VMware AirWatch Certificate Authentication for EAS with SEG and TMG

For VMware AirWatch

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

Table of Contents

Chapter 1:
Exchange ActiveSync with Secure Email Gateway and Threat Management Gateway

The implementation of certificate distribution through Workspace ONE UEM allows for the authentication of devices through client authentication certificates.

Utilizing certificate authentication eliminates the need for the device user to supply user credentials to authenticate for email access.

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 document 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.

System Requirements for EAS with SEG and TMG

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

- 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: 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.

For TMG to EAS

- 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.

For TMG to SEG to EAS

- 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.

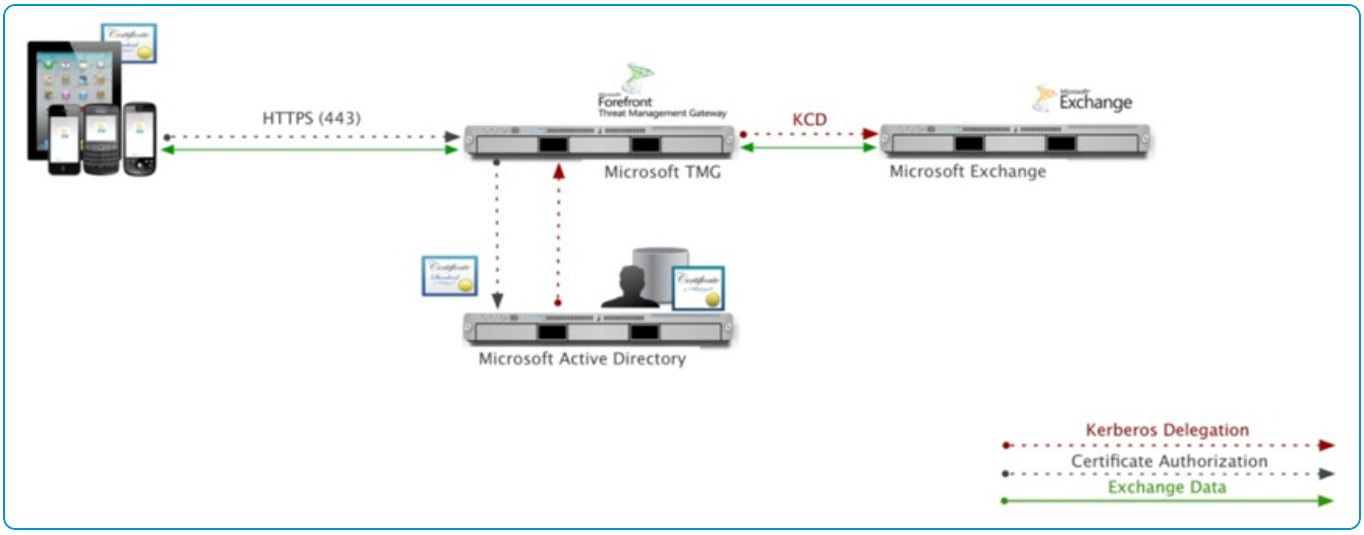
The first diagram shows the connection through the Microsoft TMG and the second diagram shows the same as the first with the addition of the Workspace ONE UEM Secure Email Gateway (SEG).

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.

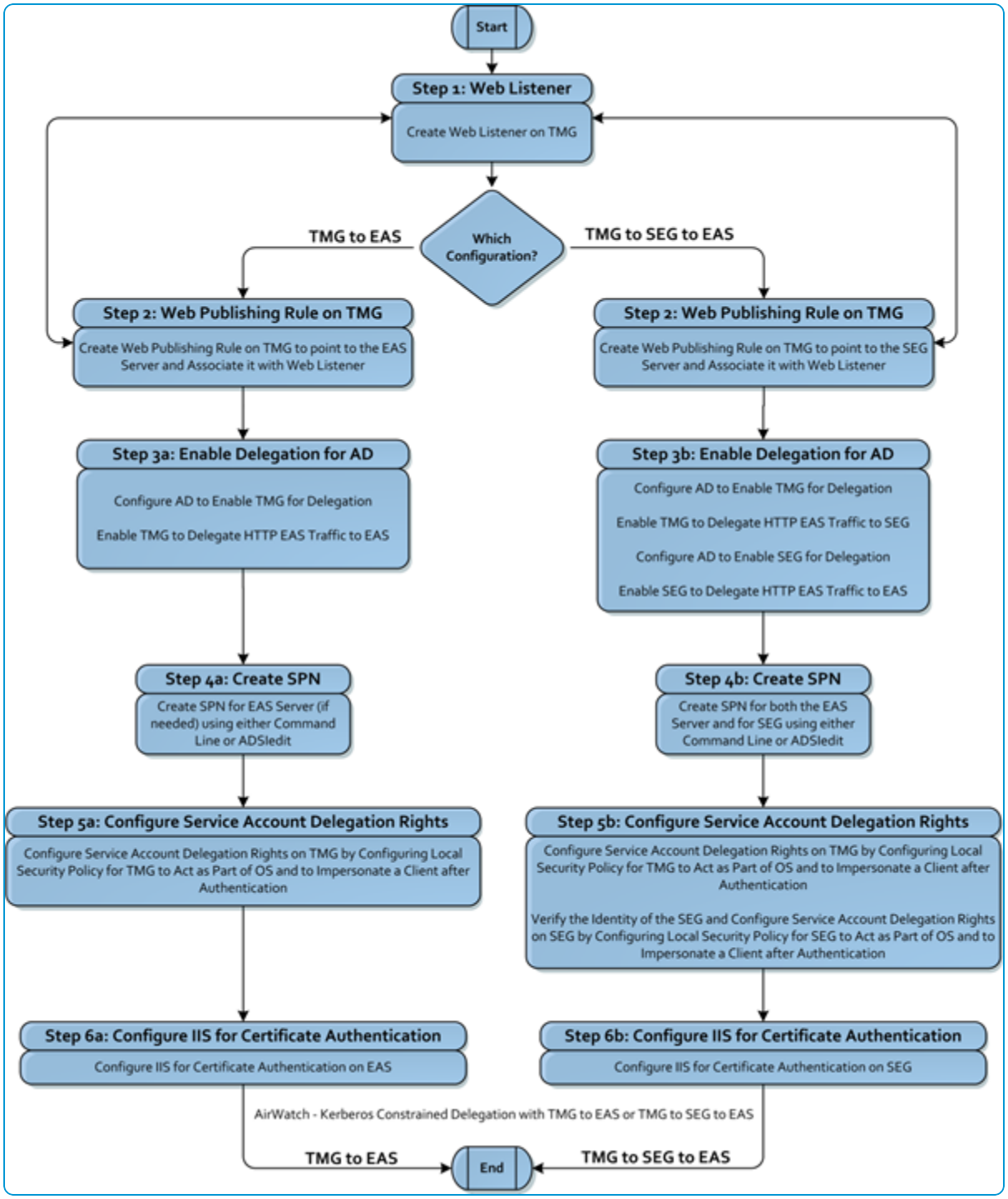
This is accomplished by authenticating that user and their device with a certificate. Regardless of the enterprise email server being used, the methodology of certificate authentication is basically the same.

