Kerberos Constrained Delegation Authentication for SEG V2

Implementing KCD Authentication for SEG V2

Workspace ONE UEM v9.7

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

Table of Contents

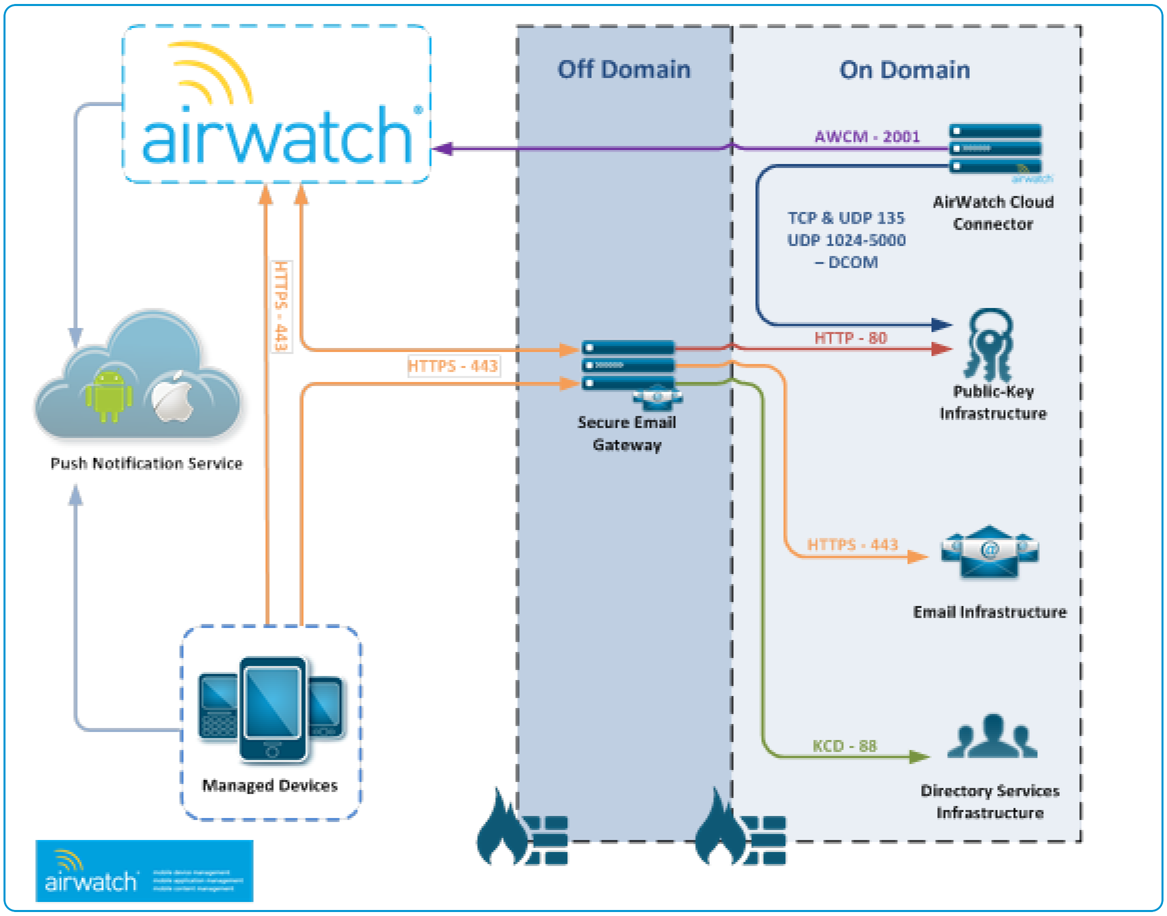
Chapter 1:
Introduction

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 SEG to use client certificate authentication, you must meet the following pre-requisites:

- A Windows Server (2008 R2 or higher)
- A Certificate Authority (CA) integrated with Workspace ONE UEM to issue certificates to your mobile devices. In this documentation, Microsoft is used as an example for a CA. However, Workspace ONE UEM supports certificates from multiple CAs.
- A trust relationship between the CA and the Directory Services server.
- A domain service account to use as the Principal Identity with designated permission to impersonate users to the EAS service.
- A Certificate Revocation List (CRL) for CA that is accessible over HTTP and CRL distribution point. For more information, see Configure Certificate Revocation List over HTTP for CA on page 18 .
- 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 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 Additional Information on page 16.

