Kerberos Constrained Delegation Authentication for SEG V2

VMware Workspace ONE UEM

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

https://docs.vmware.com/

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

Contents

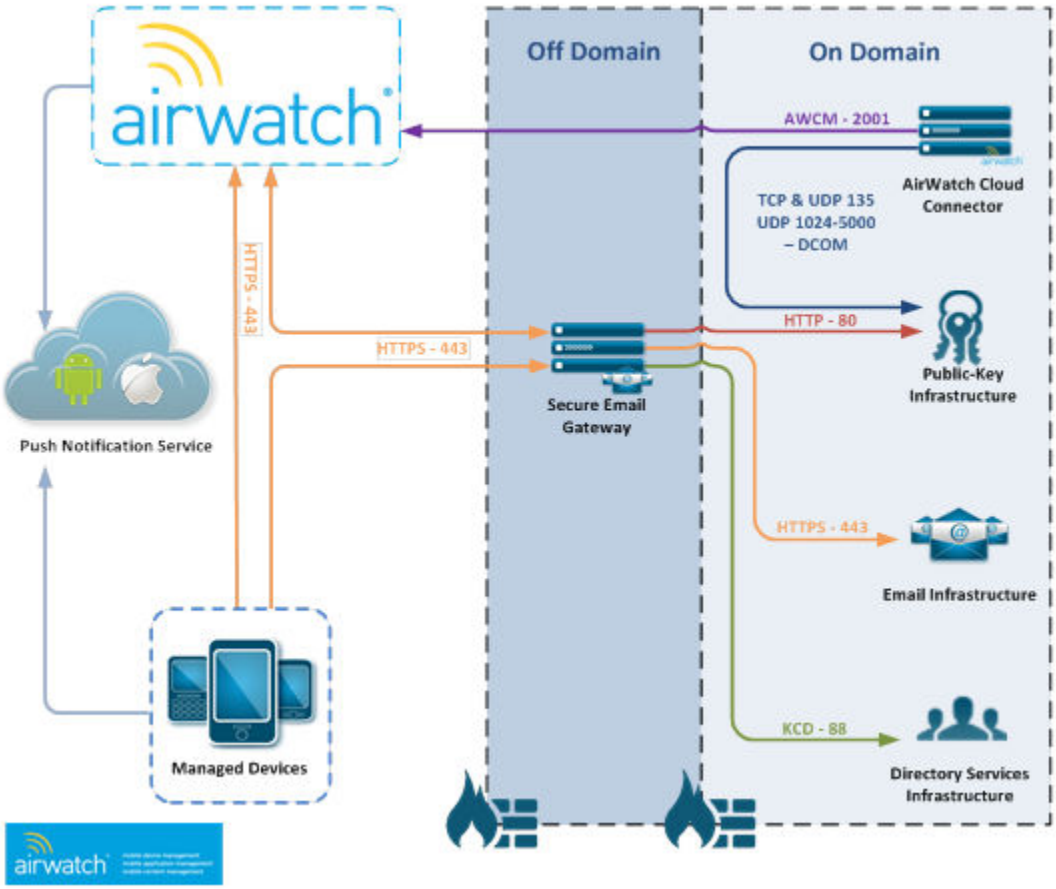
Introduction to Kerberos Constrained Delegation Authentication for SEG V2

1

Use certificates and kerberos to authenticate instead of usernames and passwords.

Kerberos Constrained Delegation (KCD) eliminates the use of basic authentication for email. The devices are issued certificates within their Exchange ActiveSync profile, instead of username and password authentication for email. SEG uses the unique user certificate to request secure Kerberos tickets from the domain controller, and embeds these tickets with the ActiveSync request to Exchange. In this way, authentication and authorization is secured by Workspace ONE UEM powered by AirWatch, while also providing a seamless user experience.

The following diagram shows a typical SaaS deployment.



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

This chapter includes the following topics:

Requirements for Using the Client Certificate Authentication

Before configuring the SEG to use client certificate authentication, 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 Chapter 4 Configure Certificate Revocation List over HTTP .
- 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 EAS servers in an array, you need to create an Alternate Service Account (ASA) in Active Directory. Instructions can be found in the Leveraging an ASA Credential Type.

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

Configure KCD for Cross Domain Authentication

2

Set up the Target Service Principal Name (SPN) for the Exchange Server.

If there are multiple EAS servers in an array, you must create an Alternate Service Account (ASA) in the 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:

Procedure

1. If the SEG is not referring to the Exchange server by its Fully Qualified Domain Name (FQDN) or its Machine Name, create a SPN for your Domain Controller to allow delegation by the service account.

