

VMware AirWatch Certificate Authentication for EAS with SEG

For VMware AirWatch

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

Copyright © 2018 VMware, Inc. All rights reserved. This product is protected by copyright and intellectual property laws in the United States and other countries as well as by international treaties. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

Table of Contents

Chapter 1: Workspace ONE UEM Certificate Authentication for EAS with SEG	3
Prerequisites, EAS with SEG	3
Communications Flow, EAS with SEG	4
Implementation Methodology, EAS with SEG	5
Chapter 2: Install, Set Up, Configure Certificate	6
Step 1: Register Target Service, EAS with SEG	6
Step 2: Configure Delegation Settings on the SEG Server, EAS with SEG	8
Step 3: Enable EAS Server to Accept Kerberos Tickets, EAS with SEG	10
Step 4: Configure IIS for Certificate Authentication on the SEG, EAS with SEG	10
Step 5: Configure Delegation Rights on the SEG Service Account, EAS with SEG	15
Chapter 3: Troubleshooting, EAS with SEG	18
Troubleshooting Checks	18
Chapter 4: Additional SETSPN Commands, EAS with SEG	21
View SPN: SETSPN -l <computerName>	21
Add SPN: SETSPN -s <service>/<targetName> <computerName>	21
Remove SPN: SETSPN -d <service>/<targetName> <computerName>	21
Query for existing SPN: SETSPN -Q <service>/<targetName> <computerName>	22
Check for duplicate SPN in the entire forest: SETSPN -X	22
Chapter 5: Appendix	23
Install the Role in IIS, EAS with SEG	23

Chapter 1:

Workspace ONE UEM Certificate Authentication for EAS with SEG

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.

Prerequisites, EAS with SEG

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

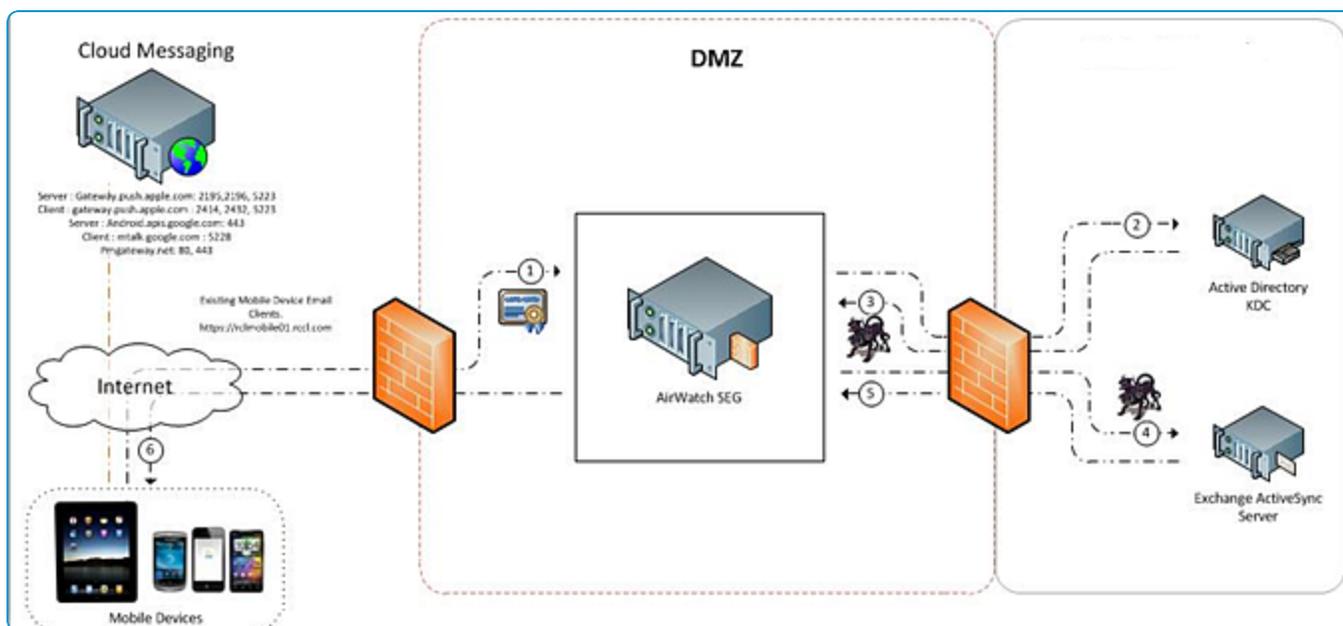
- An internal certificate authority (CA) server must be used to create user's certificates. An external CA cannot be used (e.g., VeriSign, etc.) to create user's certificates.
- Installed and operational Secure Email Gateway (SEG). For more information, see the **Workspace ONE UEM Secure Email Gateway 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

Chapter 2:

Install, Set Up, Configure Certificate

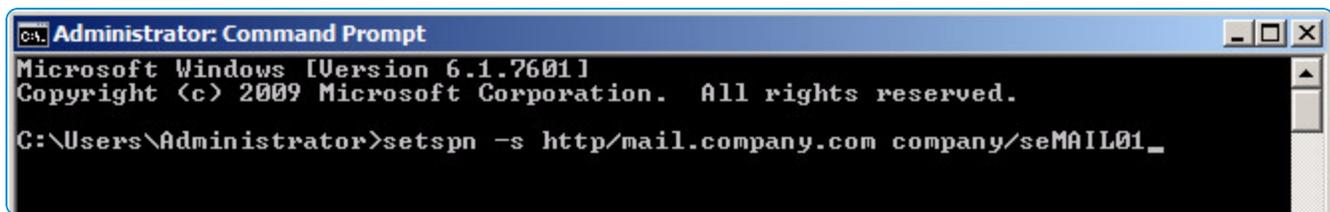
This section provides instructions to configure the certificate authority (CA) of your choice to work with the Workspace ONE™ UEM console. Take the following steps and procedures to integrate the certificate.

