

Exchange ActiveSync Certificate Authorities

Integrating Certificate Authorities for EAS Email Servers
VMware Workspace ONE UEM 1903



vmware®

You can find the most up-to-date technical documentation on the VMware website at:

<https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Copyright © 2019 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

- 1 Exchange ActiveSync Certificate Authorities 4**
- 2 Workspace ONE UEM Certificate Authentication for EAS with NDES-MSCEP 5**
 - Prerequisites for EAS with NDES-MSCEP 5
 - Install, Set Up, Configure Certificate 5
 - Testing and Troubleshooting, EAS with NDES-MSCEP 12
- 3 Workspace ONE UEM Certificate Authentication for EAS with ADCS 15**
 - System Requirements, EAS with ADCS 15
 - High Level Design, EAS with ADCS 16
 - Implementation Approach, EAS with ADCS 16
 - Install, Set Up, Configure Certificate 17
 - Testing and Troubleshooting, EAS with ADCS 25
- 4 Workspace ONE UEM Certificate Authorities for EAS with SEG 27**
 - Prerequisites, EAS with SEG 27
 - Communications Flow, EAS with SEG 28
 - Implementation Methodology, EAS with SEG 29
 - Install, Set Up, Configure Certificate 30
 - Troubleshooting, EAS with SEG 41
 - Additional SETSPN Commands, EAS with SEG 44
 - Install a Role in IIS 45
 - Install the Role in IIS, EAS with SEG on Windows Server 2012 45
- 5 Exchange ActiveSync with Secure Email Gateway and Threat Management Gateway 46**
 - System Requirements for EAS with SEG and TMG 47
 - High Level Design for EAS with SEG and TMG 48
 - Implementation Approach for EAS with SEG and TMG 49
 - Install, Set Up, Configure Certificate 53
 - Troubleshooting for EAS with SEG and TMG 71

Exchange ActiveSync Certificate Authorities

1

Set up certificate authentication for your Exchange ActiveSync (EAS) email server within your deployment of Workspace ONE UEM.

The implementation of certificate distribution through Workspace ONE UEM allows for the authentication of devices through client authorities certificates. Utilizing certificate authorities eliminates the need for the device user to supply user credentials to authenticate for email access.

For deployments 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.

Workspace ONE UEM is set up to integrate with four ActiveSync configurations.

- [Chapter 5 Exchange ActiveSync with Secure Email Gateway and Threat Management Gateway](#)
- [Chapter 3 Workspace ONE UEM Certificate Authentication for EAS with ADCS](#)
- [Chapter 4 Workspace ONE UEM Certificate Authorities for EAS with SEG](#)
- [Chapter 2 Workspace ONE UEM Certificate Authentication for EAS with NDES-MSCEP](#)

Documentation for other supported Certificate Authorities protocols for Workspace ONE UEM is available at docs.vmware.com.

Workspace ONE UEM Certificate Authentication for EAS with NDES-MSCEP

2

This documentation explains the configurations required for the Microsoft Exchange Client Access Server (CAS) and Workspace ONE UEM to allow a device to connect to Microsoft Exchange ActiveSync (EAS) using a certificate for authentication.

This chapter includes the following topics:

- [Prerequisites for EAS with NDES-MSCEP](#)
- [Install, Set Up, Configure Certificate](#)
- [Testing and Troubleshooting, EAS with NDES-MSCEP](#)

Prerequisites for EAS with NDES-MSCEP

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

- A certificate authority server must be set up and configured as described in [Setting up a Microsoft CA for NDES/SCEP/MSCEP](#). The CA must be an Enterprise CA as opposed to a Stand Alone CA (Stand Alone does not allow for the configuration and customization of templates).
 - A Network Device Enrollment Service, also referred to as MSCEP server setup. NDES is only available in the Enterprise version of Microsoft Server 2008 and 2008 R2.
- Microsoft Exchange with ActiveSync enabled.
- Internet Information Services (IIS) on the EAS server must have the option “Client Certificate Mapping Authentication” installed.

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.

Step 1: Set Up a Trust between Active Directory and the Certificate Authority, EAS with NDES-MSCEP

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**.

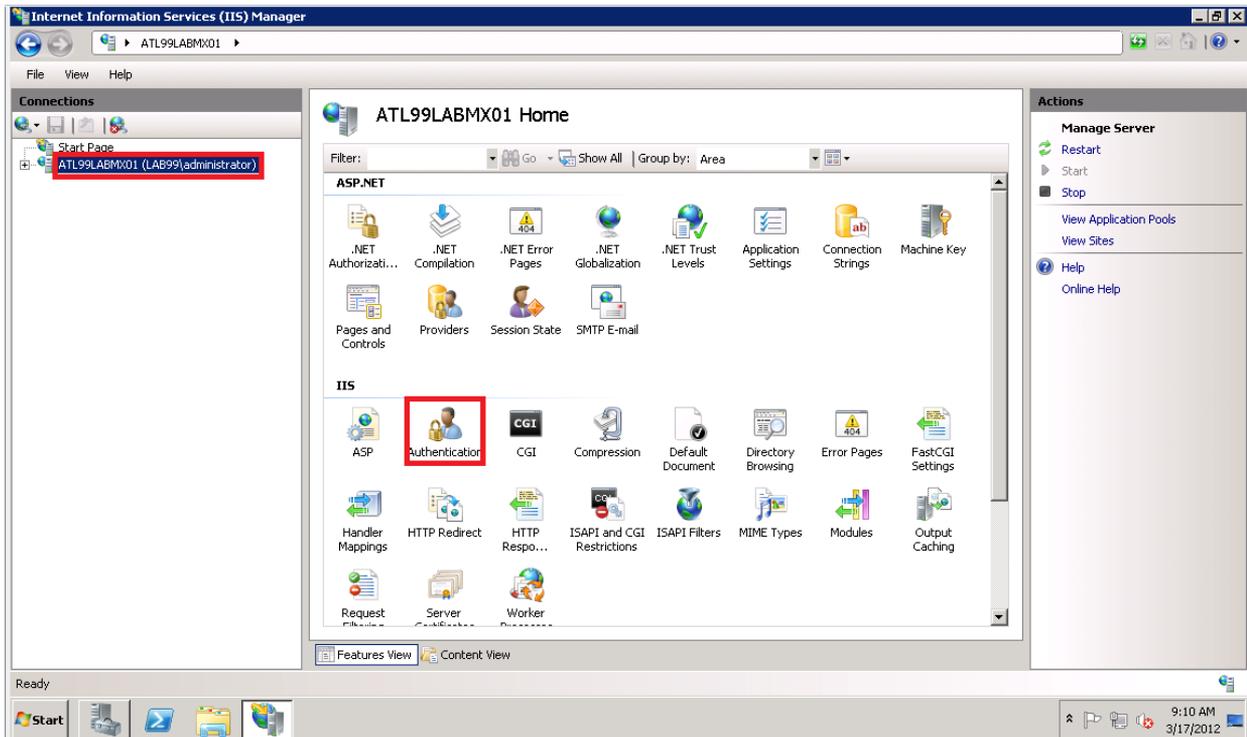
Step 2: Set Permissions on Exchange Server

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 run **Internet Information Services (IIS)**.
- 3 Select the server in the **Connections** pane.

- 4 Under IIS, double-click the **Authentication** icon.



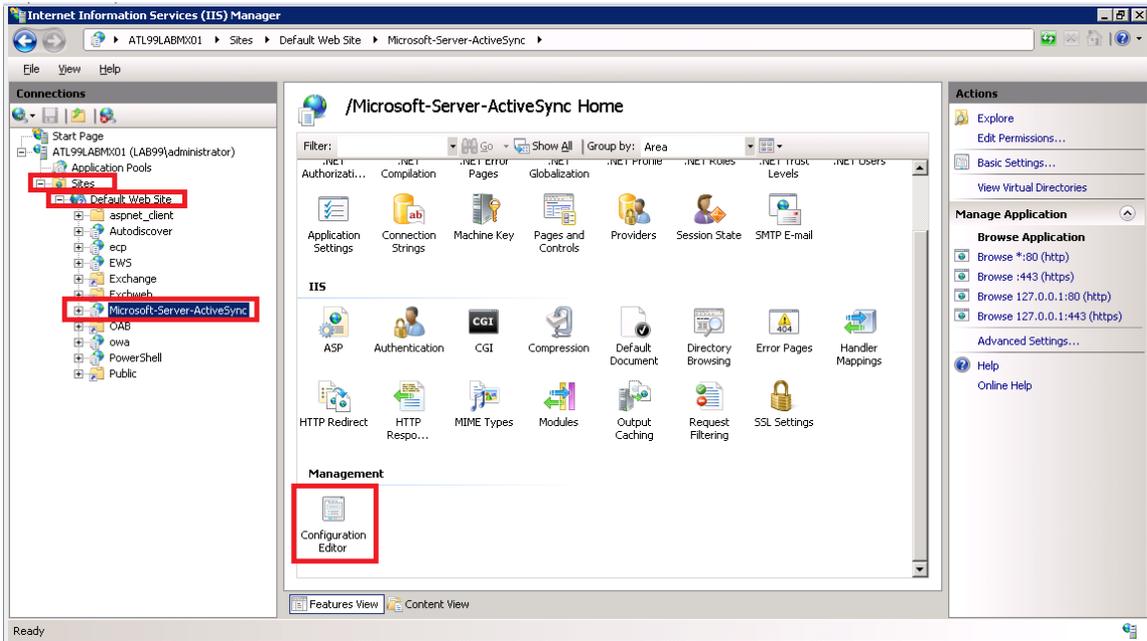
- 5 Select **Active Directory Client Certificate Authentication** and then select **Enable**.

Configuration Editor

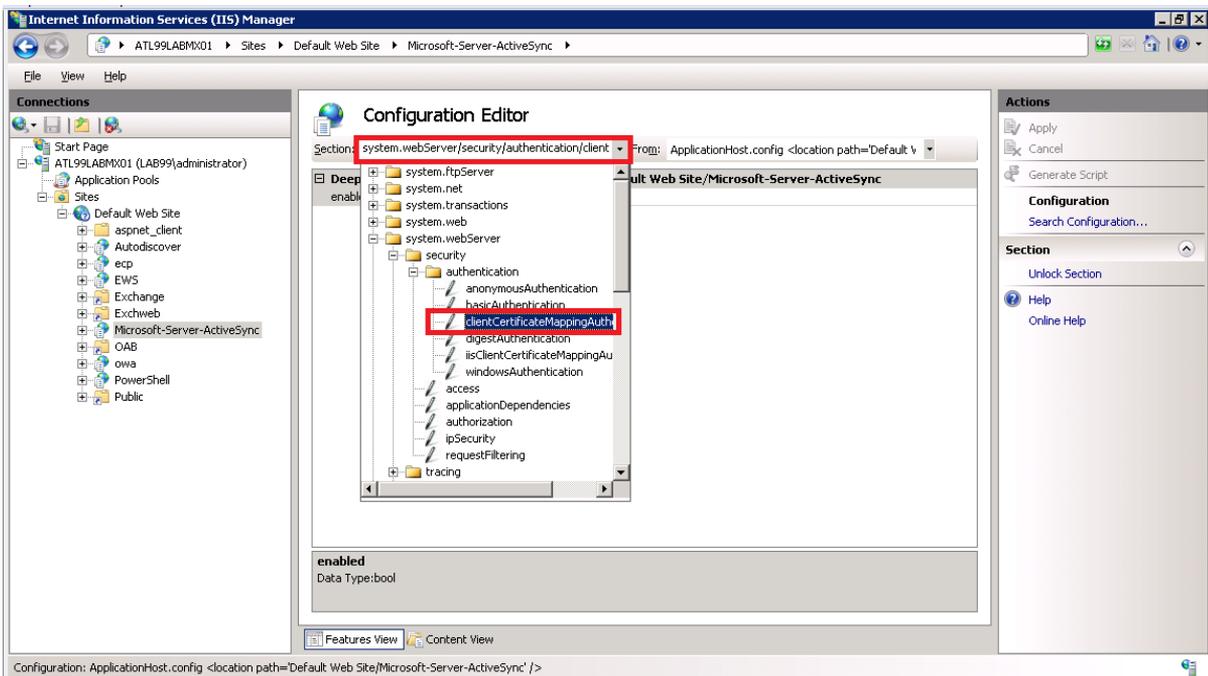
- 1 Select + to expand **Site** and then **Default website** to display all available configuration editors.
 - a If you are using MS Server 2008 R2 or later, the **Configuration Editor** icon appears; Select **Microsoft-Server-ActiveSync** and double-click on the **Configuration Editor** icon. Skip 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/clientCertificateMappingAuth  
entication /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**.

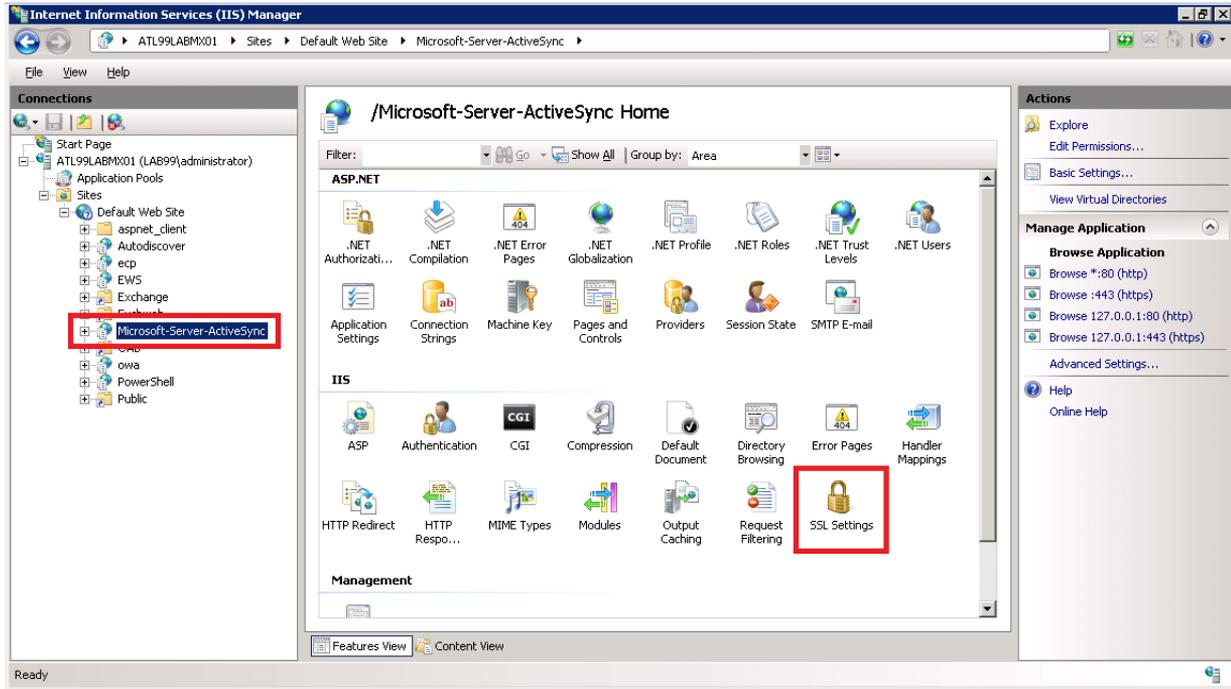


- 4 Select **True** from the drop-down menu on the Enabled option.

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: Configuring Certificate Authority And Certificate Template In Workspace ONE UEM, EAS with NDES-MSCEP

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. There are two steps to this process.

- Configure the certificate authority.
 - Configure the certificate template.
- 1 Open the Workspace ONE UEM console.
 - 2 Login as a user with Workspace ONE UEM Administrator privileges or higher.
 - 3 Navigate to **Devices > Certificates > Certificate Authorities**.
 - 4 Click **Add**.
 - 5 Select from the **Generic SCEP** from the Authority Type drop-down menu prior to completing any other configuration settings for the certificate authority.
 - 6 Enter the following details about the CA in the remaining fields:
 - Enter the actual certificate authority Name in the **Certificate Authority** field. This is the name of the CA to which the NDES/SCEP/MSCEP endpoint is connected. This can be found by launching the **Certification Authority** application on the CA server.
 - Enter a brief **Description** for the new CA.
 - Enter the URL of the CA server in the **SCEP URL** field.
 - Select the **Challenge Type** radio button that reflects whether or not a challenge phrase is required for authentication. For additional authentication, choose **Static** or **No Challenge**.
 - If you select **Static**, enter an authentication phrase consisting of a key or password used to authenticate the device with the certificate enrollment URL.
 - 7 Click **Test Connection**. If you select Save prior to **Test Connection**, a “Test is unsuccessful” error displays.
 - 8 Click **Save**.
 - 9 Select the **Request Templates** tab
 - 10 Click **Add** to add a new certificate template.
 - 11 Complete the certificate template information:
 - Enter a 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 box.:
This is typically 2048 and should match the setting on the certificate template that is being used by NDES/SCEP/MSCEP.
- Select the **Private Key Type** using the applicable checkbox.
This should match the setting on the certificate template that is being used by NDES/SCEP/MSCEP.
- 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.
- Select the **Publish Private Key** checkbox to publish the private key to the specified web service endpoint (Directory Services or custom web service)

12 Click **Save**.

Step 4: Create Profile for Exchange ActiveSync, EAS with NDES-MSCEP

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.

Testing and Troubleshooting, EAS with NDES-MSCEP

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 UEM configuration.

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.

Active	Profile Name	Type	Platform / OS / Model	Ownership	Managed By	Installed/Assigned
<input checked="" type="checkbox"/>	A SE Demo Profile	Optional	Apple iOS / Any / Any	C	World-Wide Enterprises	0 / 4
<input checked="" type="checkbox"/>	_OS X Sample Profile	Optional	Apple Mac OS X / Any ...	C	World-Wide Enterprises	0 / 0
<input checked="" type="checkbox"/>	ActiveSync_Test	Auto	Windows PC / Any / Any	Any	Enterprise Sales	3 / 4
<input checked="" type="checkbox"/>	AirWatch Demos_1326	Auto	Windows Phone / Any ...	Any	AirWatch Demos	0 / 2
<input checked="" type="checkbox"/>	AirWatch Email Conta...	Auto	Android / Any / Any	Any	AirWatch Demos	3 / 70

- 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 UEM profile 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.

Workspace ONE UEM Certificate Authentication for EAS with ADCS

3

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

This chapter includes the following topics:

- [System Requirements, EAS with ADCS](#)
- [High Level Design, EAS with ADCS](#)
- [Implementation Approach, EAS with ADCS](#)
- [Install, Set Up, Configure Certificate](#)
- [Testing and Troubleshooting, EAS with ADCS](#)

System Requirements, EAS with ADCS

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

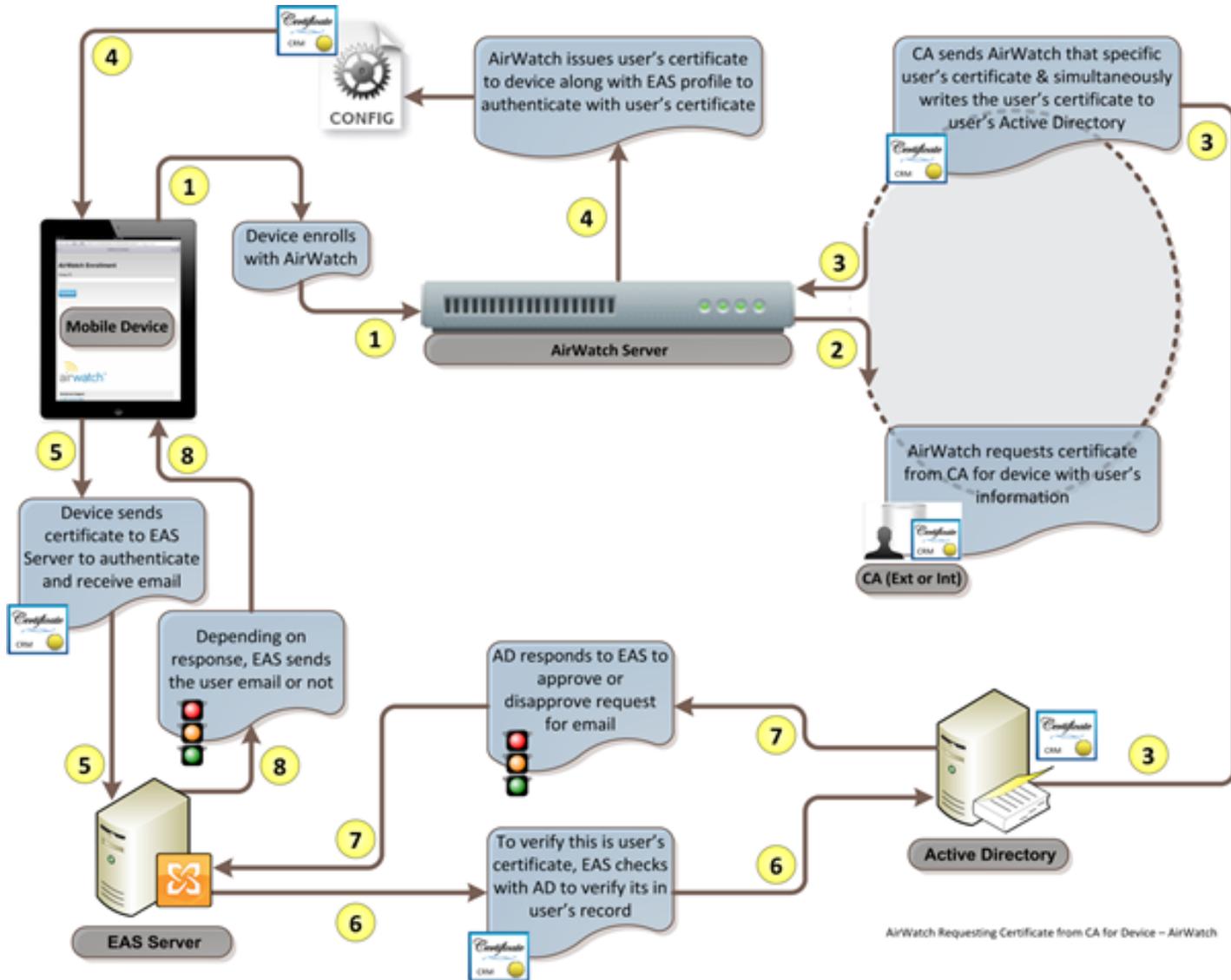
- A certificate authority server must be set up and configured. If you want guidance as to the methodology of setting up a certificate authority, refer to [Setting Up a Microsoft Certificate Authority for Use with Workspace ONE UEM](#). The certificate authority must be an enterprise certificate authority 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.

