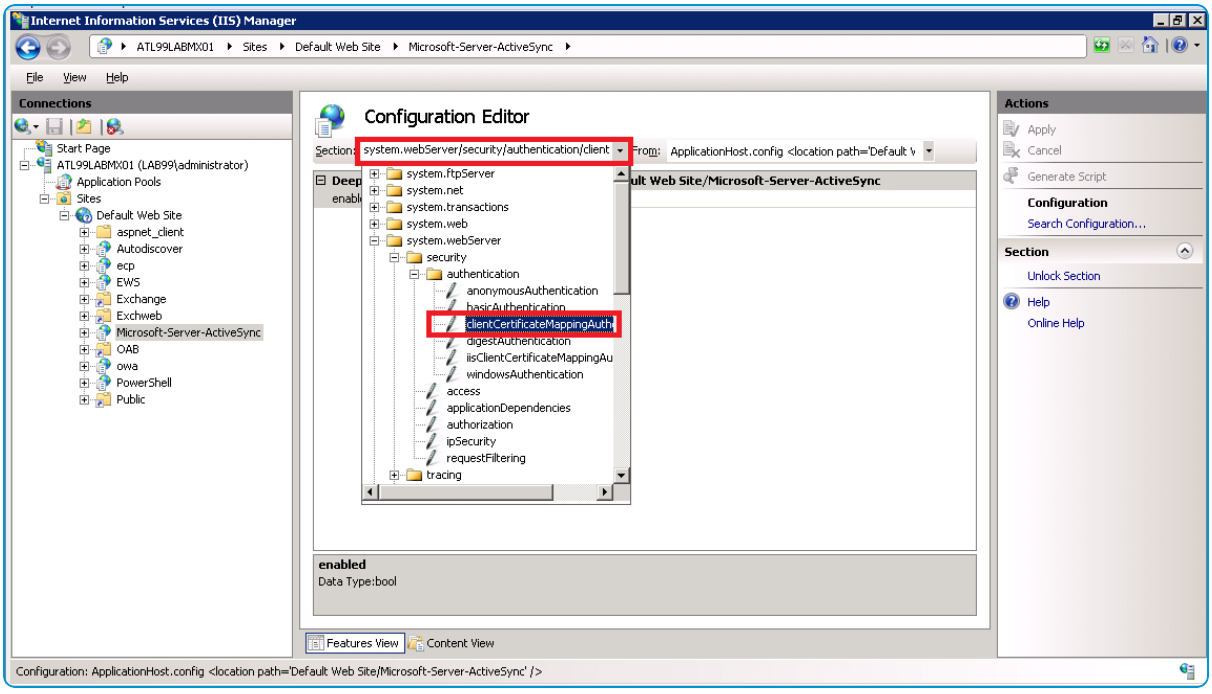
```
appcmd.exe set config "Microsoft-Server-ActiveSync" -
section:system.webServer/security/authentication/clientCertificateMappingA
uthentication /enabled:"True" /commit:apphost
```

If you performed this step, then skip the remaining steps and advance to Setting up Secure Socket Layer (SSL).