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.

Credential Name

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

Groups and Roles

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.

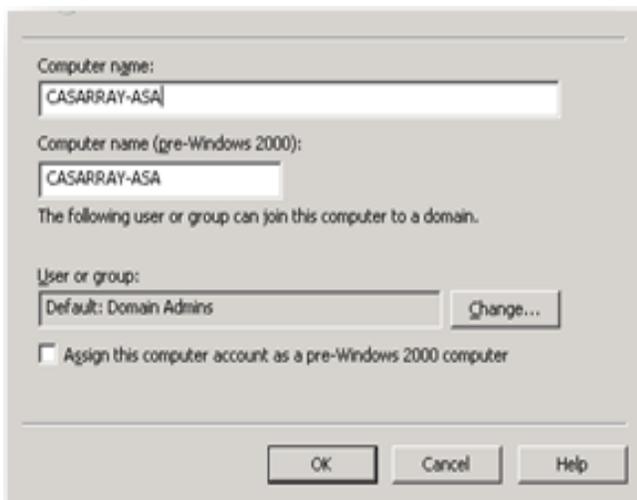
If you are deploying a user account for the ASA credential, this means that the account only needs to be a member of the Domain Users security group.

Password

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*
```

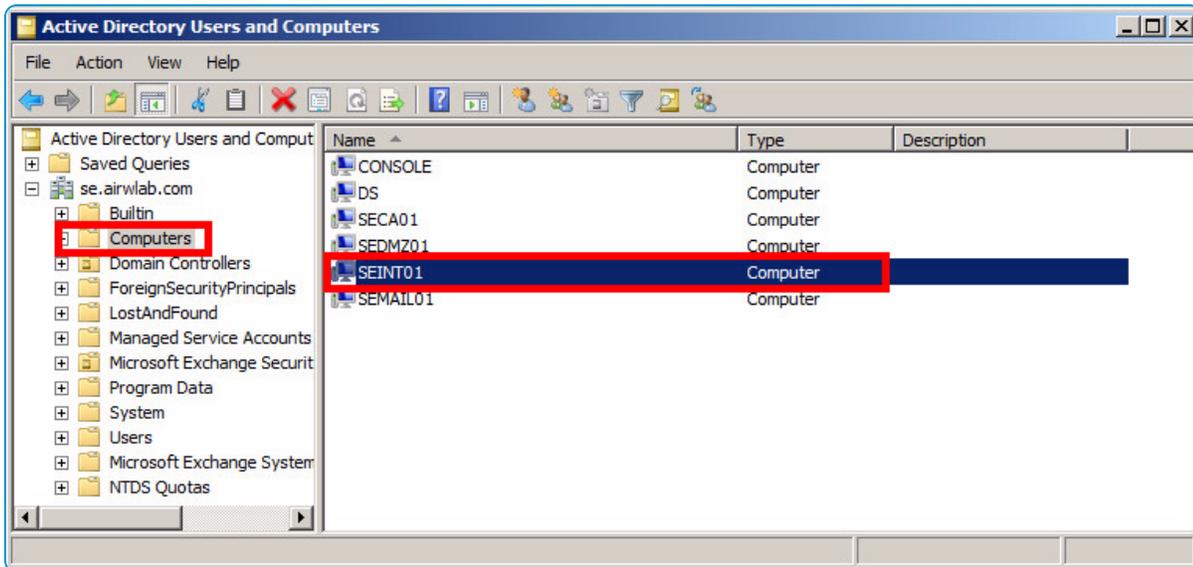
Next, you must **Configure Delegation Settings on the SEG Server**.

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

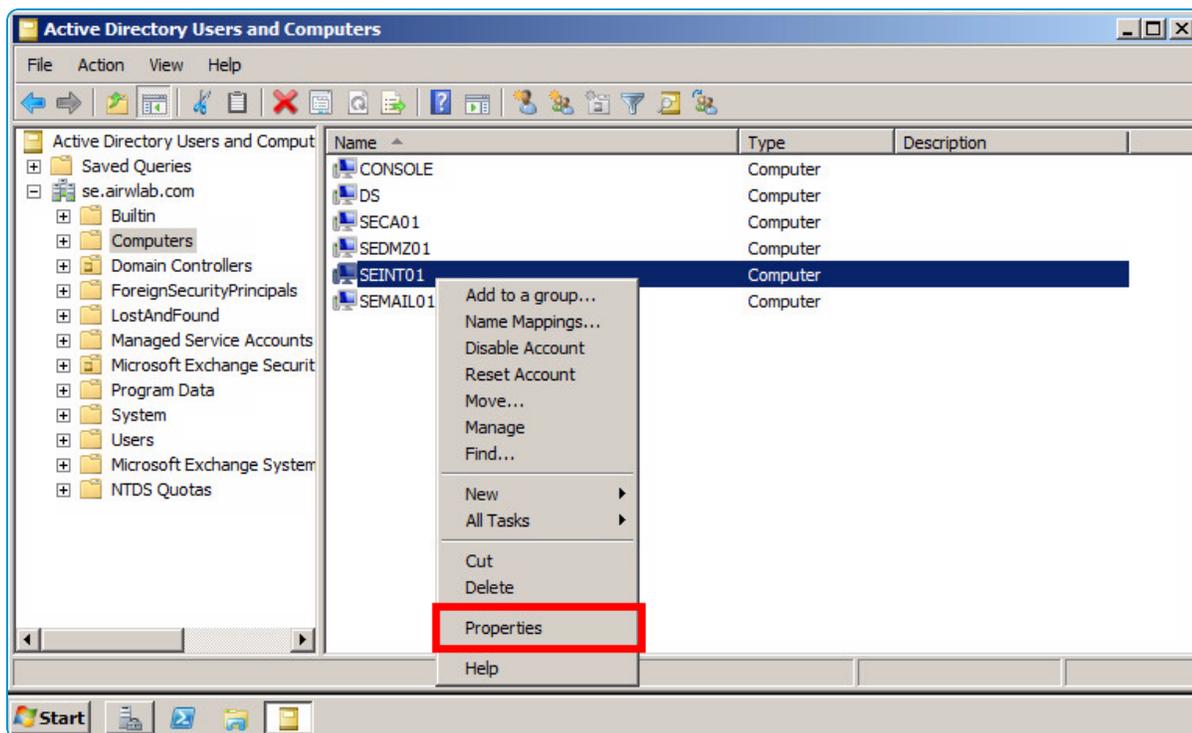
In order for the Secure Email Gateway (SEG) to impersonate a user when authenticating on an Exchange ActiveSync (EAS) server, the SEG server must be given the appropriate permissions in the Active Directory (AD) server. You must also enable SEG to delegate HTTP EAS traffic to the EAS server.

Configure AD to Give Permissions to SEG to Impersonate a User