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, EAS with ADCS](#).

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 Profile for Exchange ActiveSync, EAS with ADCS](#).

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.

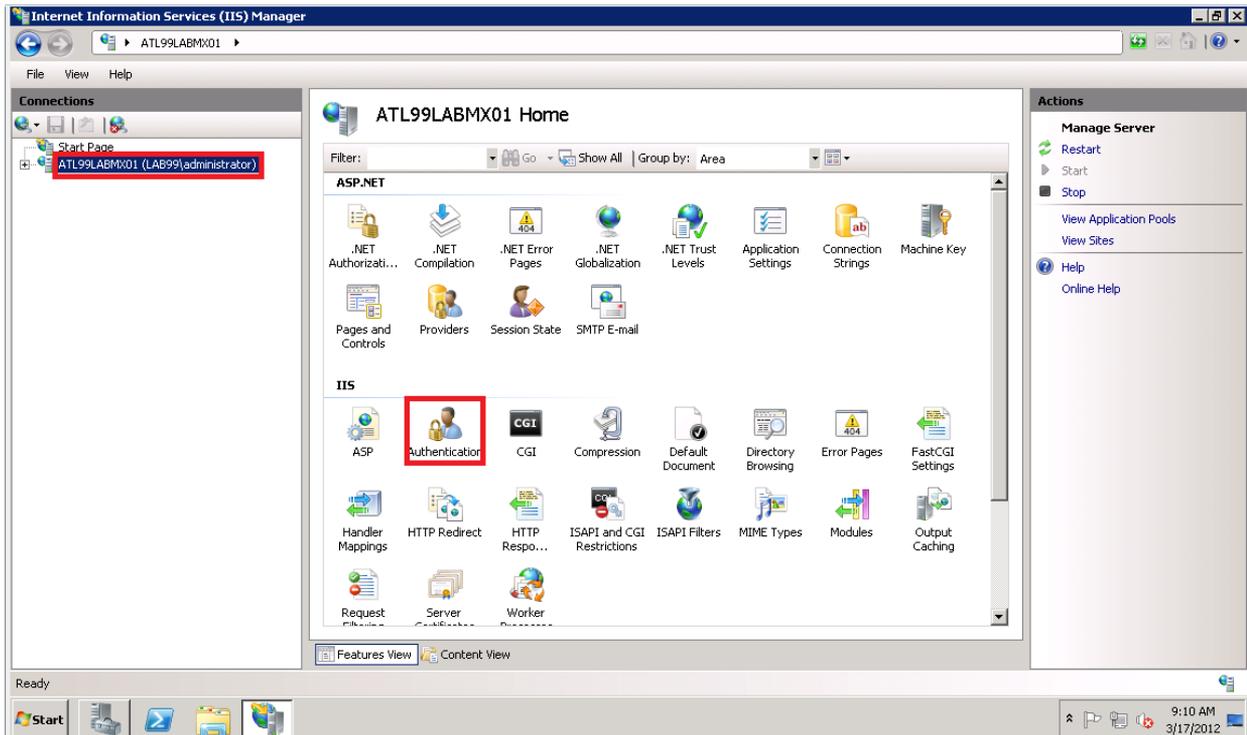
- 4 Select **Enterprise PKI** from the list of Available snap-ins and then select **Add**.
- 5 Click **OK**.
- 6 Right-click **Enterprise PKI** and select **Manage AD Containers**.
- 7 Select the **NT AuthCertificates** tab and verify the Certificate Authority is listed. If not, select **Add** to add 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 run **Internet Information Services (IIS)**.
- 3 Select the server in the **Connections** pane.
- 4 Under IIS, double-click the **Authentication** icon.



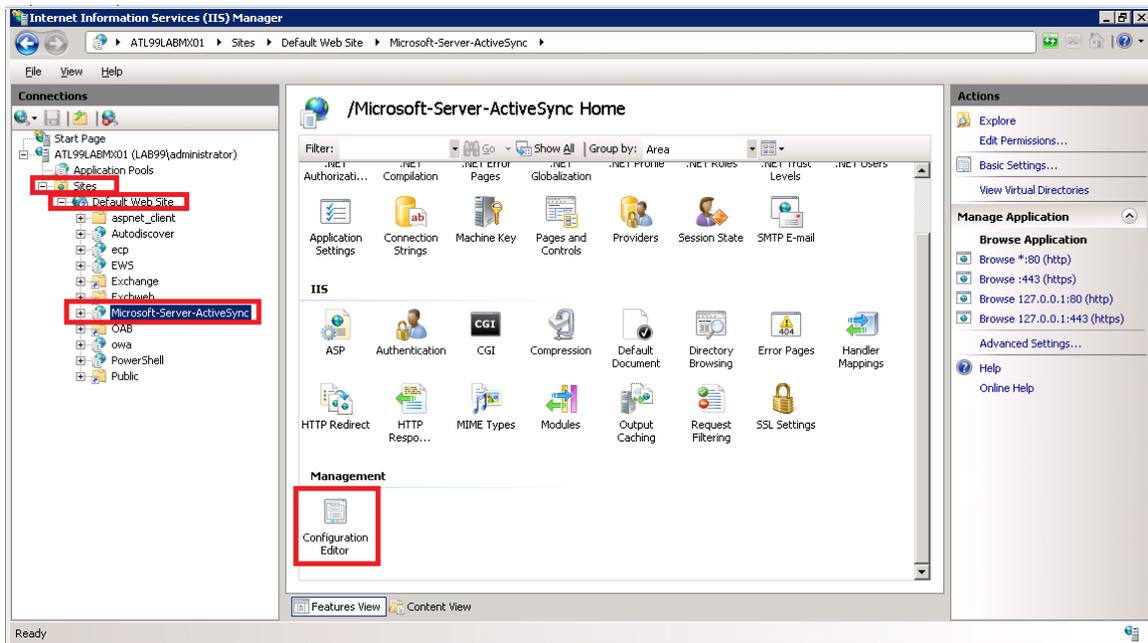
- 5 Select **Active Directory Client Certificate Authentication** and then select **Enable**.

Configuration Editor

- 1 Select **+** 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:

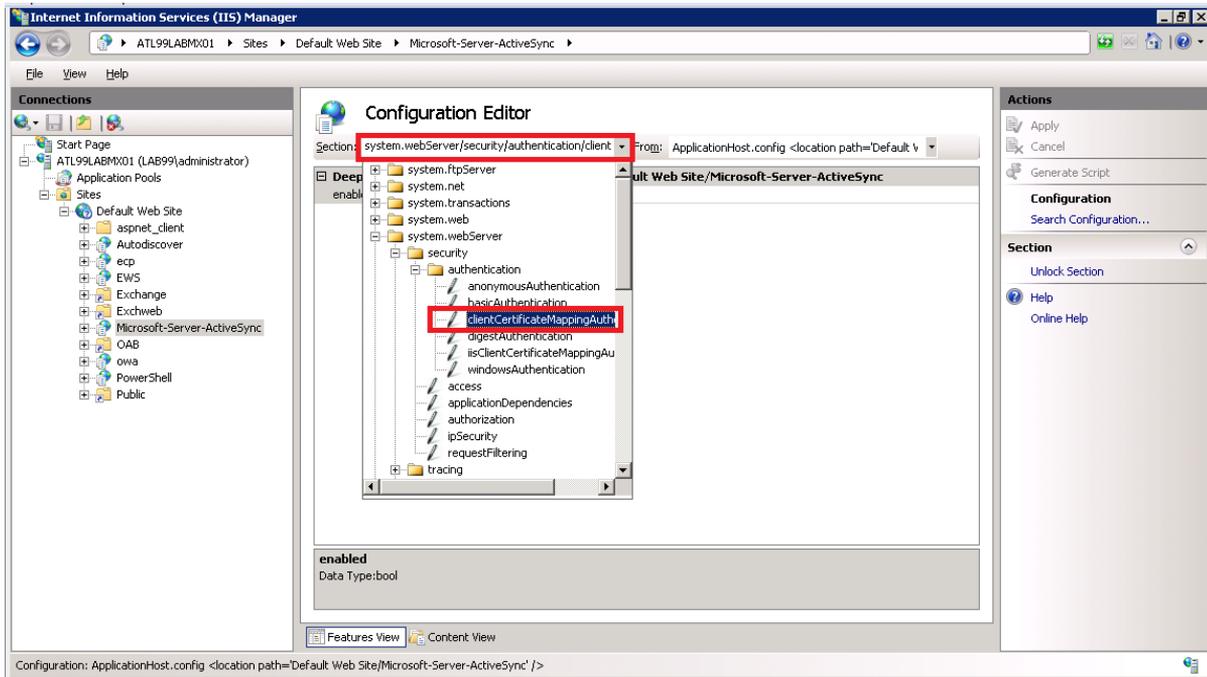
```
appcmd.exe set config "Microsoft-Server-ActiveSync" -
section:system.webServer/security/authentication/clientCertificateMappingAuth
entication /enabled:"True" /commit:apphost
```

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**.

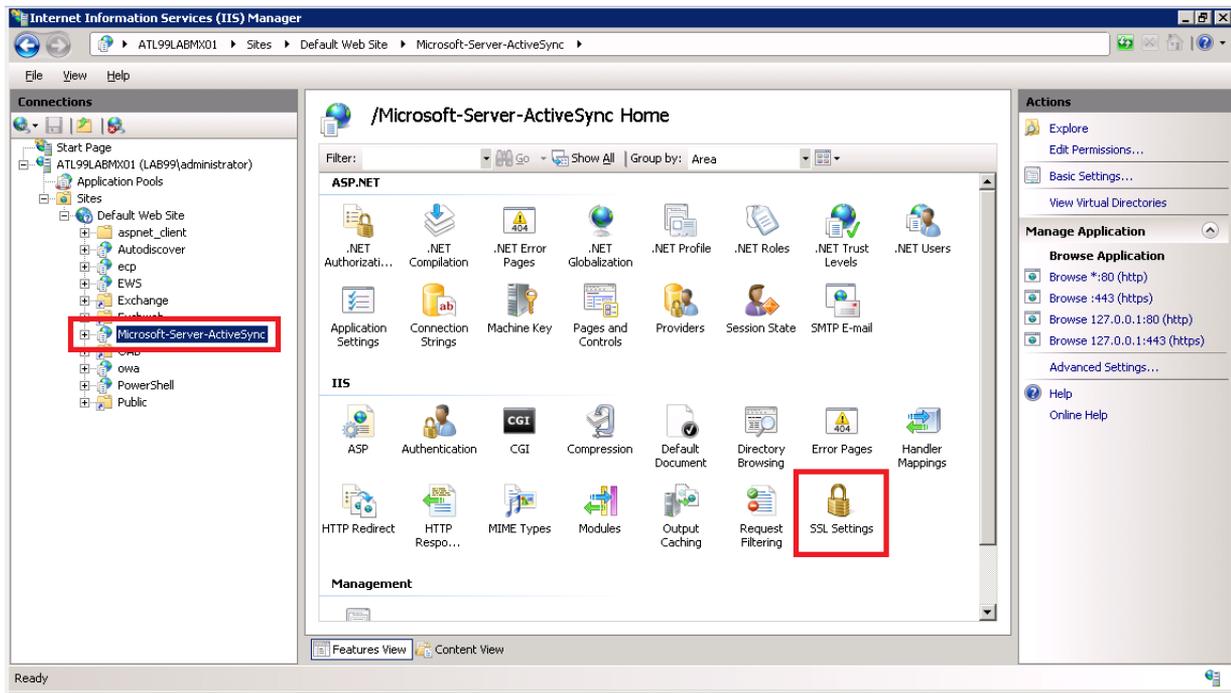


4 Select **True** from the drop-down menu on the Enabled option.

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://` or `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.

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.

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.

- 2 Ensure the permissions of the client access server (e.g., ADCS) Admin Account is applied correctly to the certificate authority and the certificate template.
- 3 Ensure the account information is entered correctly in the Workspace ONE UEM configuration.

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

List View

+ Add + Bulk Import Filter Grid

Status: Active Publish: All Platform: Any Setting Group: All

Group: World-Wide Enterprises Status: Active Publish: All Platform: Any Setting Group: All

Active	Profile Name	Type	Platform / OS / Model	Ownership	Managed By	Installed/Assigned
<input checked="" type="checkbox"/>	A SE Demo Profile	Optional	Apple iOS / Any / Any	C	World-Wide Enterprises	0 / 4
<input checked="" type="checkbox"/>	_OS X Sample Profile	Optional	Apple Mac OS X / Any ...	C	World-Wide Enterprises	0 / 0
<input checked="" type="checkbox"/>	ActiveSync_Test	Auto	Windows PC / Any / Any	Any	Enterprise Sales	3 / 4
<input checked="" type="checkbox"/>	AirWatch Demos_1326	Auto	Windows Phone / Any ...	Any	AirWatch Demos	0 / 2
<input checked="" type="checkbox"/>	AirWatch Email Conta...	Auto	Android / Any / Any	Any	AirWatch Demos	3 / 70

- 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 UEM profile 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.

Workspace ONE UEM Certificate Authorities for EAS with SEG

4

The Secure Email Gateway by Workspace ONE UEM provides an added layer of management visibility to mobile email and provides enforceable access-control based on security policies for corporations that are serious about mobile email management and security.

However, for maximum security and control, corporations may couple the Secure Email Gateway with certificate-based authentication to their email infrastructure. In order to accommodate the addition of certificate-based authentication, Kerberos Delegation must be utilized.

This documentation discusses how to configure your infrastructure for Kerberos Delegation to enable EAS certificate authentication with the SEG.

This chapter includes the following topics:

- [Prerequisites, EAS with SEG](#)
- [Communications Flow, EAS with SEG](#)
- [Implementation Methodology, EAS with SEG](#)
- [Install, Set Up, Configure Certificate](#)
- [Troubleshooting, EAS with SEG](#)
- [Additional SETSPN Commands, EAS with SEG](#)
- [Install a Role in IIS](#)
- [Install the Role in IIS, EAS with SEG on Windows Server 2012](#)

Prerequisites, EAS with SEG

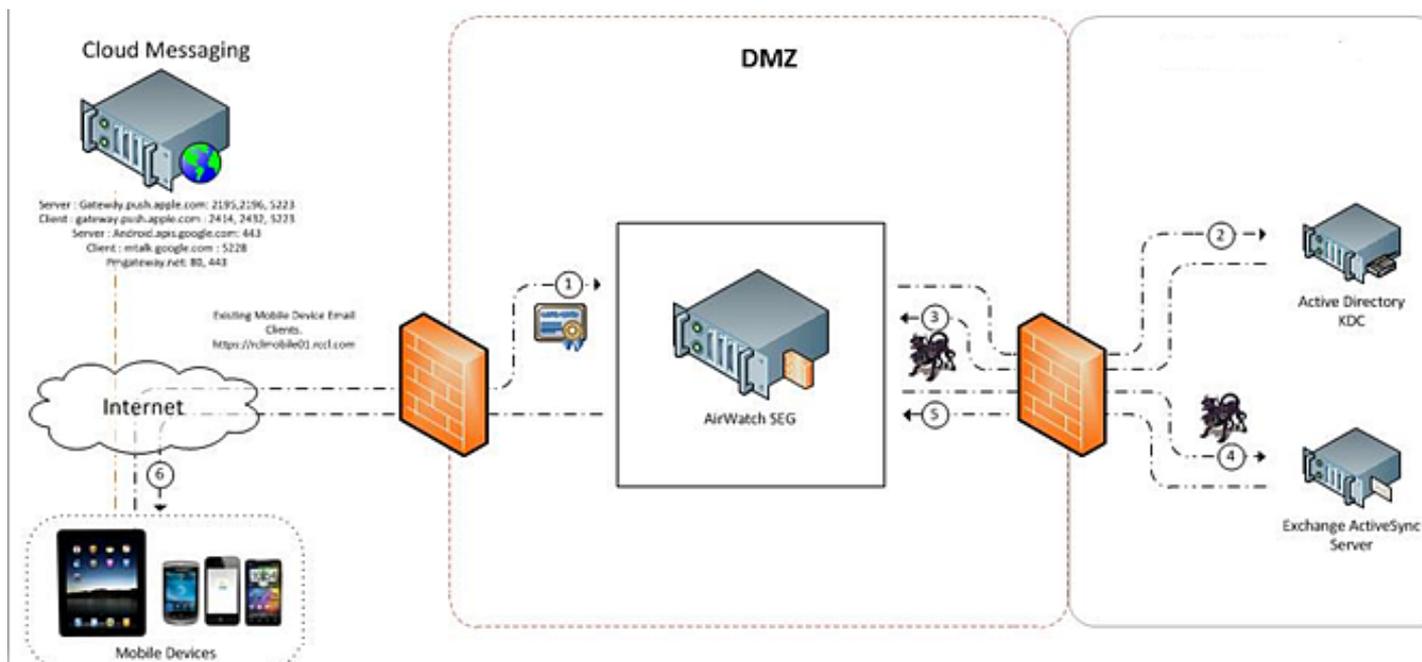
Before configuring the Secure Email Gateway (SEG) to use certificate authentication, you must have the following.

- An internal certificate authority (CA) server must be used to create user's certificates. An external CA cannot be used (e.g., VeriSign, etc.) to create user's certificates.
- Installed and operational Secure Email Gateway (SEG). For more information, see the **Workspace ONE UEM Secure Email Gateway Guide**.
- Windows Server 2003 or 2008 Standard with latest service packs and recommended updates from Microsoft (<http://www.update.microsoft.com/>).

- A device with an Exchange ActiveSync (EAS) profile and certificate from a domain enterprise certificate authority.
- A SEG that is configured as a member of the same domain as the enterprise certificate authority.
- Administrative permissions to be able to configure your enterprise.
 - Secure Email Gateway (SEG)
 - Active Directory (AD)
 - Exchange ActiveSync (EAS) server
- A certificate authority properly configured to issue certificates throughout Workspace ONE UEM through MSCEP/NDES or DCOM.
- A trust relationship between the certificate authority (CA) providing the certificates and the directory services server. This will entail:
 - Export the root CA certificate to a .cer file.
 - At the command prompt, type the following command and press ENTER:
`Certutil -dspublish -f <filename> NTAAuthCA`
`certutil -enterprise -addstore NTAAuth CA_CertFilename.cer`

Communications Flow, EAS with SEG

This diagram highlights the communications flow for a device attempting to connect to the Exchange ActiveSync (EAS) server through the Workspace ONE UEM Secure Email Gateway (SEG) using a certificate for authentication. A detailed account of this interaction is shown below in the legend.



