Implementing Cross-Domain Kerberos Constrained Delegation Authentication

Configure Cross-Domain KCD

Workspace ONE UEM v9.6

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

Table of Contents

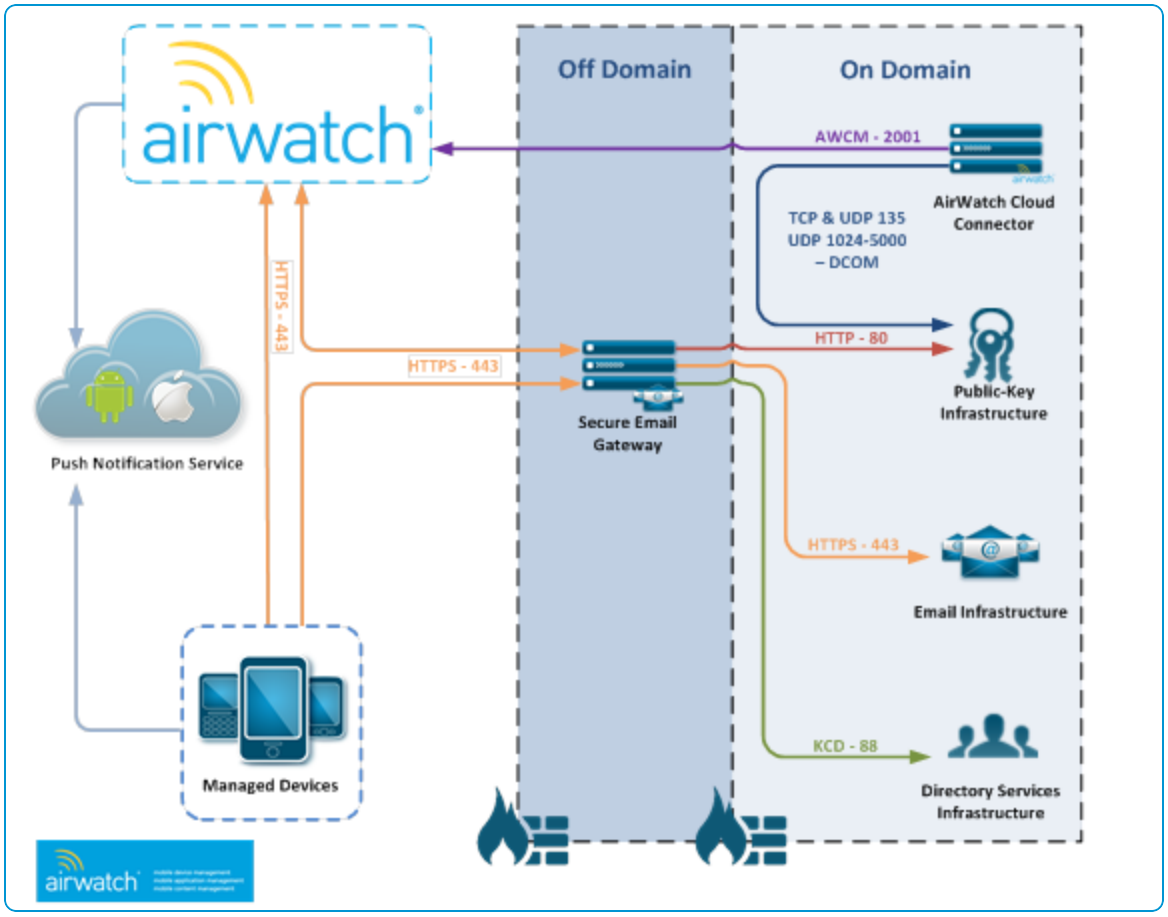
Chapter 1:
Introduction

Kerberos authentication eliminates the use of username or password authentication for email. In replacement, devices are issued certificates with the Exchange ActiveSync profile making the authentication transparent to use. 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 and managed by the Kerberos Distribution Center (KDC).

Workspace ONE now supports KCD authentication with the SEG in a multi or cross-domain scenario.

With this configuration, the client presents a certificate to the Workspace ONE Secure Email Gateway (SEG). This client certificate is authenticated by IIS on the SEG server. The SEG then leverages a domain service account to request a Kerberos ticket for the user from the KDC. The Kerberos ticket is forwarded to the Exchange server to authenticate the user.

The diagram shows a typical SaaS deployment.



It is not required that the PKI infrastructure should be part of the domain.

Prerequisites

Before configuring the Secure Email Gateway (SEG) to use cross-domain client certificate authentication, you must meet the following pre-requisites:

- A Windows Server (2008 R2+) that is not a member of the same domain as that of the Exchange server being authenticated to.
- A Certificate Authority (CA) integrated with Workspace ONE to issue certificates to your mobile devices. In this documentation, Microsoft is used as an example for a CA. However, Workspace ONE supports the certificates from other CAs apart from Microsoft.
  For more information on configuring Workspace ONE to issue certificates from your Certificate Authority to your Enterprise devices.
- 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> NTAuthCA
certutil -enterprise -addstore NTAuth CA_CertFilename.cer
```

- Android and iOS devices enrolled in Workspace ONE ready to receive EAS profiles. Supported devices may expand in the future so refer to your platform guides to determine compatibility for specific devices regarding support for EAS profiles with client certificates.
- A domain service account to be used as the Principal Identity with designated permission to impersonate users to the EAS service.
- Administrative access to the following in your enterprise environment:
  - Active Directory (AD) Users & Computers.
  - Exchange ActiveSync (EAS) or Client Access Servers (CAS).
  - Windows Server on which the SEG is to be installed.
  - Certificate Authority (CA).

Note: If there are multiple CAS or EAS servers in an array, you need to create an Alternate Service Account (ASA) in Active Directory. Instructions can be found in the Appendix.

Communication paths should be as noted below:

Source	Port	Protocol	Destination
SEG	80	HTTP	CRL Distribution Point

SEG	88	LDAP\kerberos	Domain Controller
SEG	80/443	HTTP (S)	Exchange ActiveSync
SEG	443	HTTPS	AW API
DS/CN	443	HTTPS	SEG
Device	443	HTTPS	SEG

Chapter 2:
Cross Domain Configuration

Setup the Target Service Principal Name (SPN) for the Exchange Server

If there are multiple CAS or EAS servers in an array, you need to create an Alternate Service Account (ASA) in Active Directory and then continue with Assigning Delegation Rights to the Service Account. If you have only one EAS or CAS server in your environment follow the instructions:

1. If the SEG is referring to the Exchange server by its Fully Qualified Domain Name (FQDN) or its Machine Name you can skip this step. If you are using a different DNS name to refer to the Exchange server from the SEG then, you need to create a SPN in order for your Domain Controller to allow delegation by the service account.
2. To set the SPN, open a command line window from a server on the domain being authenticated to and run the following command:

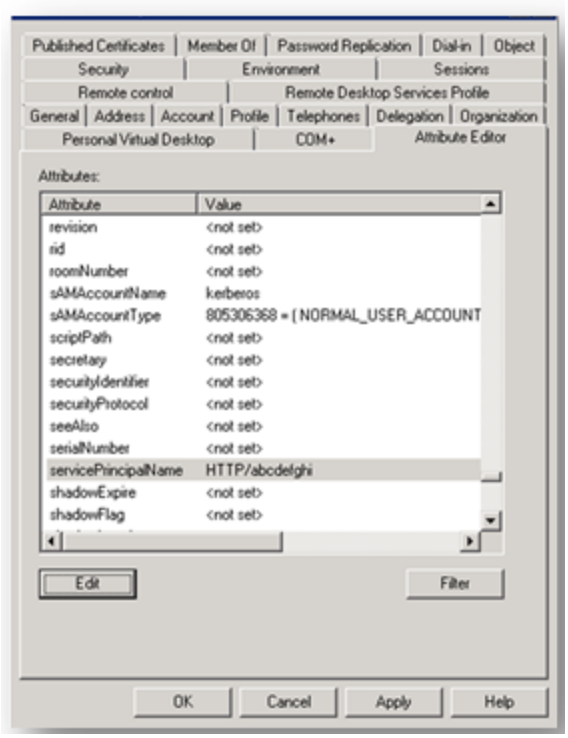
```
setspn -s HTTP/{EX_DNS_NAME} {EX_MACHINE_NAME}
```

Where **{EX_DNS_NAME}** is the name the SEG uses to refer to the Exchange server and {EX_MACHINE_NAME} is the actual machine name of the Exchange server. You need to select this SPN when assigning delegation rights to the Service Account.

Assign Delegation Rights to the Service Account

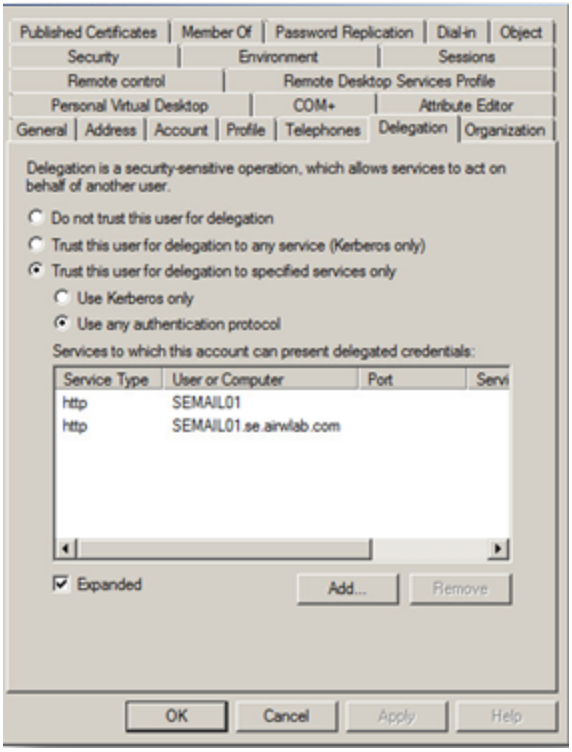
1. Open **Active Directory Users and Computers** on the domain that you are authenticating to and navigate to **View** and enable the **Advanced Features**.
2. If you do not already have a service account created for the SEG to use for the Kerberos request, create one now. Refer to this account as a**w_KCDsvc**.
3. Right-click the service account, select **Properties**. In the **Properties** menu, select the **Attribute Editor** tab.
4. In order to assign delegation rights to a user account, Microsoft requires that the account be assigned a Service

Principal Name (SPN). The SPN for the service account is not used for anything other than this. Find the **servicePrincipalName** attribute in the list and edit it to be in the format **HTTP/aw_KCDsvc**.



5. After setting up the SPN for the user account, close the **Properties** window and reopen it in order to access the **Delegation** tab. Delegation cannot be set for a user account until an SPN is set.

6. On the **Delegation** tab, select the option **Trust this user for delegation to specified services only** and also **Use any authentication protocol**. Select **Add** and search and select the Exchange server (or the ASA account) for which you want to provide the delegation rights.