1. Select **Active Directory Users** and **Computers** 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.



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



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

Enable SEG to delegate HTTP EAS traffic to the EAS server

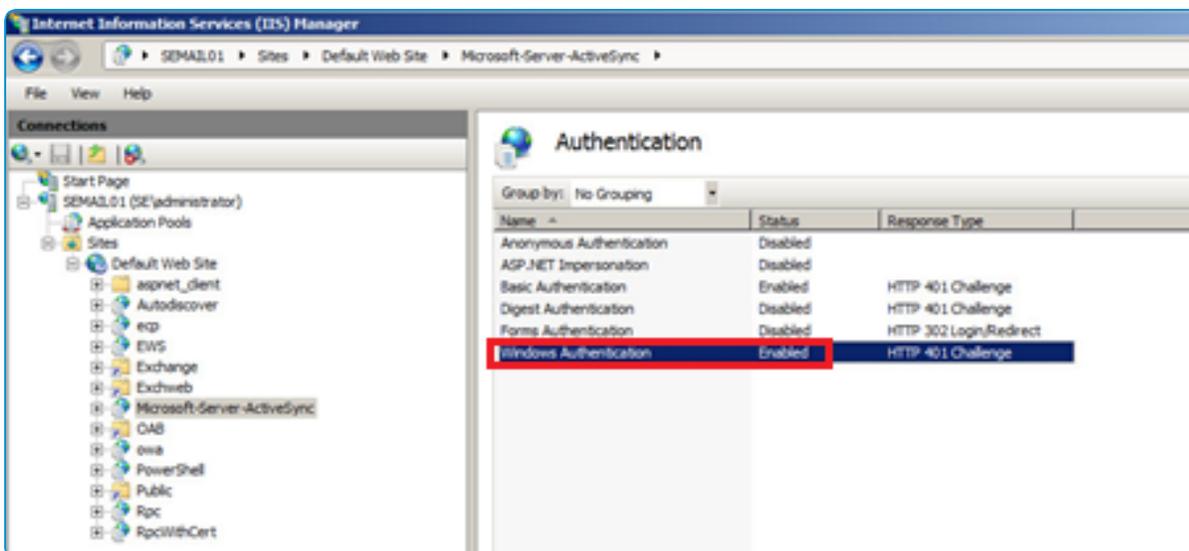
1. Click **Users or Computers** on the **Add Services** window. The **Select Users or Computers** window displays.
2. Enter the name of the Exchange ActiveSync Server or ASA account (if applicable) and select **OK**. The **Add Services** window displays.
3. Select the **http** service registered in step 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 **Enable EAS Server to Accept Kerberos Tickets**.

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**.



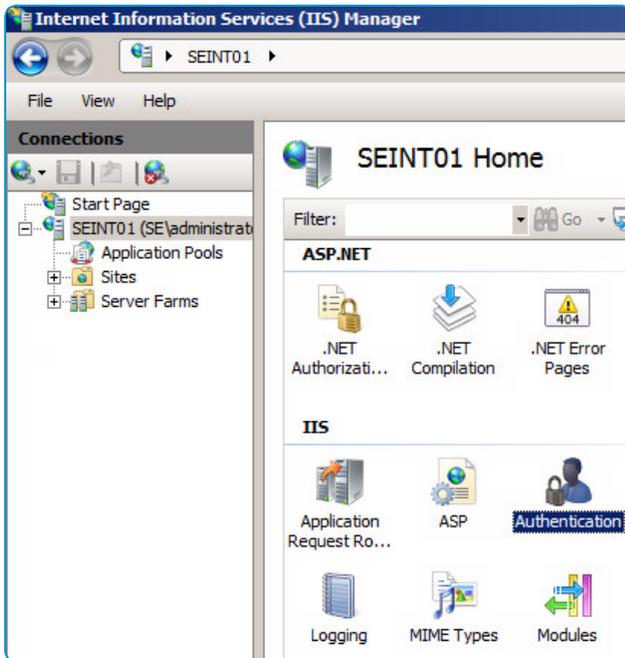
Next, **Configure IIS for Certificate Authentication on the SEG**.

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

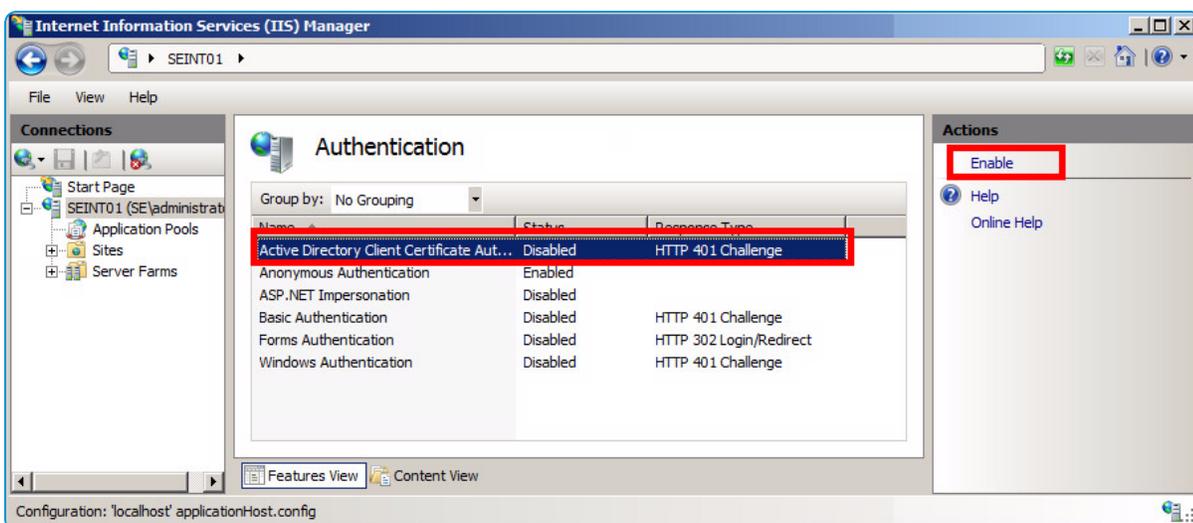