Legend

1. The device contacts the SEG with a certificate that contains UPN and email in the Subject Alternative Name section of the cert.
2. The SEG authenticates the user with Active Directory from the information in the cert.
3. The Active Directory server (KDC) issues a ticket to the SEG with the user's credentials.
4. The SEG sends the user's credentials to Exchange ActiveSync (EAS) with the mail request.
5. The EAS responds to the SEG with the mail information.
6. The SEG responds to the device with the mail information.

Implementation Methodology, EAS with SEG

Regardless of the enterprise infrastructure being used, the implementation 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 the user has a seamless experience receiving their email.

Registering Target Service

Initially, you need to identify the service for which SEG will delegate the traffic to EAS server. This can be accomplished by creating the SPN (Service Principal Name).

Permitting the SEG Server for Kerberos Delegation to the EAS Server

By default, no infrastructure is permitted to grant access to other servers using Kerberos delegation. Therefore, administrators must first configure security settings on the directory server so that the SEG server can delegate access to the EAS server using HTTP (for EAS traffic). Specifically for Microsoft Active Directory infrastructure, this entails:

- Configuring AD to give permissions to SEG to impersonate a user.
- Enabling SEG to delegate HTTP EAS traffic to the EAS server.

Enabling EAS Server to Accept Kerberos Tickets

The EAS server requires “Windows Authentication” enabled in order to analyze the Kerberos ticket received from the SEG server.

Configuring the SEG Server for Certificate Authentication

Once the domain security settings have been adjusted, the SEG server must be configured for certificate authentication. In order for the SEG to authenticate the user's device that is assigned to a particular certificate, Internet Information Services (IIS) on the SEG server must be configured to accept that certificate. Specifically this can be accomplished by:

- Setting up Active Directory to Authenticate

- Using the Configuration Editor to Set Up Email Authentication
- Setting Up Secure Socket Layer (SSL)
- Adjusting uploadReadAheadSize Memory Size

Enabling the SEG EAS Service Account to Begin Kerberos Delegation

Lastly, administrators must enable the SEG EAS Service account to start granting access to the EAS server through user impersonation. This effectively completes the setup and users may begin authenticating with certificates to receive their corporate mail. Administrators can complete this by:

- Verifying the identity of the SEG
- Configuring local security policy for SEG to act as part of the operating system
- Configuring local security policy for SEG to impersonate a client after authentication

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.

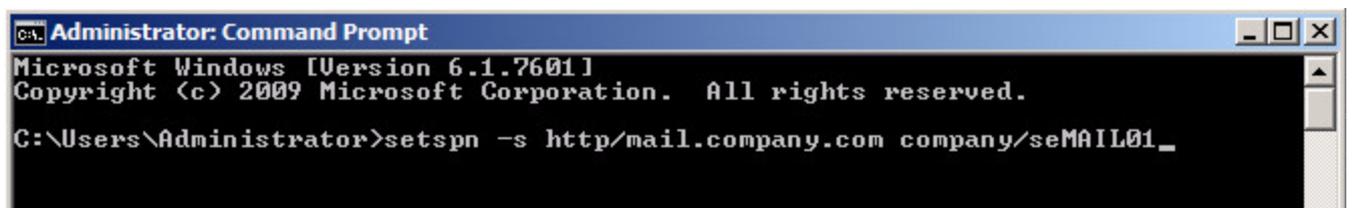
Take the following steps and procedures to integrate the certificate.

Step 1: Register Target Service, EAS with SEG

In order for the SEG server to be able to delegate traffic to a specific service, you need to identify and register the service. The target service must match the Exchange server Hostname on the “web.config” file of the “Web Listener” folder on SEG.

The “SETSPN” command is used to register the service and this can be executed on AD server or EAS server.

```
SETSPN -s HTTP/<target service name> <target computer name>
```



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -s http/mail.company.com company/seMAIL01_
```

If your environment has multiple Client Access Servers (CAS) or multiple Exchange ActiveSync (EAS) servers, then you must specify the domain name with the target computer name. For example, {domain}/{asa_account} or {domain}/{exchangebox}. An alternate service account needs to be created to represent the Client Access Services.

Create an ASA Credential Type

You can create a computer account or a user account for the alternate service account. Because a computer account does not allow interactive logon, it may have simpler security policies than a user account and therefore is the preferred solution for the ASA credential.

If you create a computer account, the password doesn't actually expire however Workspace ONE UEM still recommends updating the password periodically. Local group policy can specify a maximum account age for computer accounts and there might be scripts scheduled to periodically delete computer accounts that do not meet current policies.

Periodically updating the password for computer accounts ensures that your computer accounts are not deleted for not meeting local policy. Your local security policy determines when the password needs to be changed.

There are no particular requirements for the name of the ASA credential. You can use any name that conforms to your naming scheme.

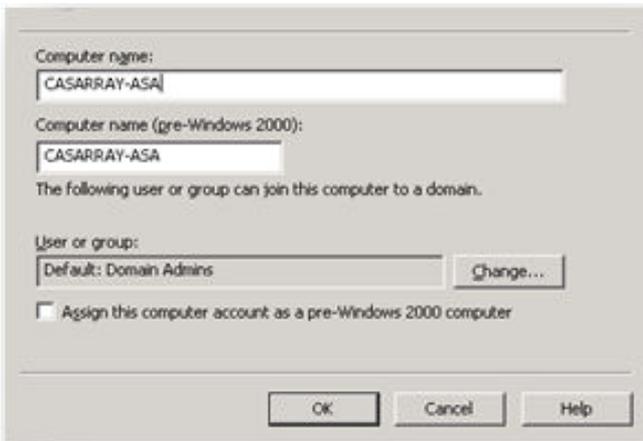
The ASA credential does not need special security privileges. If you are deploying a computer account for the ASA credential, this means that the account only needs to be a member of the Domain Computers security group.

If you are deploying a user account for the ASA credential, this means that the account only needs to be a member of the Domain Users security group.

The password you provide when you create the account is actually never used. Instead, the script resets the password. So when you create the account, you can use any password that conforms to your organization's password requirements.

All computers within the Client Access Services must share the same service account. In addition, any Client Access servers that may be called on in a datacenter activation scenario must also share the same service account.

- 1 Create the alternate service account (ASA) for the CAS in the domain by opening the Active Directory User and Computers and creating new computer account. Type a name for the ASA, using CASARRAY- ASA as example. Verify that the account has replicated to all Domain Controllers before proceeding.



- 2 Verify the CAS's FQDN, since this name is used for the SPN that is attached to the ASA. In order to check the CAS's FQDN, run the next command in PowerShell.

```
Get-ClientAccessArray
```

- 3 Create the SPN using the setspn command.

```
setspn -s http/<target service name> {ASA_ACCOUNT}$
```

- 4 Verify that all relevant SPNs have been assigned by running the following command from PowerShell.

```
setspn -L {ASA_ACCOUNT}
```

- 5 To set ASA to the CAS servers, run the Alternate Service Account credential script in the Exchange Management Shell **RollAlternateServiceAccountPassword.ps1**

```
.\RollAlternateServiceAccountPassword.ps1 -ToArrayMembers {CAS-FQDN} -  
GenerateNewPasswordFor "{DOMAIN}\{ASA_ACCOUNT}$" -Verbose
```

- 6 You can see a 'Success' message when the script has completed running. To verify that the ASA credentials have been deployed properly, use the following command.

```
Get-ClientAccessServer -IncludeAlternateServiceAccountCredentialStatus | fl name,*alter*
```

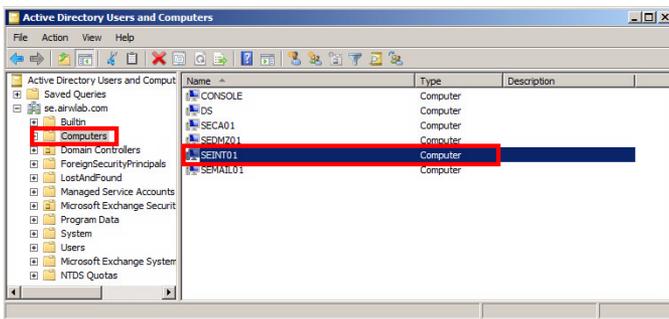
Next, you must [Step 2: Configure Delegation Settings on the SEG Server, EAS with SEG](#).

Step 2: Configure Delegation Settings on the SEG Server, EAS with SEG

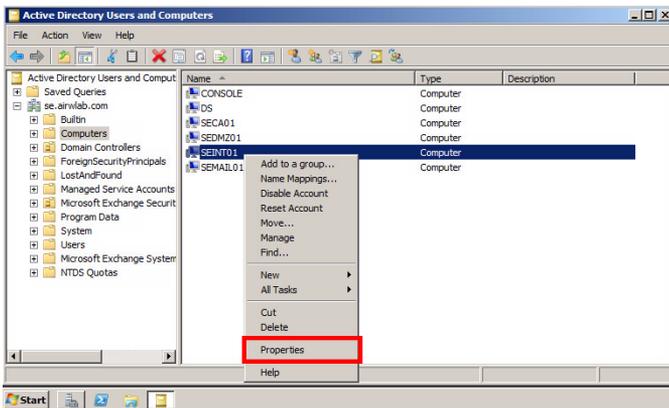
In order for the Secure Email Gateway (SEG) to impersonate a user when authenticating on an Exchange ActiveSync (EAS) server, the SEG server must be given the appropriate permissions in the Active Directory (AD) server. You must also enable SEG to delegate HTTP EAS traffic to the EAS server.

Configure AD to Give Permissions to SEG to Impersonate a User

- 1 Select **Active Directory Users and Computers** and **Computers** on the AD server.
- 2 In the left-hand pane, select the folder where the SEG server is located (e.g., **Computers**). The available SEG servers display in the right-hand pane as shown below.



- 3 Right-click on the SEG server name and then select **Properties**.



- 4 The **Properties** window for the SEG server displays. Click on the **Delegation** tab.
- 5 Select the **Trust this computer for delegation to specified services only**.
- 6 Select **Use any authentication protocol**.
- 7 Click **Add**.

Enable SEG to delegate HTTP EAS traffic to the EAS server

- 1 Click **Users or Computers** on the **Add Services** window. The **Select Users or Computers** window displays.

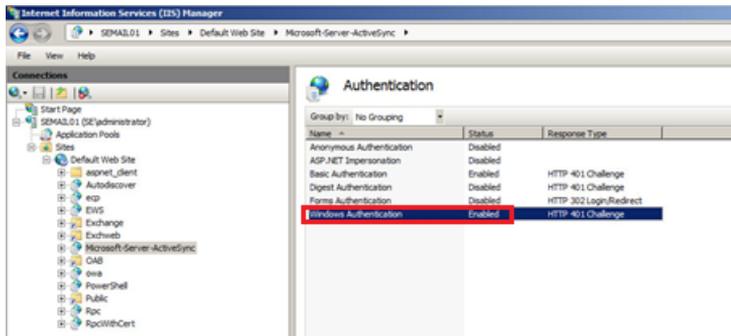
- 2 Enter the name of the Exchange ActiveSync Server or ASA account (if applicable) and select **OK**. The **Add Services** window displays.
- 3 Select the **http** service registered in step 1 under Available services and select **OK**. A list displaying http and your EAS server on the **Delegation** tab appears.
- 4 Click **OK**.

Next, you must [Step 3: Enable EAS Server to Accept Kerberos Tickets, EAS with SEG](#).

Step 3: Enable EAS Server to Accept Kerberos Tickets, EAS with SEG

Configure the EAS server to accept Kerberos tickets.

- 1 Open IIS manager on the EAS server.
- 2 On the **Connections** pane, expand **Sites** and select **Microsoft-server-activesync**.
- 3 In the main pane, under IIS, select **Authentication** and enable **Windows Authentication**.



Next, [Step 4: Configure IIS for Certificate Authentication on the SEG, EAS with SEG](#).

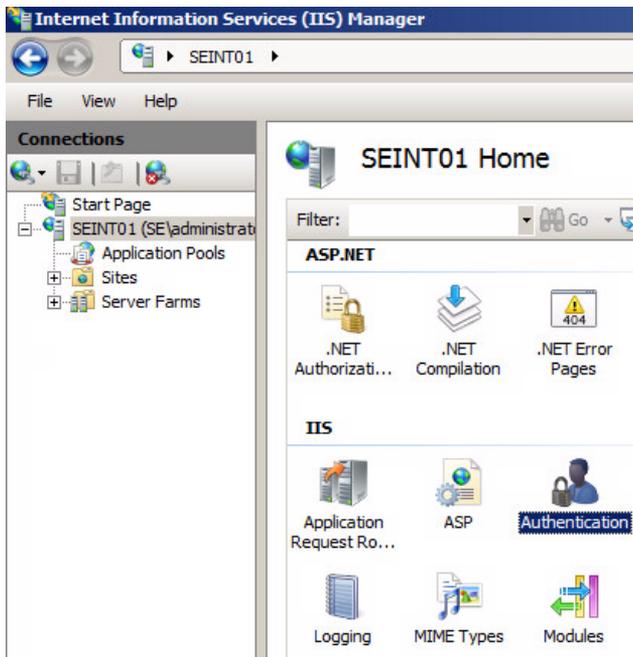
Step 4: Configure IIS for Certificate Authentication on the SEG, EAS with SEG

In order for the SEG to authenticate the user's device that is assigned to a particular certificate, **Internet Information Services (IIS)** on the SEG server must be configured to accept that certificate.

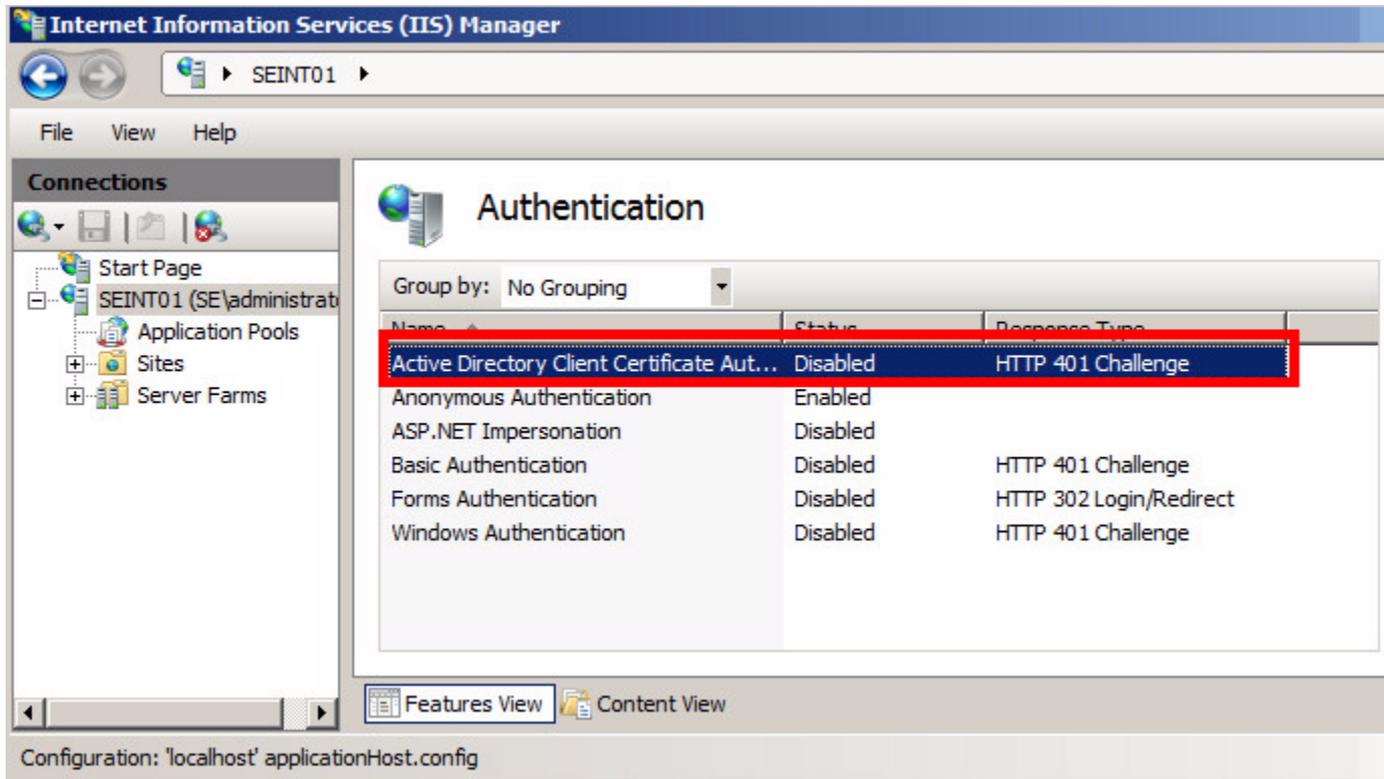
Set up Active Directory to Authenticate

- 1 On the SEG Server, launch **Internet Information Services (IIS)** by selecting **Start > Run**.
- 2 Type `inetmgr` and select **OK**. The IIS Manager window appears.
- 3 In the left-hand **Connections** pane select the SEG server

- 4 In the main pane, under the **IIS** section, double-click the **Authentication** icon.



- 5 Select **Active Directory Client Certificate Authentication**. If this option is not available, see [Install a Role in IIS](#).
- 6 In the right-hand pane, select **Enable**.

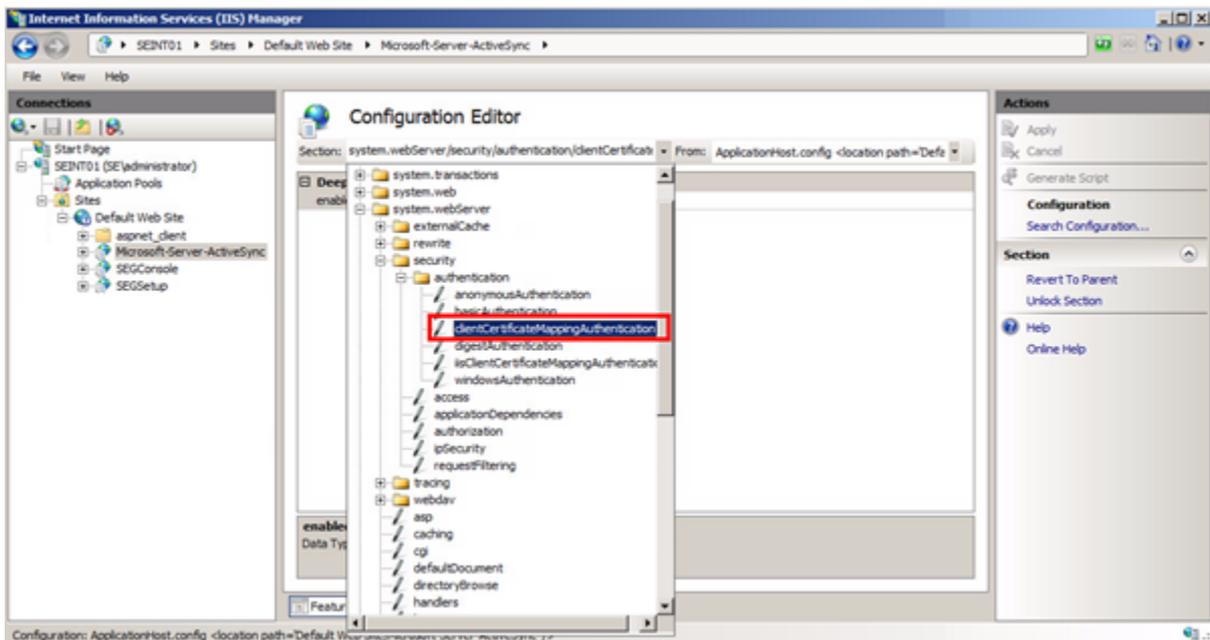


Use the Configuration Editor to Set Up Email Authentication

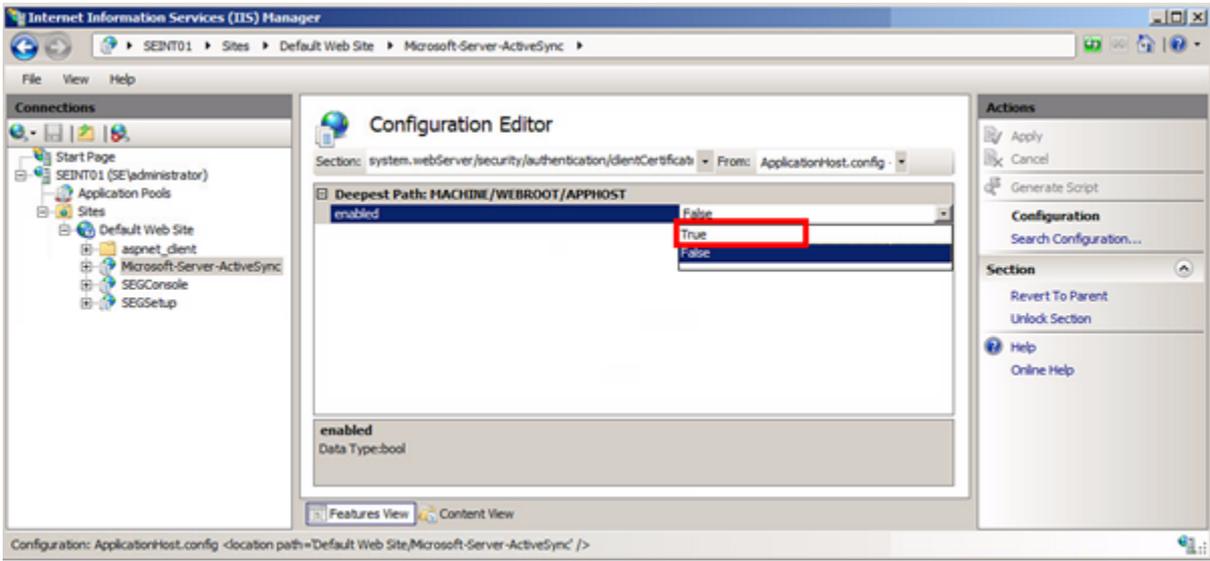
- 1 Click + to expand the **Sites** folder.
- 2 Click + to expand the **Default Web Site** and display the email sever you want to configure.
 - a If you are using MS Server 2008 R2 or later, the **Configuration Editor** icon appears as shown in the screen below. This icon does not appear in older versions of MS Server. Select **Microsoft-Server-ActiveSync** and double-click the **Configuration Editor** icon. If applicable, proceed directly to step 3.
 - b If you are using Exchange ActiveSync (EAS) servers older than 2008 R2, you will 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/clientCertificateMappingAuth
          entication /enabled:"True" /commit:apphost
```