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 on page 8 or Configure TMG to SEG to EAS Server on page 9.

Step 1: Create a Web Listener on the TMG

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

Step 2: Create a Web Publishing Rule on TMG to Publish Traffic to EAS or SEG

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. 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 Configure TMG to SEG to EAS Server on page 9

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.

Step 3a: Enable Delegation from Active Directory when using a TMG

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

Step 4a: Create a Service Principal Name (SPN) for 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.

Step 5a: Configure Service Account Delegation Rights on TMG

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

Step 6a: Configure IIS for Certificate Authentication with TMG

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 in Configure TMG to EAS Server on page 8 with the addition of the following steps (3b through 6b) that are related to adding a SEG between the TMG and EAS servers.

Step 3b: Enable Delegation from Active Directory when using a SEG

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

Step 4b: Create a Service Principal Name (SPN) for the SEG

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

Step 5b: Configure Service Account Delegation Rights on SEG

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

Step 6b: Configure IIS for Certificate Authentication with SEG

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

Chapter 2:
Install, Set Up, Configure Certificate

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

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, see the topic entitled **Create a Web Publishing Rule on TMG to Publish Traffic to EAS or SEG** on the following page.

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 the previous topic **Create a Web Listener on the 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**.
22. Click **Next**.

    Note: This is selected to make sure only users with the appropriate credentials are allowed to access.

    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, proceed to **Enable Delegation from Active Directory when using a TMG**.

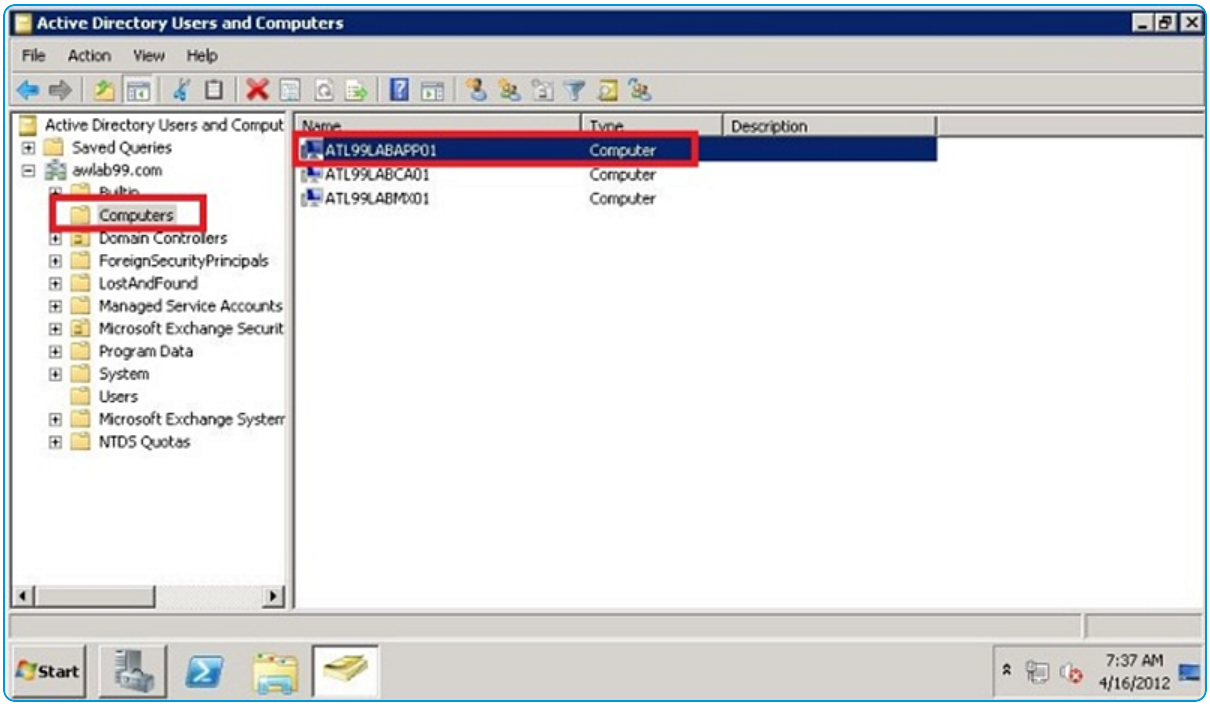
Enable Delegation from Active Directory when using a TMG, EAS with SEG and TMG

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.

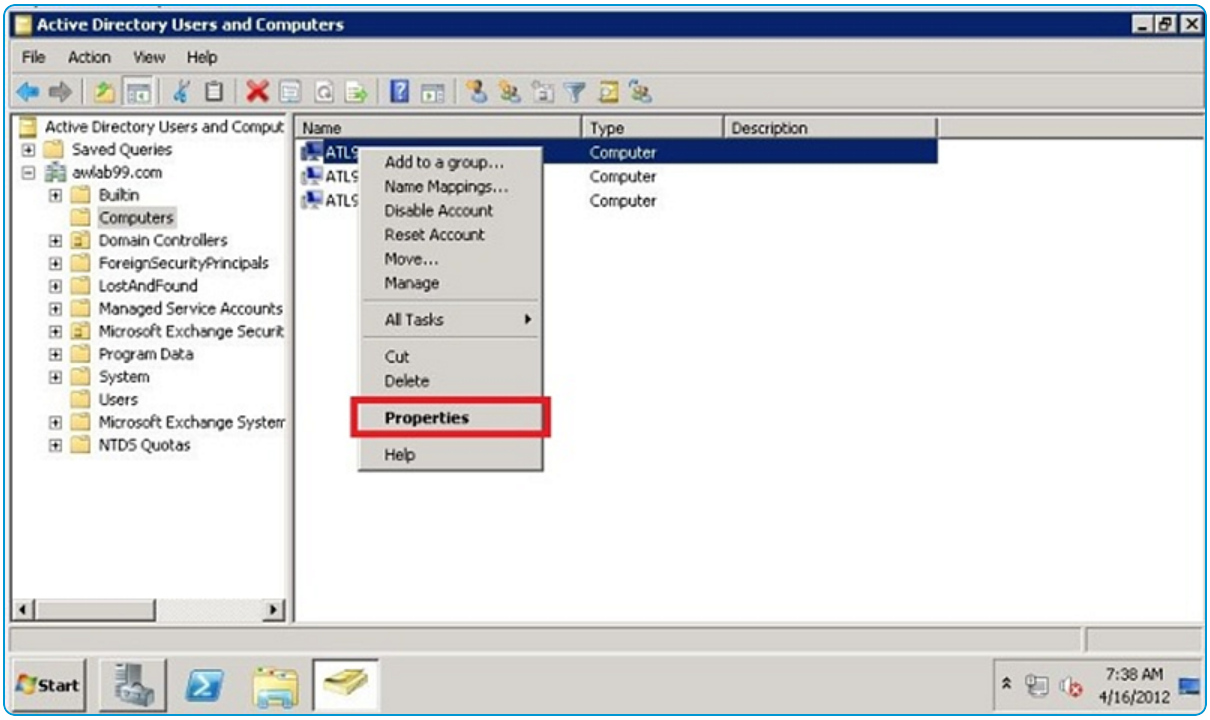
This step must be completed whether or not you are employing the use of a Secure Email Gateway (SEG). There are instructions at the end of this topic that direct you to the next step, SEG or no SEG.