   If the SEG is referring to the Exchange server by its Fully Qualified Domain Name (FQDN) or its Machine Name, skip this step.

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}
   ```

   Wherever **{EX_DNS_NAME}** is the name, the SEG uses it to refer to the Exchange server and {EX_MACHINE_NAME} is the actual machine name of the Exchange server, you must select this SPN when assigning delegation rights to the Service Account.

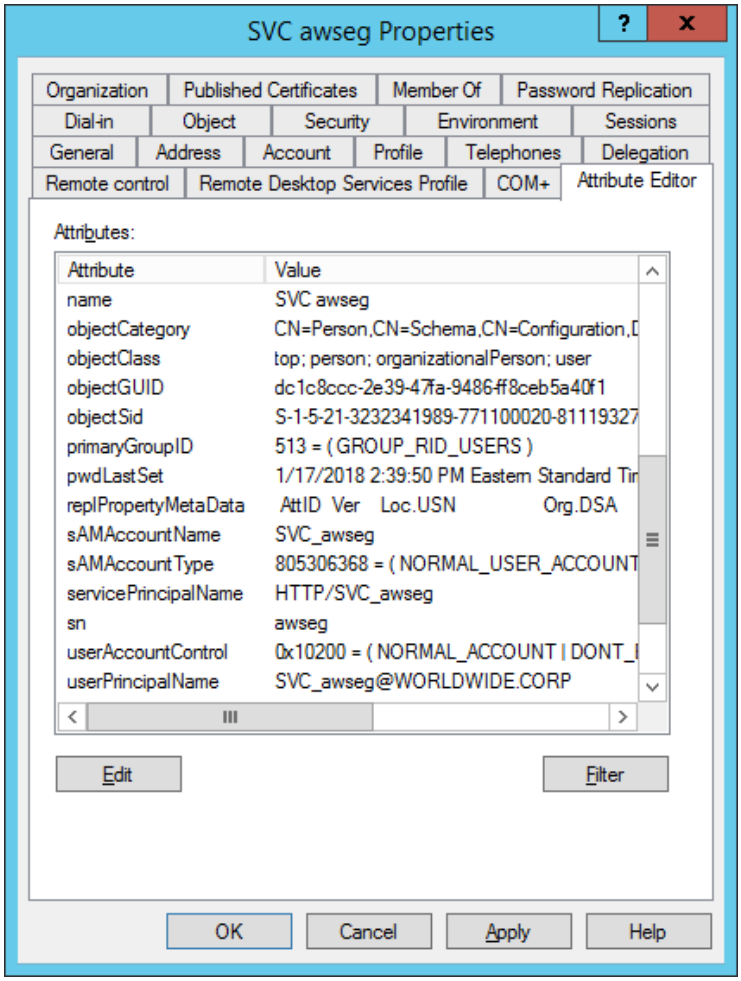
Assign Delegation Rights to the Service Account

Configure delegation rights for the service account.

Procedure

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.

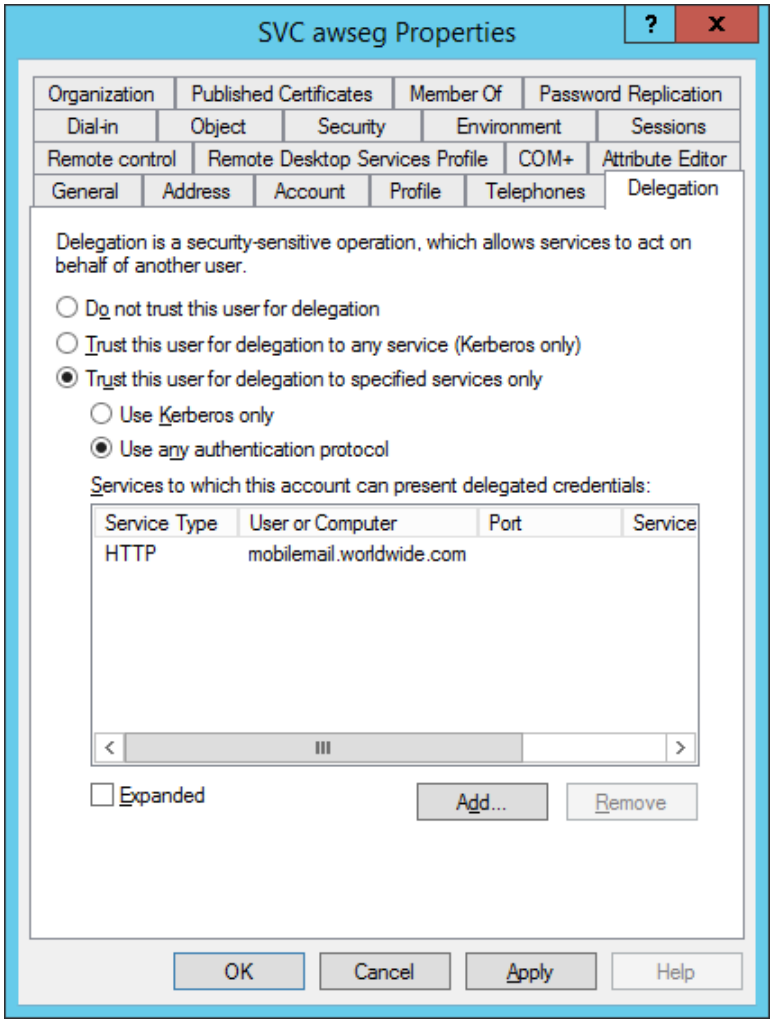