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
AW	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:

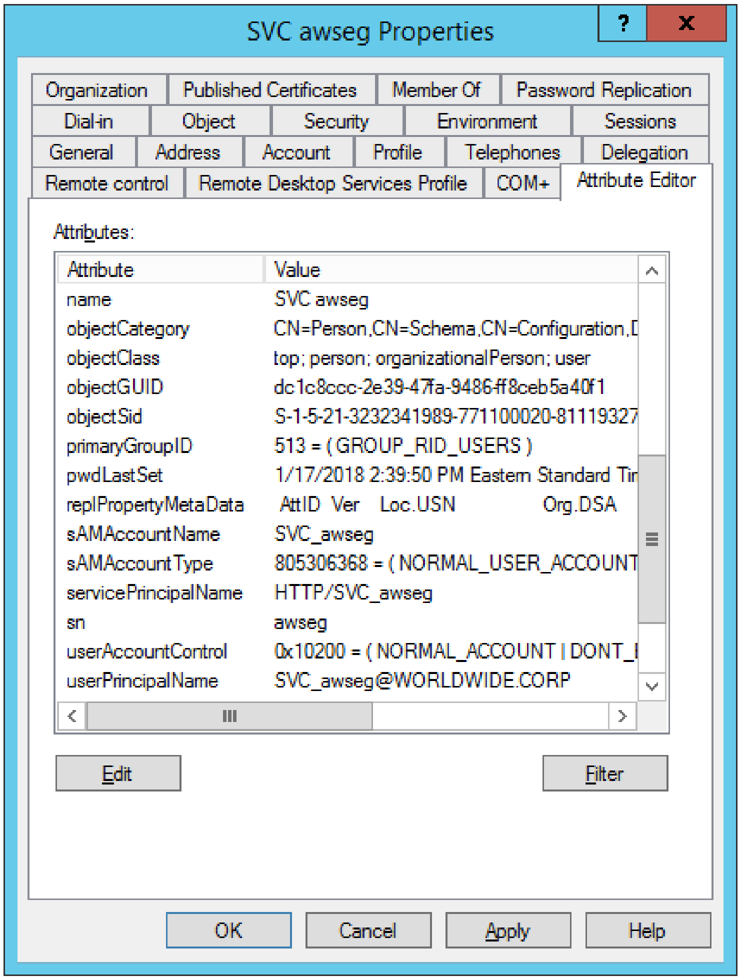
```
setspn -s HTTP/{EX_DNS_NAME} {EX_MACHINE_NAME}
```

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 have a Service Account created for the SEG to use for the Kerberos request, create a Service Account and name the Service Account **SVC awseg**.
3. Right-click the Service Account, and select **Properties**. In the **Properties** menu, select the **Attribute Editor** tab.
4. To assign delegation rights to a user account, Microsoft requires that the account be assigned a Service Principal

Name (SPN). Find the **servicePrincipalName** attribute in the list and edit it to be in the format **HTTP/SVC_awseg**.