In order for the SEG to authenticate the user's device that is assigned to a particular certificate, **Internet Information Services (IIS)** on the SEG server must be configured to accept that certificate.

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 the Role in IIS in VMware AirWatch Certificate Authentication for EAS with SEG](https://docs.vmware.com) available on docs.vmware.com.
6. In the right-hand pane, select **Enable**.

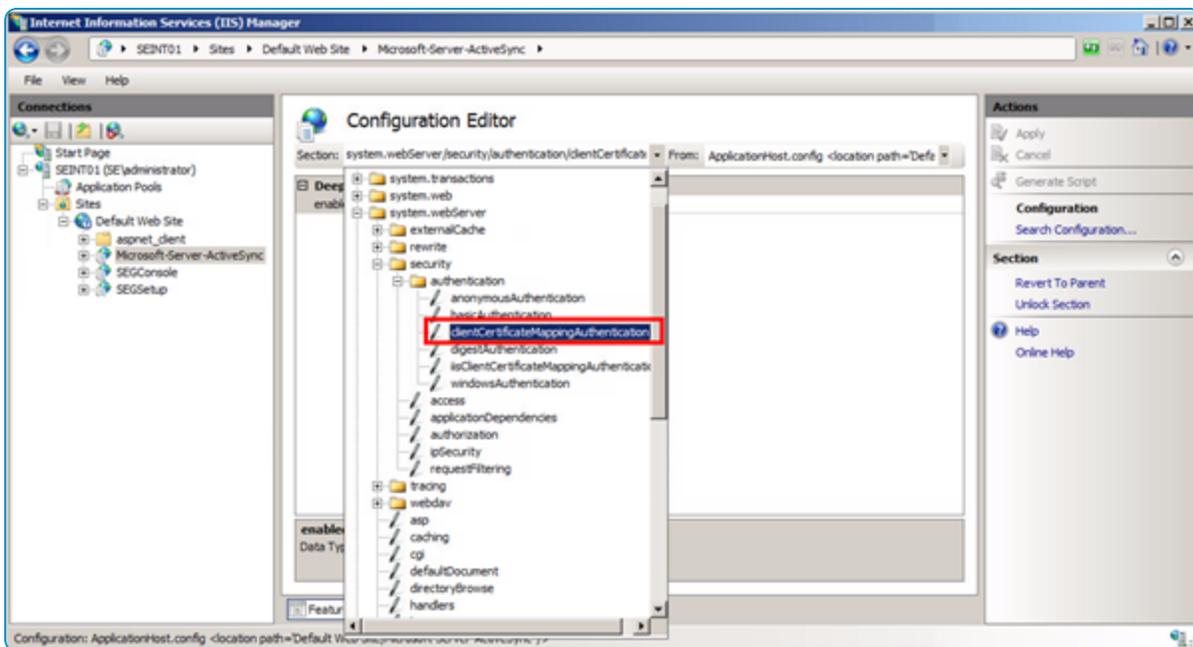


Use the Configuration Editor to Set Up Email Authentication

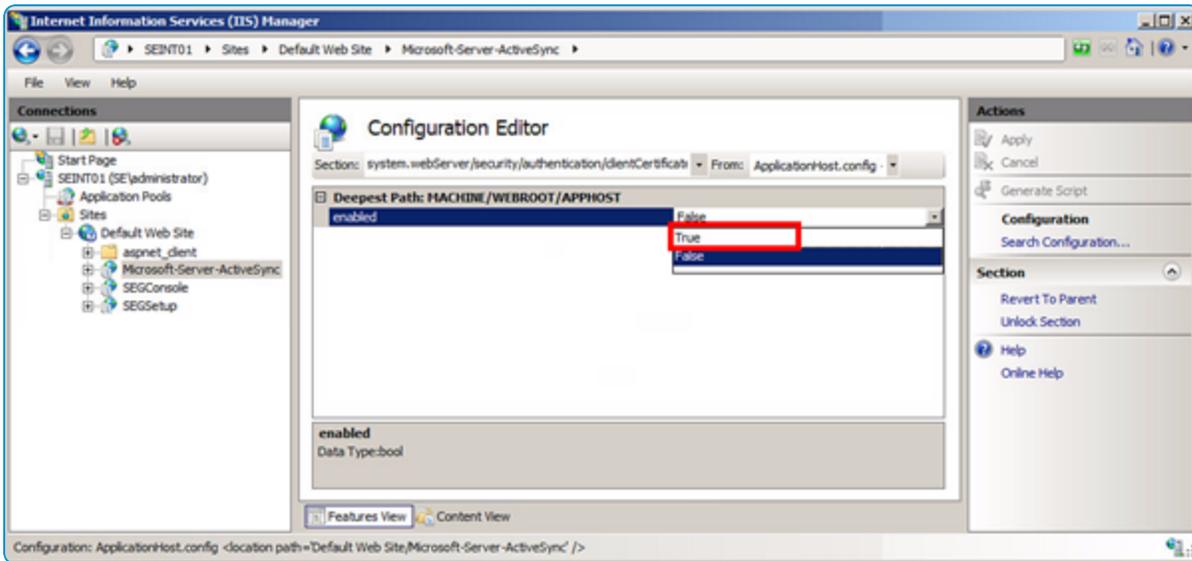
1. Click + to expand the **Sites** folder.
2. Click + to expand the **Default Web Site** and display the email sever you want to configure.
 - a. If you are using MS Server 2008 R2 or later, the **Configuration Editor** icon appears as shown in the screen below. This icon does not appear in older versions 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
                uthentication /enabled:"True" /commit:apphost
```