2. Navigate to **system.webserver/security/authentication** in the Section drop-down menu.

3. Select **clientCertificateMappingAuthentication**.

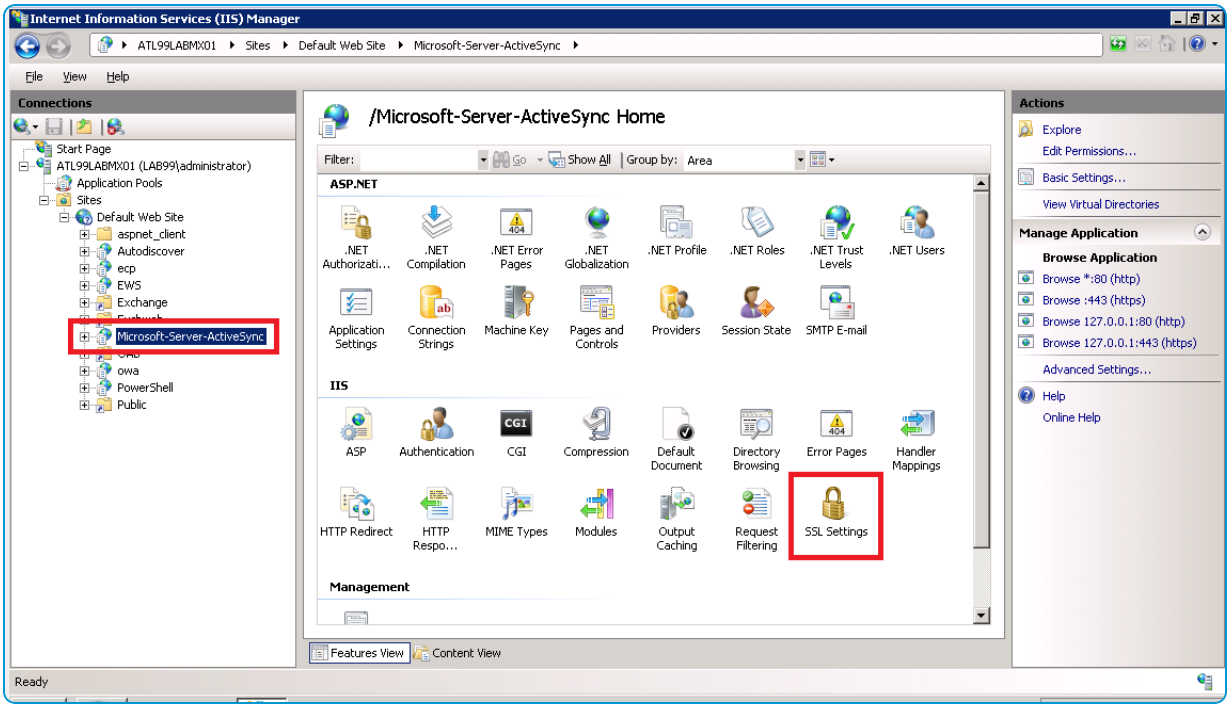


4. Select True from the drop-down menu on the Enabled option.

Set Up Secure Socket Layer

If only certificate authentication is being used, then you must configure Secure Socket Layer (SSL).

1. Select **Microsoft-Server-ActiveSync**, and then double-click the **SSL Settings** icon.



2. Select **Accept** if other types of authentication are allowed. If only certificate authentication is allowed, then select the **Require SSL** check box and then select **Required**.

Adjust uploadReadAheadSize Memory Size

Since certificate-based authentication uses a larger amount of data during the authentication process, you must increase the value of the **uploadReadAheadSize** from 48 KB to 10 MB to account for the increased amount of data. Specifically, The following steps guide you through the configuration:

1. Open a command prompt by selecting **Start > Run**.
2. Type cmd in the dialog box and select OK.
3. Enter the following commands:

```
C:\Windows\System32\inetsrv\appcmd.exe set config -section:system.webServer/serverRuntime
/uploadReadAheadSize:"10485760" /commit:apphost
```

```
C:\Windows\System32\inetsrv\appcmd.exe set config "Default Website" -
section:system.webServer/serverRuntime /uploadReadAheadSize:"10485760" /commit:apphost
```

If the name of the site has been changed in IIS, then replace `Default Website` with the new name in the second command.

4. Perform an IIS reset by entering the following command:
   `iisreset`

Step 3: Configure Certificate Authority and Certificate Template in Workspace ONE UEM, EAS with ADCS

In order for Workspace ONE UEM to retrieve a certificate from a certificate authority, you must correctly configure the Workspace ONE UEM console to use the certificate.

- Configure the certificate authority.
- Configure the certificate template.

Configure the Certificate Authority

1. Login to the Workspace ONE UEM console with Administrator privileges or higher.
2. Navigate to **Devices > Certificates > Certificate Authorities** from the Workspace ONE UEM console main menu.
3. Click **Add**.
4. Select **Microsoft ADCS** from the Authority Type drop-down menu prior to completing any other configuration settings for the certificate authority.
5. Enter the information about the **Certificate Authority**.
   - Enter the exact name for the new **Certificate Authority**.
   - Enter a brief **Description** for the new certificate authority.
   - Microsoft ADCS should already be selected for the **Authority Type** as described previously.
   - Select **ADCS** as the **Protocol**.
   - Enter the URL of the server in the **Server Hostname** field. The server hostname must be entered in the following format: https://{servername}/certsrv/adcs/. The site can be http or https depending on how the site is set up. The URL must include the trailing /.
   - Enter the **Authority Name**. This is the name of the certificate authority that the ADCS endpoint is connected to. This can be found by launching the **Certification Authority** application on the certificate authority server.
   - Verify **Service Account** is selected for **Authentication**.
   - Enter the **Username** and **Password**. This is the username and password of the ADCS Admin Account with sufficient access to allow Workspace ONE UEM to request and issue certificates.
6. Click **Save**.