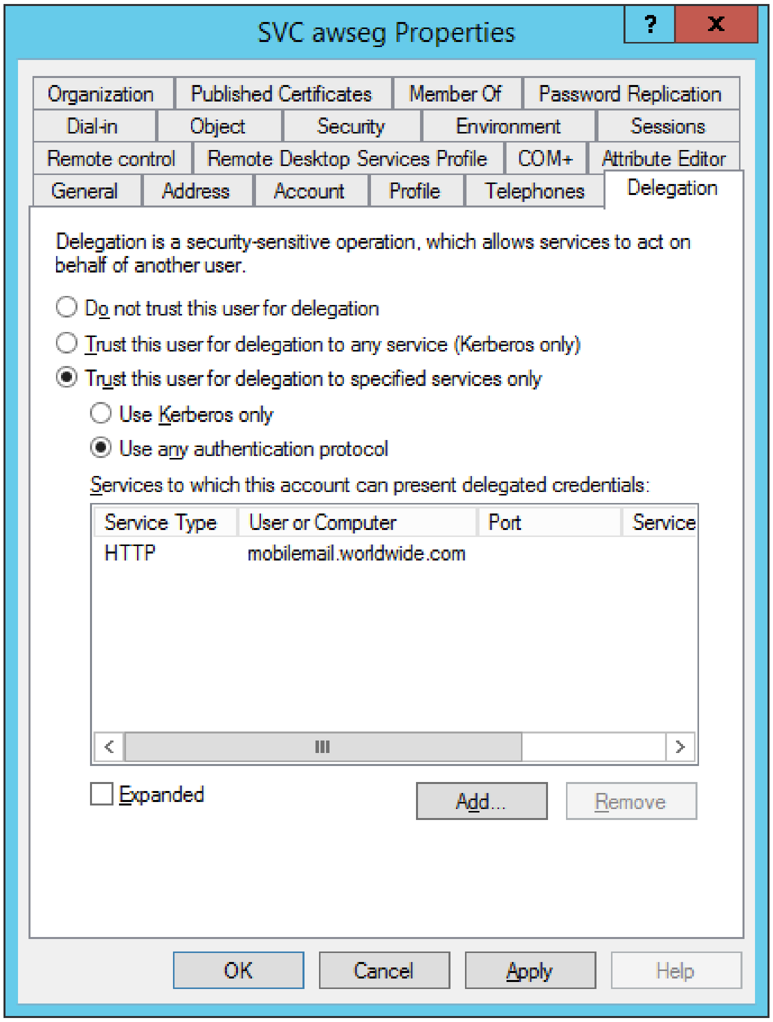


Attribute	Value
name	SVC awseg
objectCategory	CN=Person,CN=Schema,CN=Configuration,D
objectClass	top; person; organizationalPerson; user
objectGUID	dc1c8ccc-2e39-47fa-9486-ff8ceb5a40f1
objectSid	S-1-5-21-3232341989-771100020-81119327
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	1/17/2018 2:39:50 PM Eastern Standard Tir
replPropertyMetaData	AttID Ver Loc.USN Org.DSA
sAMAccountName	SVC_awseg
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
servicePrincipalName	HTTP/SVC_awseg
sn	awseg
userAccountControl	0x10200 = (NORMAL_ACCOUNT | DONT_I
userPrincipalName	SVC_awseg@WORLDWIDE.CORP

5. After setting up the SPN for the user account, close the **Properties** window and reopen it 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**.

7. Select **Add** and then search and select the Exchange server (or the ASA account) for which you want to provide the delegation rights. You should provide the actual machine name of the Exchange server {EX_MACHINE_NAME}. For example EXCH. 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. If you have not set the SPN, select the HTTP service type for your server.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation

○ Trust this user for delegation to any service (Kerberos only)