7. Scroll through the list to find the HTTP service type. If you set the SPN for the Exchange server in Step 2, select the SPN you created. Otherwise, select the HTTP service type for your server.

Update CDP/AIA for the Certificate

By default, Microsoft CA's are configured to publish and make available CRL's only through LDAP. Because the SEG server is not on the domain it is not able to check the default CRL of the Certificate Authority. Disabling the CRL checking greatly reduces the security of your PKI infrastructure. In order to address this, make the CRL available over HTTP from the SEG.

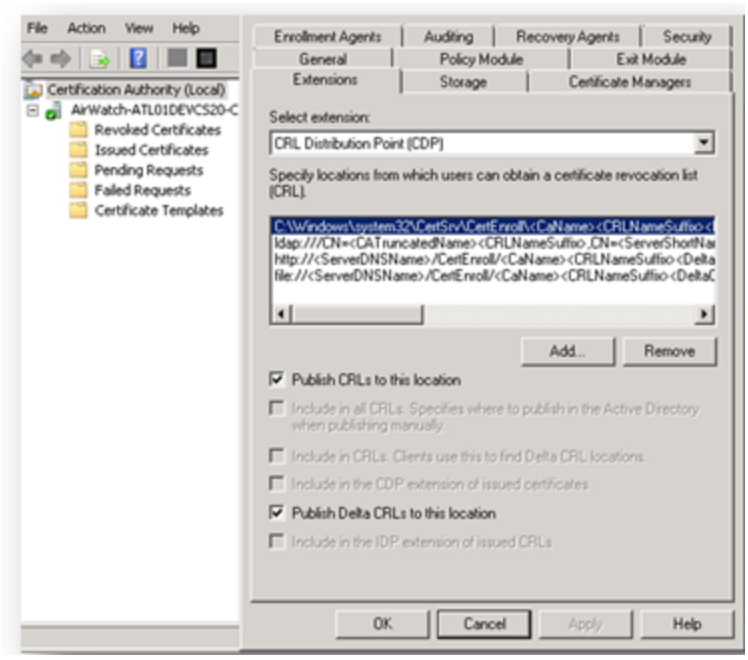
No certificates in the client certificate chain can have an LDAP distribution point for any certificates used to authenticate to an off domain server.

Note: If using a Certificate Authority with a CDP accessible from the SEG, then continue with **Adding the Service Account to the Local IIS_IUSRS Group of the CAS/EAS Server**.

The following configuration steps are assuming configuration from a Root CA.

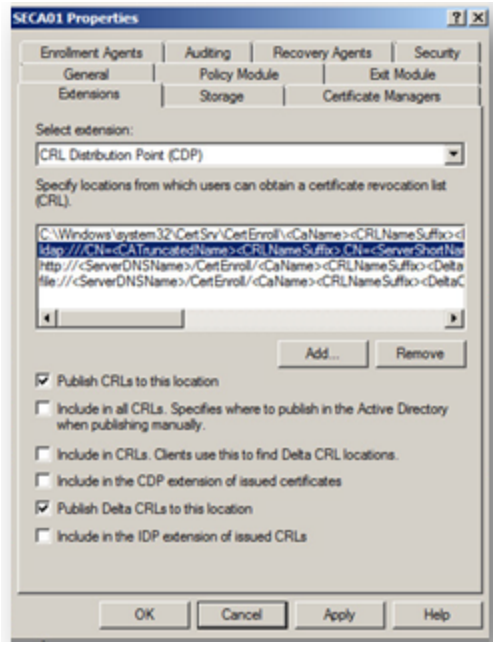
1. Open the Certificate Authority Manager, right-click the CA name and select **Properties**.

2. Choose **Extensions** tab and edit the **CRL Distribution Point (CDP)**.

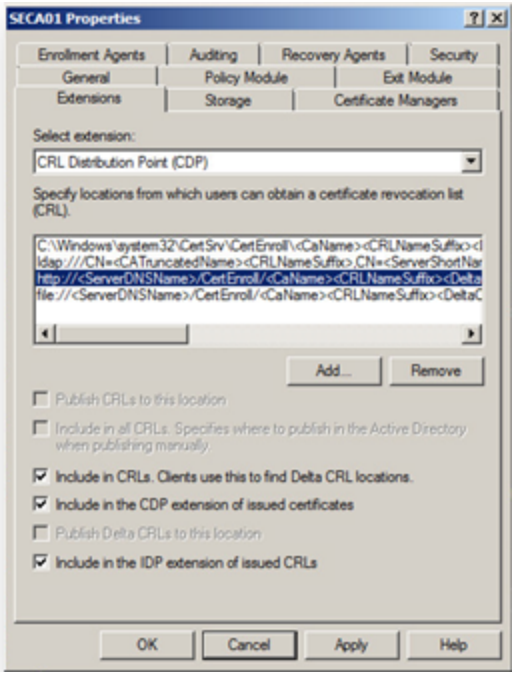


3. The first location should be a file path. This is where the CRL is stored on your server. This is the Physical Path of the Virtual Directory you create for the CDP.

4. The second path is through LDAP. Change this path to only have the Publish CRL's to this location and Publish Delta CRLs to this location selected. This allows any previously issued certificates to be checked for revocation correctly.

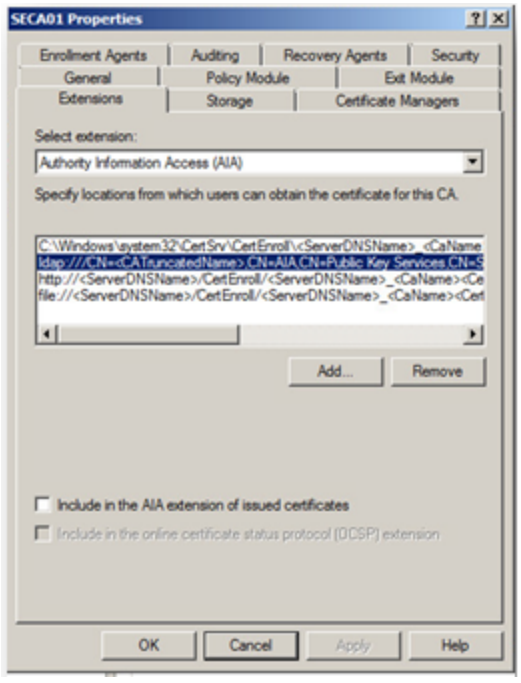


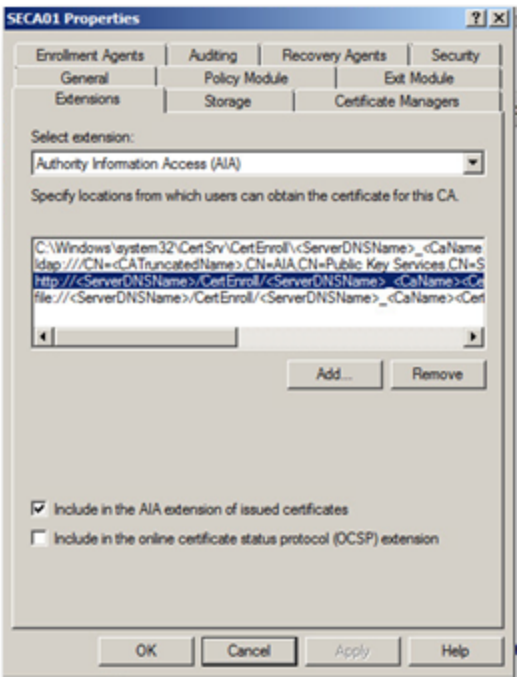
5. Select all available options for the HTTP distribution point. You won't be able to select the 'Publish to…' options. Note the **http://{path}**, use this in the next step to create the Virtual Directory for this path to make the CRL available from the SEG server.



6. Check the file:// distribution point and ensure none of the options are selected. Do not close the menu. Next, change the AIA Extension.

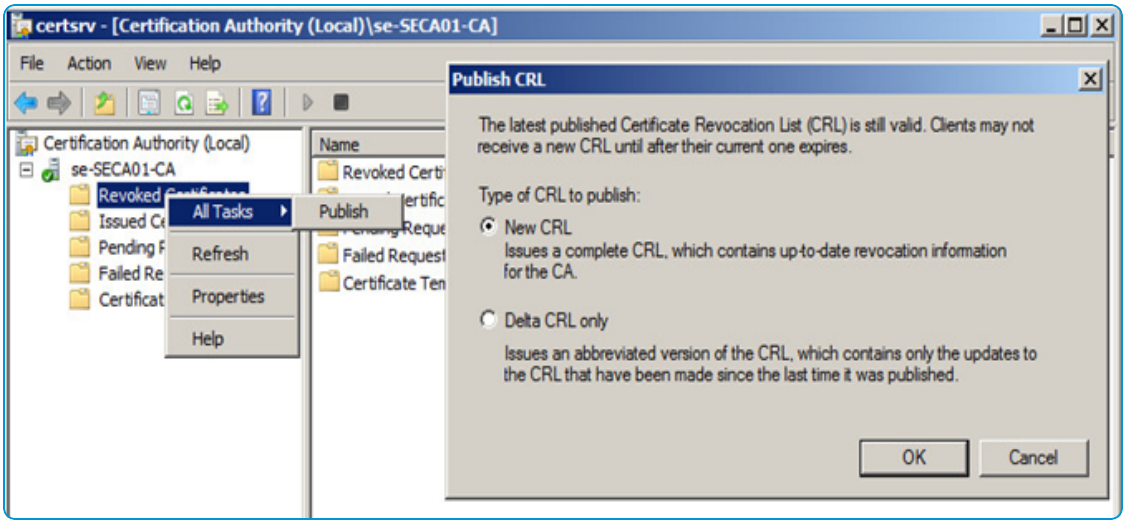
7. Select the extension drop down menu and select **Authority Information Access (AIA)**. Set the options to match the following images. Remove the LDAP and add the HTTP distribution point. Note the file path for publication; this should match the CDP file path. Use this in the next step to create the Virtual Directory to make the CRL available through HTTP. The file:// location should have no options selected. Select **OK** to save your changes. Select **Yes** to restart Active Directory Certificate Services.





8. Now that the CRL Distribution Point (CDP) and Authority Information Access (AIA) Extensions have been updated,

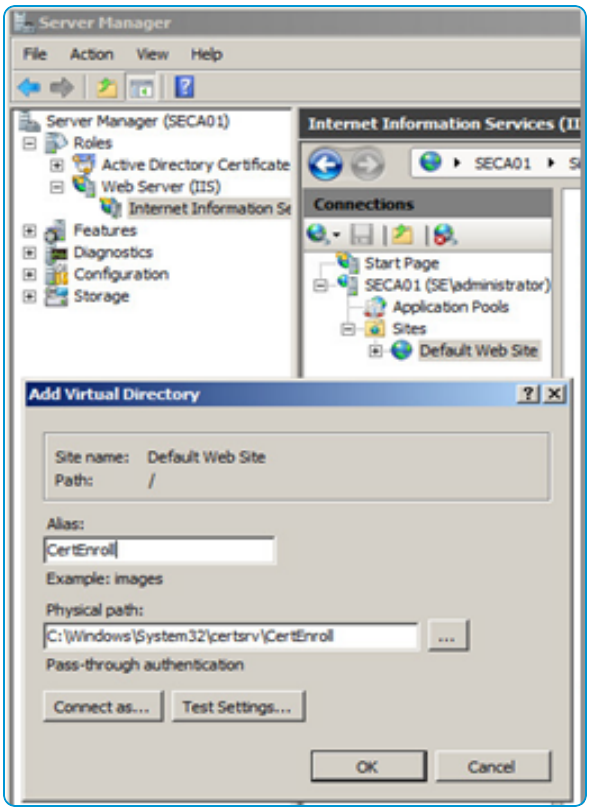
you need to republish the CRL to reflect the changes. Navigate back to **Certification Authority Manager** and expand the Certificate Authority. Right-click the **Revoked Certificates** directory and select **All Tasks > Publish** and then select **New CRL** and select **OK**.



Create Internet Information Services (IIS) Virtual Directory for the CRL Distribution Point

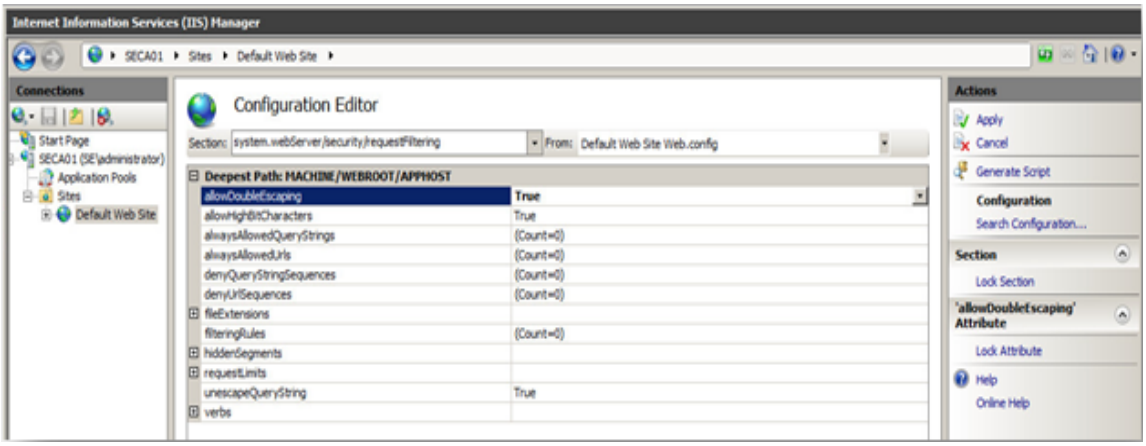
Configure IIS on the Certificate Authority to allow retrieval of the CRL over HTTP. You can choose to set this up on a separate HTTP server but it would require configuring the CRL to be published to that server and configuring a new HTTP CRL Distribution Point for the certificates. If you would like to configure this we suggest you refer to Microsoft's documentation for best practices.

1. If IIS is installed on the Certificate Authority, open IIS Manager and navigate to the **Default Website**. Right-click and select **Add Virtual Directory**.



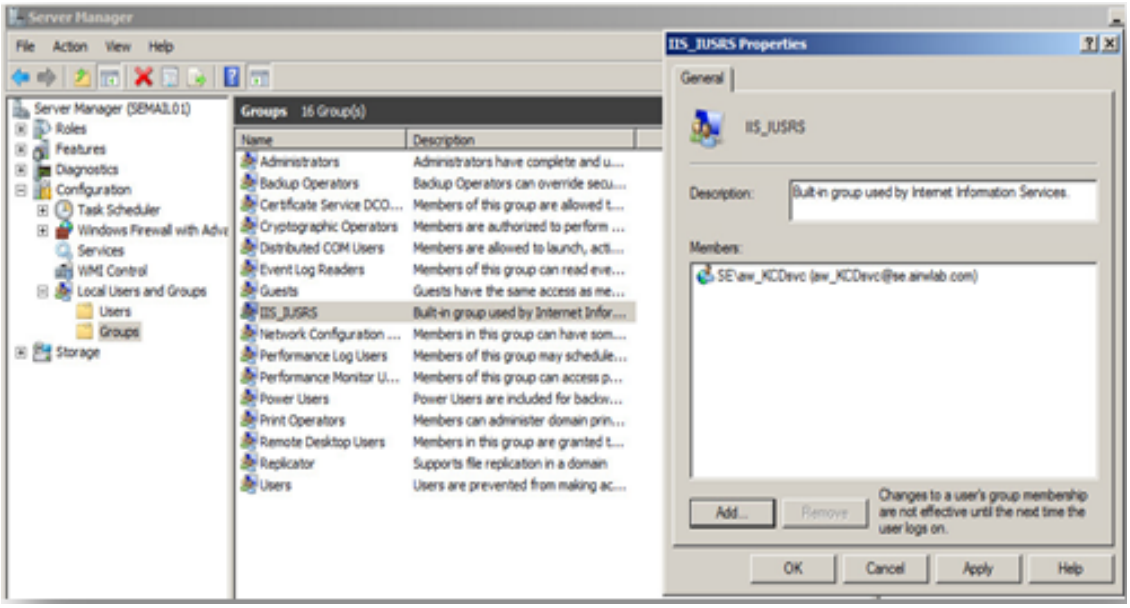
2. Set the alias to **CertEnroll** to match the distribution point configured in the CA CDP Extensions.
3. Set the Physical Path to the file path the CRL is being published to as set in the CA CDP Extensions. The default setting is **C:\Windows\System32\certsrv\CertEnroll**. Select **OK** to close the menu and save your settings.