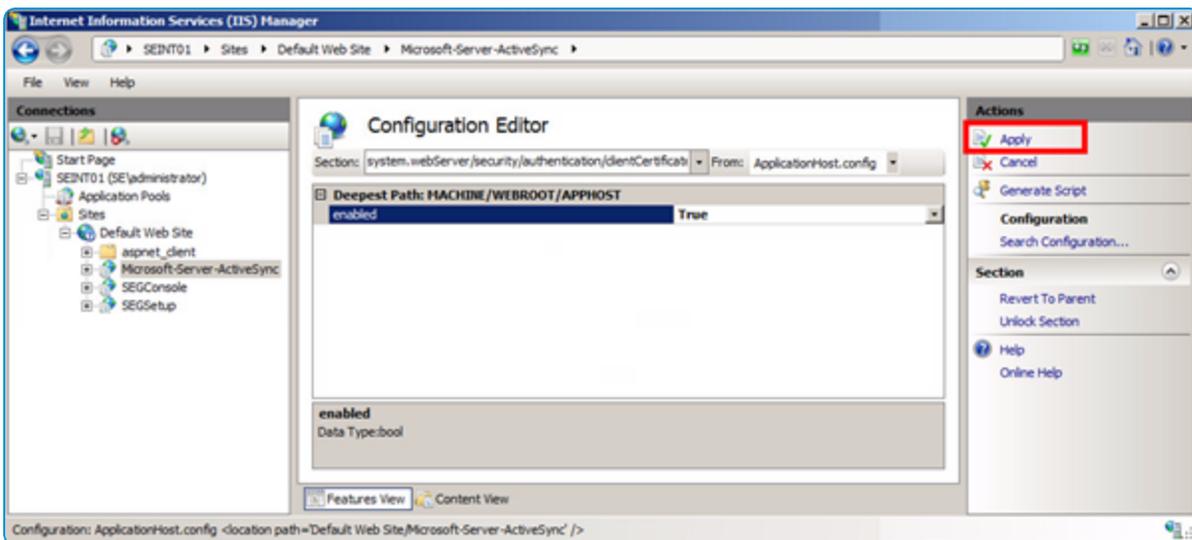
 If you performed this step, then skip the remaining steps and advance to Setting up Secure Socket Layer (SSL).
3. Navigate to **system.webserver/security/authentication** under **Section**.
4. Select **clientCertificateMappingAuthentication**.