● Trust this user for delegation to specified services only

○ Use Kerberos only

● Use any authentication protocol

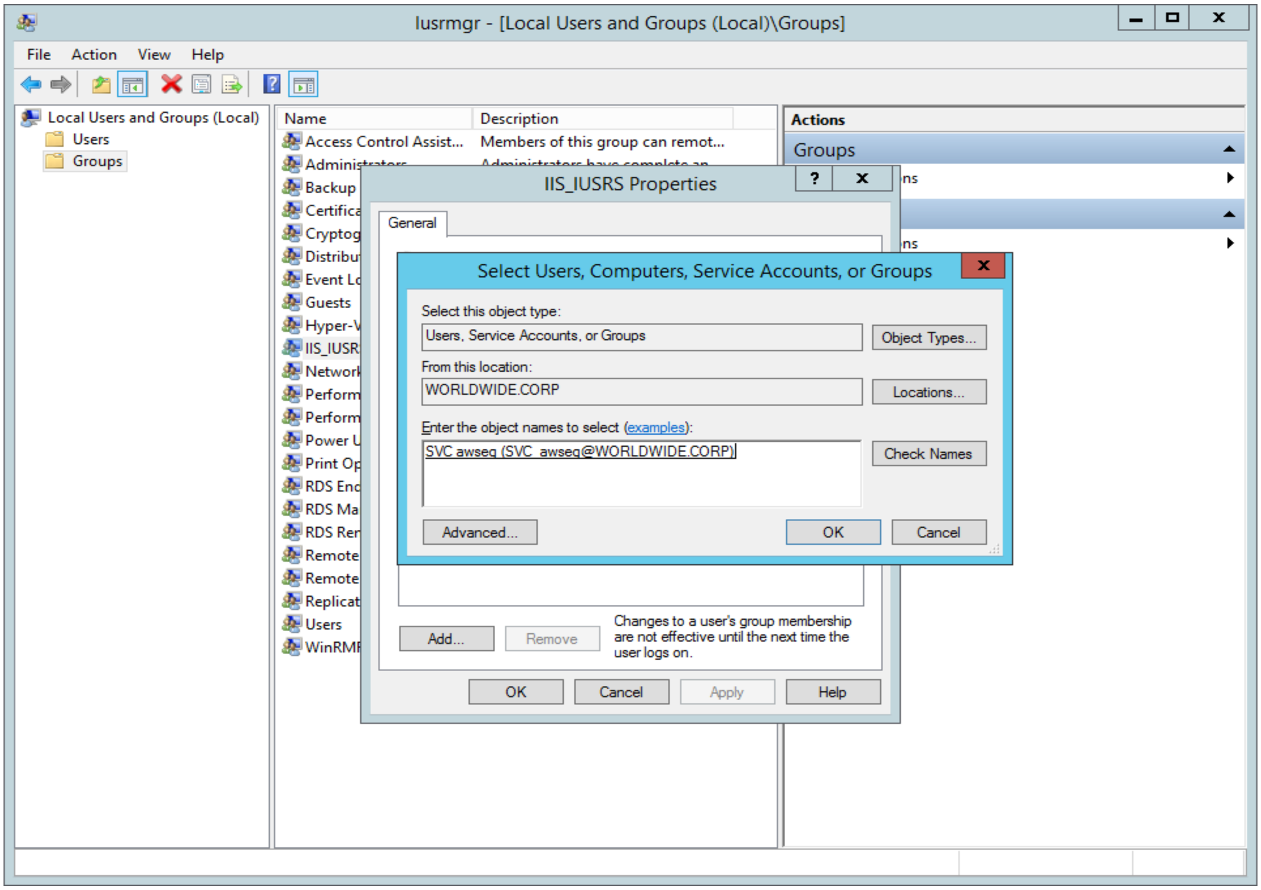
Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service
HTTP	mobilemail.worldwide.com		