4. Enable **Double Escaping** in IIS to allow the '+' in the Delta CRL's filename to be accessed through HTTP. Select the **Default Web Site** and open the **Configuration Editor**.
5. Set **allowDoubleEscaping** to **True** and select **Apply** in the **Actions** panel. This is required to allow the Delta CRL to be

accessed through the CDP.



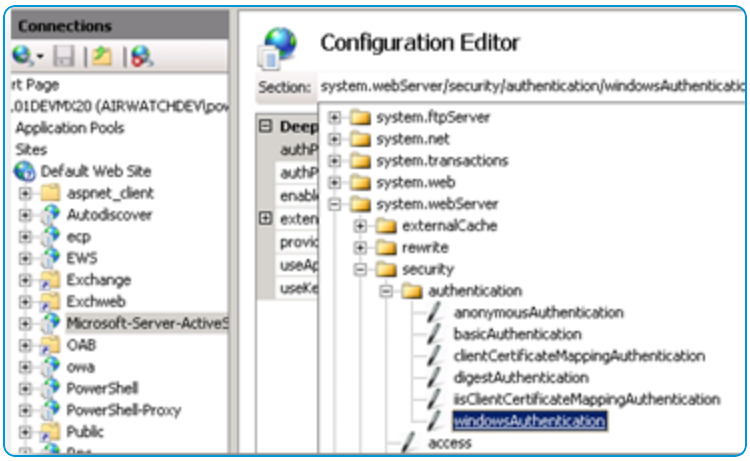
Add Service Account to Local IIS_IUSRS Group of the CAS/EAS Server

1. On the CAS/EAS server, open **Server Manager** and navigate to **Configuration > Local Users and Groups > Groups**.
2. Right-click **IIS_IUSRS** and select **Add to Group**. Select Add… to search for the aw_KCDsvc service account and add the user to the local group then select **OK**.

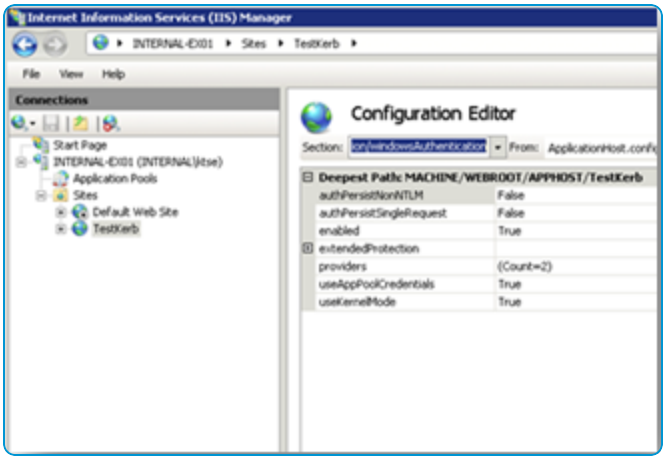


Enable Windows Authentication on the CAS/EAS

1. On the Exchange Server, open IIS Manager and navigate to the **Microsoft-Server-ActiveSync** Virtual Directory. Select **Authentication** then enable **Windows authentication** and disable **Anonymous authentication**.



2. In the **Microsoft-Server-ActiveSync Virtual Directory**, access the **Configuration Editor** and navigate to **system.webServer > security > authentication > windowsAunthentication** and set **useAppPoolCredentials** and **useKernelMode** to **True**.



Configure Secure Email Gateway (SEG) on the Workspace ONE UEM console

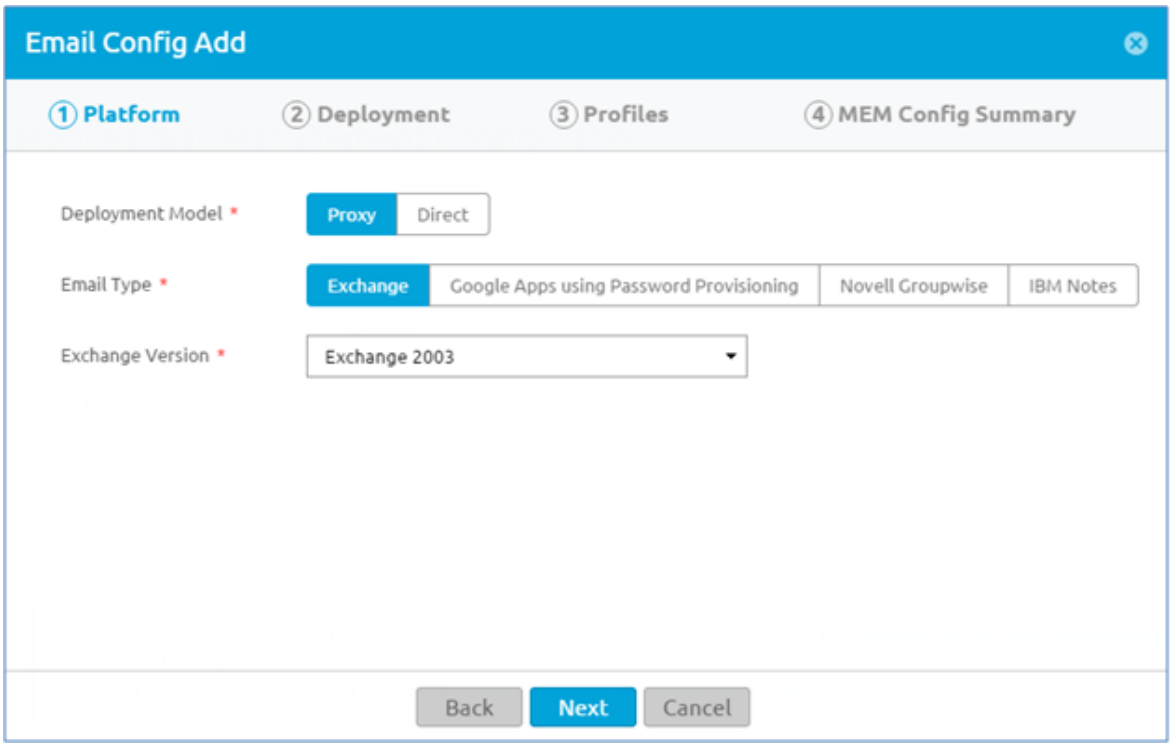
For detailed information regarding SEG configuration, please refer to the VMware AirWatch SEG Installation and Admin Guides . This guide aims to provide a simplified set of instructions to get you going for a basic configuration.

Check to ensure:

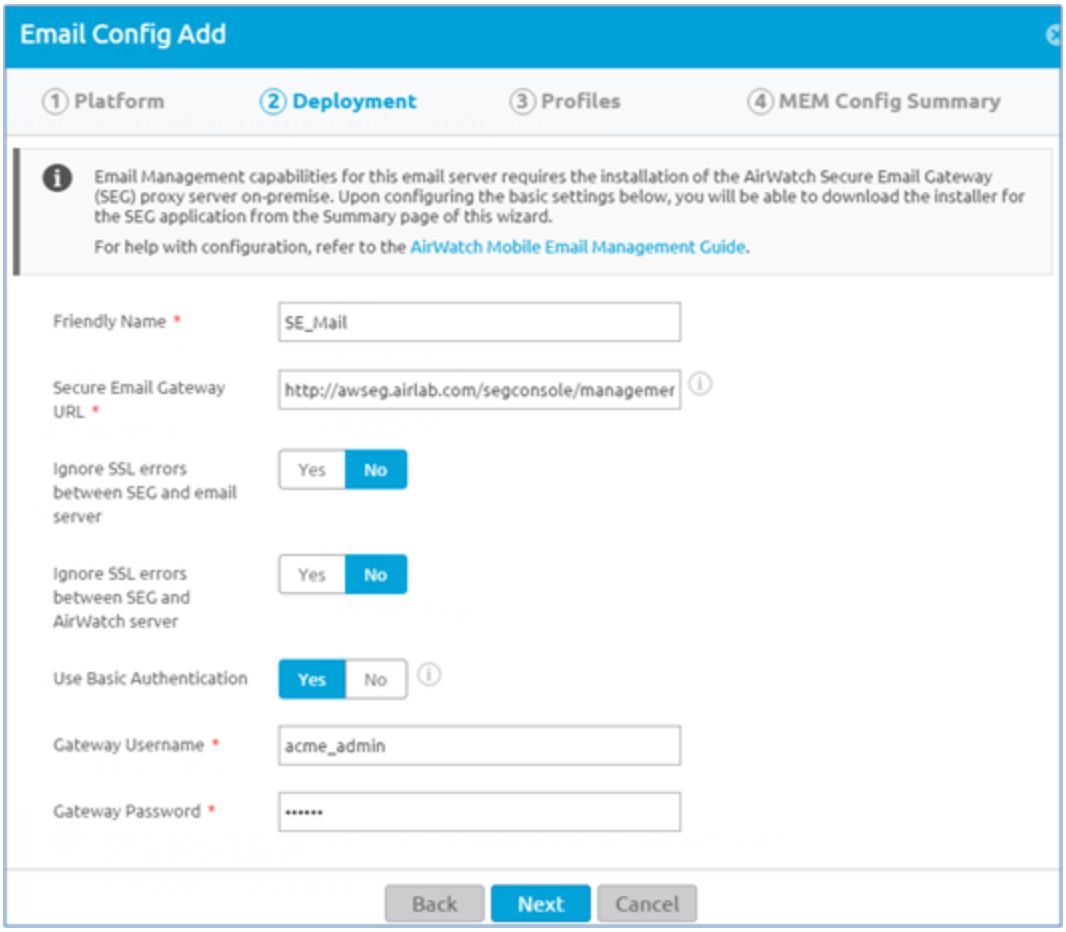
- There is a valid administrative account with permissions to the SOAP API at the MEM configured Organization Group.
- There is a SOAP API Certificate generated in the UEM console.

Next, continue with the following steps.

1. From the UEM console main menu, navigate to **Email > Settings**, and select **Configure**.



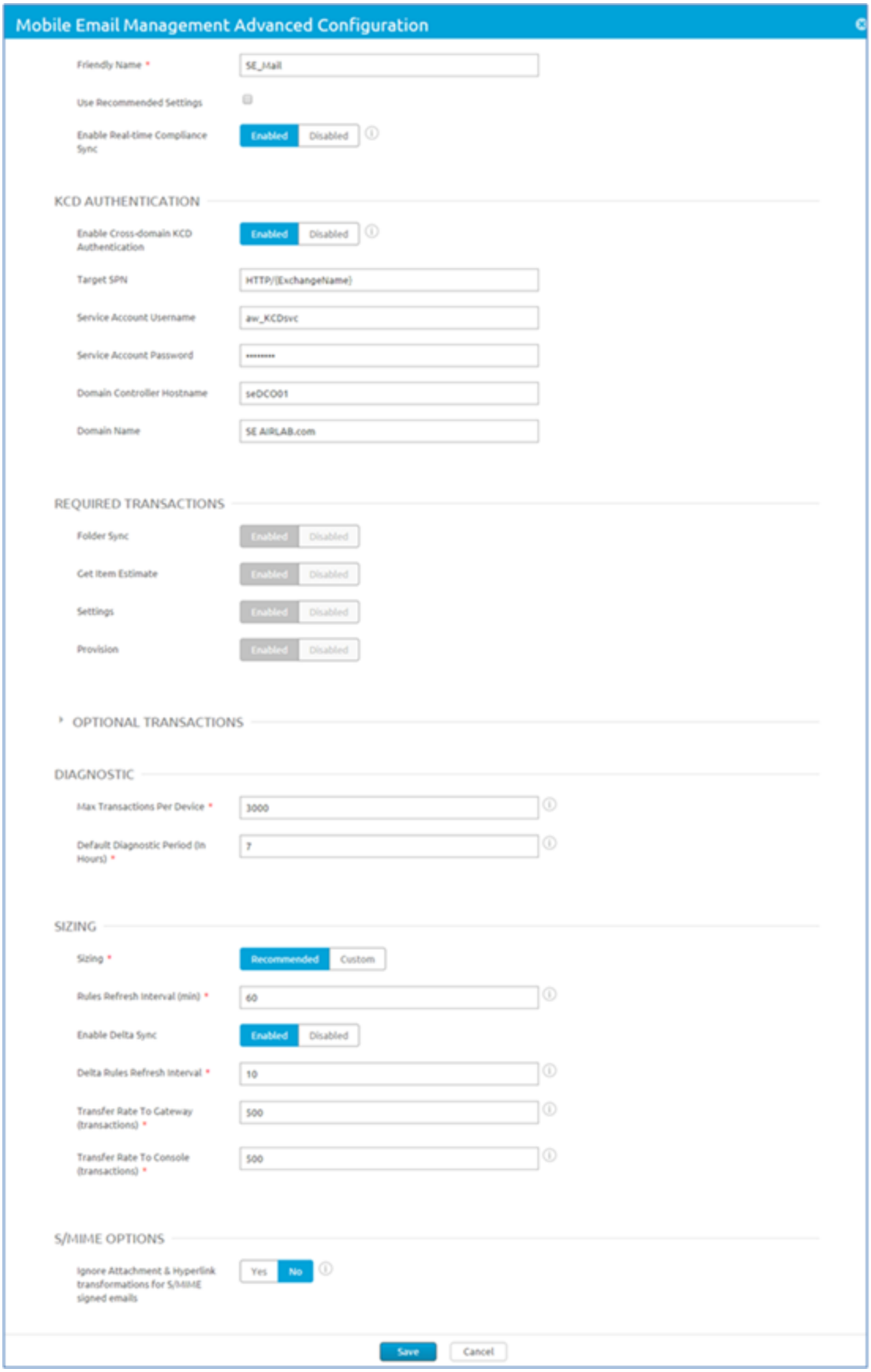
2. On the **Email Config Add** page, choose your **Microsoft Exchange Version** and then select **Next**.
3. Enter a **Friendly Name** and your Exchange DNS name in the **Secure Email Gateway URL** field and select **Next**.



4. You may select to create profiles at the MEM Profile Deployment menu or select **Next** and create the profiles later. If you create them here you need to edit them to match the settings further in the setup guide.

5. Confirm settings and select **Save**. Next, select **Advanced**.

6. On the Mobile Email Management Advanced Configuration page, clear the **Use Recommended Settings** checkbox and select the **Enable Cross-domain KCD Authentication** checkbox. This option does not display during the SEG Setup unless it is enabled on the console.



7. Enter the required fields:

Settings	Description
Target SPN	HTTP/{exchangeName}. This is the ASA or CAS/EAS Server name without the domain. For example if the Exchange server DNS name is semail01.se.airwlab.com, the Target SPN is HTTP/semail01
Service Account Username	Username with delegation rights, for example, aw_KCDsvc.
Service Account Password	Password for aw_KCDsvc account.
Domain Controller Hostname	The DC server name without the domain
Domain Name	Domain name in uppercase. For example, if the DC FQDN is sedc01.se.airwlab.com enter SE.AIRWLAB.COM

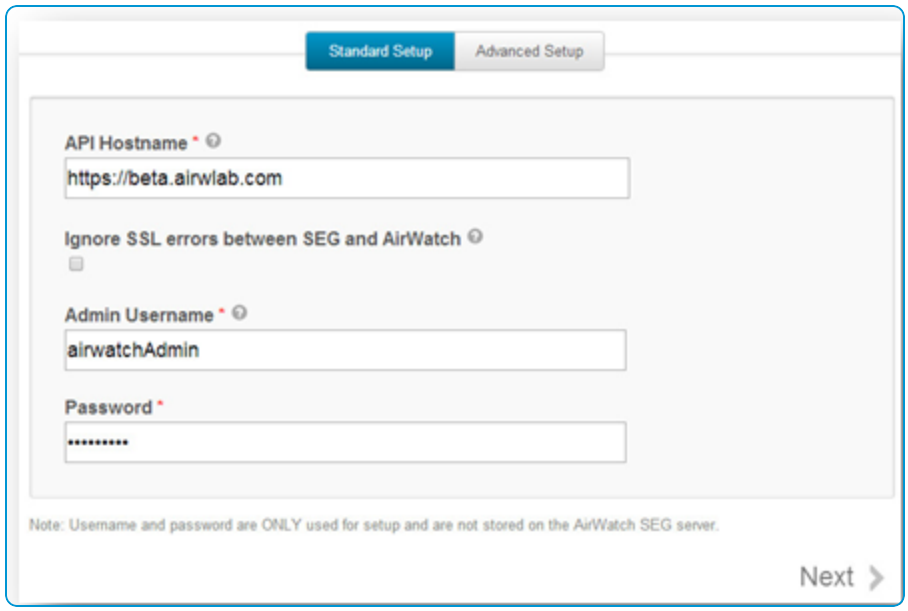
8. Select **Save** and then select **AirWatch Secure Email Gateway Installer** to download the installation package from the SEG server. The link is in the SEG Proxy Settings menu.

Note: SEG supports multiple domains. No additional configuration is required on the UEM console. It depends on the SEG's connectivity to each domain controller.

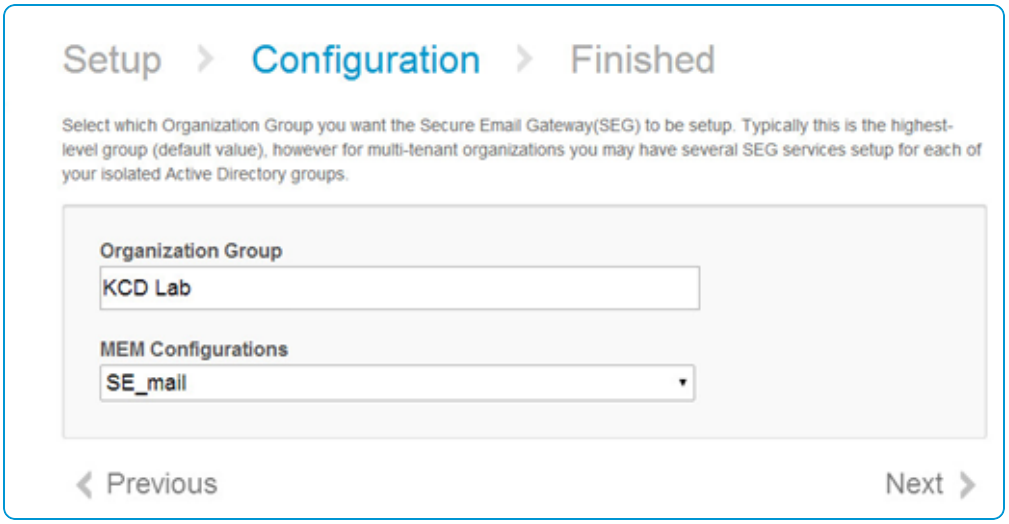
Install SEG

This step briefly describes how to install the SEG in a basic configuration. For more details refer to the MEM and SEG Admin Guides.

1. From the SEG server, download the SEG installer from your Organization Group in the UEM console.