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.



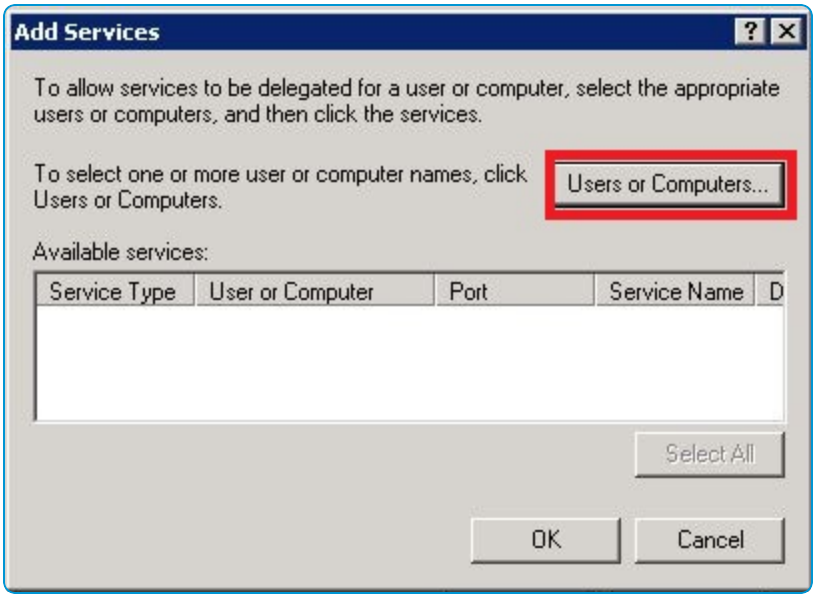
3. Right-click the TMG server name and select **Properties**. The **Properties** window for the TMG server displays.



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.

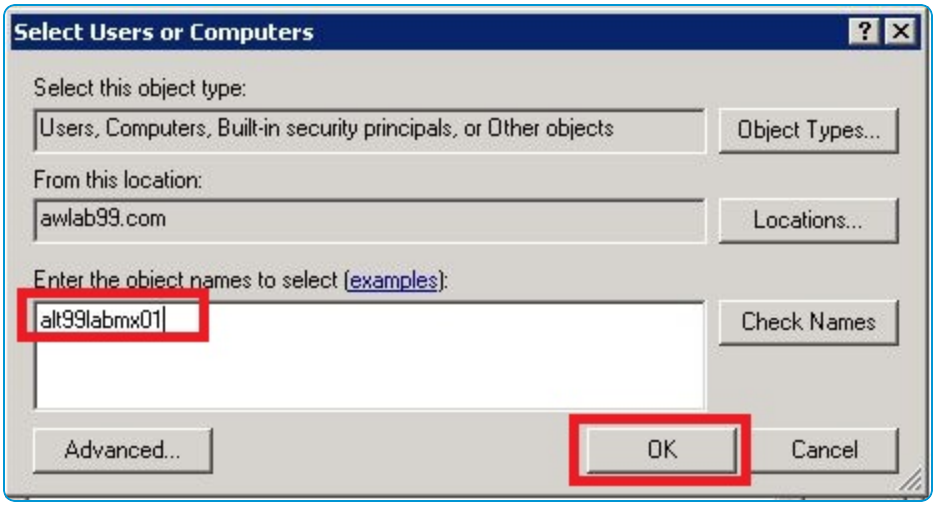
Next, you must enable the TMG to delegate HTTP EAS traffic to the EAS server.

8. Click **Users or Computers**



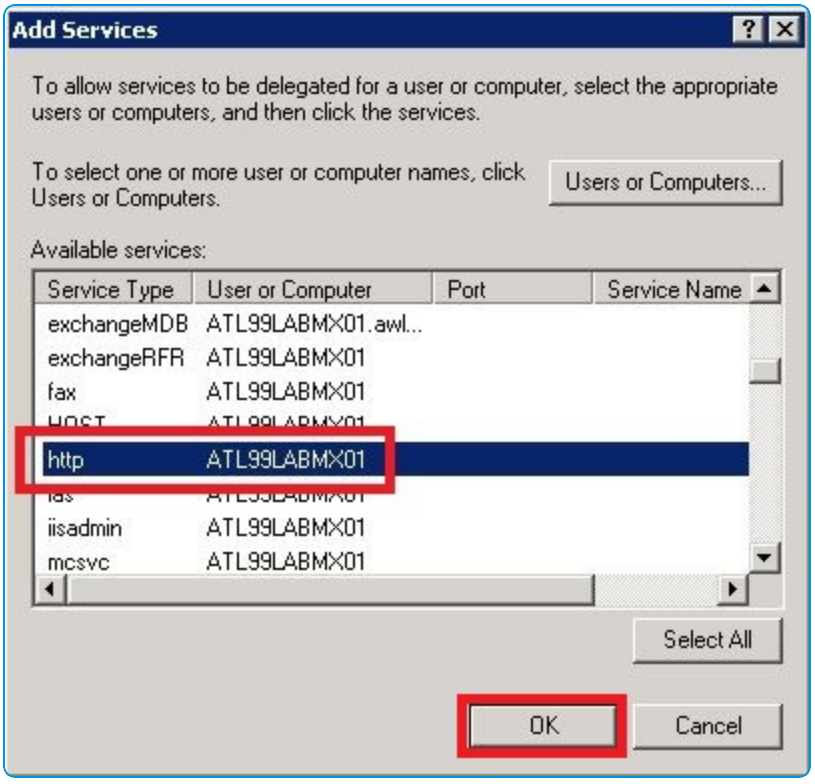
9. The **Select Users or Computers** window displays. Enter the name of the EAS server.