□ Expanded

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 SVC_awseg Service Account, add the user to the local group, and then select **OK**.



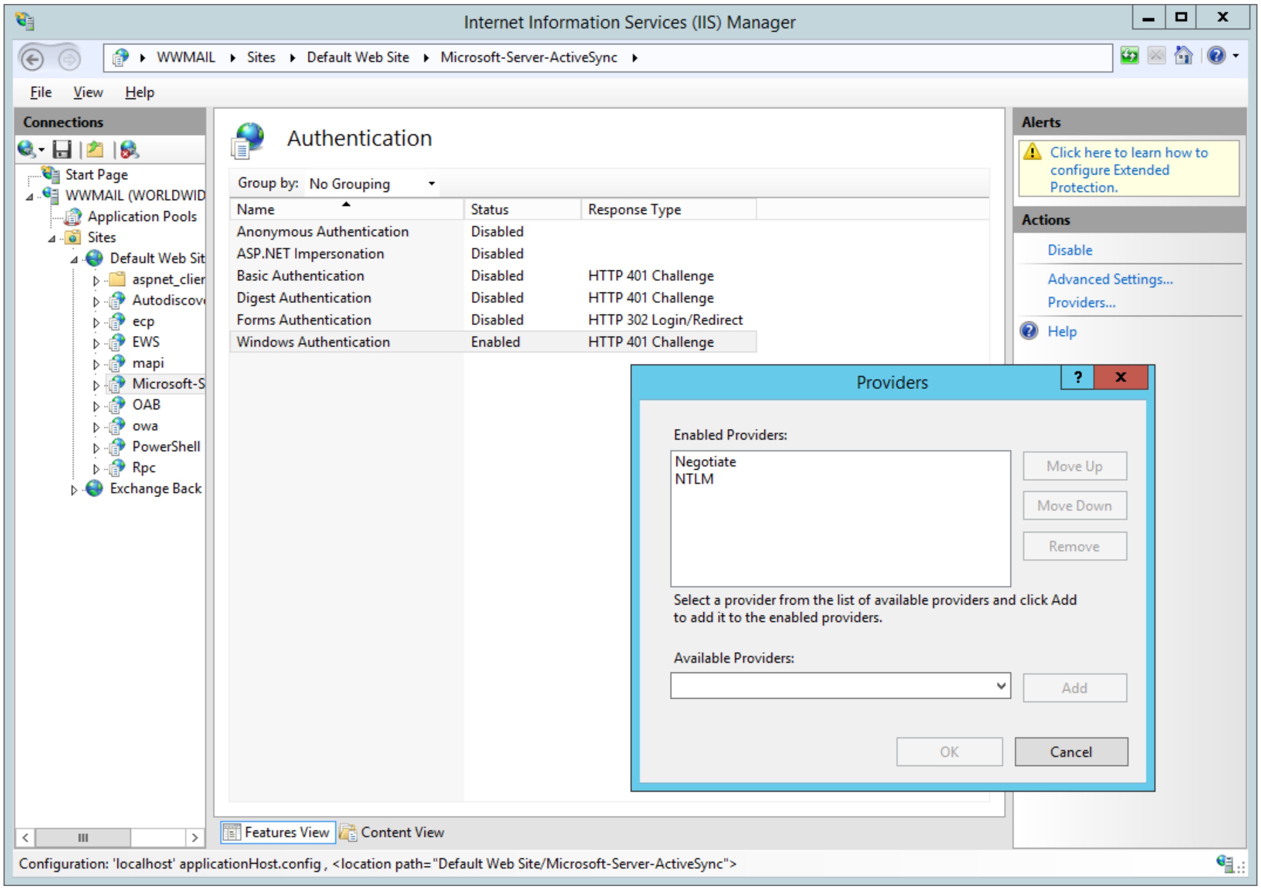
Select this object type: Users, Service Accounts, or Groups