2. Launch the installation wizard and when the wizard appears, select **Next**. After reading the EULA, if you accept the terms select the appropriate options and select **Next**. If you have questions about the EULA, contact Workspace ONE Support.
3. Select the installation path and select **Next** to continue. Then select **Next** to install to the Default Website.
4. If IIS URL Rewrite Module 2 is not installed, you are prompted to download it from Microsoft and install it. Continue with the installation, this IIS component is required for the SEG to function appropriately. When the installation completes, select **Finish** to continue with the SEG installation.
5. If Microsoft Application Routing Version 2 is not installed, you are prompted to install it. Continue with the installation. These IIS components are required for the SEG to function appropriately. When the installation completes, select **OK** to continue with the SEG installation.
6. Select **Install** and wait for the installation to complete and then select **Finish**. It is a good idea to check the Windows Installer Log for any errors. The Workspace ONE SEG Setup Web console should open in a browser. If it does not, look on the desktop for a shortcut to the console.
7. Enter your environments API server address and Administrative credentials to the Workspace ONE SOAP API. This requires a valid admin account at the SEG's Organization Group with a SOAP API certificate generated. Then select **Next**. Workspace ONE does not recommend choosing to **Ignore SSL Errors** but you may select this option if needed.



8. Select the **Organization Group** where your SEG is configured and make sure the MEM Configuration matches the Friendly Name chosen in the previous step.



9. Enter the **Email Server Hostname** as the SEG should refer to the CAS/EAS Server. Keep in mind that if using SSL, the SSL certificate presented by the server should contain the hostname used to access it in the SAN or Common Name of the certificate. If it does not, there can be a trust issue between the SEG and Exchange which can cause the chain break.

10. Select **Verify** to test authentication from the SEG to the CAS/EAS Server using Basic authentication. This validates that the email server is reachable from the SEG and that there are no connection or trust errors. Close this window when you receive a successful verification. If verification fails, you should check the SEGSetup log located in the\AirWatch\Logs\SEGSetup directory for more information.

11. Validate that the settings configured in the UEM console match what you see here and then select **Next**.

    - This guide covers installation of a single SEG only. For more information on SEG Clustering, refer to the SEG Admin and Installation Guides. To continue, select **Next**.

12. In order for the server configuration changes to be committed, an IIS reset is required. Open a command prompt and issue the command iisreset. You may also restart both the **IIS Admin Service** and the **World Wide Web Publishing Service** with the **Server Manager > Services UI**.

13. The user must manually change the Secure Email Gateway to use 32-bit application mode.

    - Check identity of the secureEmailgateway application pool. It should be set to NetworkService.
    - Check that the App Pool is set to Enable 32-Bit application mode.

14. The SEG Service Installation and Configuration is now complete. You may change the log level of the SEG here. Only turn the log level up during troubleshooting as it places an unnecessary load on the server during normal operation.

Final configuration steps on SEG

1. The SEG server needs to trust the domain certificate authority. To establish this trust, you need to add the Root CA Certificate into the Local Computer Trusted Root Certification Authorities store on the SEG server. To do this, launch **MMC** on the SEG server and add the **Certificate Snap-In** for the **Local Computer** and then import the domain's Root CA certificate into the Trusted Root Certification Authorities store. If there are intermediate CA's in the chain, their certificates should be added to the Intermediate Certificate Authorities store.

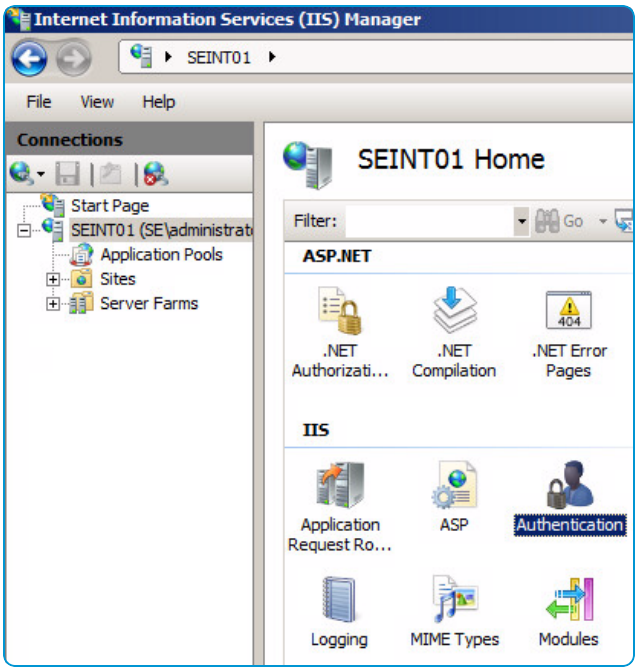