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 employing the use of a SEG, then skip ahead to the topic **Create a Service Principal Name (SPN) for the EAS Server**. Otherwise, proceed to **Enable Delegation from Active Directory when using a SEG**.

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 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, see **Create a Service Principal Name (SPN) for the EAS Server**.

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.

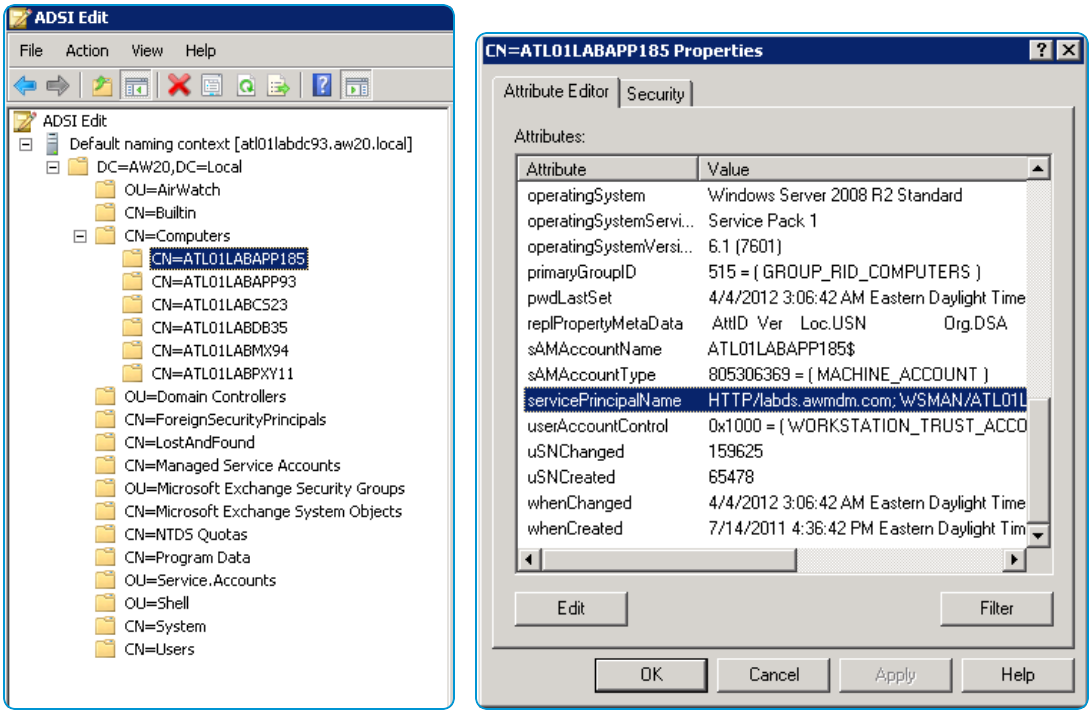
- Command line prompt.
- The ADSIedit module.

From the Command Line

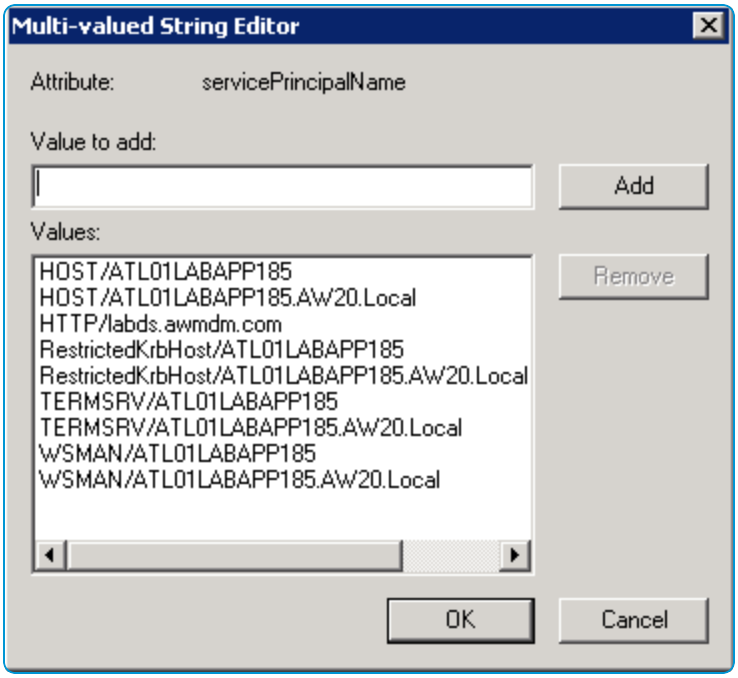
```
Setspn –A http/<internaladdress> domain/computeraccountname
```

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.
8. 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.



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



11. 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 ahead to the topic **Configure Service Account Delegation Rights on TMG**. Otherwise, see **Create a Service Principal Name (SPN) for the SEG**.

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 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**.