From this location: WORLDWIDE.CORP

Enter the object names to select (examples): SVC awseg (SVC_awseg@WORLDWIDE.CORP)

Enable Windows Authentication on the CAS/EAS

1. On the Exchange Server, open IIS Manager and navigate to the **Microsoft-Server-ActiveSync** Virtual Directory.
2. Select **Authentication**, enable **Windows authentication** and then disable **Anonymous authentication**. If Exchange server returns a 401, add **NTLM** and **Negotiate** as providers to Windows Authentication.



Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

Providers

Enabled Providers:

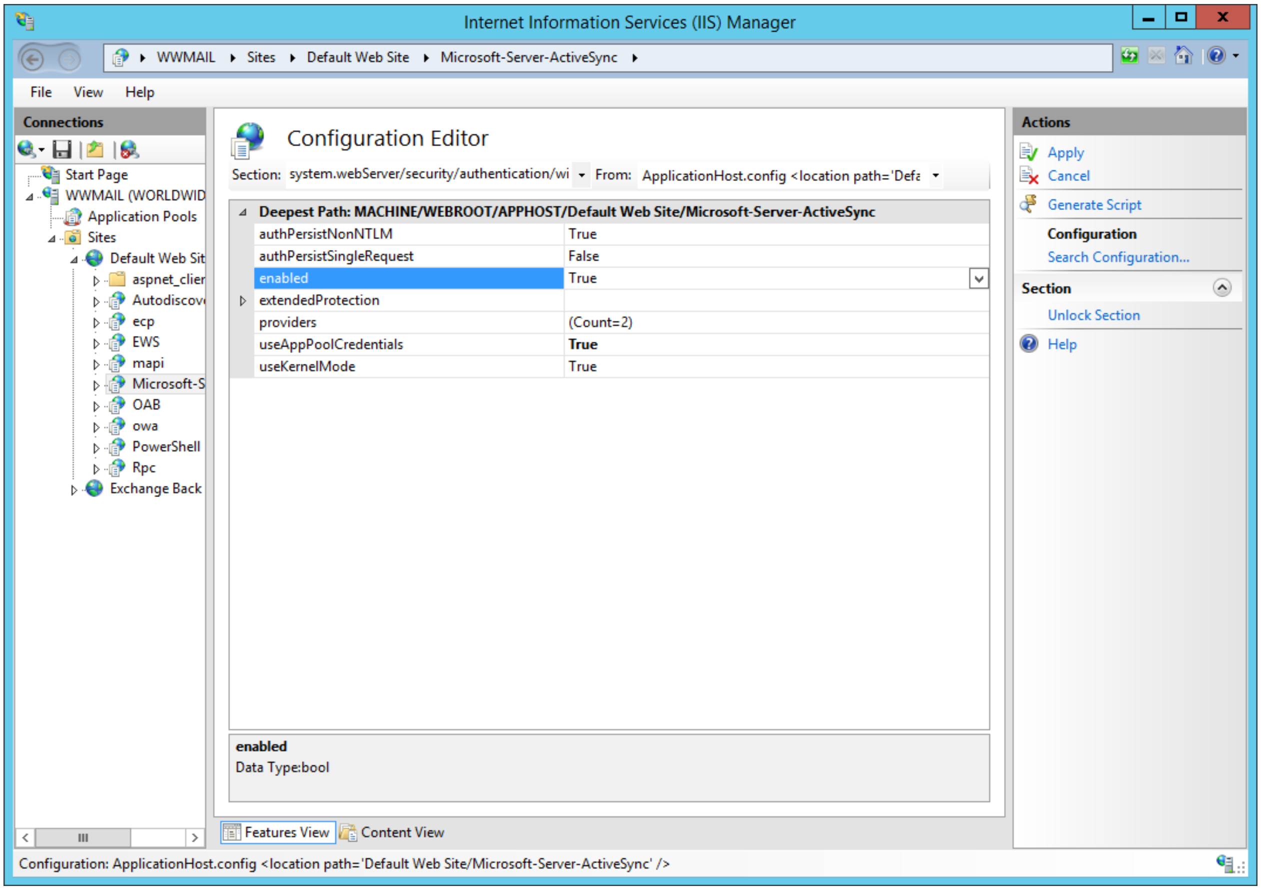
Negotiate
NTLM

Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

Configuration: 'localhost' applicationHost.config , <location path="Default Web Site/Microsoft-Server-ActiveSync">

3. In the **Microsoft-Server-ActiveSync Virtual Directory**, access the **Configuration Editor** and navigate to **system.webServer > Security > Authentication > WindowsAuthentication**. Select **Enabled**, set **useAppPoolCredentials** and **useKernelMode** values to **True**.



Section: system.webServer/security/authentication/wi From: ApplicationHost.config <location path='Defa

Deepest Path: MACHINE/WEBROOT/APPHOST/Default Web Site/Microsoft-Server-ActiveSync

authPersistNonNTLM	True
authPersistSingleRequest	False
enabled	True
extendedProtection	
providers	(Count=2)
useAppPoolCredentials	**True**
useKernelMode	True

enabled
Data Type:bool

Configuration: ApplicationHost.config <location path='Default Web Site/Microsoft-Server-ActiveSync' />

Chapter 3:
Configure Secure Email Gateway (SEG)

Configure SEG on the UEM Console

This chapter provides information about configuring the SEG V2 for KCD using the UEM console.

Prerequisites

SEG is configured and installed. For detailed information regarding SEG configuration, see the *SEG Installation Guide* and *Admin Guides* .

Procedure

1. Navigate to **Email > Email Settings > Advanced**.
2. Deselect the **Use Recommended Settings** check box.
3. From the Client Certificate Chain, select **Upload** and then select **Choose File** to upload the certificate chain used to issue client certificates.
4. From the Require Client Certificate, select **Enable**. Enable the Require Client Certificate if it is a security requirement.
5. Select **Enable** to enable KCD Authentication.
6. From the KCD Authentication menu item, select **Target SPN** text box and enter the Target SPN in *HTTP/{exchangeName}* format. For example, HTTP/mobilemail.worldwide.com.
7. Select **Service Account User Name** text box and enter the name of your Service Account. For example, SVC_awseg.
8. Select **Service Account Password** text box and enter the password for your Service Account.
9. Select **Add Domain**.The Add Domain menu item displays the Domain and Domain Controller text boxes.
   a. Select the **Domain** text box and enter the domain name. The domain name is case-sensitive and must be entered in uppercase. For example, AMER.WORLDWIDE.CORP.

   b. Select the **Domain Controller** text box and enter the domain controller server name. For example, amer.worldwide.corp. The domain and domain controllers must be added in pairs and all domains must have trust with the primary domain.