Configure the Certificate Template

1. Select the **Request Templates** tab and then select **Add**. The **Certificate Template - Add/Edit** screen displays.
2. Complete the certificate template information:
   - Enter the exact **Name** for the new request template.
   - Enter a brief **Description** for the new certificate template.

- Select the certificate authority that was just created from the **Certificate Authority** drop-down menu.
- Enter the **Subject Name** or Distinguished Name (DN) for the template. The text entered in this field is the Subject of the certificate, which can be used by the network administrator to determine who or what device received the certificate.

  A typical entry in this field is “CN=WorkspaceONEUEM.{EnrollmentUser}” or “CN={DeviceUid}” where the {} fields are Workspace ONE UEM lookup values.
- Select the private key length from the **Private Key Length** drop-down menu.

  This is typically 2048 and should match the setting on the certificate template that is being used by ADCS.
- Select the private key type from the **Private Key Type** drop-down menu.

  This is typically “Signing & Encryption” and should match the certificate template that is being used by ADCS. For use with Exchange Active Sync it should be “Signing & Encryption”.
- Click **Add** to the right of **San Type** to include one or more Subject Alternate Names with the template. This is used for additional unique certificate identification. In most cases, this needs to match the certificate template on the server. Use the drop-down menu to select the San Type and enter the subject alternate name in the corresponding data entry field. Each field supports lookup values.
- Select the **Automatic Certificate Renewal** checkbox to have certificates using this template automatically renewed prior to their expiration date. If enabled, specify the **Auto Renewal Period** in days.
- Select the **Enable Certificate Revocation** checkbox to have certificates automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.
- For Lotus Domino configurations only, select the **Publish Private Key** checkbox to publish the private key to the specified web service endpoint.
- For iOS devices only, enable **Force Key Generation on Device** which generates a public and private key pair on the device, improving performance and security.

3. Click **Save**

Step 4: Create Profile for Exchange ActiveSync, EAS with ADCS

The final step in setting up the Exchange Active Sync Certificate Authentication is creating and deploying the Workspace ONE UEM profile that pushes the Exchange Server settings to the device. This profile contains the information necessary for the device to connect to Exchange, as well as the certificate that the device uses to authenticate.

1. Navigate to **Devices > Profiles > List View**.
2. Click **Add**.
3. Click the applicable device platform to launch the **Add a New Profile** dialog.
4. Configure the **General** settings for the profile. The General settings determine how the profile is deployed and who receives it as well as other overall settings.
5. Select **Credentials** from the profile options at left and then select **Configure**.
6. Select **Define Certificate Authority** from the Credential Source drop-down menu.

7. Select the certificate authority you created previously from the **Certificate Authority** drop-down menu.
8. Select the certificate template you created previously from the **Certificate Template** drop-down menu.
9. Select **Exchange ActiveSync** from the profile options at left and then select **Configure**.

   You must configure the Credentials payload settings before the Exchange ActiveSync payload settings.
10. Configure the **Exchange ActiveSync** settings:
    - Enter an account name in the **Account Name** field. This is the name that displays on the device to indicate which email account is active so it should be accurately descriptive.
    - Enter the Exchange ActiveSync host in the **Exchange Active Sync Host** data entry field. This is the actual endpoint of the mail server.

      Do not include “http://”, “https://” at the beginning or “/Microsoft-server-activesync” at the end.
    - Ensure the **Use SSL** checkbox is selected. Authentication using certificates fails over a non-SSL connection.
    - Deselect the **Use S/MIME** checkbox if enabled by default.
    - The **Domain** data entry field should contain the email domain for the user account.
    - The **Username** data entry field should contain the email address of the user when on the device.
    - The **Email Address** text box should contain the email address of the user when on the device

      Domain, Username, and Email Address can be obtained using Lookup Values which will retrieve the text stored in the applicable field of the User Profile.
    - Select the credential you created previously from the **Payload Certificate** drop-down menu.
11. Click **Save** or select **Save and Publish** to publish this profile to a device.