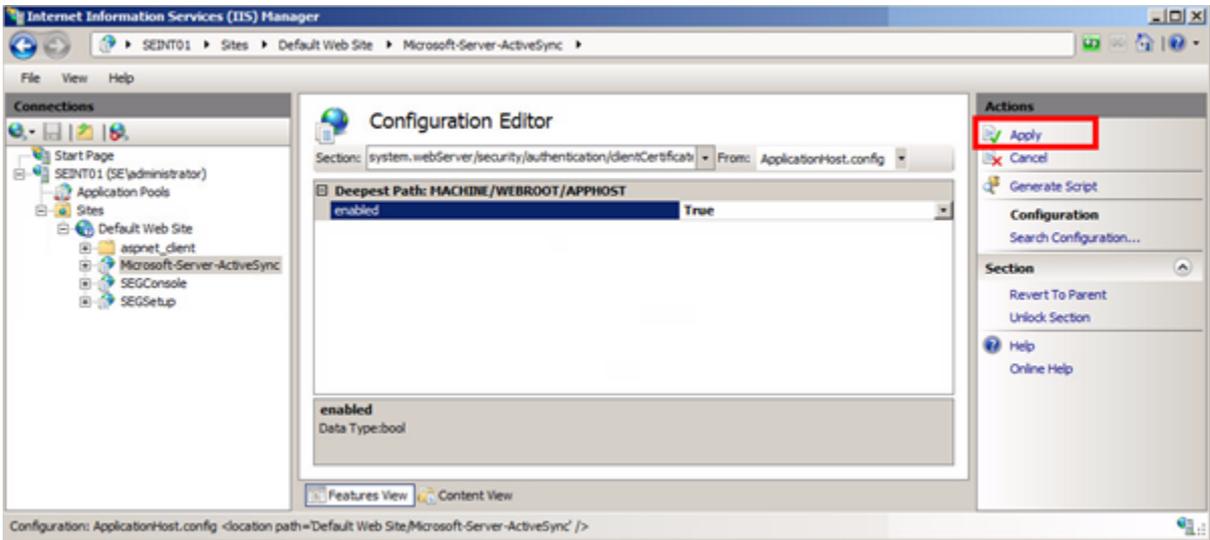
If you performed this step, then skip the remaining steps and advance to Setting up Secure Socket Layer (SSL).
- 3 Navigate to **system.webserver/security/authentication** under **Section**.
- 4 Select **clientCertificateMappingAuthentication**.



5 Select **True** from the **Enabled** drop-down menu.



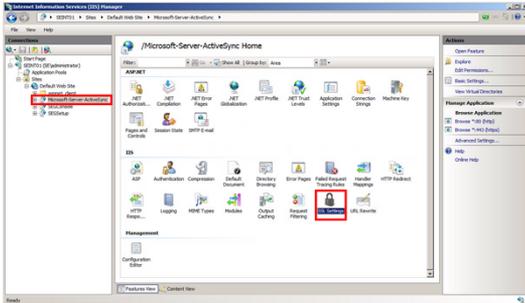
6 Click **Apply**.



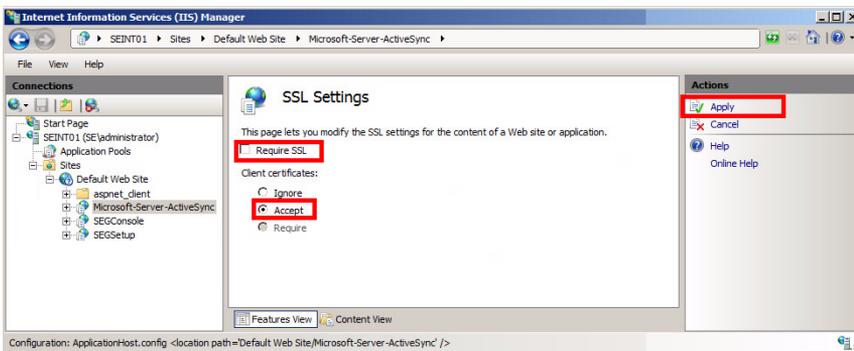
Set Up Secure Socket Layer (SSL)

If only certificate authentication is being used then you must configure Secure Socket Layer (SSL). Otherwise, if authentication other than certificates is used then you do not need to configure SSL.

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



- 2 If only certificate authentication is allowed, select **Require SSL** and then **Required**. If other types of authentication are allowed, select **Accept**.
- 3 Click **Apply**.



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 **cmd** command prompt by selecting **Start > Run**.
- 2 Type **cmd** and select **OK**. A text editor window appears.
- 3 Increase the value of the uploadReadAheadSize from the default of 48KB to 10MB by entering the following commands:

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

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

“Default Web Site” is used in the sample code above. 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 Type the following command to reset the IIS:

```
iisreset
```

Last, you must [Step 5: Configure Delegation Rights on the SEG Service Account, EAS with SEG](#).

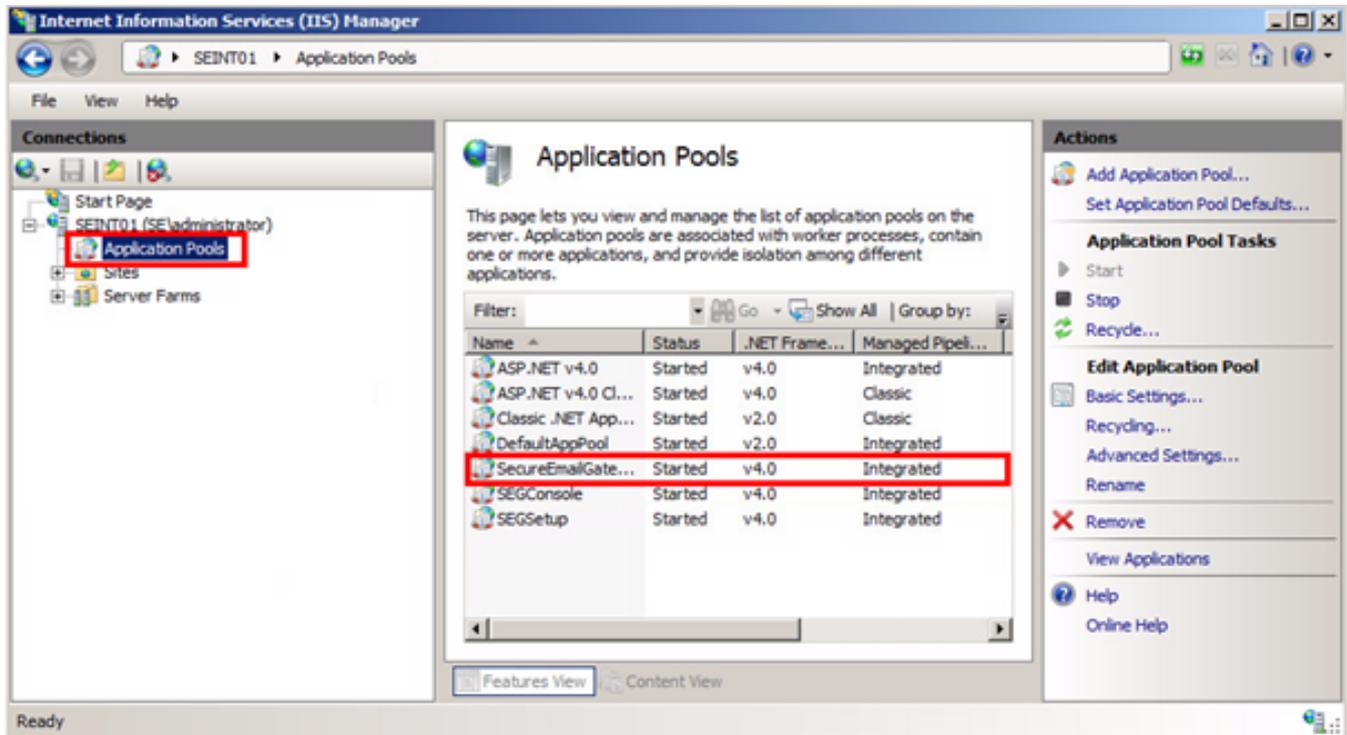
Step 5: Configure Delegation Rights on the SEG Service Account, EAS with SEG

In addition to configuring delegation rights on the SEG server, the service account attached to the SEG Application Pool must also be given delegation permissions.

Verify the Identity of the SEG

- 1 Launch **Internet Information Services (IIS) Manager** by selecting **Start > Run**. In the dialog box type “inetmgr” and select **OK**. The IIS Manager window appears.
- 2 In the left-hand **Connections** pane, select the SEG server.
- 3 Click the **Application Pools** folder.
- 4 In the right-hand **Application Pools** pane, locate the **SecureEmailGateway**.

- Under the Identity column, verify the identity of the **SecureEmailGateway** is **Network Service**.

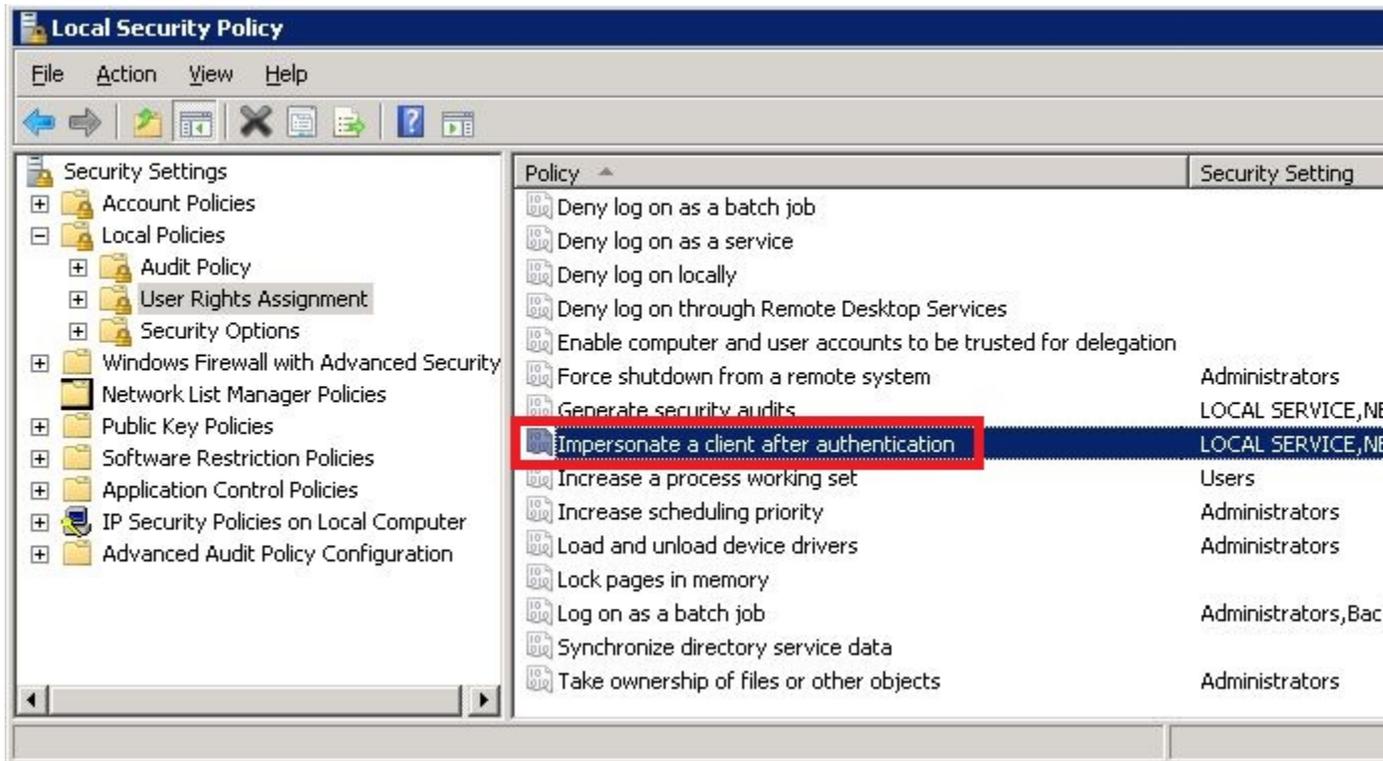


Configure Local Security Policy for SEG to Act as Part of the Operating System

- On the SEG server, open a command prompt by selecting **Start > Run**.
- Type `cmd` and then select **OK**.
- In the command prompt, type `secpol.msc` and then select **OK**. A **Local Security Policy** window displays.
- In the left-hand pane, select **Security Settings > Local Policies > User Rights Assignments**.
- In the right-hand pane, under **Policy**, select **Act as part of the operating system**. A dialog window appears.
- Click **Add User or Group**.
- Type the name of the Service Account attached to the Application Pool. The name must be the same as the name associated to the SEG (i.e., Network Service).
- Click **OK**. The **Local Security Policy** window displays.

Configure Local Security Policy for SEG to Impersonate a Client after Authentication

- 1 In the right-hand pane, under **Policy**, double-click on **Impersonate a client after authentication**.



- 2 The Service Account attached to the Application Pool must be the same as the name associated to the SEG (i.e., Network Service). Verify that name displays in the list. If not, do the following:
 - a Click **Add User or Group**.
 - b Add the name of the Service Account.
- 3 Select the Service Account in the list (i.e., Network Service).
- 4 Click **OK**.

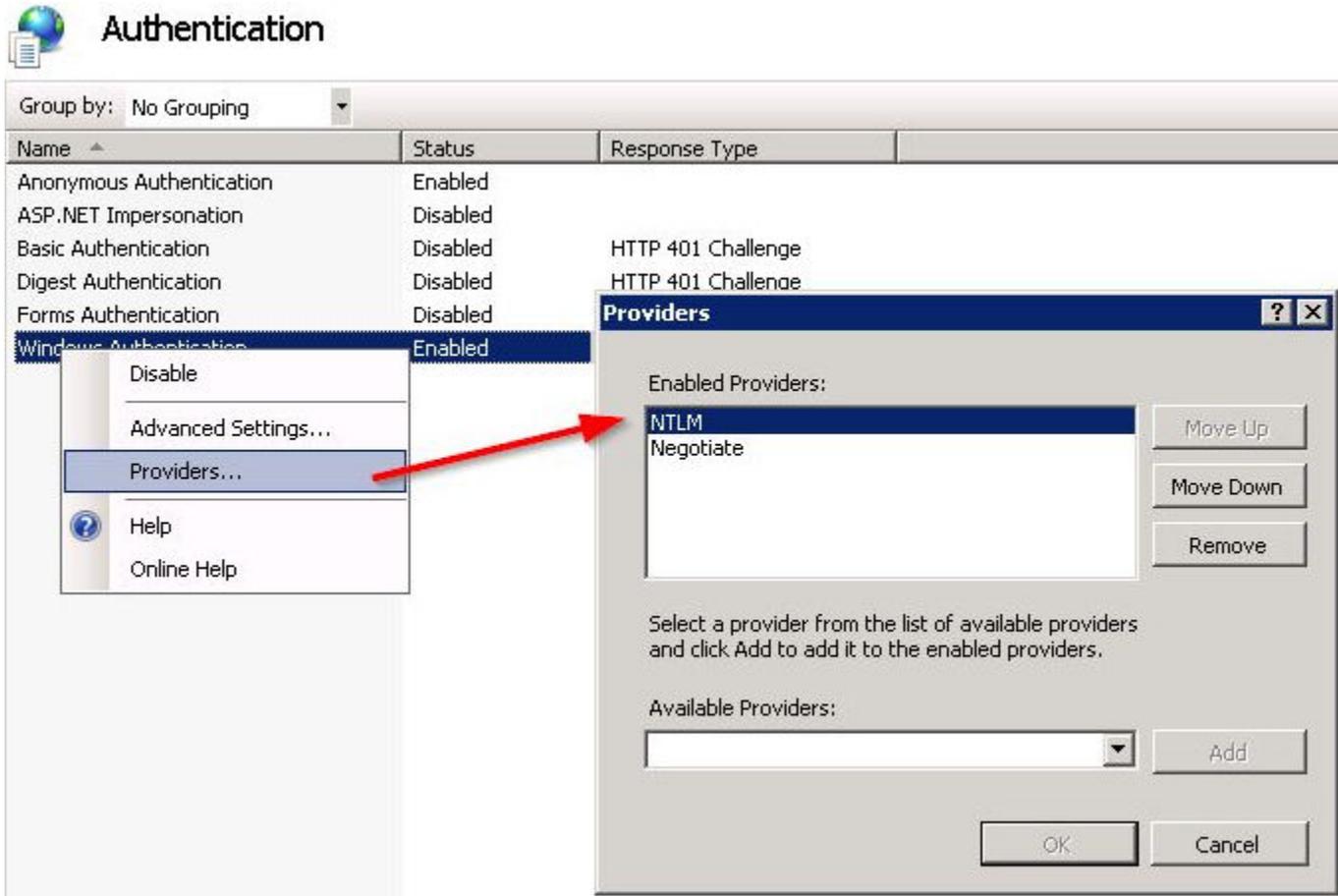
Troubleshooting, EAS with SEG

You can confirm that the SEG is performing certificate authentication by pushing a user's profile to the device and testing whether or not the device is able to connect and sync with the configured SEG endpoint.

If the device does not connect and displays a message that the certificate cannot be authenticated or the account cannot connect to EAS, then the problem is related to the configuration.

Troubleshooting Checks

- If Exchange server returns a 401, add **NTLM** and **Negotiate** as providers to **Windows Authentication**.



- Make sure that a certificate is being issued by the CA to the device by checking the following information.
 - Go to the internal CA Server, launch the certification authority application, and browse to the issued certificates section.
 - Find the last certificate that was issued and it should have a subject that matches the one created in the certificate template section earlier in this documentation.

If there is no certificate then there is an issue with the CA, client access server (e.g., SCEP), or with the Workspace ONE UEM connection to client access server.
 - Check that the permissions of the client access server (e.g., SCEP) Admin Account are applied correctly to the CA, and the template on the CA.
 - Check that the account information is entered correctly in the Workspace ONE UEM configuration.