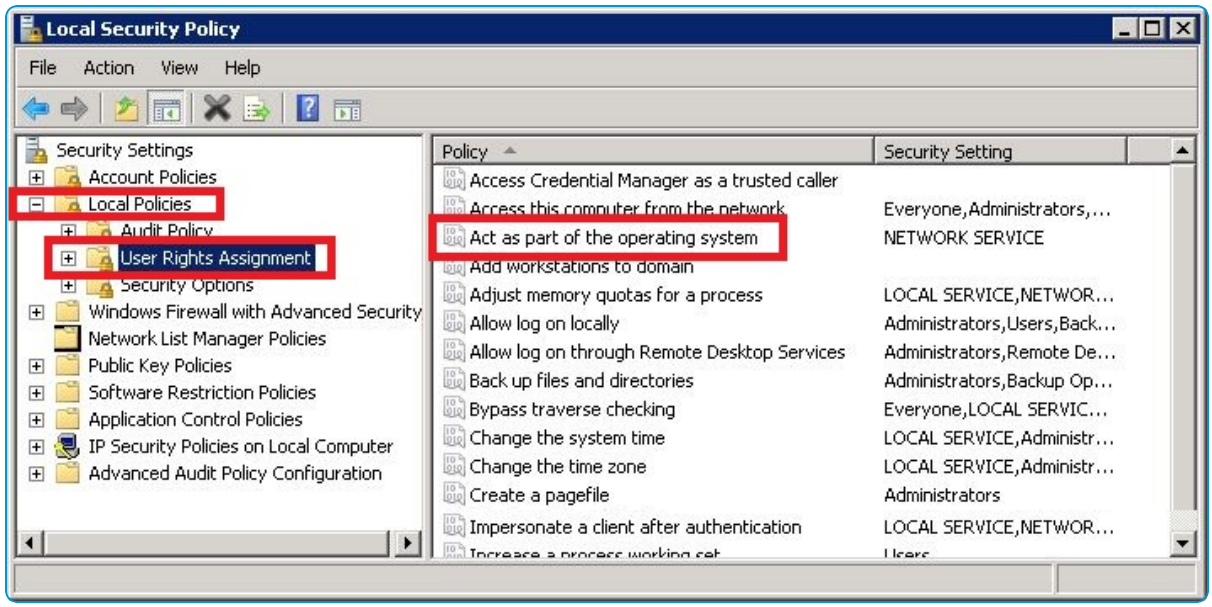
Configure Service Account Delegation Rights on TMG, EAS with SEG and TMG

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.

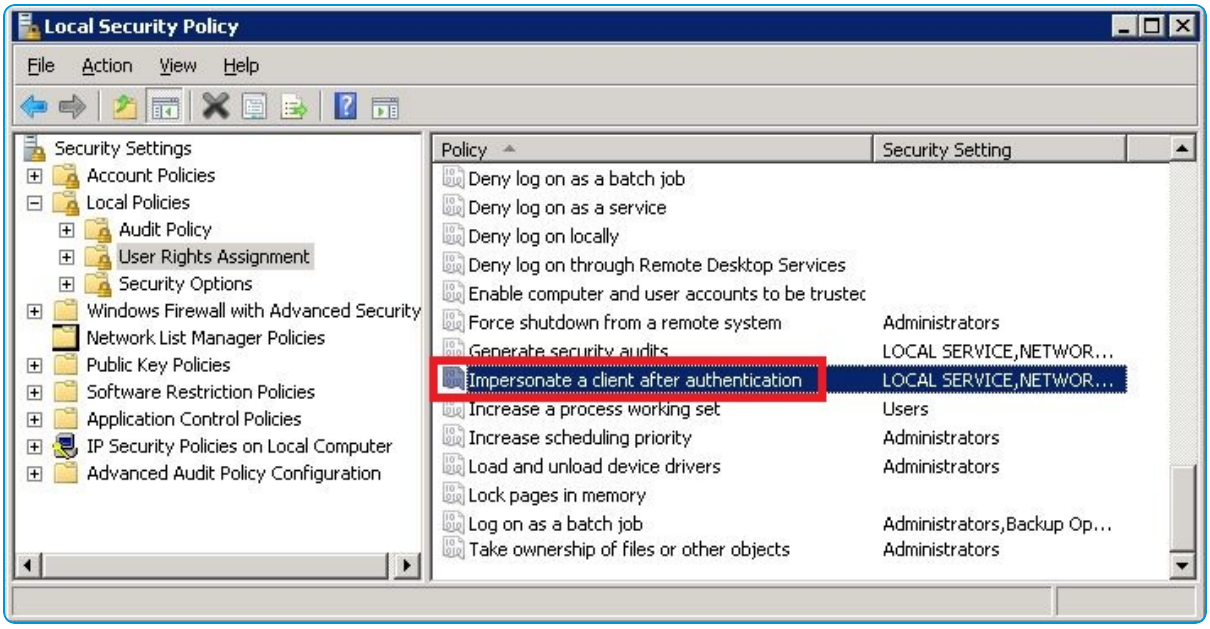
First, you must configure the local security policy for TMG to act as part of the operating system.

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

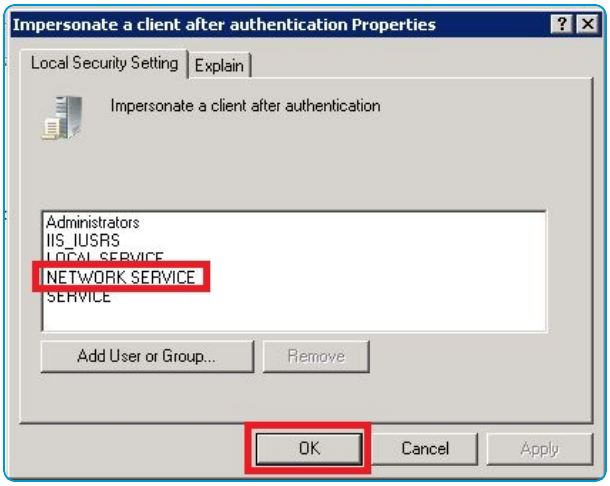


6. Click **Add User or Group**.
7. Type the name of the Service Account attached to the Application Pool. The name must be the same as the name associated to the TMG (i.e., Network Service).
8. Click **OK**. The **Local Security Policy** window displays.

   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 TMG**. Otherwise, proceed to **Create a Service Principal Name (SPN) for the SEG**.

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** and replacing all references to TMG with SEG.