Chapter 3:
Testing and Troubleshooting, EAS with ADCS

You can confirm that the certificate is operational by pushing a profile to the device and testing whether or not the device is able to connect and sync to the configured Exchange ActiveSync endpoint. If the device does not connect and shows a message indicating the certificate cannot be authenticated or the account cannot connect to Exchange ActiveSync, then there is a problem in the configuration.

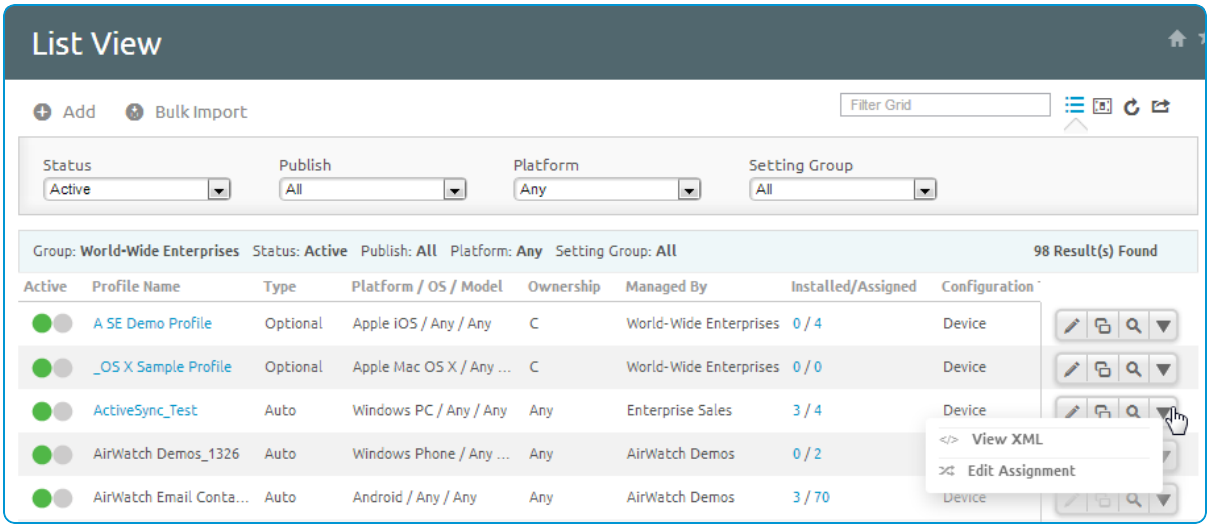
Ensure a certificate is being issued by the certificate authority to the device by checking the following information:

1. Launch the certification authority application on the certificate authority server and browse to the issued certificates section.
2. Locate the last certificate issued and verify it shows a subject matching the subject created when the certificate was generated in the Workspace ONE UEM console.

   If there is no certificate, then there is an issue with the certificate authority, client access server (e.g., ADCS), or the Workspace ONE UEM connection to client access server.
3. Ensure the permissions of the client access server (e.g., ADCS) Admin Account is applied correctly to the certificate authority and the certificate template.
4. Ensure the account information is entered correctly in the Workspace ONE UEMconfiguration.

If the certificate is being issued, ensure that it is in the profile and on the device:

1. Navigate to **Devices > Profiles > List View**.
2. Click to the right of the applicable Exchange ActiveSync profile to launch the Actions menu and select **View XML**.



3. On the device, access the list of installed profiles.
4. View details for the applicable profile and ensure the certificate is present.
5. Confirm that the certificate contains the **Subject Alternative Name** (or SAN) section and within that section there is an **Email** and **Principal** name with the appropriate data. If this section is not in the certificate, then either the template is incorrect or the certificate authority has not been configured to accept SAN. Refer to the section on configuring the certificate authority.
6. Confirm the certificate contains the **Client Authentication** in the **Enhanced Key Usage** section. If not present, then the template is not configured correctly.

If the certificate is on the device and contains the correct information, then the problem is most likely with the security settings on the Exchange ActiveSync server. Confirm the address of the Exchange ActiveSync server is entered correctly in the Workspace ONE UEMprofile and that all security settings have been adjusted to allow certificate authentication on the Exchange ActiveSync server.

A reliable test is to manually configure a single device to connect to the Exchange ActiveSync server using certificate authentication. This should work outside of Workspace ONE UEM and until this works properly, Workspace ONE UEM will not be able to configure a device to connect to Exchange ActiveSync with a certificate.