- Verify the **Server URL** and the **SCEP Challenge URL** contain the correct information and end with a “/”.
- Launch a browser and enter the **SCEP Challenge URL**. The website should prompt you for credentials. After entering the SCEP Admin Account username and password, it should return with the challenge passphrase.
- If the certificate is being issued, make sure that it is in the Profile Payload and on the device.
 - Navigate to **Devices > Profiles > List View**. Click the action icon for the device and select **</ > View XML** to view the profile XML. There is certificate information that appears as a large section of text in the payload.
 - On the device, go to the profiles list, select Details and see if the certificate is present.
 - Confirm that the certificate contains the **Subject Alternative Name** (or SAN) section and that in 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 [Step 4: Configure IIS for Certificate Authentication on the SEG, EAS with SEG](#).
 - Confirm that the certificate contains the **Client Authentication** in the **Enhanced Key Usage** section. If this is 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 SEG server.
 - Confirm that the address of the SEG server is correct in the Workspace ONE UEM profile and that all the security settings have been adjusted for allowing certificate authentication on the SEG server.
- A very good test to run is to manually configure a single device to connect to the SEG/EAS 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 EAS with a certificate.
 - Refer to the External References and Documents section for a link to a step by step guide for configuring a device to connect to EAS using a certificate.
- If none of the steps above resolve the problem, try authenticating independent of Workspace ONE UEM. This is done by eliminating the Workspace ONE UEM (e.g., SEG) and only using a certificate to authenticate the device. If this doesn't work then there are other problems occurring. Until those problems are resolved, you will not be able to use the SEG to handle certificate authentication.
- If you cannot authenticate, verify the clocks on the SEG and Kerberos. Kerberos produces a ticket for the SEG to authenticate the user on the mail server. The timestamp on that ticket must be no more than five minutes apart from the SEG's time clock. Verify the time clock on the SEG and Kerberos are within five minutes apart. You also might want to consider the use of Network Time Protocol daemons to keep all time clocks synchronized.
- If you cannot authenticate, evaluate your network. If you only have one Kerberos server configured, it is possible the server is not operational. Without it, no one can log in. To stop this from occurring, you might consider using multiple Kerberos servers and fallback authentication mechanisms.

Additional SETSPN Commands, EAS with SEG

View SPN: SETSPN -l <computerName>

```

CA. Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>setspn -l awlabcas01

```

Add SPN: SETSPN -s <service>/<targetName> <computerName>

```

CA. Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>setspn -s http/webmail.airwatch.com awlabcas01

```

Remove SPN: SETSPN -d <service>/<targetName>
<computerName>

```

CA. Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>setspn -d http/webmail.airwatch.com awlabcas01

```

Query for existing SPN: SETSPN -Q <service>/<targetName>
<computerName>

```

CA. Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>setspn -q http/webmail.airwatch.com awlabcas01_

```

Check for duplicate SPN in the entire forest: SETSPN -X

```

CA. Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>setspn -x

```

Install a Role in IIS

Install a Role in IIS with SEG on Windows Server 2008 or Windows Server 2008 R2.

Procedure

- 1 On the taskbar, select **Start**, point to **Administrative Tools**, and then select **Server Manager**.
- 2 In the **Server Manager** hierarchy pane, expand **Roles**, and then select **Web Server (IIS)**.
- 3 In the **Web Server (IIS)** pane, scroll to the **Role Services** section, and then select **Add Role Services**.
- 4 On the **Select Role Services** page of the **Add Role Services Wizard**, select **Client Certificate Mapping Authentication**, and then select **Next**.
- 5 On the **Confirm Installation Selections** page, select **Install**.
- 6 On the **Results** page, select **Close**.

Install the Role in IIS, EAS with SEG on Windows Server 2012

Install the Role in IIS, EAS with SEG on Windows Server 2012 or Windows Server 2012 R2

Procedure

- 1 On the taskbar, select **Server Manager**.
- 2 In **Server Manager**, select the **Manage** menu, and then select **Add Roles and Features**.
- 3 In the **Add Roles and Features wizard**, select **Next**. Select the installation type and select **Next**. Select the destination server and select **Next**.
- 4 On the **Server Roles** page, expand **Web Server (IIS)**, expand **Web Server**, expand **Security**, and then select **Client Certificate Mapping Authentication**. select **Next**.
- 5 On the **Select features** page, select **Next**.
- 6 On the **Confirm installation selections** page, select **Install**.
- 7 On the **Results** page, select **Close**.

Exchange ActiveSync with Secure Email Gateway and Threat Management Gateway

5

Organizations can use reverse proxies such as Microsoft's Threat Management Gateway (TMG) to authenticate users and pass the traffic along to backend Exchange ActiveSync (EAS) servers. In order to accomplish this, Kerberos constrained delegation (KCD) is used to allow the TMG to delegate authentication to servers on the backend.

The Workspace ONE UEM Secure Email Gateway (SEG) can be further harnessed to allow for additional controls in regards to which devices are allowed to sync mail.

The intent of this documentation is to discuss two configurations – TMG to EAS server and TMG to SEG to EAS server and define the configurations required in order to setup certificate authentication on a TMG to proxy request to backend EAS or SEG servers.

Threat Management Gateway

Forefront Threat Management Gateway is a secure web gateway that provides comprehensive protection against web-based threats by integrating multiple layers of protection. Forefront TMG acts as a reverse proxy in front of the EAS or SEG server and publishes traffic to the internal endpoints.

Kerberos Constrained Delegation

The Kerberos authentication protocol is used to confirm the identity of users that are attempting to access resources on a network.

Kerberos authentication uses tickets that are encrypted and decrypted by secret keys and do not contain user passwords. These tickets are requested and delivered in Kerberos messages. Two types of tickets are used: Ticket-Granting Tickets (TGTs) and Service tickets.

Kerberos constrained delegation provides a way for domain administrators to limit the network resources that a service trusted for delegation can access. This is accomplished by configuring the account (computer or domain account) under which the service is running to be trusted for delegation to a specific instance of a service running on a specific computer. Such a trust can also be applied to a set of specific instances of delegated services running on specific computers.

Each instance of a service that uses Kerberos authentication needs to have a Service Principal Name (SPN) defined for it so that clients can identify that instance of the service on the network.

The SPN is registered in the Active Directory Service-Principal-Name attribute of the Windows account under which the instance of the service is running. This way, the SPN is associated with the account under which the instance of the service specified by the SPN is running. When a service needs to authenticate to another service running on a specific computer, it uses that service's SPN to differentiate it from other services running on that computer.

This chapter includes the following topics:

- [System Requirements for EAS with SEG and TMG](#)
- [High Level Design for EAS with SEG and TMG](#)
- [Implementation Approach for EAS with SEG and TMG](#)
- [Install, Set Up, Configure Certificate](#)
- [Troubleshooting for EAS with SEG and TMG](#)

System Requirements for EAS with SEG and TMG

The following is required in order to complete the configurations outlined in this documentation.

- Ability to pass through all firewalls used to isolate the TMG and SEG from the AD and EAS servers.
- An external certificate authority (CA) cannot be used (e.g., VeriSign, etc.) to create user's certificates.
- An internal certificate authority (CA) server must be used to create user's certificates. If you need guidance as to the methodology of setting up an internal CA, contact Workspace ONE UEM Support.

Important Important: CAs 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. Creating an optimal design requires careful planning and lab testing before you deploy it in a production environment.

- The internal CA, TMG, and SEG must be configured within the same enterprise domain in order to pass user certificates.
- Administrative access privileges to the Active Directory, Microsoft TMG, Workspace ONE UEM Secure Email Gateway (SEG) if installed, and EAS servers.
- Internet Information Services (IIS) with the Client Certificate Mapping Authentication option installed on the:
 - TMG for TMG to EAS configurations
 - SEG for TMG to SEG to EAS configurations
- 80% of the current resources on the Exchange ActiveSync (EAS) server.
- Connectivity from TMG and SEG to the AD and EAS servers.

Other Prerequisites

Before configuring the Threat Management Gateway (TMG) and Secure Email Gateway (SEG) to use certificate authentication, you must have the following.

- Installed and operational Threat Management Gateway (TMG).
- Windows Server 2003 or 2008 Standard with latest service packs and recommended updates from Microsoft.
- A device with an Exchange ActiveSync (EAS) profile and certificate from a domain enterprise certificate authority (CA).
- A TMG that is configured as a member of the same domain as the enterprise certificate authority.
- Administrative permissions to configure your enterprise.
 - Threat Management Gateway (TMG)
 - Active Directory (AD)
 - Exchange ActiveSync (EAS) server
- A certificate authority properly configured to issue certificates through Workspace ONE UEM.
- Everything included in the previous section.
- Installed and operational Secure Email Gateway (SEG).
- A SEG that is configured as a member of the same domain as the enterprise certificate authority.
- Administrative permissions to be able to configure your enterprise SEG.

High Level Design for EAS with SEG and TMG

The diagrams below highlight the communications flow for a device attempting to connect to the Exchange ActiveSync (EAS) server using a certificate for authentication.

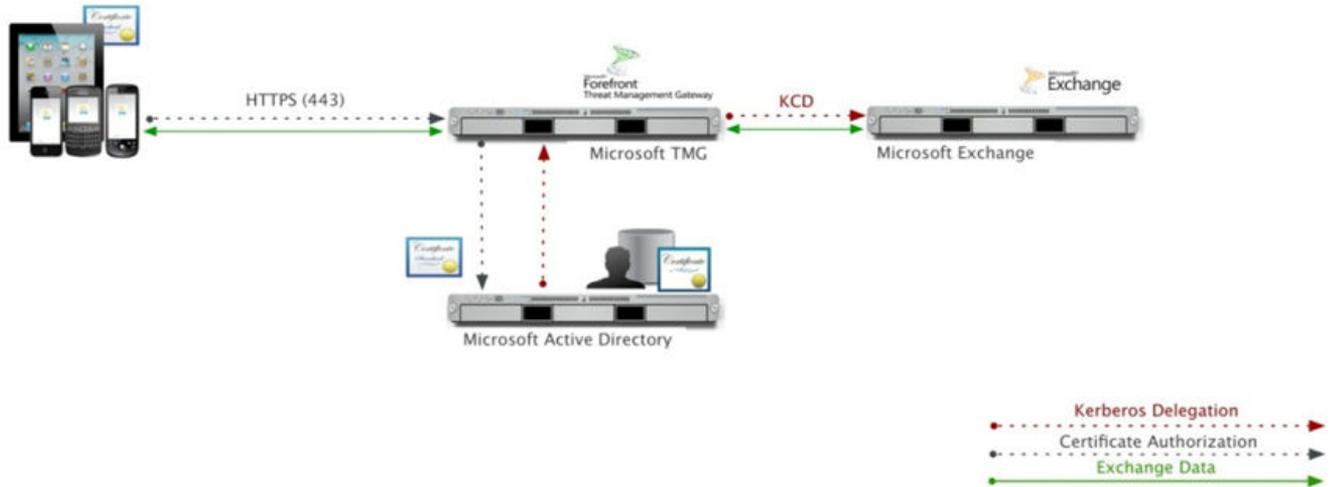
The first diagram shows the connection through the Microsoft TMG and the second diagram shows the same as the first with the addition of the Workspace ONE UEM Secure Email Gateway (SEG).

The TMG and SEG reside in a Demilitarize Zone (DMZ) to protect enterprise servers from outside intruders. As such, certificate authentication is handled indirectly using Kerberos.

TMG to EAS Server

- A request is made by Workspace ONE UEM to the enterprise domain certificate authority (can only be issued by an internal CA) to produce a certificate for the user that contains User Principal Name (UPN) mapping and their email address in the Subject Alternative Name (SAN) of the certificate.
- Since the TMG is a member of the same enterprise domain as the internal CA, it receives the certificate from the CA and authenticates the certificate against Active Directory (AD).

- Once authenticated with AD, Kerberos issues a ticket to TMG with the user's credentials allowing the TMG to impersonate (authenticate) the user's device to the EAS server.
- EAS accepts the TMG's impersonation (authentication) and allows the user to access email.



Implementation Approach for EAS with SEG and TMG

Before your enterprise email server can securely pass email to the user's device, you need to configure your email server to perform the following tasks.

- Recognize the user's device
- Trust the end-user is the authorized user of the device.

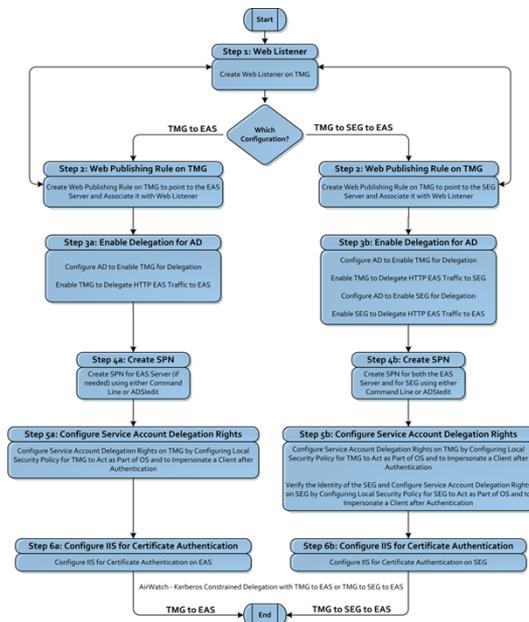
This is accomplished by authenticating that user and their device with a certificate. Regardless of the enterprise email server being used, the methodology of certificate authentication is basically the same.

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 a certificate and ensures the user has a seamless experience receiving their email.

The following sections discuss two different implementation approaches.

- TMG to EAS
- TMG to SEG to EAS.

The first section describes the approach for both configurations and the next two sections describe the approach for the configuration involving Secure Email Gateway. In all sections, steps are referenced, which correlate to the steps that provide detailed information.



Configure Either TMG to EAS or TMG to SEG to EAS Server

This implementation includes steps 1 and 2, which are required for configuring either TMG to EAS or TMG to SEG to EAS servers. After you complete these steps, you need to advance to either [Configure TMG to EAS Server](#) or [Configure TMG to SEG to EAS Server](#).

First, regardless of the configuration, the web listener is always created on the TMG so the first step is to create a web listener on the TMG in order for it to pre-authenticate the connection and incoming requests from clients, and then allow those devices to securely access the user's email by:

- Creating a Name for the Web Listener
- Setting Up Secure Socket Layer (SSL)
- Setting Up an External IP Address for the Web Listener
- Associating a Certificate to the Web Listener
- Selecting SSL for Client Certificate Authentication
- Completing the Wizard

Next, regardless of the configuration, the web publishing rule is always created on the TMG. Depending on the configuration, the TMG points to either the EAS or SEG server. If your configuration is a TMG to EAS, you need to create a web publishing rule on the TMG server to publish Exchange Client Access traffic directly to an EAS server, whereas if your configuration is TMG to SEG to EAS, you must use the SEG server as the published website instead of the EAS server. You can create a web publishing rule for either configuration by:

- Creating a Name for the Web Publishing Rule. You can use more than one web publishing rule for each web listener.
- Selecting the Version of Exchange Server

- Publishing the Rule to a Single Web Site or Load Balancer
- Selecting SSL to Connect to a Published Web Server
- Configuring the Internal Domain Name for the EAS or SEG Server
- Configuring the Public Name Domain for the Published Site
- Associating the Publishing Rule to the Web Listener

A web publishing rule is associated with the web listener you created in [Create a Web Listener on the TMG, EAS with SEG and TMG](#). When applying a web publishing rule, you need to specify the web listener to be used along with it in the TMG.

- Selecting Kerberos Constrained Delegation and Service Principal Name
- Applying the Publishing Rule to All Authenticated Users
- Saving the Configurations for the Exchange Publishing Rule
- Advance to either Configuring TMG to EAS Server or Configuring TMG to SEG to EAS Server

Configure TMG to EAS Server

This implementation is only for TMG to EAS configurations. It includes steps 3a through 6a for configuring a TMG to EAS server.

After creating the listener and rule, you need to enable delegation from AD. In order for the TMG to impersonate a device user when authenticating on an EAS server, the TMG server must be given the appropriate permissions in the Active Directory (AD) server by doing the following:

- Configuring AD to enable the TMG for delegation
- Enabling the TMG to delegate HTTP EAS traffic to the EAS server

Now that delegation is enabled, you need to create a Service Principal Name (SPN) for the EAS server, if needed. This can sometimes depend on the customer configuration and server (i.e. if an internal web address is referenced in the Authentication Delegation page), but by default with a single server, you only need to specify the server name with the http service. Use one of the following two methods to add an SPN. Both of the following methods require a domain account that has access to write to the Active Directory: from the command line or from ADSIedit.

After creating an SPN, you first need to configure delegation rights on the TMG server and then give permissions to the service account that is attached to the TMG Application Pool by doing the following:

- Configuring local security policy for TMG to act as part of the Operating System
- Configuring local security policy for TMG to impersonate a client after authentication

The last step is to authenticate the user's device that is assigned to a particular certificate by configuring **Internet Information Services (IIS)** on the EAS server to accept that certificate by doing the following:

- Enabling Active Directory client certificate authentication in IIS
- Enabling client certificate mapping authentication

- Requiring SSL for authentication
- Adjusting uploadReadAheadSize memory size

Configure TMG to SEG to EAS Server

This implementation includes steps 3a through 6a above with the addition of the following steps (3b through 6b) that are related to adding a SEG between the TMG and EAS servers.

After creating the listener and rule, you need to enable delegation from AD. In order for the TMG and SEG to impersonate a device user when authenticating on an EAS server, first you must give the appropriate permissions in the Active Directory (AD) server from the TMG to SEG servers, and then give the same permissions from the SEG to EAS servers by doing the following:

- Configuring AD to enable the TMG for delegation
- Enabling the TMG to delegate HTTP EAS traffic to the SEG server
- Configuring AD to enable the SEG for delegation
- Enabling the SEG to delegate HTTP EAS traffic to the EAS server

Now that delegation is enabled, you need to first create a Service Principal Name (SPN) for the EAS server, and then create an SPN on the SEG. Use one of the following two methods to add an SPN for the EAS server and then do it again for the SEG. Both of the following methods require a domain account that has access to write to the Active Directory:

- From the command line
- From ADSIedit

After creating an SPN, you first need to configure delegation rights on the TMG server and then give permissions to the service account that is attached to the TMG Application Pool. Once that is done, you need to follow the same procedure and configure delegation rights on the SEG and then give permissions to the service account that is attached to the SEG Application Pool. You can perform all these steps by doing the following:

- Configuring local security policy for TMG to act as part of the Operating System
- Configuring local security policy for TMG to impersonate a client after authentication
- Verifying the identity of the SEG
- Configuring local security policy for SEG to Act as Part of the Operating System
- Configuring local security policy for SEG to Impersonate a Client after Authentication

The last step is to authenticate the user's device that is assigned to a particular certificate by configuring **Internet Information Services (IIS)** on the SEG server to accept that certificate by doing the following:

- Enabling Active Directory Client Certificate Authentication in IIS
- Enabling Client Certificate Mapping Authentication
- Requiring SSL for Authentication

- Adjusting uploadReadAheadSize Memory Size

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.

Create a Web Listener on the TMG, EAS with SEG and TMG

Regardless of the configuration (TMG to EAS or TMG to SEG to EAS), the first step is to create a web listener on the Threat Management Gateway (TMG).

In order for devices to securely access mail through the TMG, the TMG must have a web listener created to accept incoming communications from devices. It also enables TMG to pre-authenticate the connection and incoming requests from the clients.

First, you must create a name for the Web Listener.

- 1 In the **Forefront TMG Management** console tree, select **Firewall Policy**.
- 2 On the task pane, select the **Toolbox** tab and then select **Network Objects > New**.
- 3 Select the **Web Listener** option.
- 4 In the **New Web Listener Definition Wizard** window, enter the **Web listener name** with an appropriate description.
- 5 Click **Next**.
Next, you must set up Secure Socket Layer (SSL)
- 6 On the **Client Connection Security** page, select **Require SSL secured connections with clients**.
- 7 Click **Next**.
Next, you must set up an external IP address for the Web listener.
- 8 On the **Web Listener IP Addresses** page, select the **External** network checkbox. Or if you have multiple IP addresses associated with this network, select one of those IP addresses.
- 9 Click **Next**.
The selection can be changed based on a client's specific configuration; but generally, you have to select the External network.
- 10 Click the **Select IP Addresses** button and then select **Specified IP Addresses on the Forefront TMG computer in the selected network**.
- 11 Below **Available IP Addresses**, select the **IP address** for the website.
- 12 Click **Add**.
- 13 Click **OK**.

14 Click **Next**.

Next, you must associate a certificate to the Web listener.

15 On the Listener SSL Certificate page, select **Select Certificate**.

16 Select the respective certificate and select **Select**. The selected certificate is used with this listener and is the URL that the TMG is routing.

Click **Next**.

Next, you must select the SSL for client certificate authentication.

17 On the **Authentication Settings** page, select **SSL Client Certificate Authentication** from the drop-down menu.

18 Click **Next**.

Next, you must complete the wizard.

19 On the **Single Sign on Settings** page, an error message appears stating **SSO is not available for the currently selected client authentication method. SSO is only available for HTML Form Authentication**.

20 Ignore the message and select **Next**.

21 Click **Finish**.

Next, you must [Create a Web Publishing Rule on TMG to Publish Traffic to EAS or SEG](#).