2. Note that the CRL's of every certificate in the chain must be reachable from the SEG server in order for revocation checking to pass and clients to authenticate. Root CA Certificate's do not contain a CRL Distribution Point (CDP) Extension by default but intermediate and client certificates should. Steps 3-4 cover how to configure your CA to publish its CRL to an HTTP distribution point. It is a requirement that this Distribution Point is accessible from your SEG server.

Configure IIS for Certificate Authentication on 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.

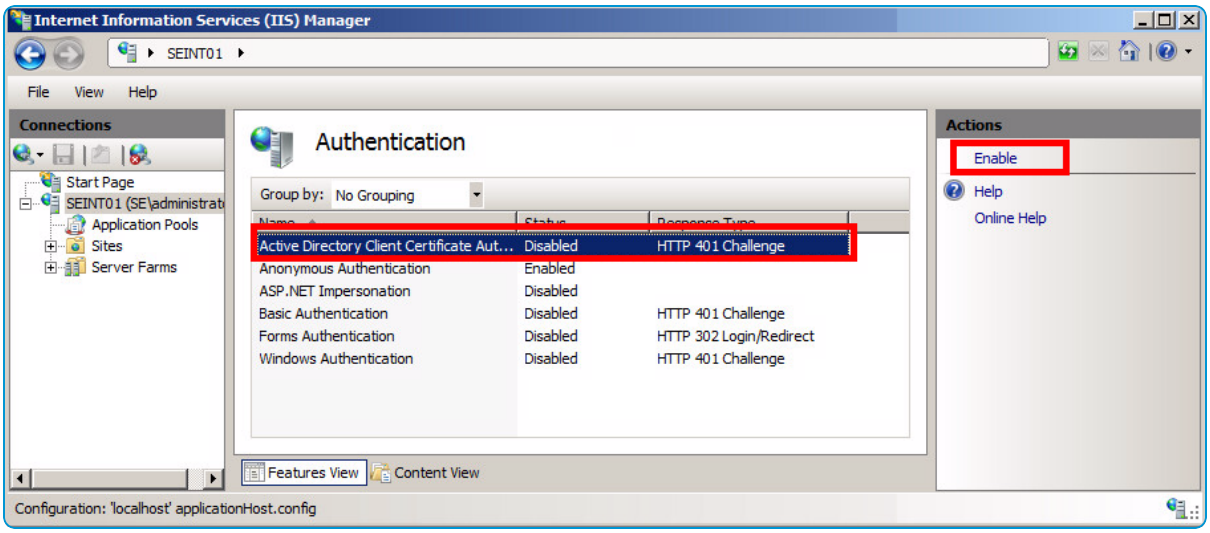
Set up Active Directory to Authenticate

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.see Install the Role in IIS in **VMware AirWatch Certificate Authentication for EAS with SEG** available on docs.vmware.com.

6. In the right-hand pane, select **Enable**.

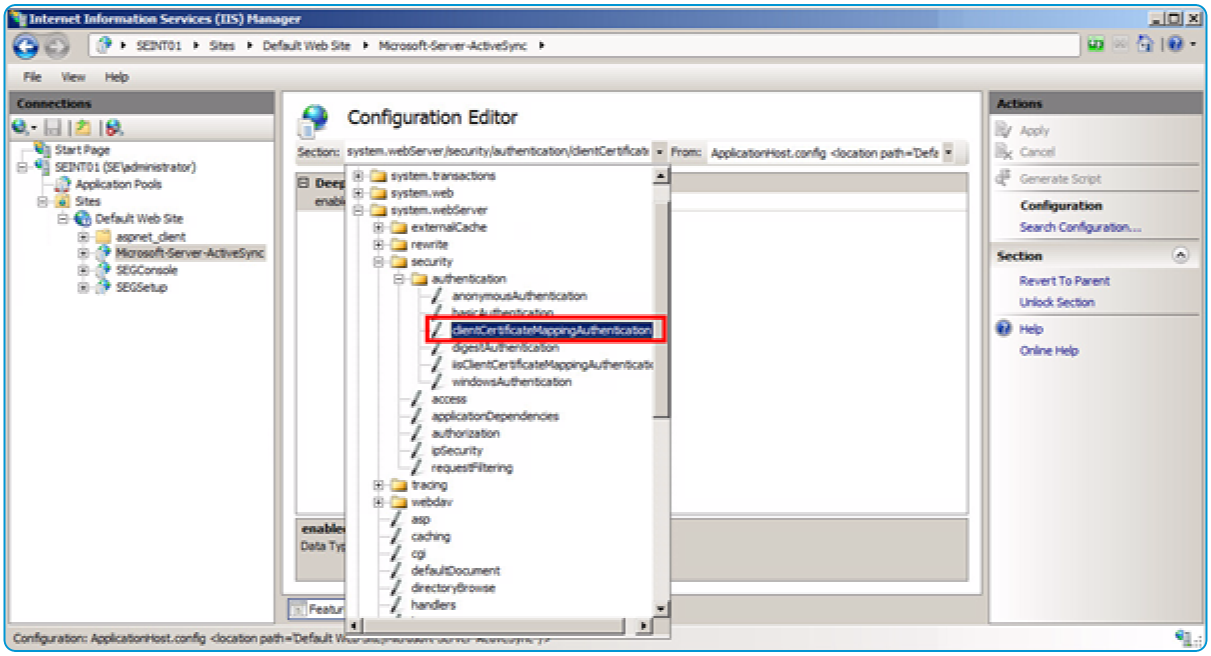


Use the Configuration Editor to Set Up Email Authentication

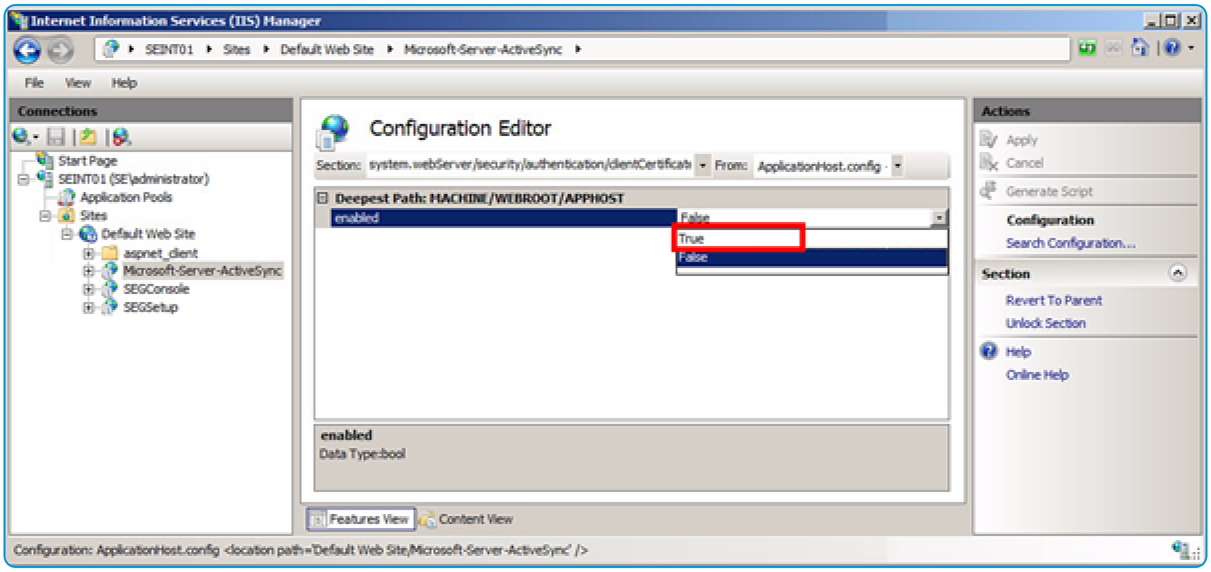
1. Click **+** to expand the **Sites** folder.
2. Click **+** to expand the **Default Web Site** and display the email sever you want to configure.
   a. If you are using MS Server 2008 R2 or later, the **Configuration Editor** icon appears as shown in the screen below. This icon does not appear in older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

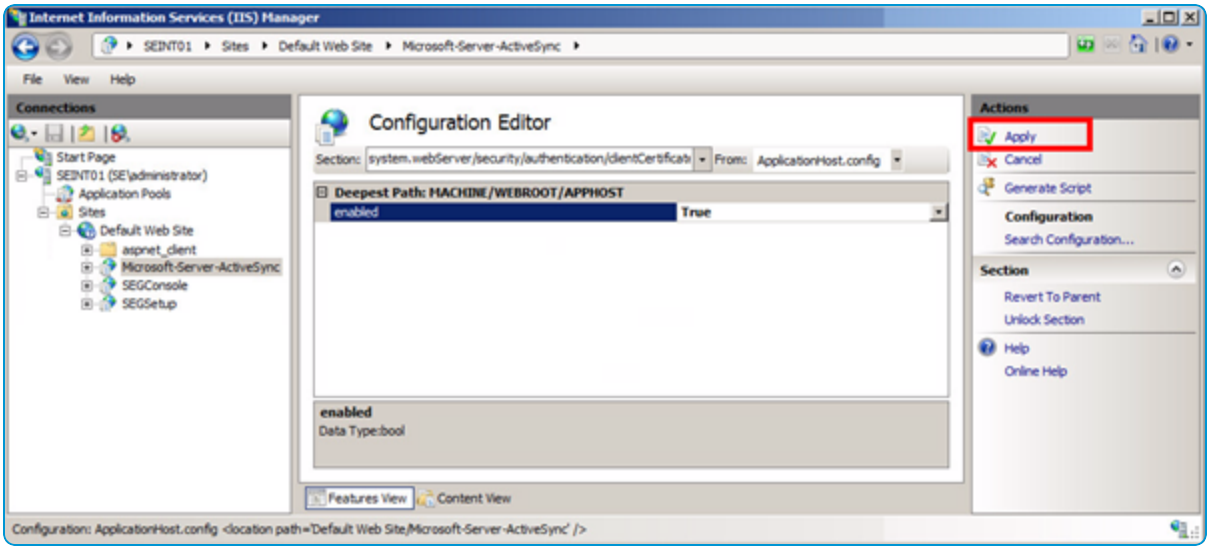
      If you performed this step, then skip the remaining steps and advance to Setting up Secure Socket Layer (SSL).
3. Navigate to **system.webserver/security/authentication** under **Section**.
4. Select **clientCertificateMappingAuthentication**.



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



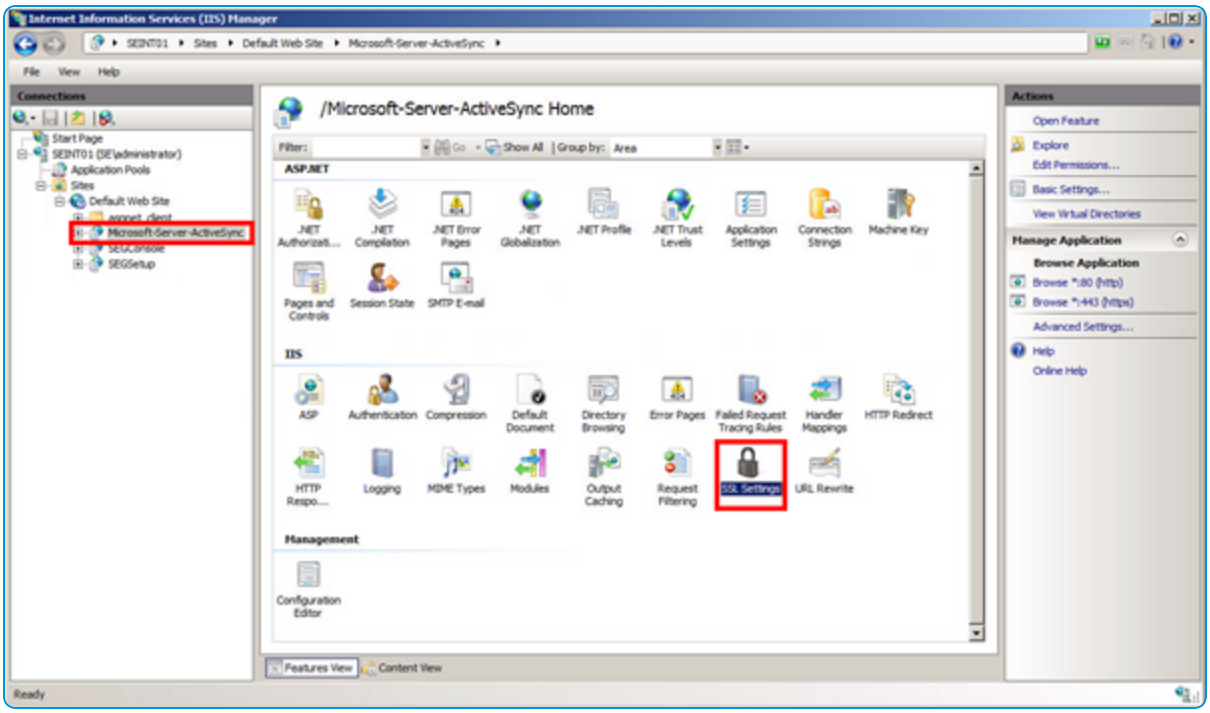
6. Click **Apply**.



Set Up Secure Socket Layer (SSL)

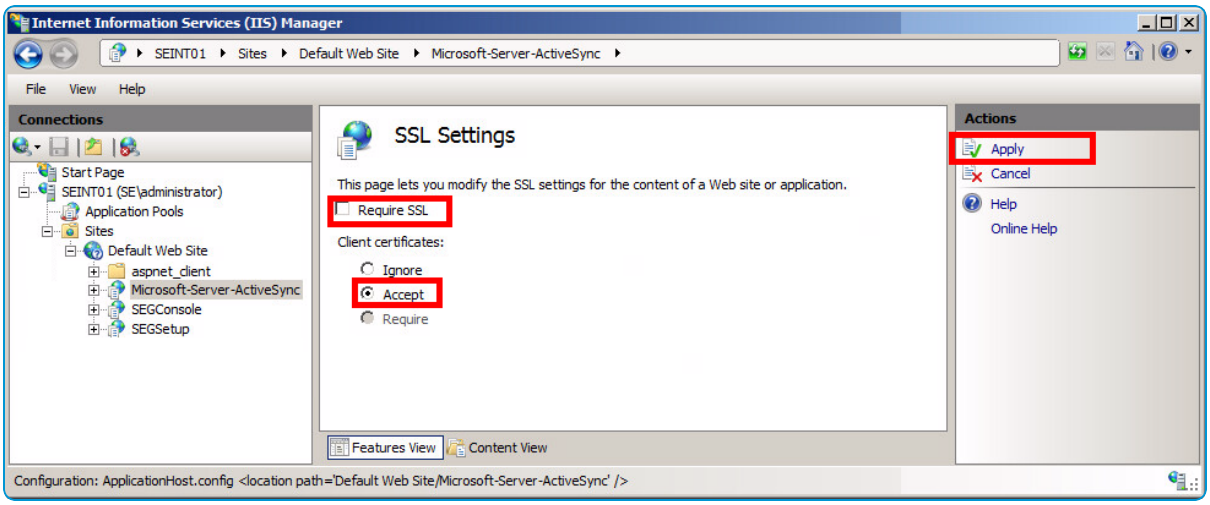
If only certificate authentication is being used then you must configure Secure Socket Layer (SSL). Otherwise, if authentication other than certificates is used then you do not need to configure SSL.

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.

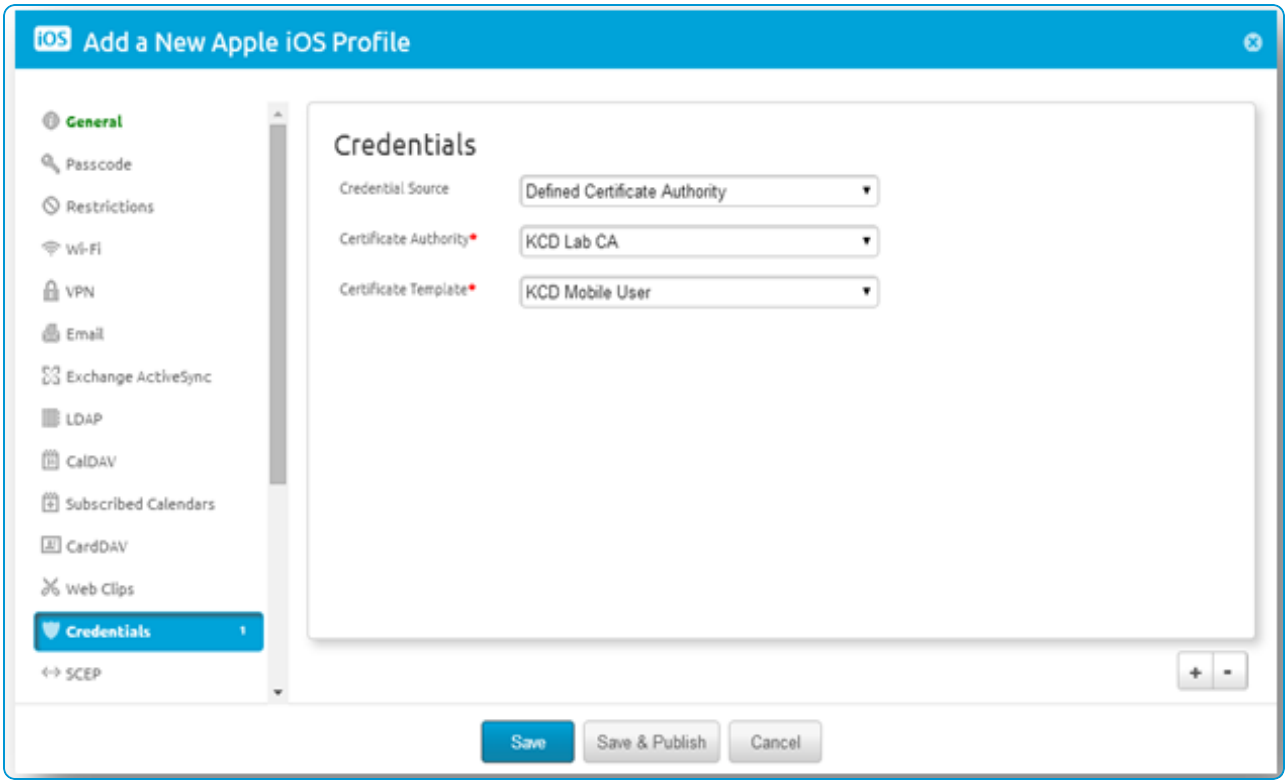
4. Type the following command to reset the IIS:

   ```
   iisreset
   ```

Configure EAS and Credential Profile

1. Navigate to **Devices > Profiles > List View** in the UEM console. Create a new profile for Android or iOS. Assign the profile a **Friendly Name**. Be aware of the **Assignment Type** and who might receive this profile when you publish the profile. Make any additional changes to the **General Settings** that you would like.

2. Select the **Credentials** payload and then select **Configure**. Select **Defined Certificate Authority** and then select your CA and template that were configured previously. Refer to Resource Portal if this has not already been completed.

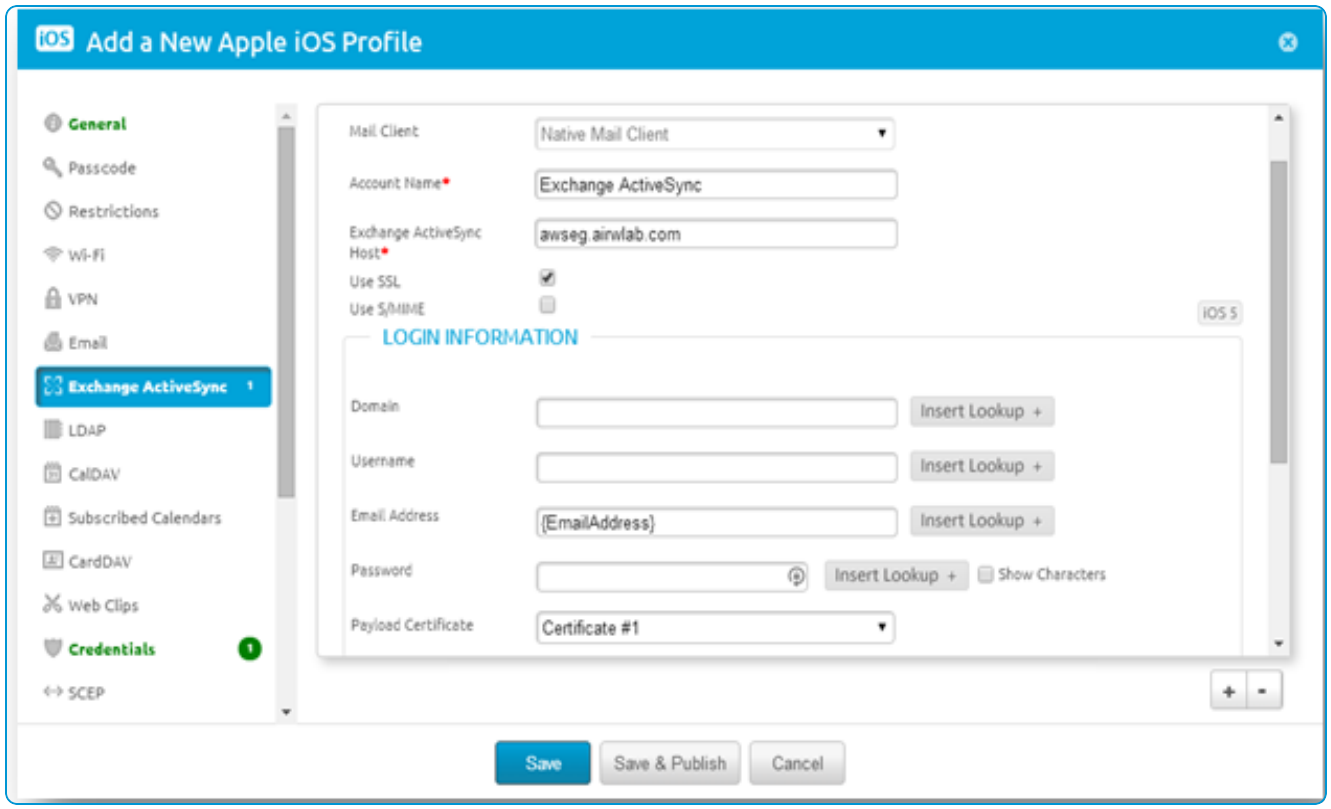


3. Select the **Exchange ActiveSync** payload. Enter the **Exchange ActiveSync Host**; this is the public DNS name of the SEG server. Ensure **Use SSL** is selected.

4. Set the **Payload Certificate** to **Certificate #1.**

5. Remove any entries in the **Domain** and **Username** fields. Set **Email Address** to the desired lookup value. You may

now **Save** or **Publish** if you are ready to push the profile to devices.



Chapter 3:
Kerberos Authentication to Load Balance Servers

Create Alternate Service Account (ASA)

If the environment has multiple Client Access Server (CAS) or Exchange ActiveSync (EAS) servers, then the service registration procedure varies. An alternate service account needs to be created to represent the CAS Array.

Leveraging 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, but we still recommend 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.

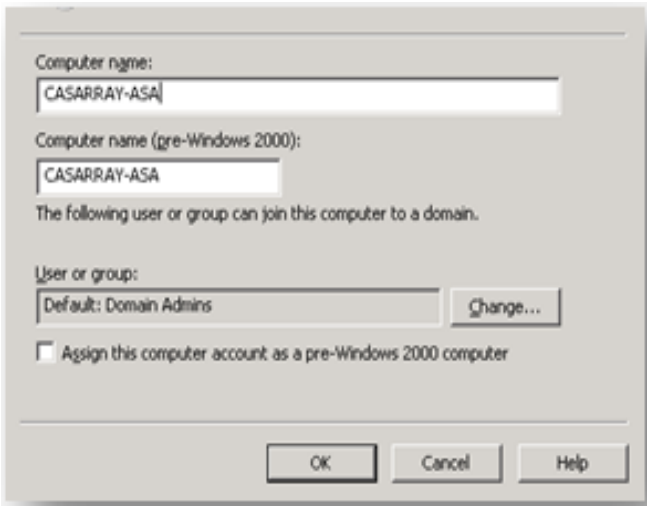
Groups and Roles

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 server array 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 ARRAY 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 array's FQDN, since this name is used for the SPN that is attached to the ASA. In order to check the CAS Array's FQDN, run the next command in PowerShell.