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



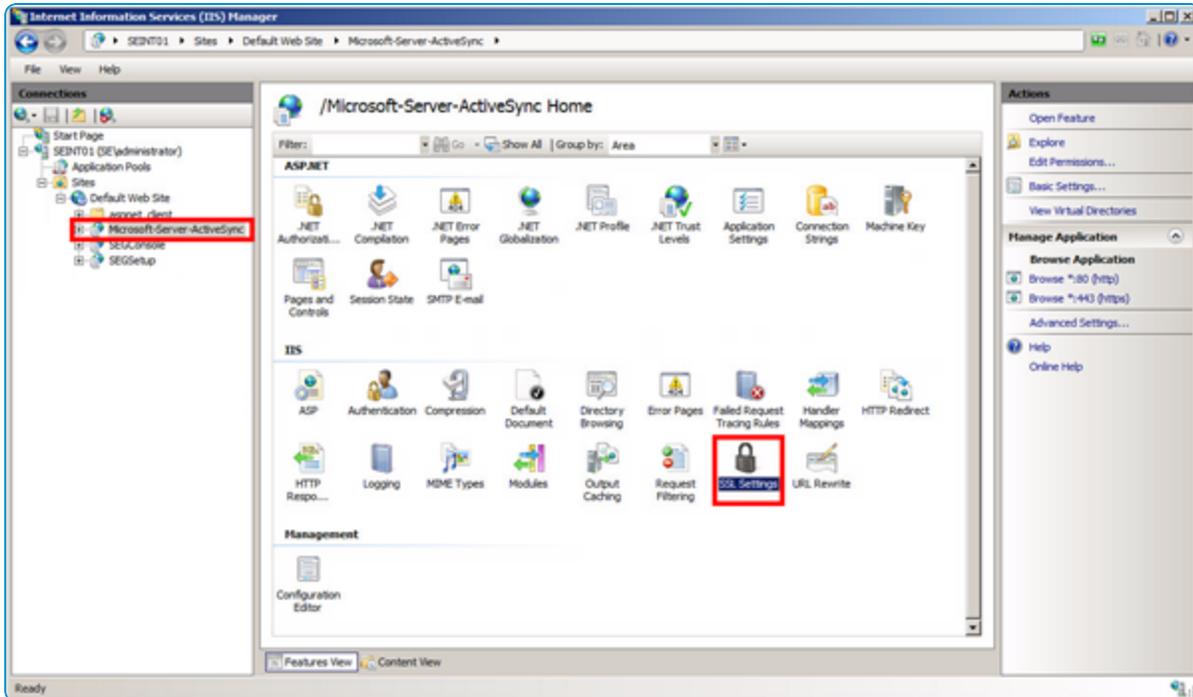
6. Click **Apply**.



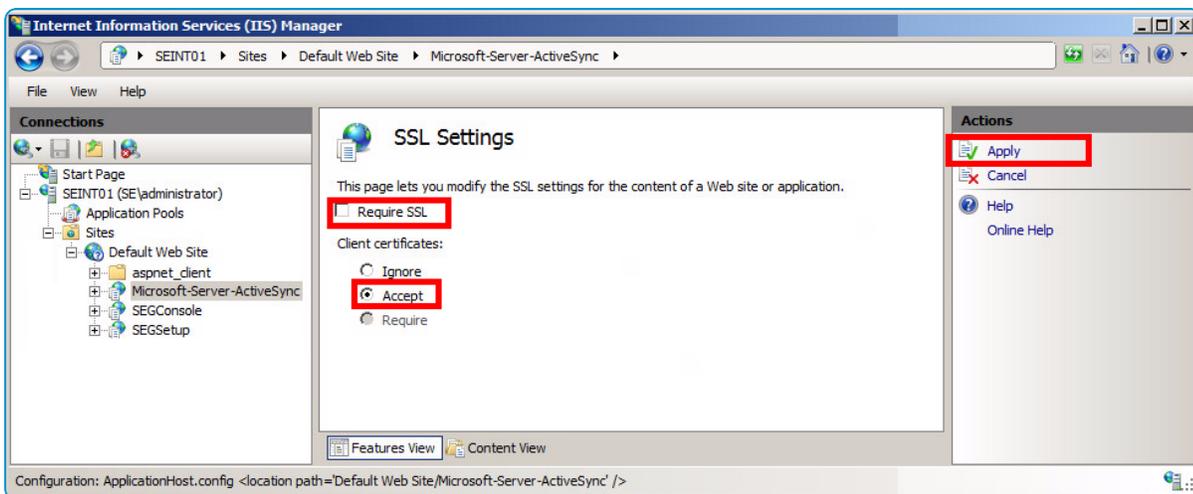
Set Up Secure Socket Layer (SSL)

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 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:apphost
```

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

“Default Web Site” is used 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
```

Lastly, you must **Configure Delegation Rights on the SEG Service Account**.