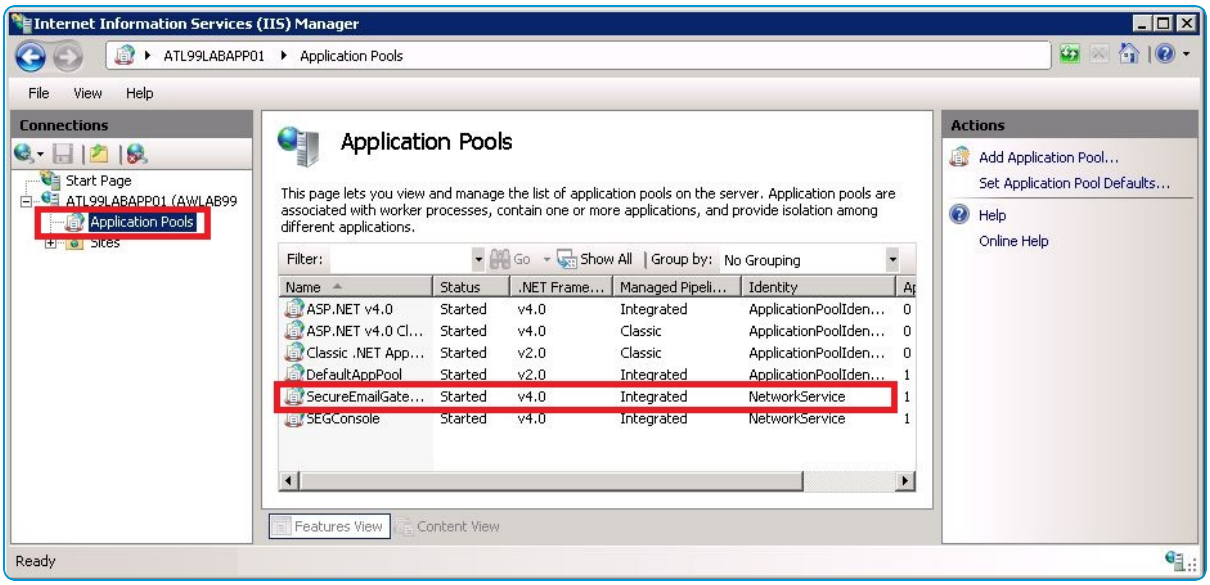
The final result is you should have completed the following.

- 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**.

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

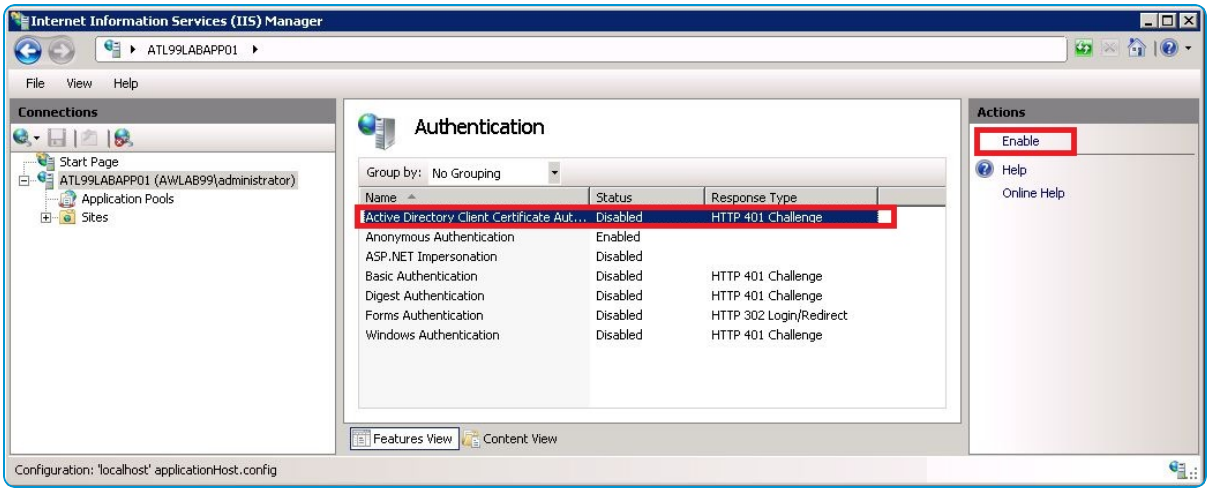
In order to authenticate the user's device that is assigned to a particular certificate, **Internet Information Services (IIS)** must be configured to accept that certificate. For the configurations shown in this document, IIS can only be configured on either a SEG or EAS server. Where IIS resides is 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 see the topic **Configure IIS for Certificate Authentication with SEG**.

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.

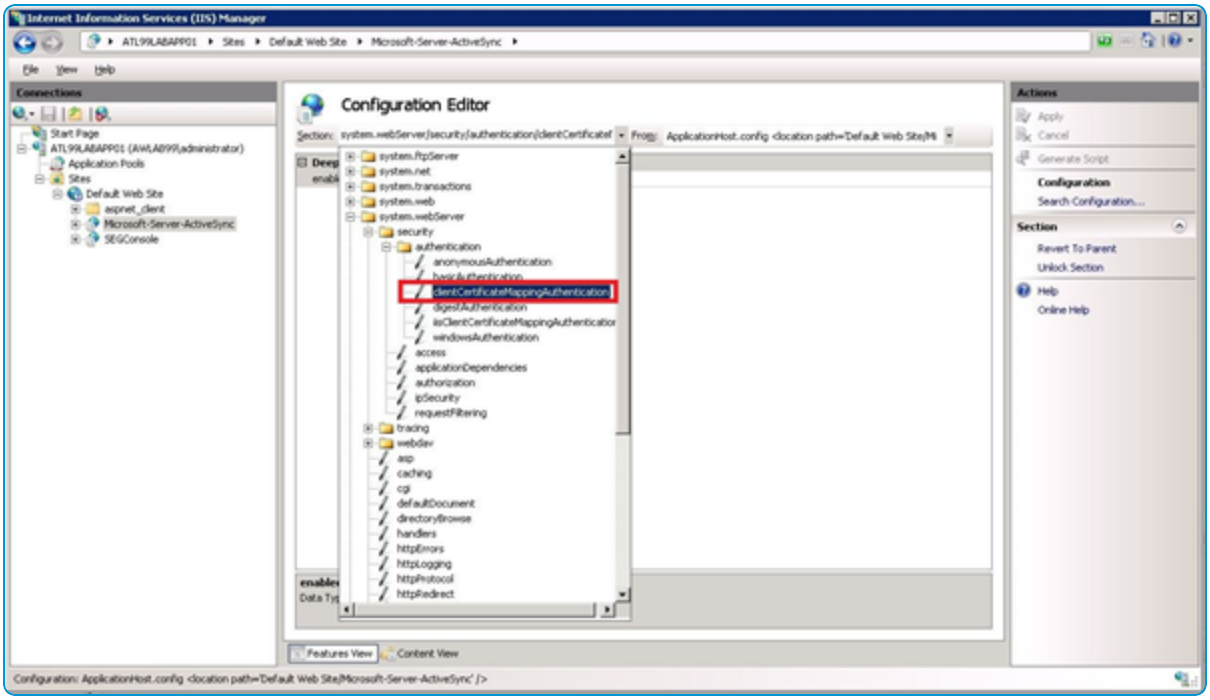
    b. If you are using Exchange ActiveSync (EAS) servers older than 2008 R2, you need to be familiar with the use of **appcmd.exe** and run it from the command prompt.

    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.