Create a Web Publishing Rule on TMG to Publish Traffic to EAS or SEG

Regardless of the configuration, the web publishing rule is always created on the Threat Management Gateway (TMG). Depending on your configuration, the TMG points to either the EAS or SEG server.

- If your configuration is a TMG to EAS, you need to create a web publishing rule on the TMG server to publish Exchange Client Access traffic directly to an EAS server.
- If your configuration is TMG to SEG to EAS, you must use the SEG server as the published website instead of the EAS server.

A web publishing rule is associated with the web listener you created in [Create a Web Listener on the TMG, EAS with SEG and TMG](#). When applying a web publishing rule, you specify the web listener to be used along with it in the TMG. You can use more than one web publishing rule for each web listener. The following procedure explains how to create a web publishing rule for both configurations.

If you are adding a SEG to an existing TMG to EAS configuration, make sure the web publishing rule is no longer configured to publish Exchange Client Access traffic to the EAS server before configuring it to publish to the SEG server.

First, you must create a name for the Web publishing rule.

1 In the **Forefront TMG Management** console tree, expand the **Server** node and then select Firewall Policy.

2 On the task pane, select **Tasks** tab, and then select **Publish Exchange Web Client Access**.

3 In the **New Exchange Publishing Rule Wizard** window, enter the Exchange Publishing rule name with an appropriate description to identify the website being published.

4 Click **Next**.

Next, you must select the version of the Exchange server.

5 On the **Select Services** page, select the **Exchange version** drop-down menu and select the version of the Exchange server being used.

6 Check the **Exchange ActiveSync** client checkbox.

7 Click **Next**.

Next, you must publish the rule to a single Web site or load balancer.

8 On the **Publishing Type** page, select **Publish a single Web site or load balancer**.

9 Click **Next**.

If there are multiple EAS servers, you have the option of selecting the second option which allows the TMG to act as a load balancer.

Next, you must select SSL to connect to a published Web server.

10 On the **Server Connection Security** page, select **Use SSL to connect to the published Web server or server farm**.

11 Click **Next**.

Next, you must configure the internal domain name for the EAS or SEG server.

12 On the **Internal Publishing Details** page, enter the internal domain name in the **Internal site name** field.

13 Click **Next**.

If this configuration is being used to setup an EAS server, put the EAS server name in the field. If this is to setup a Workspace ONE UEM SEG, put the SEG server information in the field.

Next, you must configure the public name domain for the published site.

14 On the **Public Name Details** page, select the **Accept requests for** drop-down arrow and select **This domain name (type below)** option.

15 Enter the public domain name of the EAS or SEG server in the **Public Name**.

The public DNS record information used for this website is that being published.

Next, you must associate the publishing rule to the Web listener.

16 On the **Select the Web listener** page, select the **Web Listener** drop-down arrow and select the name of the web listener you created in the previous step.

17 Click **Next**.

Next, you must select Kerberos Constrained Delegation and enter the Service Principal Name.

- 18 On the **Authentication Delegation** page, select the drop-down arrow and select **Kerberos constrained delegation**.
- 19 Enter the **Service Principal Name** in the field. Enter the same name as the name that will be used in the next step.
- 20 Click **Next**.

The **Kerberos constrained delegation** option is selected for authentication. The **Service Principal Name** section can vary depending on customer configuration, but by default with a single server, you can just specify the server name with the http service. If the TMG is to be used as a load balancer across multiple servers, then the SPN value here should be set to **http/***.

Next, you must apply the publishing rule to all authenticated users.

- 21 On the **User Sets** page, select **All Authenticated Users** to make sure only users with the appropriate credentials are allowed to access..
- 22 Click **Next**.

Next, you must save the configuration for the Exchange publishing rule.

- 23 Click **Finish** to complete the Exchange Publishing Rule wizard.

A prompt appears to inform you that you may have to configure the SPNs for the services. If you are using the server name as the SPN in the previous step, there is no further configuration necessary. If you are referencing an internal URL then you need to add the SPN and associate it with the server account in Active Directory.

Next, you must [Enable Delegation from Active Directory when using a TMG, EAS with SEG and TMG](#).

Enable Delegation from Active Directory when using a TMG, EAS with SEG and TMG

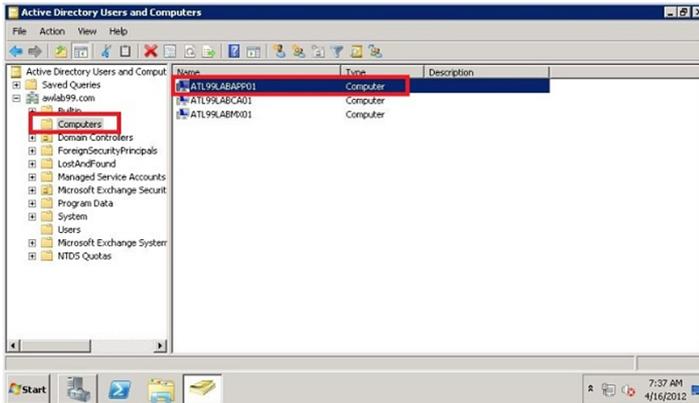
In order for the Threat Management Gateway (TMG) to impersonate a device user when authenticating on an EAS server, the TMG server must be given the appropriate permissions in the Active Directory (AD) server.

This step must be completed whether or not you are employing the use of a Secure Email Gateway (SEG). There are instructions at the end of this topic that direct you to the next step, SEG or no SEG.

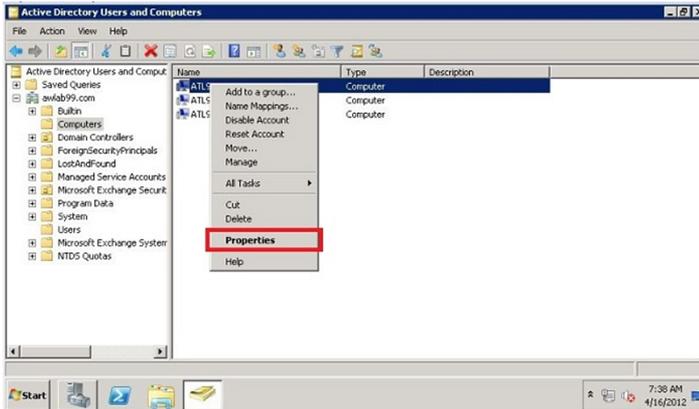
First, you must configure AD to enable the TMG for delegation.

- 1 On the AD server, select **Active Directory Users and Computers**.

- 2 In the left-hand pane, select the folder where the TMG server is located (e.g., Computers). The available TMG servers display in the right-hand pane as show below.



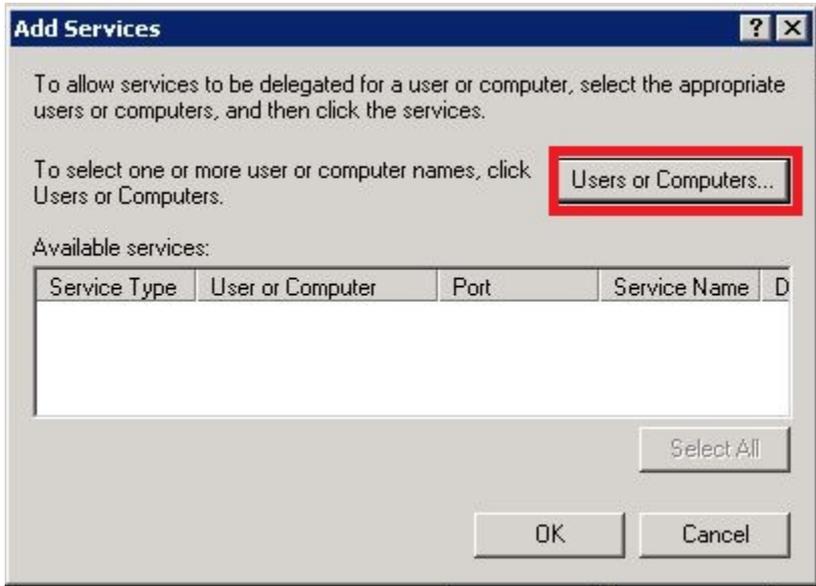
- 3 Right-click the TMG server name and select **Properties**. The **Properties** window for the TMG server displays.



- 4 Click the **Delegation** tab.
- 5 Select the **Trust this computer for delegation to specified services only**.
- 6 Select **Use any authentication protocol**.
- 7 Click **Add**. The **Add Services** window displays.

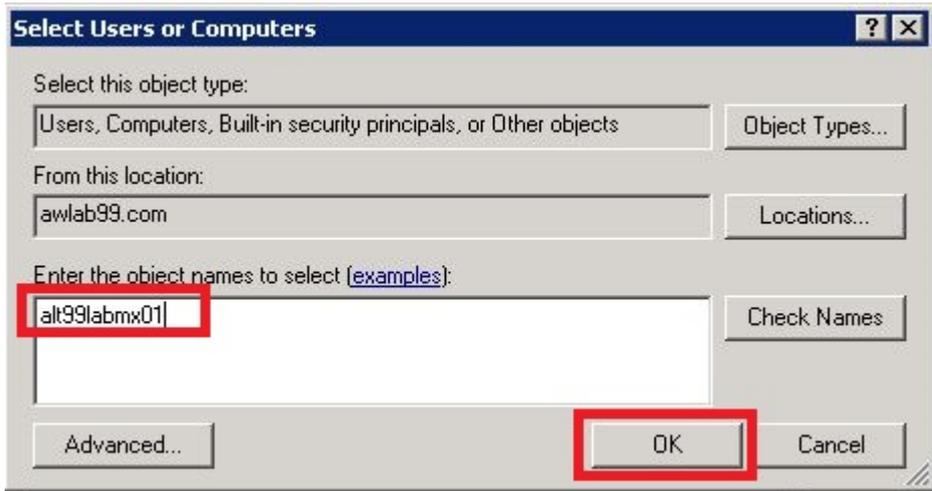
Next, you must enable the TMG to delegate HTTP EAS traffic to the EAS server.

8 Click **Users or Computers**



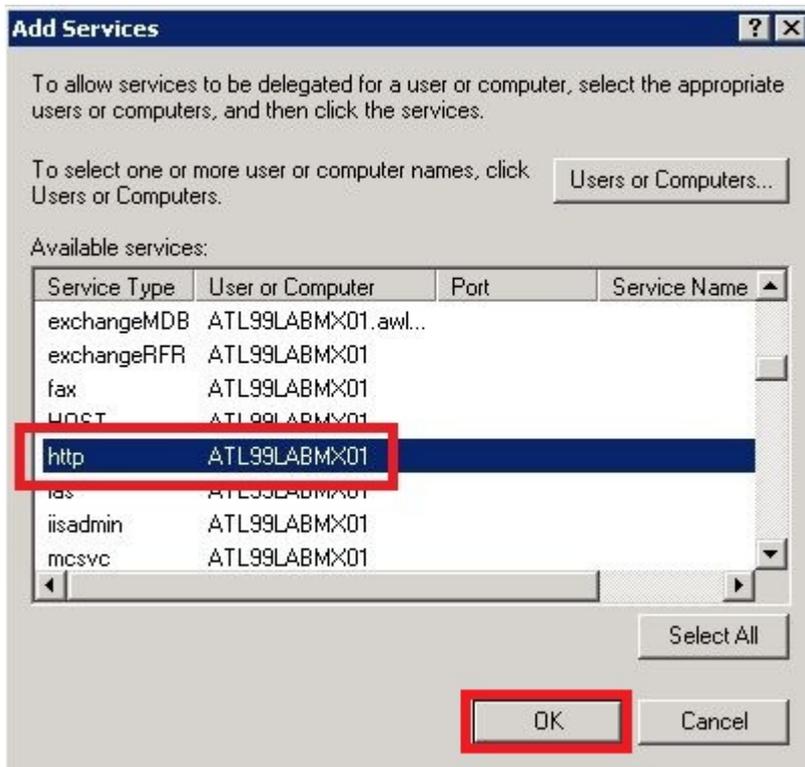
9 The **Select Users or Computers** window displays. Enter the name of the EAS server.

10 Click **OK**. The **Add Services** window displays.



11 Under **Available services**, select **http Service Type**.

12 Click **OK**.



13 You now see on the **Delegation** tab, a listing for the **http Service Type** and the name of your EAS server under the **User or Computer** column.

14 Click **OK**.

If you are not deploying a SEG, then skip to [Create a Service Principal Name \(SPN\) for the EAS Server, EAS with SEG and TMG](#). Otherwise, proceed to [Enable Delegation from Active Directory when using a SEG, EAS with SEG and TMG](#).

Enable Delegation from Active Directory when using a SEG, EAS with SEG and TMG

As mentioned previously, whenever a SEG is inserted between the TMG and EAS servers, you need to enable delegation from both the TMG and SEG servers.

To enable delegation from active directory, you need to repeat all the steps in [Enable Delegation from Active Directory when using a TMG, EAS with SEG and TMG](#) when using a TMG for the TMG to SEG servers, and then again from the SEG to the EAS servers.

- Configure AD to Enable TMG for Delegation
- Enable TMG to Delegate HTTP EAS Traffic to SEG
- Configure AD to Enable SEG for Delegation

- Enable SEG to Delegate HTTP EAS Traffic to EAS

Next, you must [Create a Service Principal Name \(SPN\) for the EAS Server, EAS with SEG and TMG](#).

Create a Service Principal Name (SPN) for the EAS Server, EAS with SEG and TMG

Service Principal Names are used to support mutual authentication between a client application and a service. In order for the EAS service to deliver email to the device, the EAS server must be furnished with an SPN from the Active Directory (AD) server.

This step must be completed whether or not you are employing the use of a Secure Email Gateway (SEG). There are instructions at the end of this topic that direct you to the next step, SEG or no SEG.

First, you must create an SPN for the EAS server.

There are two methods to add SPNs. Both require a domain account that has access to write to the Active Directory.

- Command line prompt
- The ADSIedit module

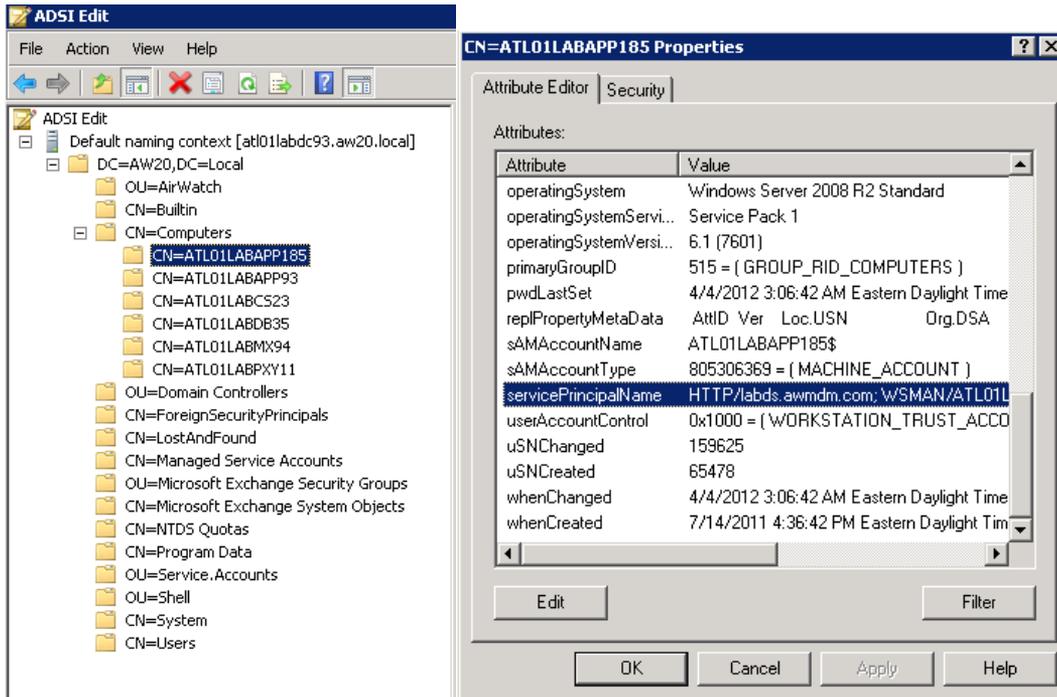
From the Command Line

```
Setspn -A http/<internaladdress> domain/computeraccountname
```

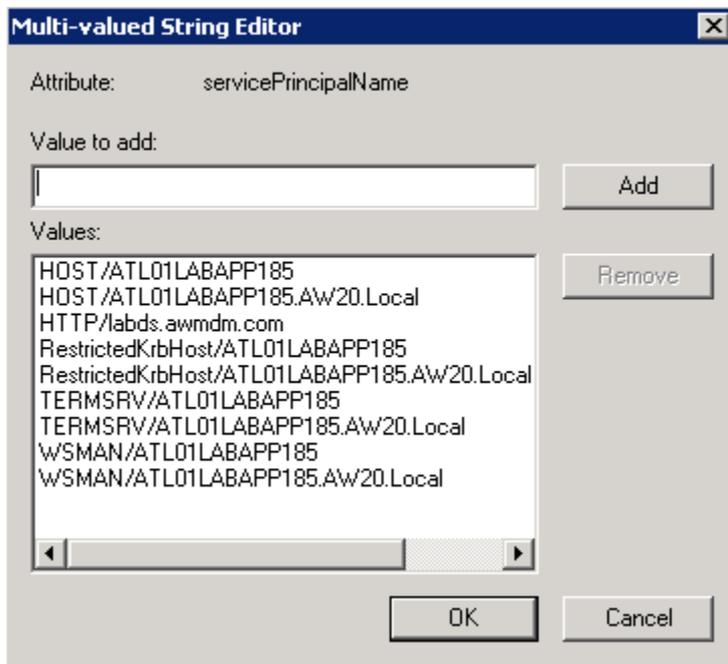
From ADSIedit

- 1 From the domain controller, open **ADSI Edit**.
 - a Open **MMC** and add **ADSIedit snap-in**, or
 - b Run menu and type `adsiedit.msc` module.
- 2 Right-click **ADSI Edit**.
- 3 In the **Connections Settings** window, select **Select a well known Naming Context**.
- 4 Click the drop-down arrow and select **Default naming context**.
- 5 Select **Default (Domain or server that you logged in to)**.
- 6 Click **OK**.
- 7 Click the **+** box to expand the directory of folders.

- In the right pane, locate the server where SPN is set, right-click it and select **Properties**. The Properties window for the SPN server displays.



- In the **Attribute Editor** tab, locate and select **servicePrincipalName**.
- Click **Edit**. A **Multi-valued String Editor** dialog box opens.



- In the **Value to add** field, type the required SPN, select **Add** after each entry, and then select **OK** twice to close the dialog box.

12 Close ADSI Edit.

If you are not employing the use of a SEG, then skip to [Configure Service Account Delegation Rights on TMG, EAS with SEG and TMG](#). Otherwise, proceed to [Create a Service Principal Name \(SPN\) for the SEG, EAS with SEG and TMG](#).

Create a Service Principal Name (SPN) for the SEG, EAS with SEG and TMG

As mentioned previously, whenever a SEG is inserted between the TMG and EAS servers, you need to first create a Service Principal Name (SPN) for the EAS server.

Then you need to create an SPN on the SEG by repeating all the steps in [Create a Service Principal Name \(SPN\) for the EAS Server, EAS with SEG and TMG](#) and replacing all references to EAS server with SEG. The SEG also needs to have a domain account that has access to write to the Active Directory.

The final result after using either the Command Line or ADSIedit should be...

- You created an SPN for the EAS server,
- You created an SPN for the SEG.

Next, you must [Configure Service Account Delegation Rights on TMG, EAS with SEG and TMG](#).