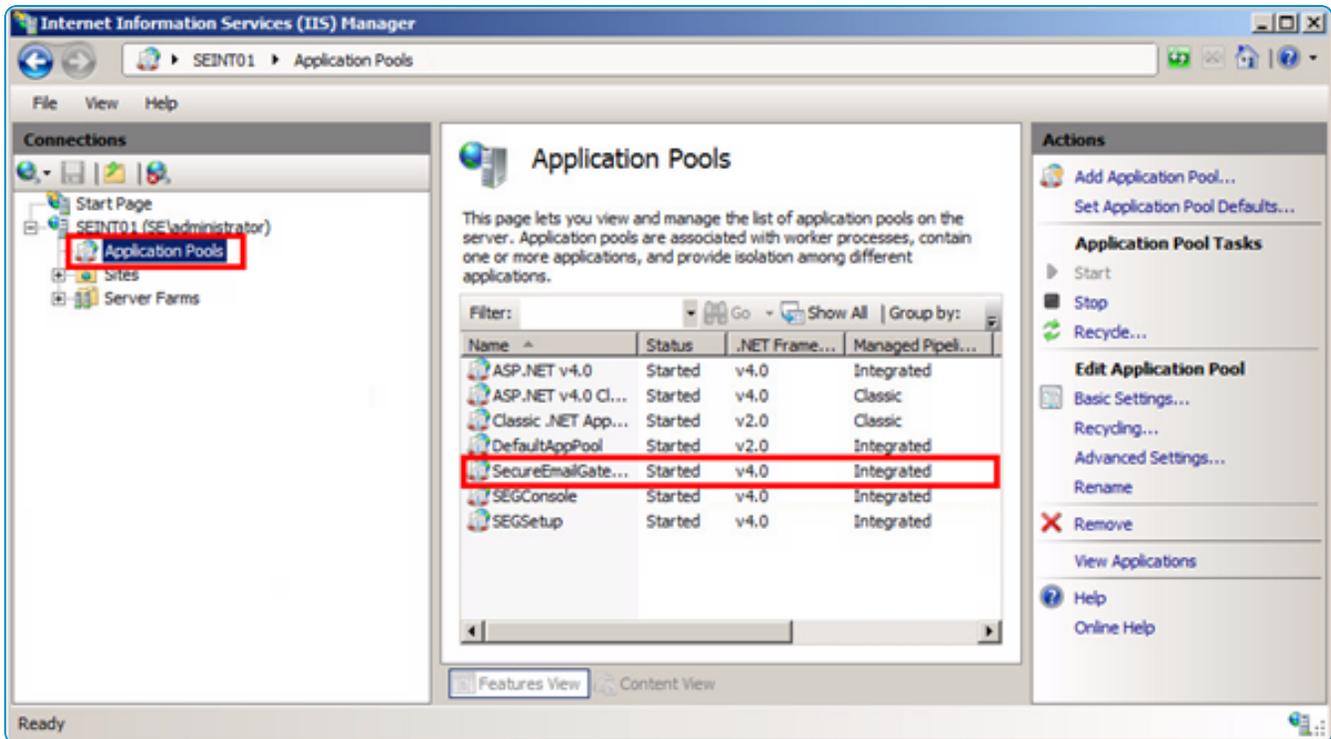
Step 5: Configure Delegation Rights on the SEG Service Account, EAS with SEG

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**.

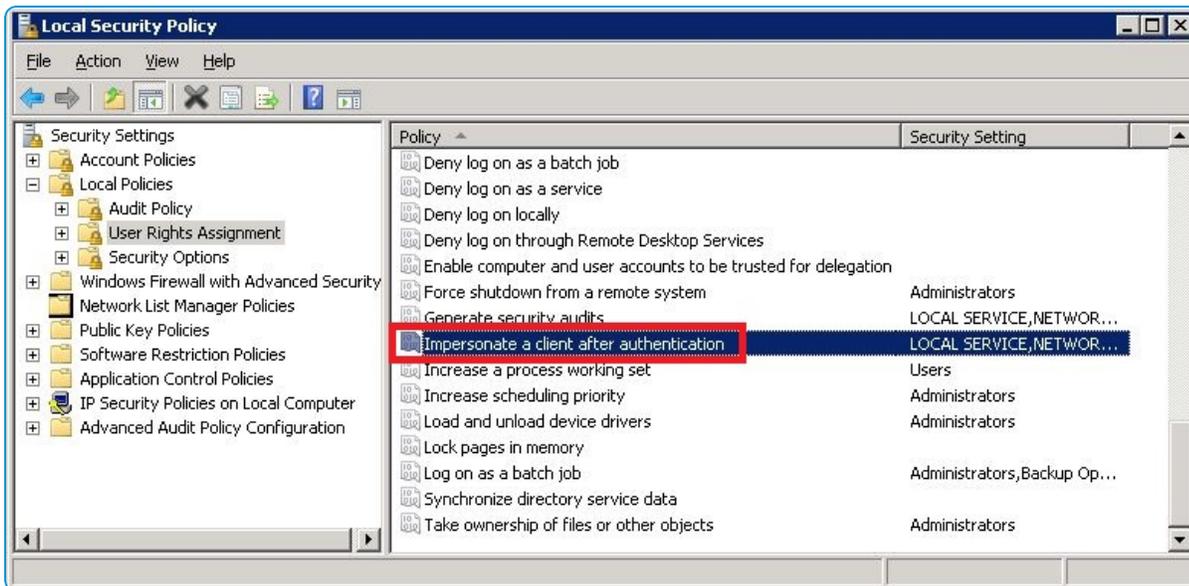


Configure Local Security Policy for SEG to Act as Part of the Operating System

- 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**.

Chapter 3:

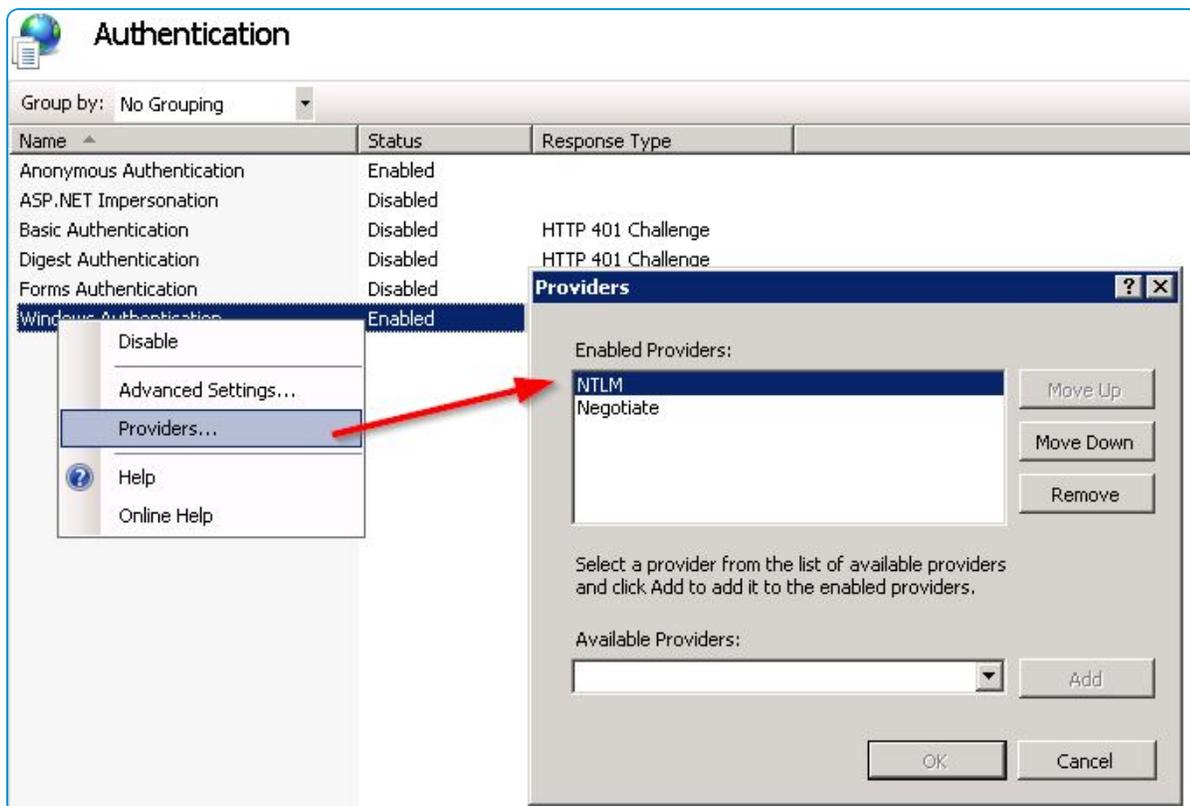
Troubleshooting, EAS with SEG

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 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.

Troubleshooting Checks

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



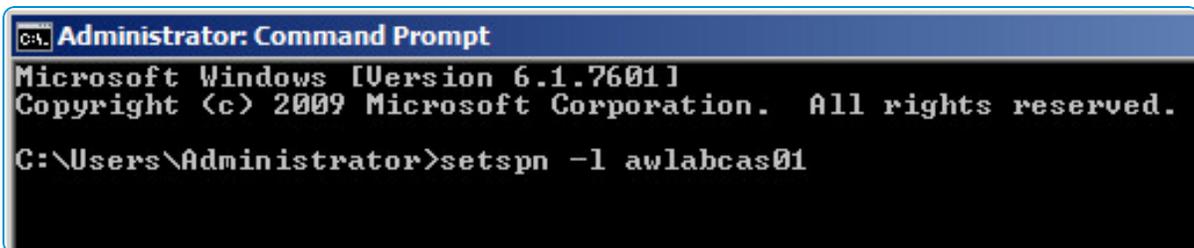
- Make sure that a certificate is being issued by the CA to the device by checking the following information.
 - Go to the internal CA Server, launch the certification authority application, and browse to the issued certificates section.
 - Find the last certificate that was issued and it should have 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 on page 10](#).
 - 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.

Chapter 4:

Additional SETSPN Commands, EAS with SEG

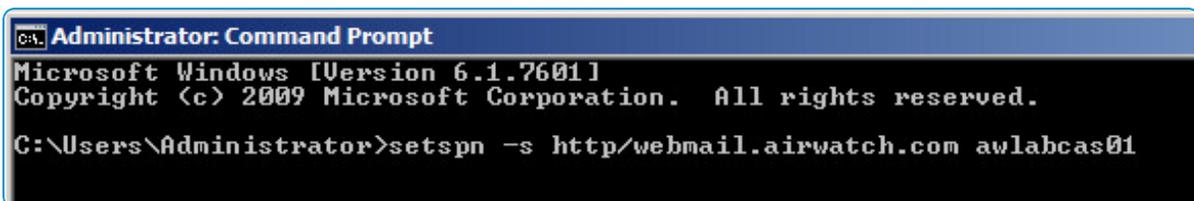
View SPN: SETSPN -l <computerName>



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

C:\Users\Administrator>setspn -l awlabcas01
```

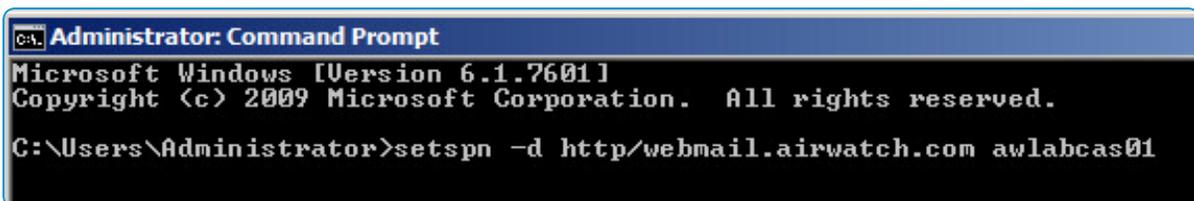
Add SPN: SETSPN -s <service>/<targetName> <computerName>



```
C:\> 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>



```
C:\> 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>

```
C:\> 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

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

C:\Users\Administrator>setspn -x
```

Chapter 5:

Appendix

Install the Role in IIS, EAS with SEG

Windows Server 2008 or Windows Server 2008 R2

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**.

Windows Server 2012 or Windows Server 2012 R2

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**.