10. Select **Save**. To apply the KCD settings, restart the SEG service.

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 the target users who receive this profile when you publish the profile. Make additional changes to the **General Settings** as per your requirement.

2. Select the **Credentials** payload and then select **Configure**. Select **Defined Certificate Authority** and then select your CA and template that are configured.

3. Select the **Exchange ActiveSync** payload. Enter the **Exchange ActiveSync Host**. The Exchange ActiveSync Host is the public DNS name of the SEG server.

4. Select **Use SSL**.

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

6. Remove any entries in the **Domain** and **Username** text boxes. Set **Email Address** to the desired lookup value.

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

Chapter 4:
Additional Information

Create an 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 (ASA) 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.

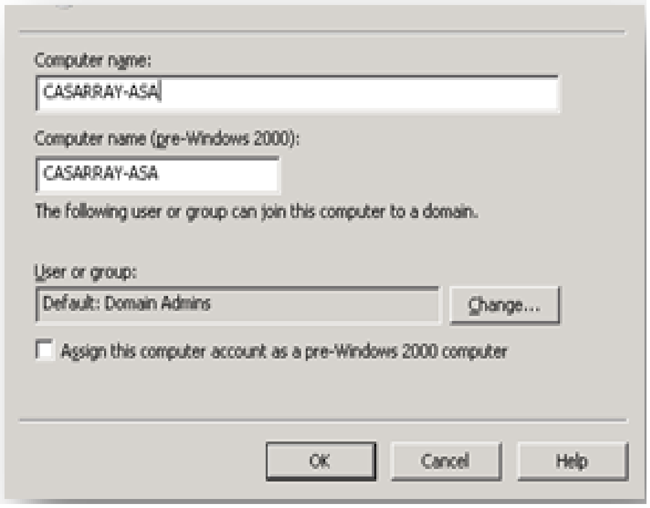
Groups and Roles

The ASA credential does not need special security privileges. If you are deploying a computer account for the ASA credential, 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, 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 CAS that are called on in a data center activation scenario must also share the same Service Account.

1. Create the ASA for the CAS ARRAY in the domain by opening the Active Directory User and Computers and creating new computer account. Enter a name for the ASA. For example, CASARRAY- ASA . Verify that the account has replicated to all Domain Controllers before proceeding.



Computer name:
CASARRAY-ASA

Computer name (pre-Windows 2000):
CASARRAY-ASA

The following user or group can join this computer to a domain.

User or group:
Default: Domain Admins

□ Assign this computer account as a pre-Windows 2000 computer

2. Verify the CAS array's FQDN. The FQDN is used for the SPN that is attached to the ASA. To check the CAS Array's FQDN, run the following command in PowerShell:

```
Get-ClientAccessArray
```

3. Create the SPN using the following command:

```
setspn -s http/{CAS-FQDN} {ASA_ACCOUNT}$
```

4. Verify that all relevant SPNs have been assigned by running the following command in 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. After the script is run, a **Success** message is displayed. To verify if the ASA credentials is deployed, 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.

Configure Certificate Revocation List over HTTP for CA

The SEG requires that the client certificate CRLs are reachable over HTTP. By default, Microsoft CA's are configured for accessing the CRL over LDAP and not HTTP. You can configure the CA for accessing CRL over HTTP by installing the AD CS role service *Certification Authority Web Enrollment*. For more information about manually configuring a CA to access the CRL over HTTP, see *Creating a Certificate Revocation List Distribution Point for Your Internal Certification Authority* page available at *blogs.technet.microsoft.com*.

Chapter 5:
Upgrade from Classic SEG with KCD

If you are upgrading from a Classic SEG deployment, create a secondary MEM configuration for SEG V2. This is because the inputs for KCD with SEG V2 are different from that of Classic SEG. The configuration changes in SEG V2 with KCD are intended to help streamline the deployment and maintenance of SEG.

Following are the configuration changes required when upgrading from Classic SEG with KCD:

- The Require Client Certificate is defined in the configuration as opposed to IIS.
- The certificate chain of trust is provided in the configuration and is not stored in the Microsoft Management Console.
- A Service Account must be used, regardless of SEG being joined to the domain. Using the computer account for Kerberos and impersonation is not supported.
- When entering domain and domain controller pairs, the domain controller needs to be explicitly provided as the Fully Qualified Domain Name (FQDN).