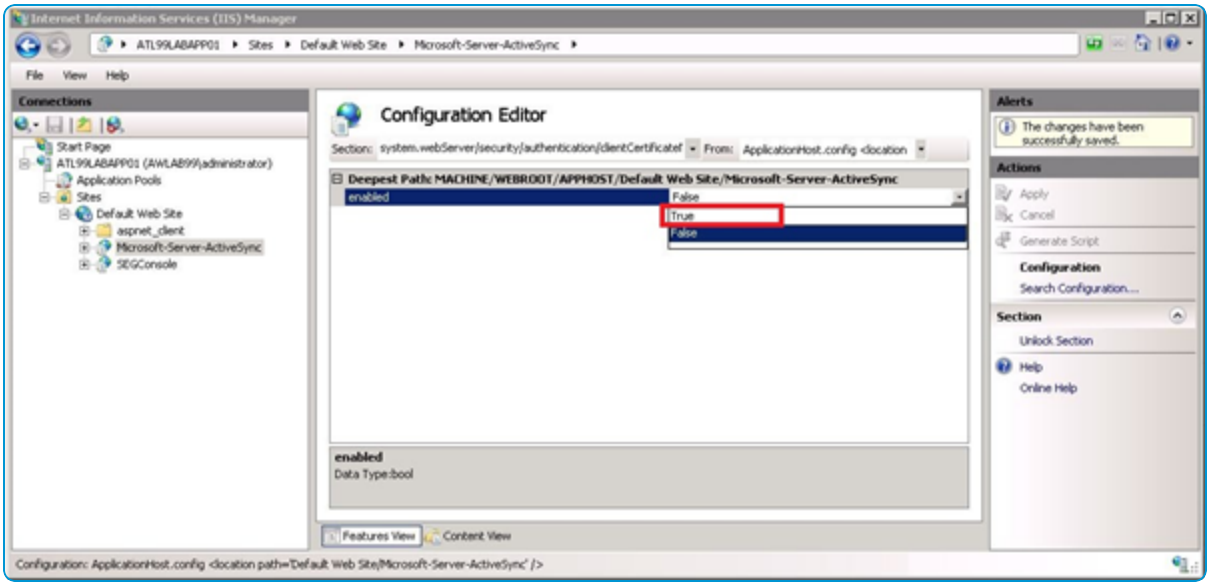
    ```
    appcmd.exe set config Microsoft-Server-ActiveSync -
    section:system.webServer/security/authentication/clientCertificateMappingA
    uthentication /enabled:True /commit:apphost
    ```

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

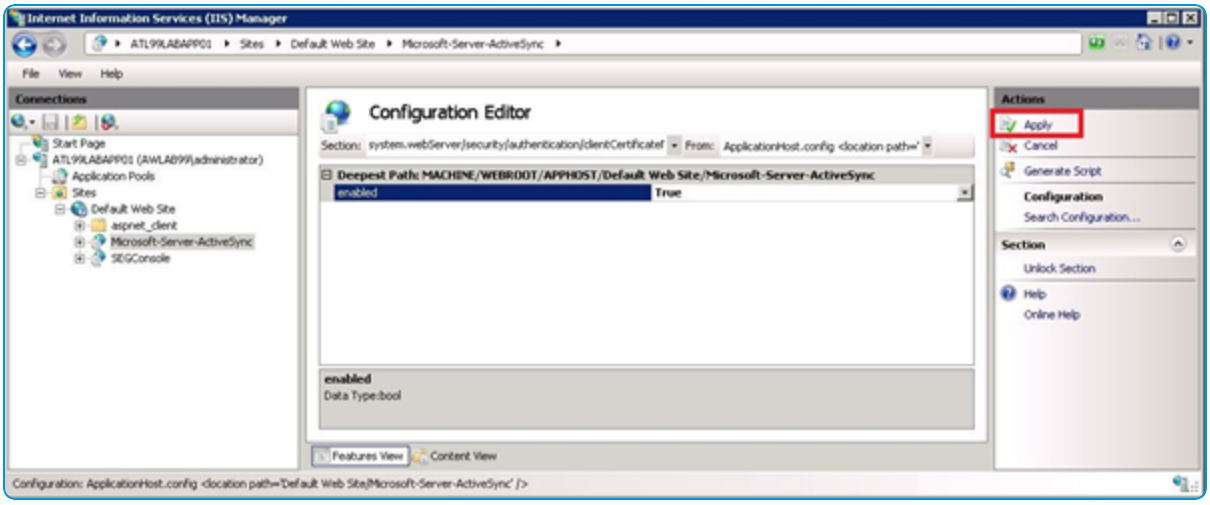
13. Select **clientCertificateMappingAuthentication**.