Configure Service Account Delegation Rights on TMG, EAS with SEG and TMG

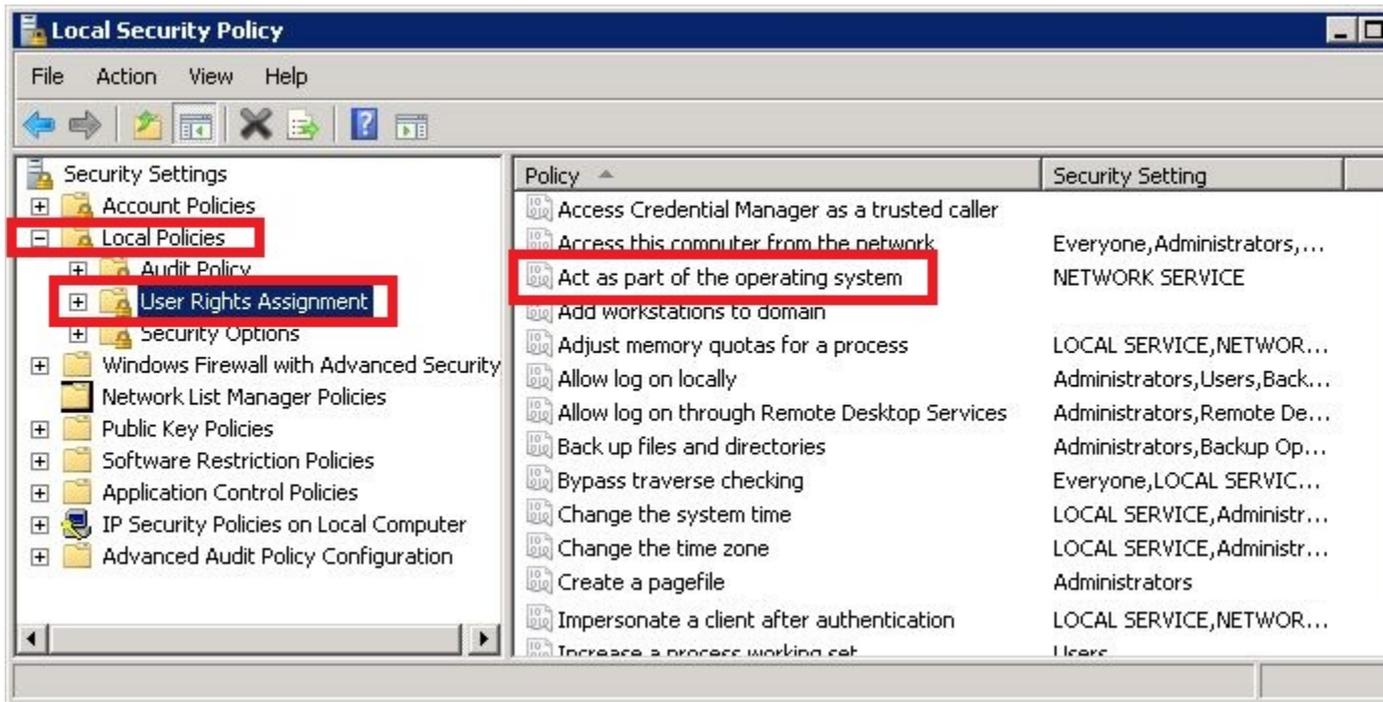
In addition to configuring delegation rights on the TMG server, the service account that is attached to the TMG Application Pool must also be given delegation permissions.

This step must be completed whether or not you are employing the use of a Secure Email Gateway (SEG). There are instructions at the end of this topic that direct you to the next step, SEG or no SEG.

First, you must configure the local security policy for TMG to act as part of the operating system.

- 1 On the TMG server, open a command prompt by selecting **Start > Run**.
- 2 Type `cmd` and then select **OK**.
- 3 In the command prompt, type `secpol.msc` and then select **OK**. A **Local Security Policy** window displays.
- 4 In the left-hand pane, select **Security Settings > Local Policies > User Rights Assignments**.

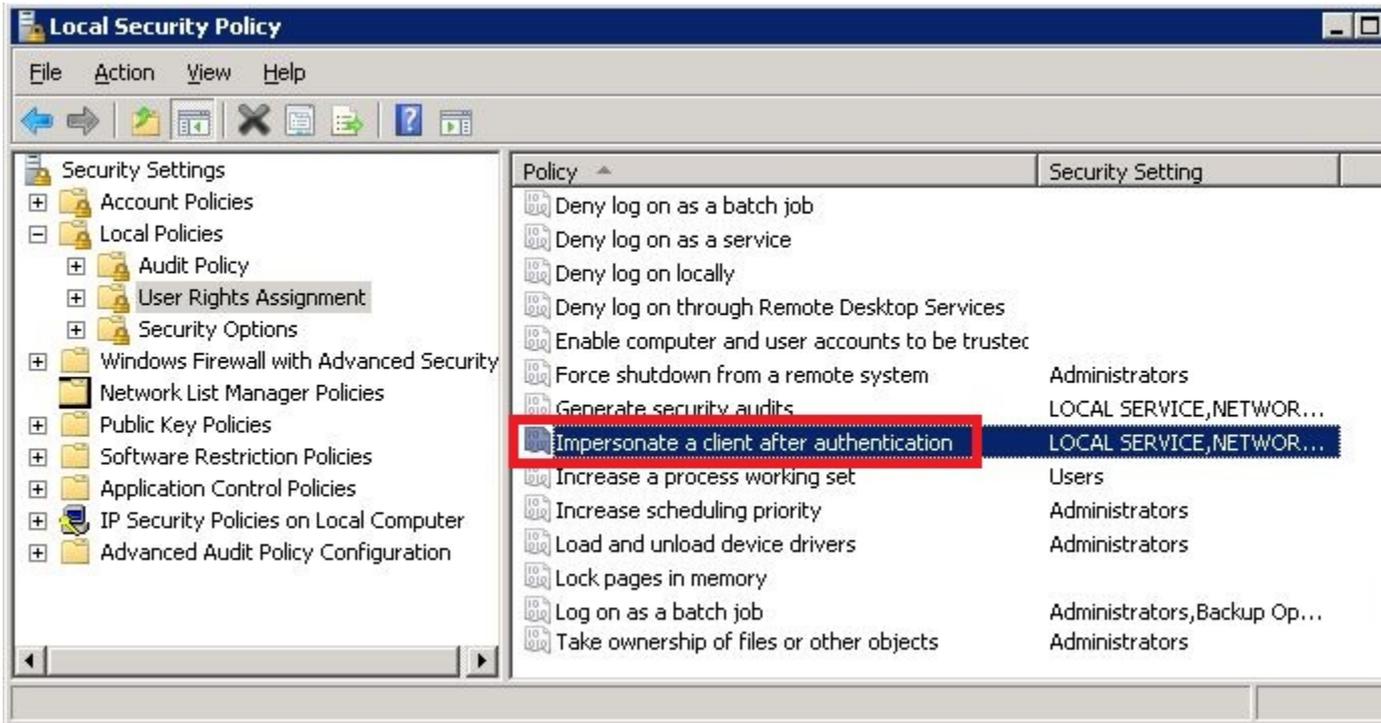
- In the right-hand pane, under **Policy**, select **Act as part of the operating system**. A dialog window appears.



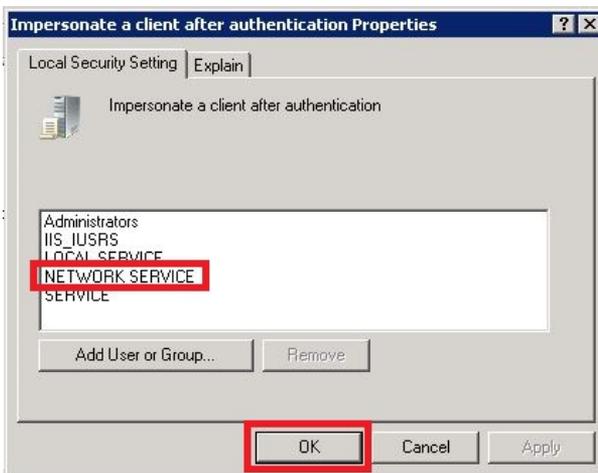
- Click **Add User or Group**.
- Type the name of the Service Account attached to the Application Pool. The name must be the same as the name associated to the TMG (i.e., Network Service).
- Click **OK**. The **Local Security Policy** window displays.

Next, you must configure the local security policy for TMG to impersonate a client after authentication.

- 9 In the right-hand pane, under **Policy**, double-click **Impersonate a client after authentication**. A **Properties** dialog box appears.



- 10 The Service Account that is attached to the Application Pool must be the same as the name associated to the TMG (i.e., Network Service). Verify that name displays in the list. If not, do the following:
 - a Click **Add User or Group**.
 - b Add the name of the Service Account.
- 11 Select the Service Account in the list (i.e., Network Service).
- 12 Click **OK**.



If you are not employing the use of a SEG, then skip to [Configure IIS for Certificate Authentication with SEG, EAS with SEG and TMG](#). Otherwise, proceed to [Create a Service Principal Name \(SPN\) for the SEG, EAS with SEG and TMG](#).

Configure Service Account Delegation Rights on SEG, EAS with SEG and TMG

Whenever a SEG is inserted between the TMG and EAS servers, you need to enable delegation rights and permissions on the SEG by repeating all the steps below, followed by [Configure Service Account Delegation Rights on TMG, EAS with SEG and TMG](#), and replacing all references to TMG with SEG.

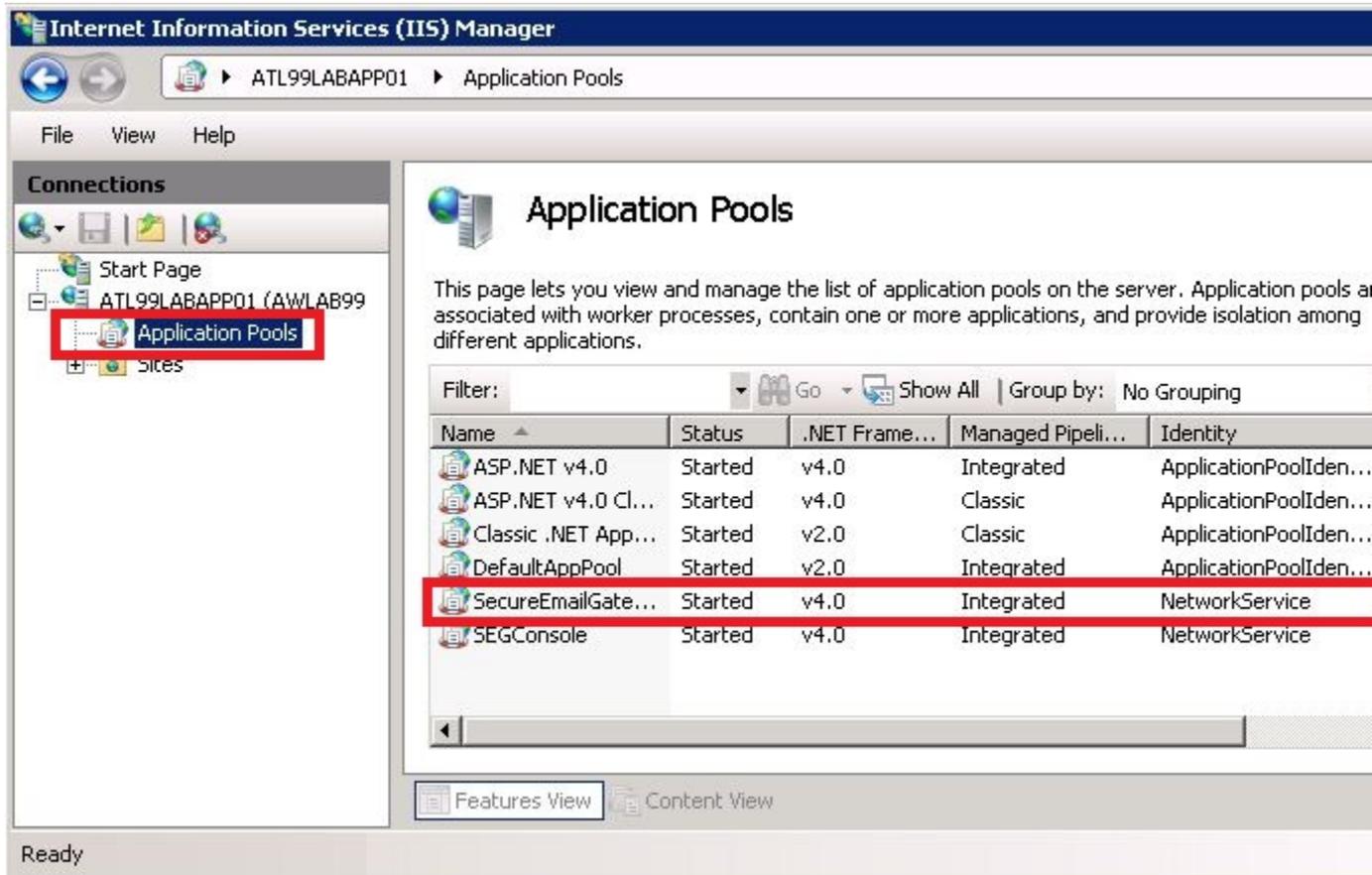
The final result is you should have completed the following.

- Configure Service Account Delegation Rights on TMG by...
 - Configuring Local Security Policy for TMG to Act as Part of OS,
 - Configuring Local Security Policy for TMG to Impersonate a Client after Authentication.
- Verify the Identity of the SEG
- Configure Service Account Delegation Rights on SEG by...
 - Configuring Local Security Policy for SEG to Act as Part of OS,
 - Configuring Local Security Policy for SEG to Impersonate a Client after Authentication.

In order to verify the service account that needs to be enabled with delegation rights, you can open IIS on the SEG server and follow this procedure. If you are already aware of the SEG service account, proceed with replacing all references to TMG with SEG.

- 1 Launch **Internet Information Services (IIS) Manager** by selecting **Start > Run**.
- 2 Type `inetmgr` and select **OK**. The IIS Manager window appears.
- 3 In the left-hand **Connections** pane, select the SEG server.
- 4 Click the **Application Pools** folder.
- 5 In the right-hand **Application Pools** pane, locate the **SecureEmailGateway**.

- 6 Under the Identity column, verify the identity of the **SecureEmailGateway** is **Network Service**.



Next, you must [Configure IIS for Certificate Authentication with SEG, EAS with SEG and TMG](#).

Configure IIS for Certificate Authentication with TMG, EAS with SEG and TMG

In order to authenticate the user's device that is assigned to a particular certificate, **Internet Information Services (IIS)** must be configured to accept that certificate. For the configurations shown in this documentation, IIS can only be configured on either a SEG or EAS server. Where IIS resides is dependent on the configuration as follows.

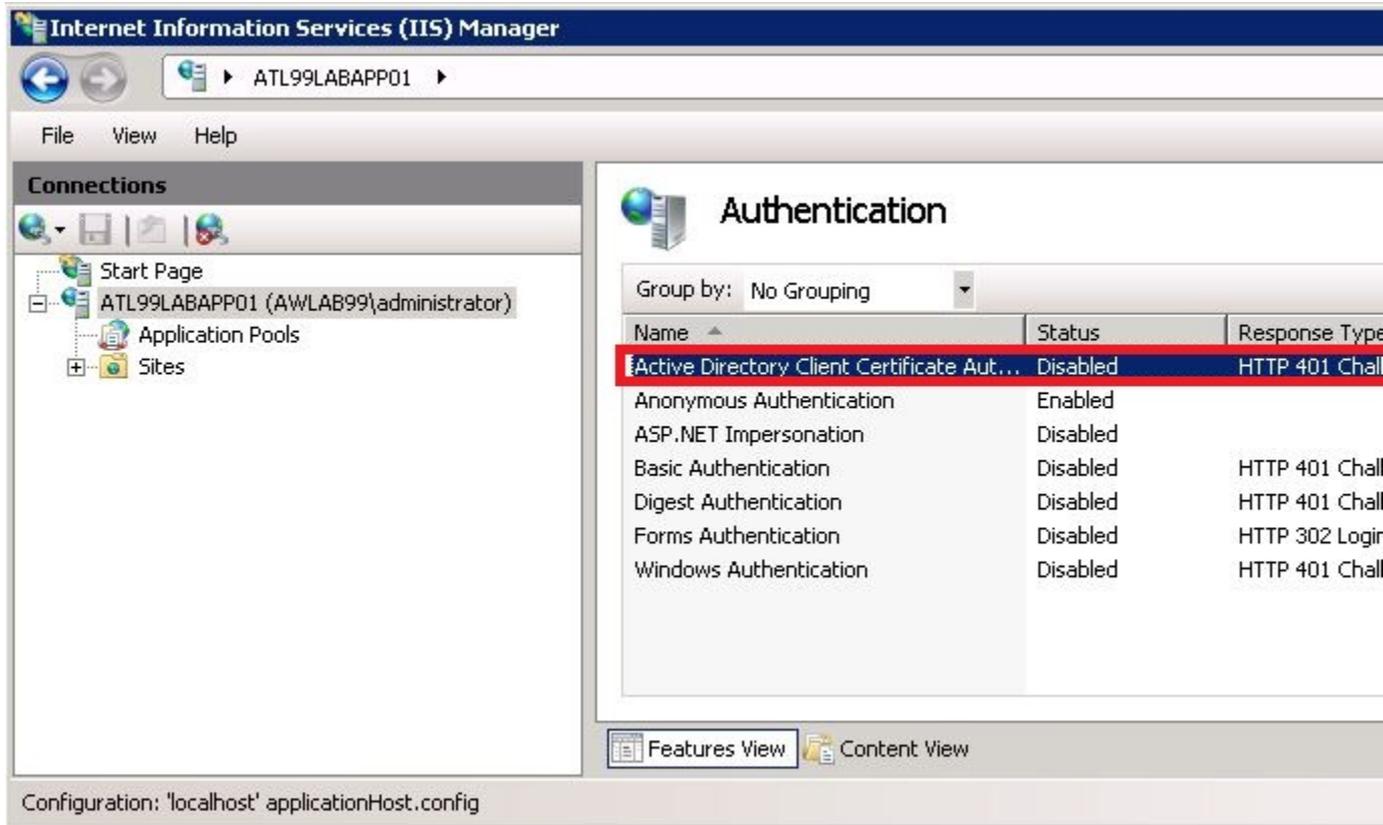
- If the configuration is TMG to EAS then you can configure IIS on the EAS server.
- If the configuration is TMG to SEG to EAS then you can configure IIS on the SEG server.

This section discusses configuring IIS on the EAS server. If a SEG is included in your configuration, skip this step and advance to [Configure IIS for Certificate Authentication with SEG, EAS with SEG and TMG](#).

First, you must enable Active Directory client certificate authentication in IIS.

- 1 On the EAS server, launch **Internet Information Services (IIS)** by selecting **Start > Run**. In the dialog box type `inetmgr` and select **OK**. The **IIS Manager window** appears.
- 2 In the left-hand **Connections** pane, select the EAS server.

- 3 In the main pane, under the **IIS** section, double-click the **Authentication** icon.
- 4 Select **Active Directory Client Certificate Authentication**.
- 5 In the right-hand pane, select **Enable**.



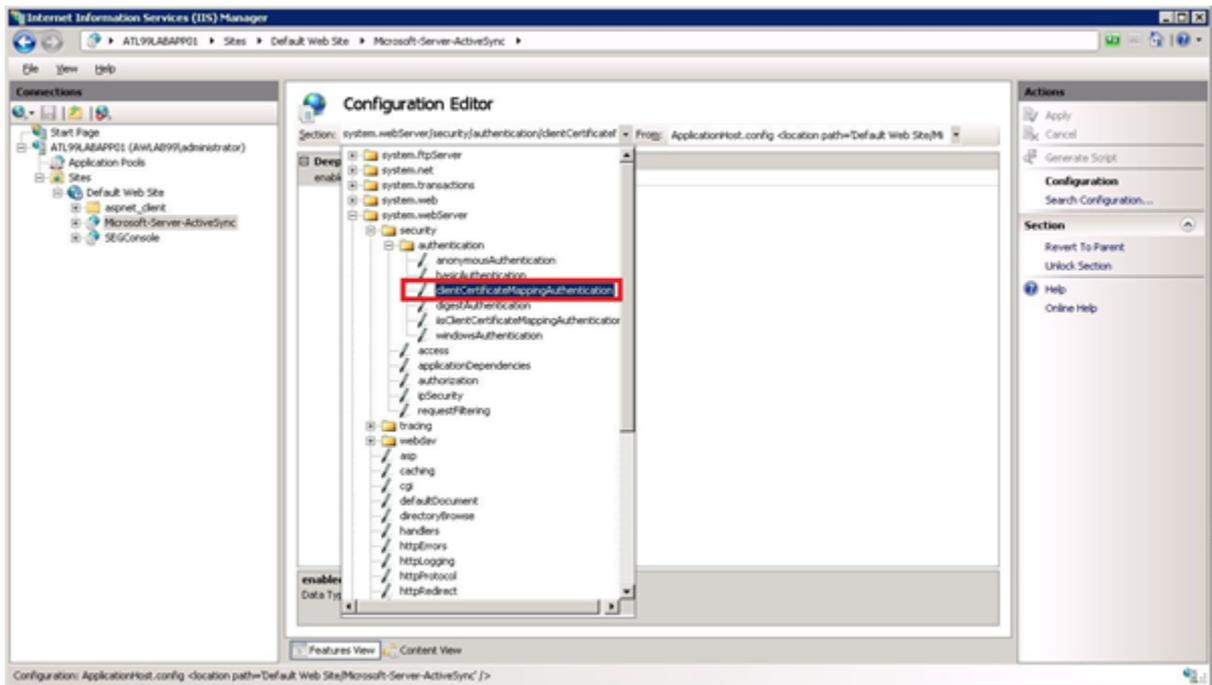
- 6 Once the above step is complete, restart the IIS Admin service from the Services console.
Next, you must enable the client certificate in the Exchange Management Console.
- 7 In the Exchange Management Console, expand **Server Configuration** and then select the Client Access Server that you want to configure.
- 8 On the **Exchange ActiveSync** tab, right-click the Microsoft-Server-ActiveSync directory and choose **Properties**.
- 9 On the **Authentication** tab, clear the **Basic authentication (password is sent in clear text)** checkbox and select the option **Require client certificates**.
Next, you must enable client certificate mapping authentication.
- 10 Click the **+** sign to expand the **Sites** folder.
- 11 Click the **+** sign to expand the **Default Web Site** and display the email sever you want to configure.
 - a If you are using MS Server 2008 R2 or later, the **Configuration Editor** icon appears as shown in the screen below. This icon does not appear in older versions of MS Server. Select **Microsoft-Server-ActiveSync** and double-click the **Configuration Editor** icon. Skip step b & c, and go to step 3.