```
Get-ClientAccessArray
```

3. Create the SPN using the setspn command.

```
setspn -s http/{CAS-FQDN} {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 "{DOMIAN}\{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*
```

7. Return to step 6 in the Assign Delegation Rights to the Service Account, and then enable the SEG to delegate HTTP EAS traffic to the newly created ASA instead of the Exchange server FQDN.

The following documents were referred for writing this section:

- http://fixexchangeserver.blogspot.com/p/configuring-asa-alternate-service.html
- http://blogs.technet.com/b/pfemsgil/archive/2012/08/03/setting-up-kerberos-with-a-client-access-server-array-exchange-2010-sp2.aspx

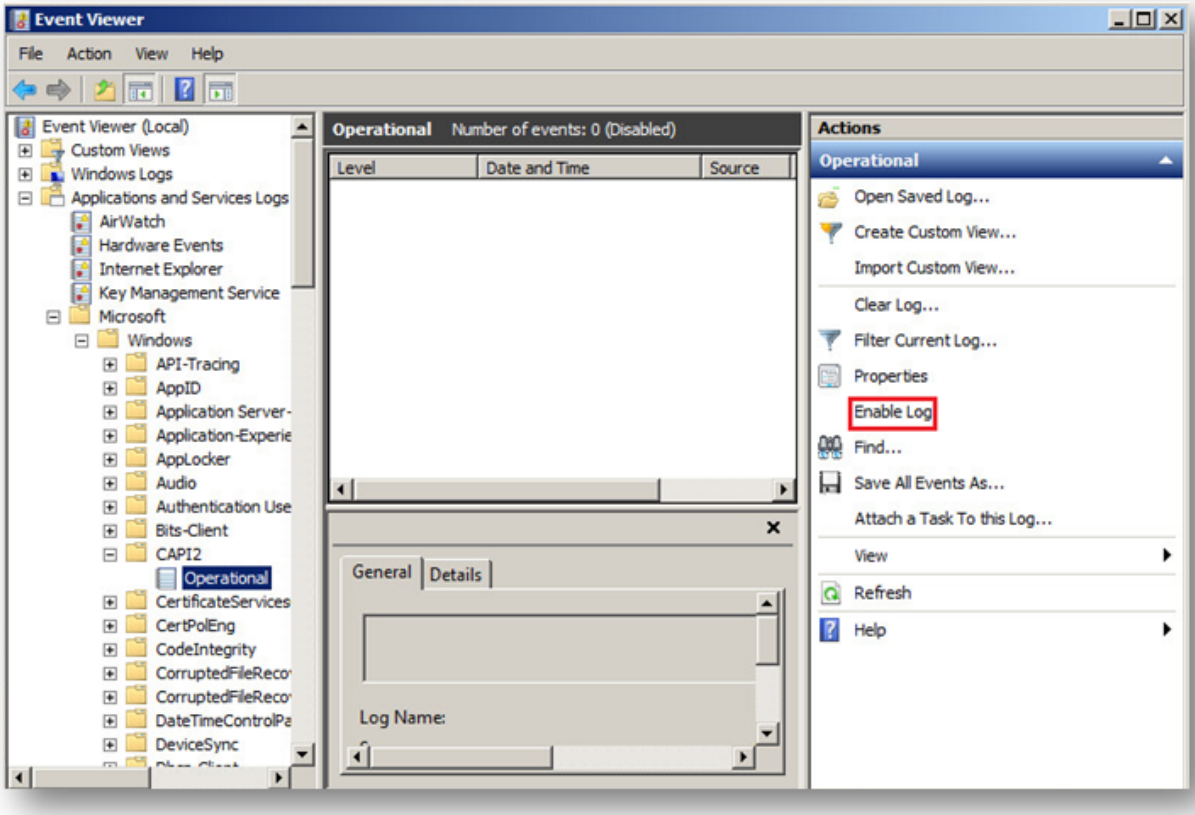
Chapter 4:
Troubleshooting

Tools and Techniques

CAPI2 Event Logging

CAPI2 (Cryptographic API) Event Logging captures information including certificate authentication logs from IIS. Enabling the CAPI2 log in Event Viewer is a simple way to quickly determine the cause of any invalid certificate errors. The CAPI2 log should be enabled on the server which is receiving the client certificates.

To enable the CAPI2 Event Log, open the **Event Viewer** and navigate to **Applications & Services Logs > Microsoft > Windows > CAPI2 > Operational** and then select **Enable Log** in the actions panel.



Once the logs are enabled you can resubmit the request from a client device with the certificate and you can see that new events become available. In order to see the events, you need to refresh the log by selecting Refresh in the Actions panel.

Note: It is important to note that there are many system events that can generate errors in this log so you should be sure to isolate the events that are generated by the client certificate being presented. You should look at the Details tab of the events to find more information. It is common to see the certificate information in the events as well as more details as to why the certificate is not being accepted. You can also use **Find...** to search for the client certificates Common Name.

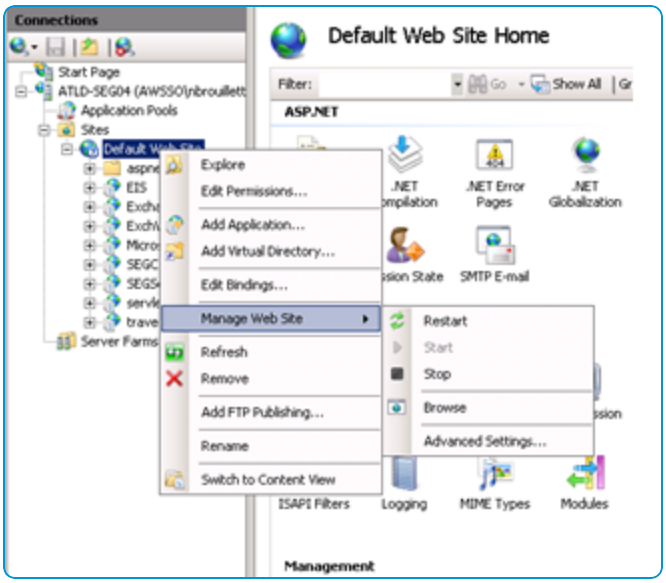
If you do not see events related to your certificate in the logs, it is likely that the certificate is not being presented to the server or that the server is not configured to accept client certificates.

Failed Request Tracing

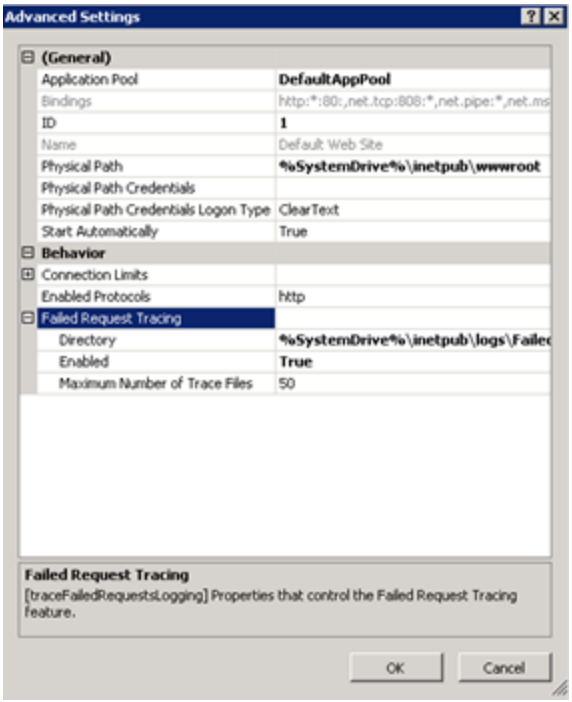
Failed Request Tracing can be helpful in gathering details about the cause of an authentication failure.

In order to enable failed request tracing:

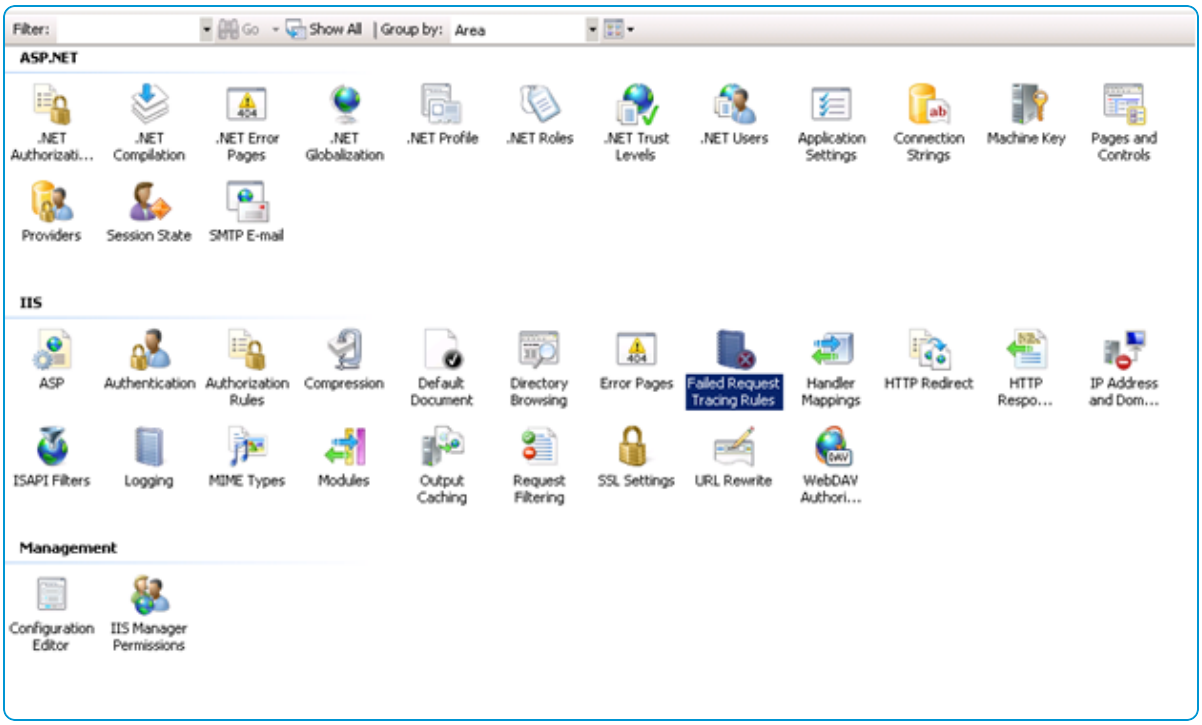
1. Open IIS, right-click the **Default Website** and select **Manage Website>Advanced Settings**.



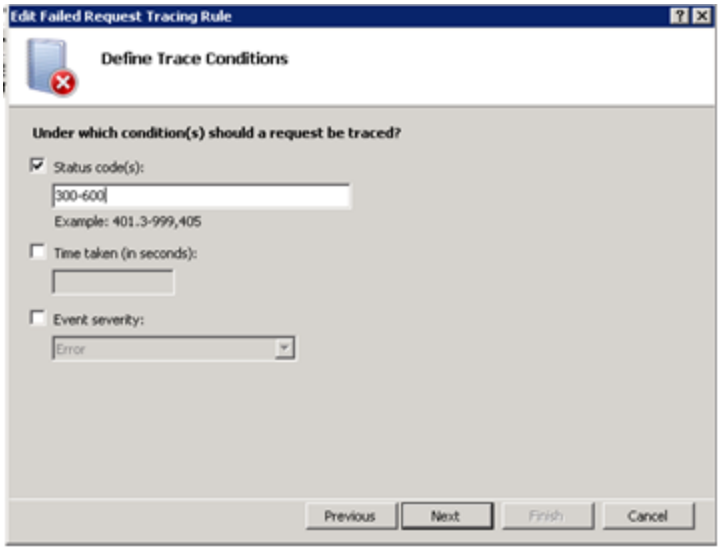
2. Under the **Behavior** header, expand **Failed Request Tracing**. Note the directory where log files are saved, and set the **Enabled** field to True. Click **OK**.



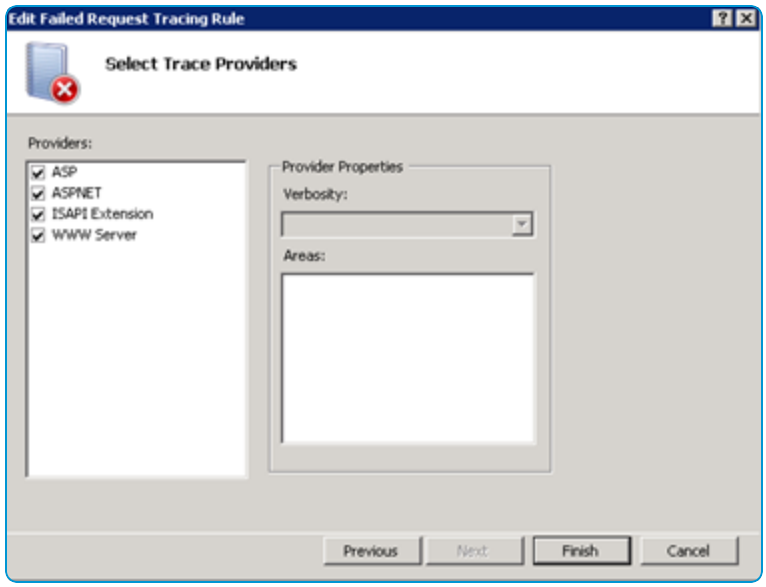
3. Double-click **Failed Request Tracing Rules** from the IIS home menu.



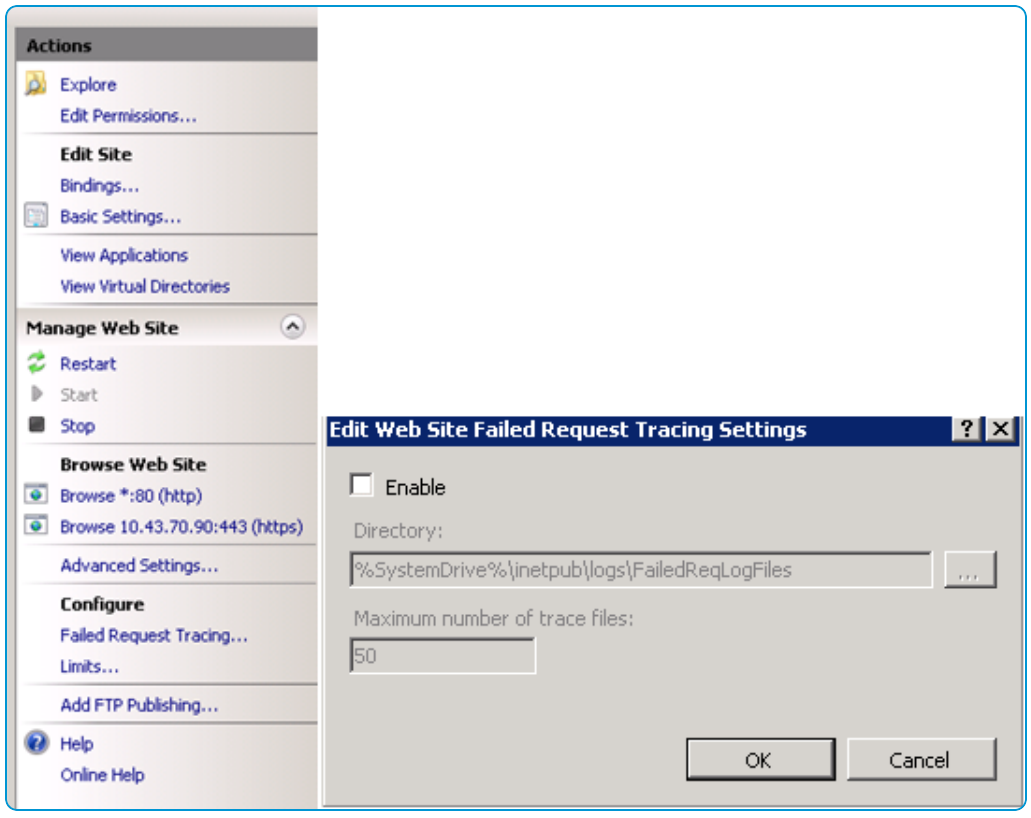
4. Edit the rule so that the appropriate status codes are tracked. A range of 300-600 will suffice for the initial troubleshooting.



5. Select **Finish** to save the edited rule.



6. To disable Failed Request Tracing,select **Failed Request Tracing** on the right hand toolbar. Then clear the **Enable** checkbox and select **OK**. Failed Request can be enabled using this method as well.



Packet Capture

Tools such as WireShark or Microsoft's Network Monitor allow you to view the packets sent and received by the server. Knowing what to look for can help you determine where issues are occurring and isolate the reason why authentication is

failing.

Kerberos Event Logging

1. Start the Registry Editor.
2. Add the following registry value:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Kerberos\Parameters

   - Registry Value: LogLevel
   - Value Type: REG_DWORD
   - Value Data: 0x1

If the Parameters subkey does not exist, create it.