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

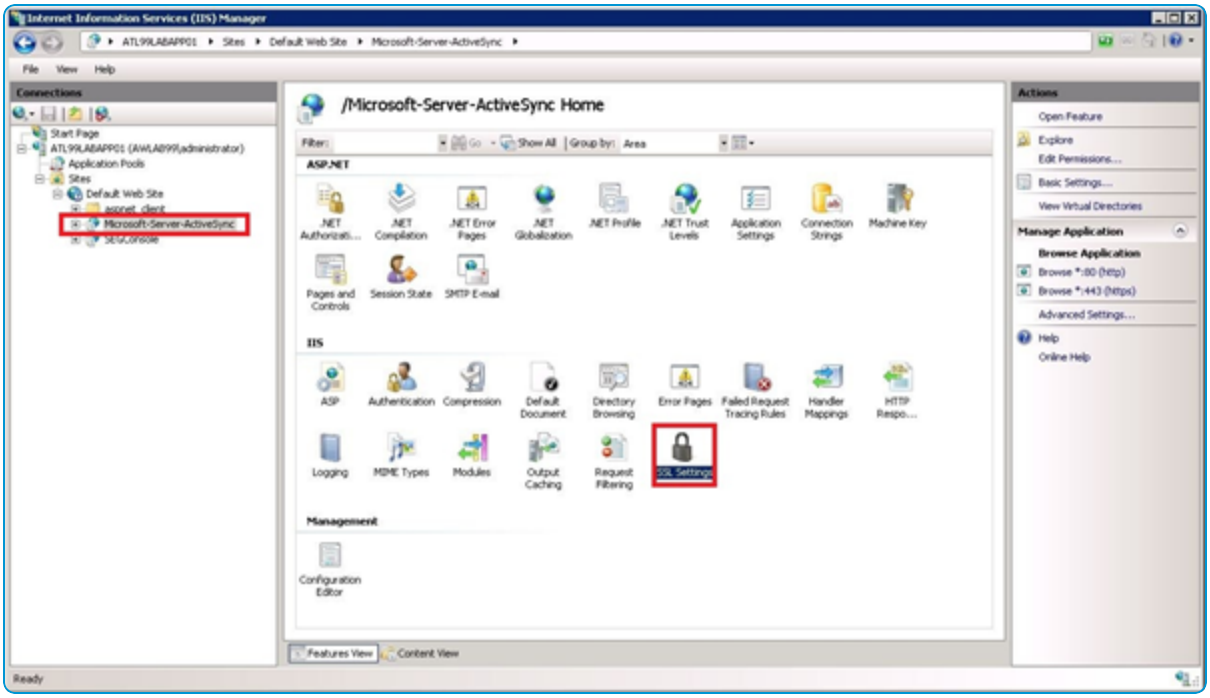


15. In the right-hand pane, select **Apply**.



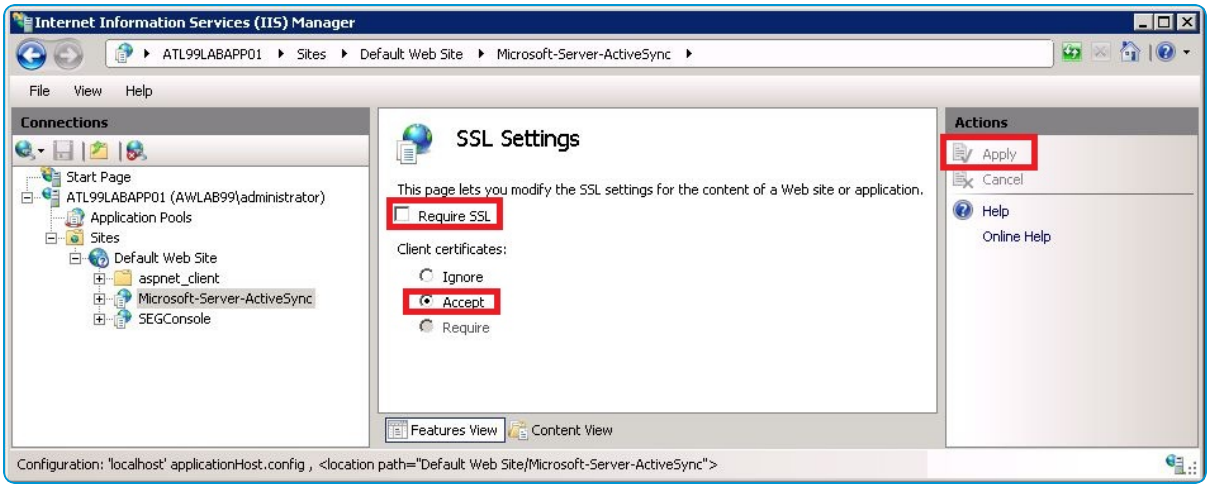
If only certificate authentication is being used then you must configure Secure Socket Layer (SSL). Otherwise, if authentication other than certificates is used then you do not need to configure SSL.

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, 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.

Chapter 3:
Troubleshooting for EAS with SEG and TMG

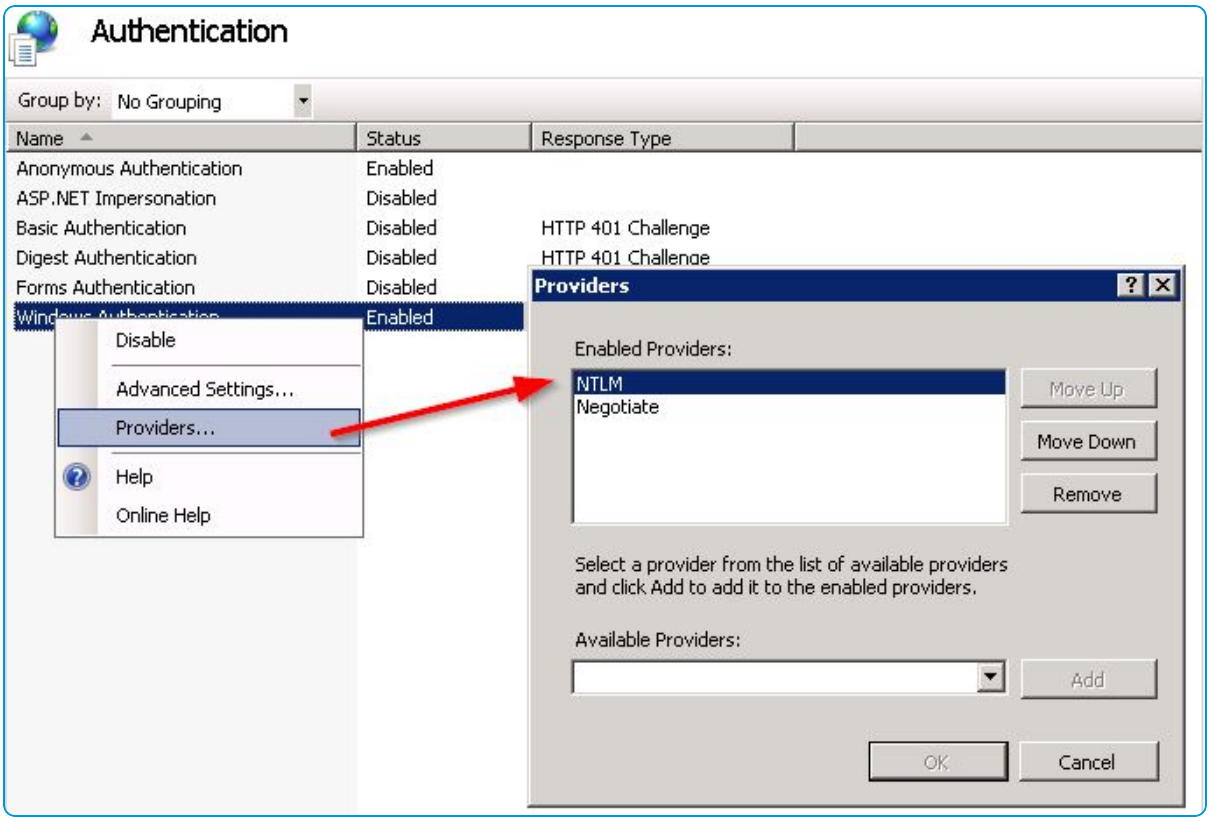
You can confirm that the SEG is performing certificate authentication by pushing a user's profile to the device and testing whether or not the device is able to connect and sync with the configured SEG end-point.

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.

Chapter 4:
Troubleshooting Checks

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 document.

  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 of 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.