- b If you are using Exchange ActiveSync (EAS) 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.

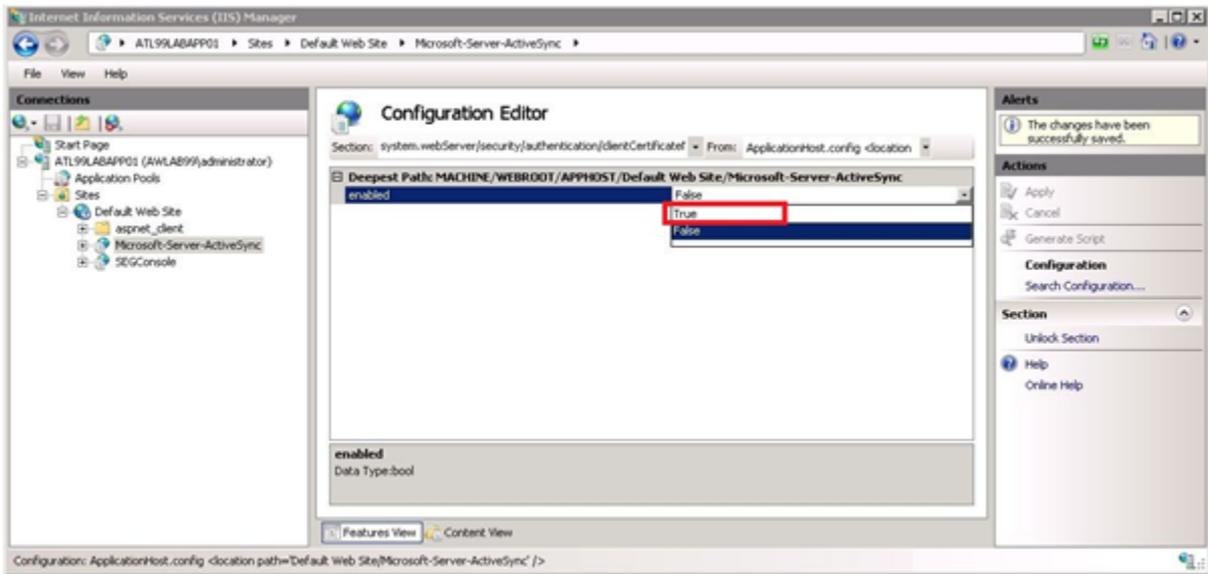
```
appcmd.exe set config Microsoft-Server-ActiveSync -  
section:system.webServer/security/authentication/clientCertificateMappingAuth  
entication /enabled:True /commit:apphost
```

12 In the **Section** drop-down, navigate to **system.webserver/security/authentication**.

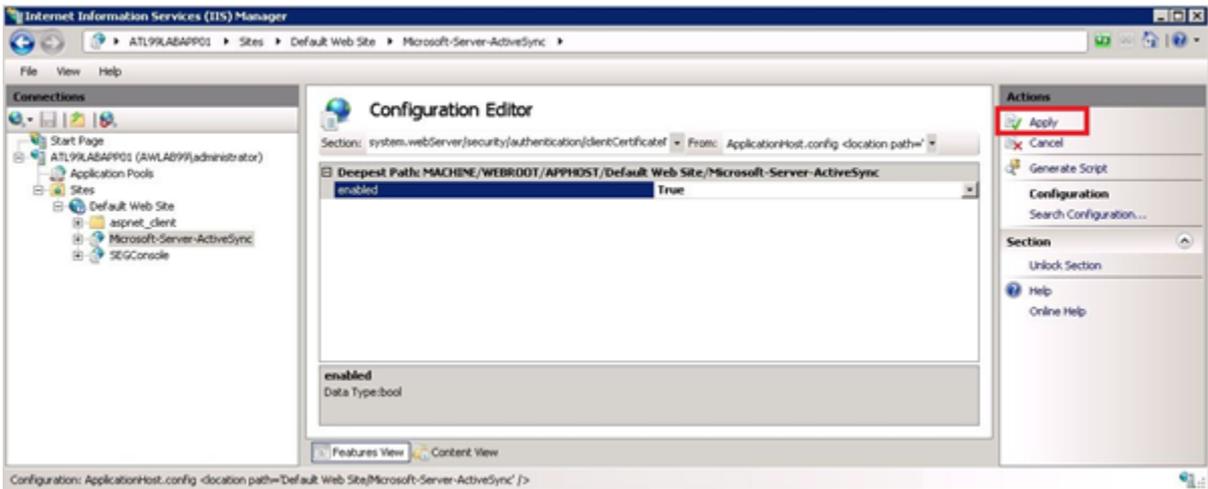
13 Select **clientCertificateMappingAuthentication**.



14 On the **Enabled** option, select **True** from the drop-down box.

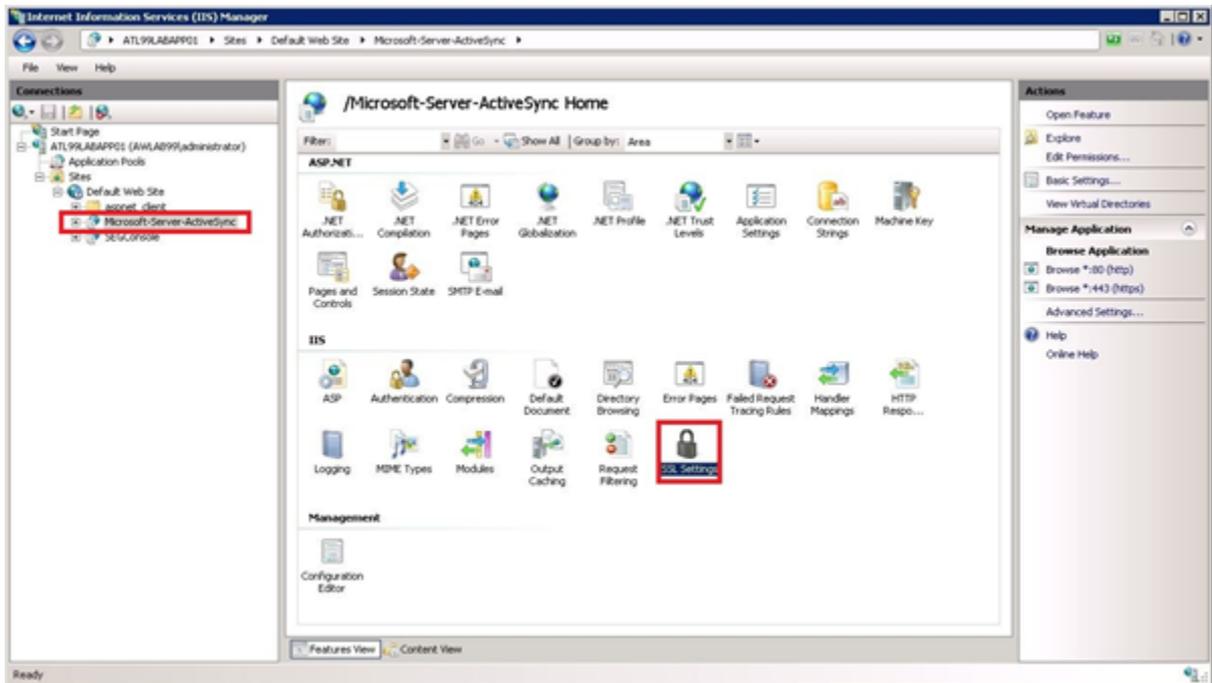


15 In the right-hand pane, select **Apply**.



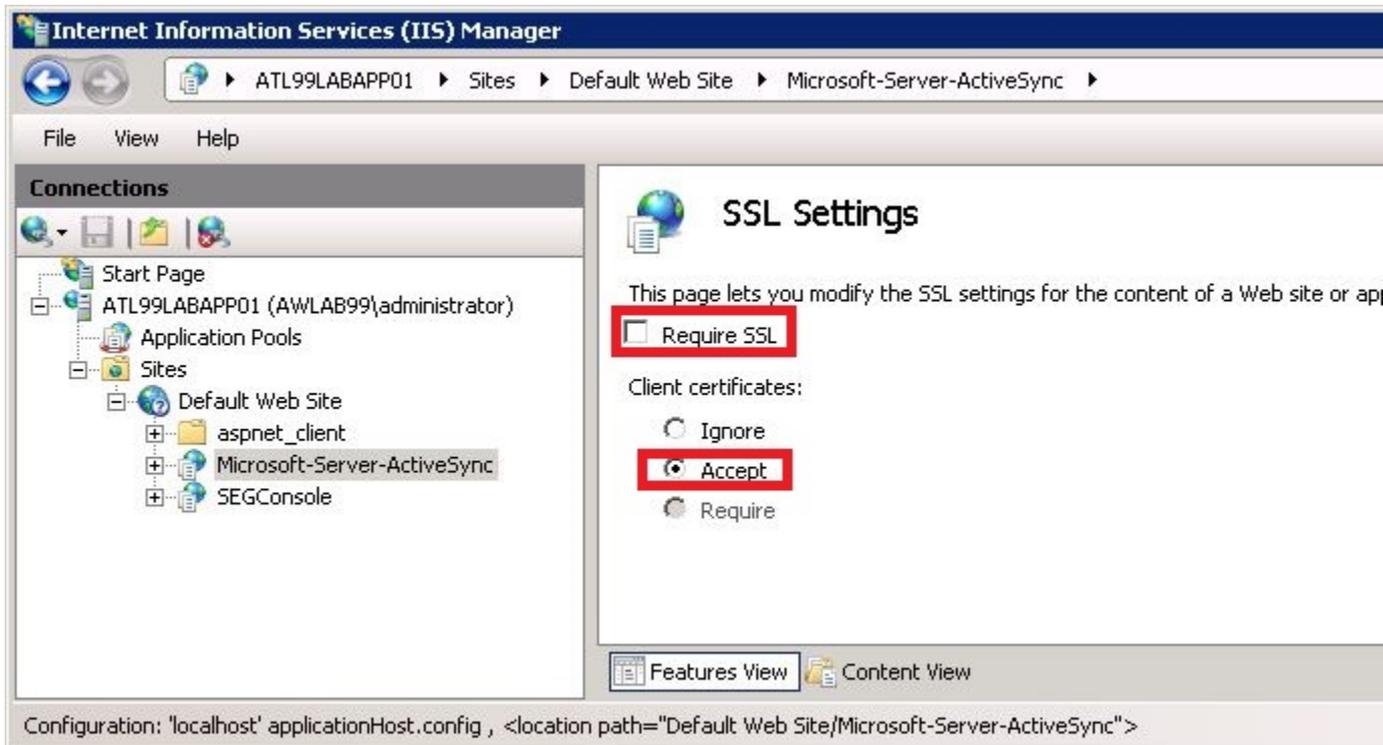
If only certificate authentication is being used then you must configure Secure Socket Layer (SSL). Otherwise, if authentication other than certificates is used then you do not need to configure SSL.

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



17 If only certificate authentication is allowed, then select **Require SSL** and select **Required**. If other types of authentication are allowed, select **Accept**.

18 In the right-hand pane, select **Apply**.



Next, you must adjust the `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.

- 19 Open a command prompt by selecting **Start > Run**.
- 20 Type `cmd` and select **OK**. A text editor window appears.
- 21 Increase the value of the `uploadReadAheadSize` from the default of 48KB to 10MB by entering 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 Web Site -
section:system.webServer/serverRuntime /uploadReadAheadSize:
10485760 /commit:apphost
```

The 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.

- 22 Type the following command to reset the IIS.

```
iisreset
```

Configure IIS for Certificate Authentication with SEG, EAS with SEG and TMG

As mentioned previously, whenever a SEG is inserted between the TMG and EAS servers, IIS is no longer configured on the EAS server, it is configured on the SEG server.

The procedure for configuring IIS is exactly the same no matter where IIS resides. For that reason, rather than duplicate the same procedure in [Configure IIS for Certificate Authentication with TMG, EAS with SEG and TMG](#), go back to that section and whenever it mentions performing a step on the EAS server, replace that reference to the EAS server with the SEG server.

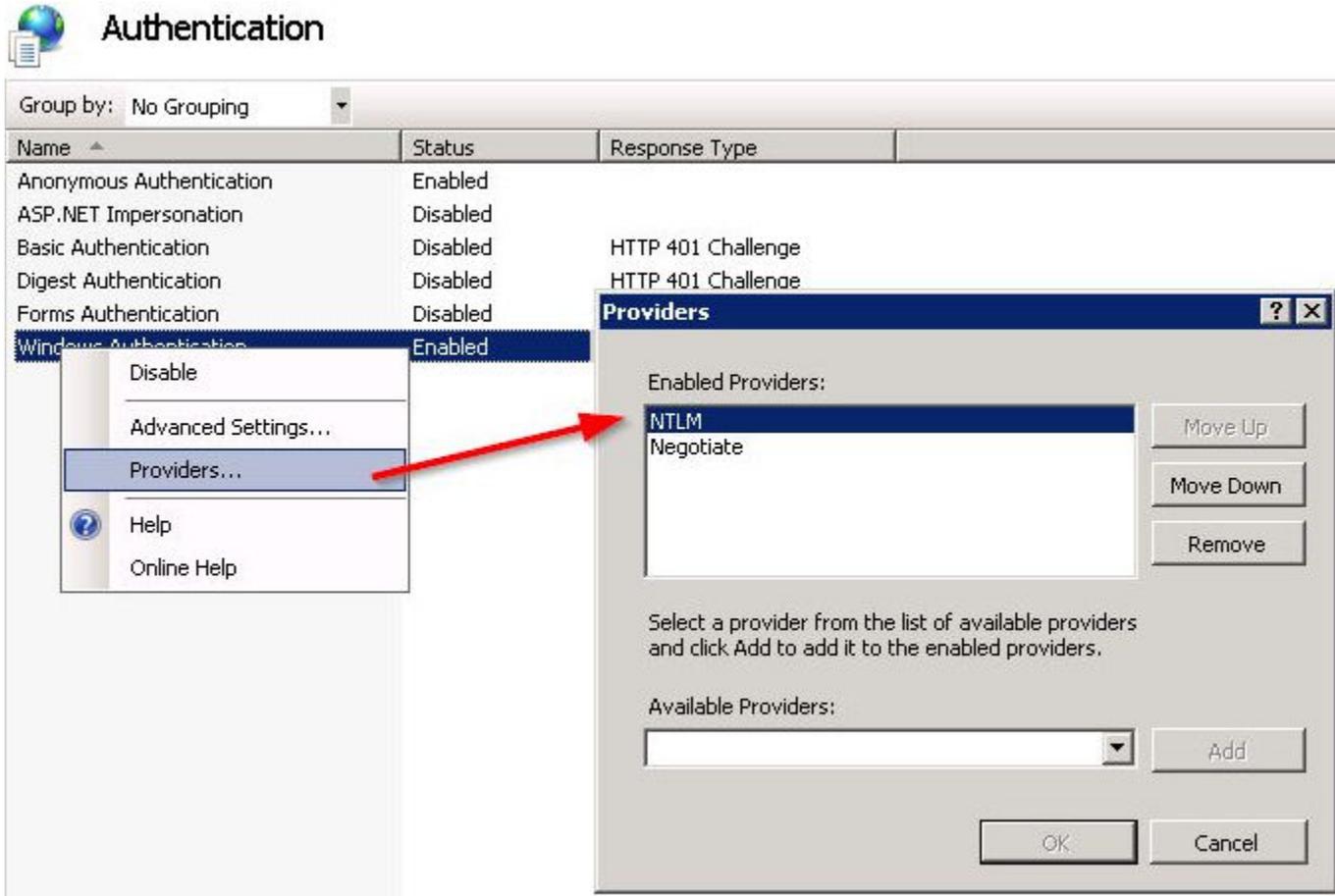
Troubleshooting for EAS with SEG and TMG

You can confirm that the SEG is performing certificate authentication by pushing a user's profile to the device and testing whether or not the device is able to connect and sync with the configured SEG endpoint.

If the device does not connect and displays a message that the certificate cannot be authenticated or the account cannot connect to EAS, then the problem is related to the configuration.

Make sure that a certificate is being issued by the CA to the device by checking the following information.

- If Exchange server returns a 401, add **NTLM** and **Negotiate** as providers to **Windows Authentication**.



- Go to the internal CA Server, launch the certification authority application, and browse to the issued certificates section.
- Find the last certificate that was issued and it should have a subject that matches the one created in the certificate template section earlier in this documentation.

If there is no certificate, then there is an issue with the CA, client access server (e.g., SCEP), or with the Workspace ONE UEM connection to client access server.

- Check that the permissions of the client access server (e.g., SCEP) Admin Account are applied correctly to the CA, and the template on the CA.
- Check that the account information is entered correctly in the Workspace ONE UEM configuration.
- Verify the **Server URL** and the **SCEP Challenge URL** contain the correct information and end with a /.
- Launch a browser and enter the **SCEP Challenge URL**. The website should prompt you for credentials. After entering the SCEP Admin Account username and password, it should return with the challenge passphrase.

- If the certificate is being issued, make sure that it is in the Profile Payload and on the device.
 - Navigate to **Devices > Profiles > List View**. Click the action icon for the device and select `</>` View XML to view the profile XML. There is certificate information that appears as a large section of text in the payload.
 - On the device, go to the profiles list, select details and see if the certificate is present.
 - Confirm that the certificate contains the **Subject Alternative Name** (or SAN) section and that in 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.
 - Confirm that the certificate contains the **Client Authentication** in the **Enhanced Key Usage** section. If this is 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 SEG server.
 - Confirm that the address of the SEG server is correct in the Workspace ONE UEM profile and that all the security settings have been adjusted for allowing certificate authentication on the SEG server.
- A very good test to run is to manually configure a single device to connect to the SEG/EAS server using certificate authentication. This should work outside of Workspace ONE UEM and until this works properly, Workspace ONE UEM cannot configure a device to connect to EAS with a certificate.
 - Refer to the External References and Documents section for a link to a step by step guide for configuring a device to connect to EAS using a certificate.
 - If you are adding a SEG to an existing TMG to EAS configuration (i.e., TMG to SEG to EAS), make sure the web publishing rule is no longer configured to publish Exchange Client Access traffic to the EAS server before configuring it to publish to the SEG server.
 - If you are adding a SEG to an existing TMG to EAS configuration (i.e., TMG to SEG to EAS), make sure the TMG is no longer configured to perform certificate authentication before you configure the SEG to handle certificate authentication.
 - If none of the steps above resolve the problem, try authenticating independent of Workspace ONE UEM. This is done by eliminating the Workspace ONE UEM (e.g., SEG) and only using a certificate to authenticate the device. If this doesn't work then there are other problems occurring. Until those problems are resolved, you will not be able to use the SEG to handle certificate authentication.
 - If you cannot authenticate, verify the clocks on the SEG and Kerberos. Kerberos produces a ticket for the SEG to authenticate the user on the mail server. The timestamp on that ticket must be no more than five minutes apart from the SEG's time clock. Verify the time clock on the SEG and Kerberos are within five minutes apart. You also might want to consider the use of Network Time Protocol daemons to keep all time clocks synchronized.

- If you cannot authenticate, evaluate your network. If you only have one Kerberos server configured, it is possible the server is not operational. Without it, no one can log in. To stop this from occurring, you might consider using multiple Kerberos servers and fallback authentication mechanisms.