Remove this registry value when it is no longer needed so that performance is not degraded on the computer. Also, you can remove this registry value to disable Kerberos event logging on a specific computer. System restart should not be required.

Disabling CRL Checking

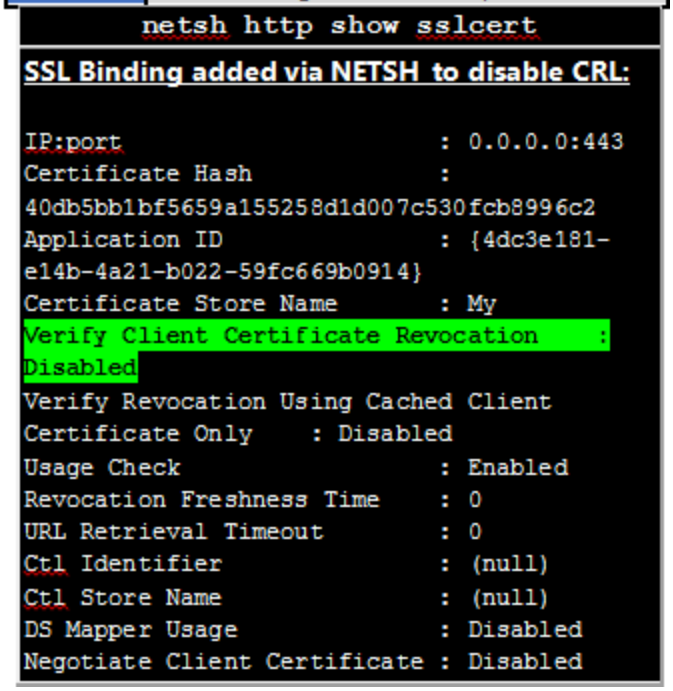
REGISTRY : HKLM\SYSTEM\CurrentControlSet\Services\HTTP\Parameters\SslBindingInfo

DWORD : DefaultSslCertCheckMode

Value : 1

DefaultSslCertCheckMode can take the following values. Refer to https://msdn.microsoft.com/en-us/library/aa364647.aspx for more info.

VALUE	MEANING
0	Enables the client certificate revocation check
1	Client certificate is not to be verified for revocation.
2	Only cached certificate revocation is to be used
4	The DefaultRevocationFreshnessTime setting is enabled
0x10000	No usage check is to be performed



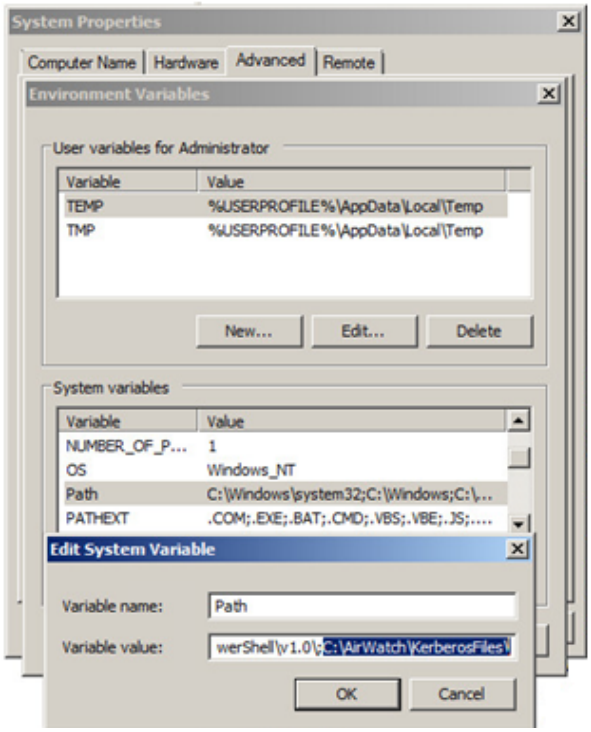
Client Certificate Revocation is always enabled by default.

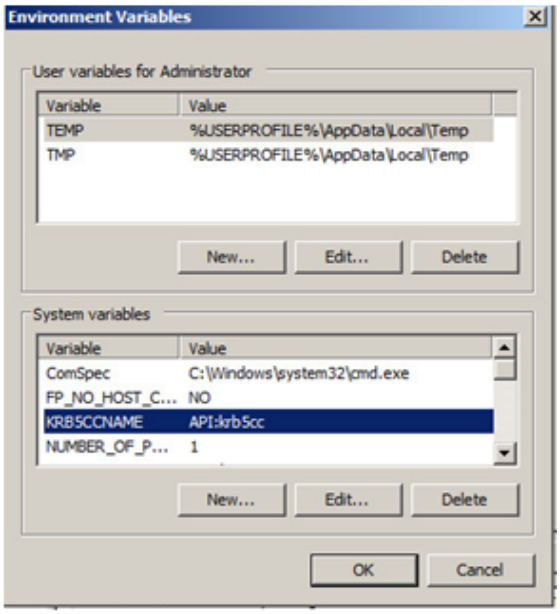
Errors and Solutions

Error A: Cannot find Kerberos or its dependencies

Solution:

- Check the **Path** Environment Variable to ensure that the {AirWatchInstallDirectory}\KerberosFiles is entered.

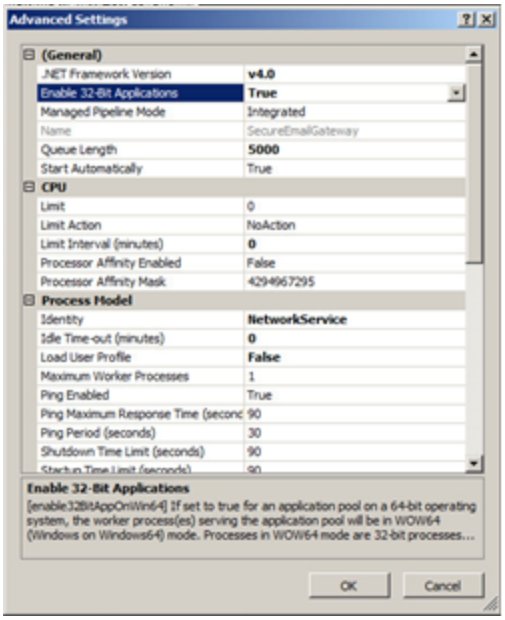




Error B: Return 500 at Beginning of Request

Solution:

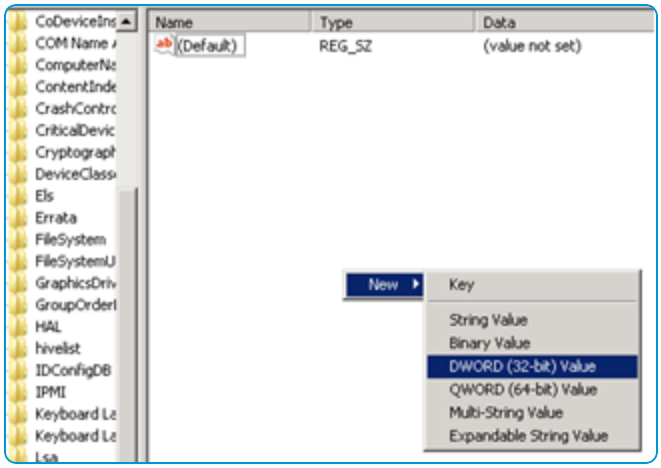
1. Check identity of secureEmailGateway application pool. It should be set to NetworkService.
2. Check that the App Pool is set to Enable 32-Bit application mode.

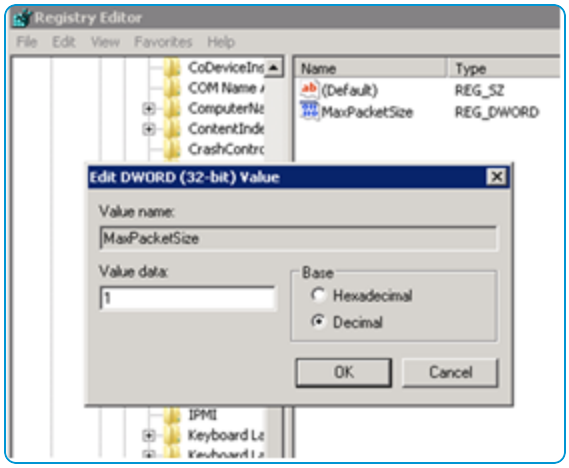


Error C: Get Kerberos token failed

Solution:

1. Check DNS, make sure exchange server is pingable.
2. Check that C:\Program Data\MIT\Kerberos5\krb5.ini is configured correctly.
3. Perform the steps for the error **0x34 - KRB_ERR_RESPONSE_TOO_BIG: Response too big for UDP (Token Error)**:
   a. Start regedit on the SEG server.
   b. Browse to **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\ Kerberos\Parameters**.
   c. Create a Dword called MaxPacketSize.
   d. Change the value of the Dword to 1.





Error D: NTAuth Store is Missing Root CA Certificate

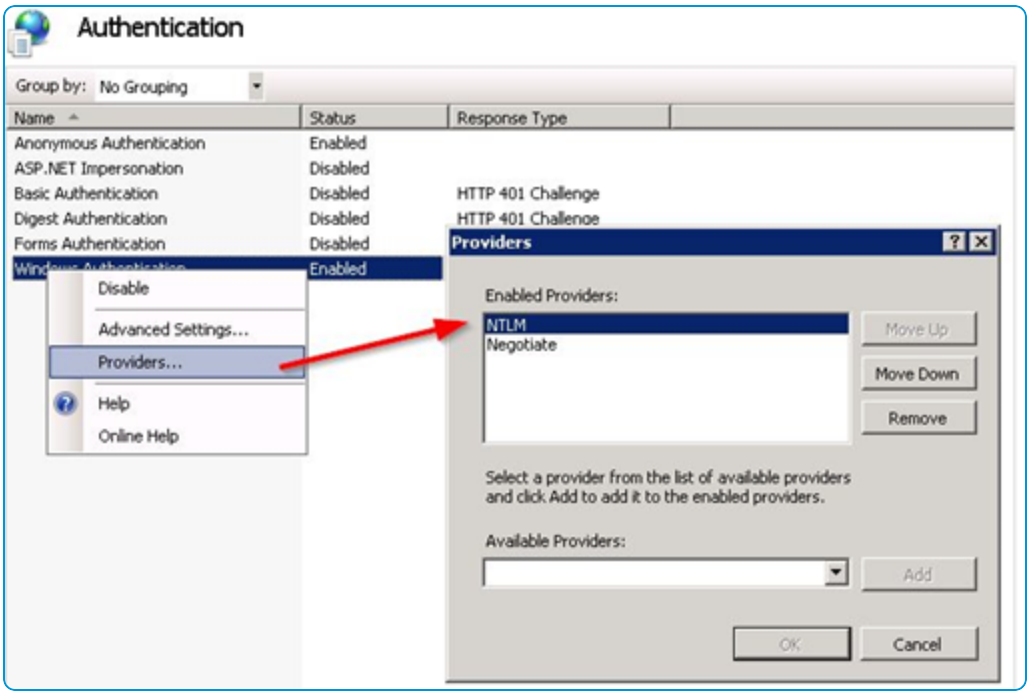
- Add the Issuing and Root CA certificates to the NTAuth store using the following command:

```
certutil -enterprise -addstore NTAuth CA_CertFilename.cer
```

Error E: Exchange returns 401 with correct SEG configuration

Solution:

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



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

   a. Go to the internal CA Server, launch the certification authority application, and browse to the issued certificates section.

   b. 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 connection to client access server.

   c. 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.

   d. Check that the account information is entered correctly in the Workspace ONEconfiguration.

   e. Verify the Server URL and the SCEP Challenge URL contain the correct information and end with a "/".

   f. 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.

3. If the certificate is being issued, make sure that it is in the Profile Payload and on the device.

   a. 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.

   b. On the device, go to the profiles list,select Details and see if the certificate is present.

   c. 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 Configuring IIS for Certificate Authentication on SEG.

d. 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.

4. 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 profile and that all the security settings have been adjusted for allowing certificate authentication on the SEG server.
5. 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 network and until this works properly, you cannot configure Workspace ONE 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.
6. If none of the steps above resolve the problem, try authenticating independent of Workspace ONE. This is done by eliminating the Workspace ONE (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.
7. 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.
8. 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 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**.