4 To assign delegation rights to a user account, Microsoft requires that the account be assigned a Service Principal Name (SPN). Find the **servicePrincipalName** attribute in the list and edit it to be in the format **HTTP/SVC_awseg**.



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 if you followed Leveraging an ASA Credential Type) 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.



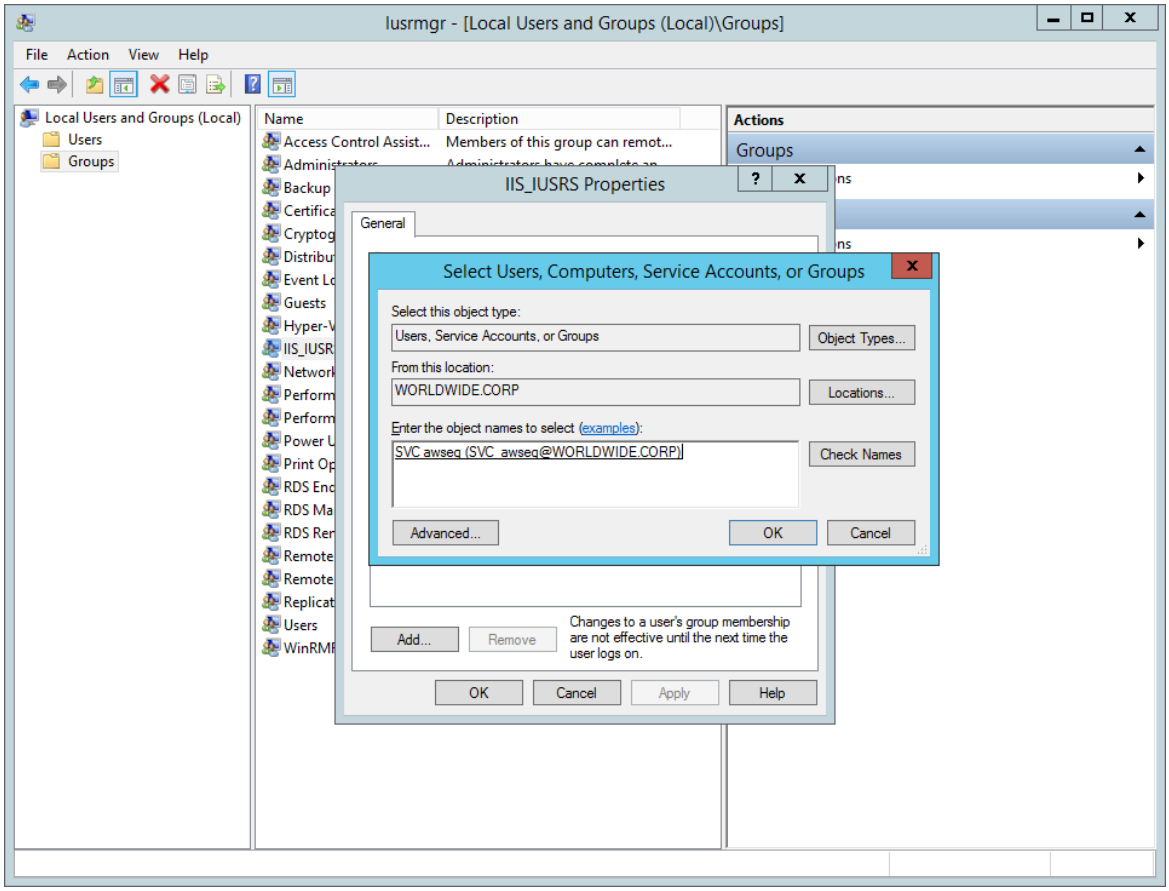
Add Service Account to Local IIS_IUSRS Group of the CAS/EAS Server

Add a service account to the IIS user groups of the ActiveSync server.

Procedure

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**.



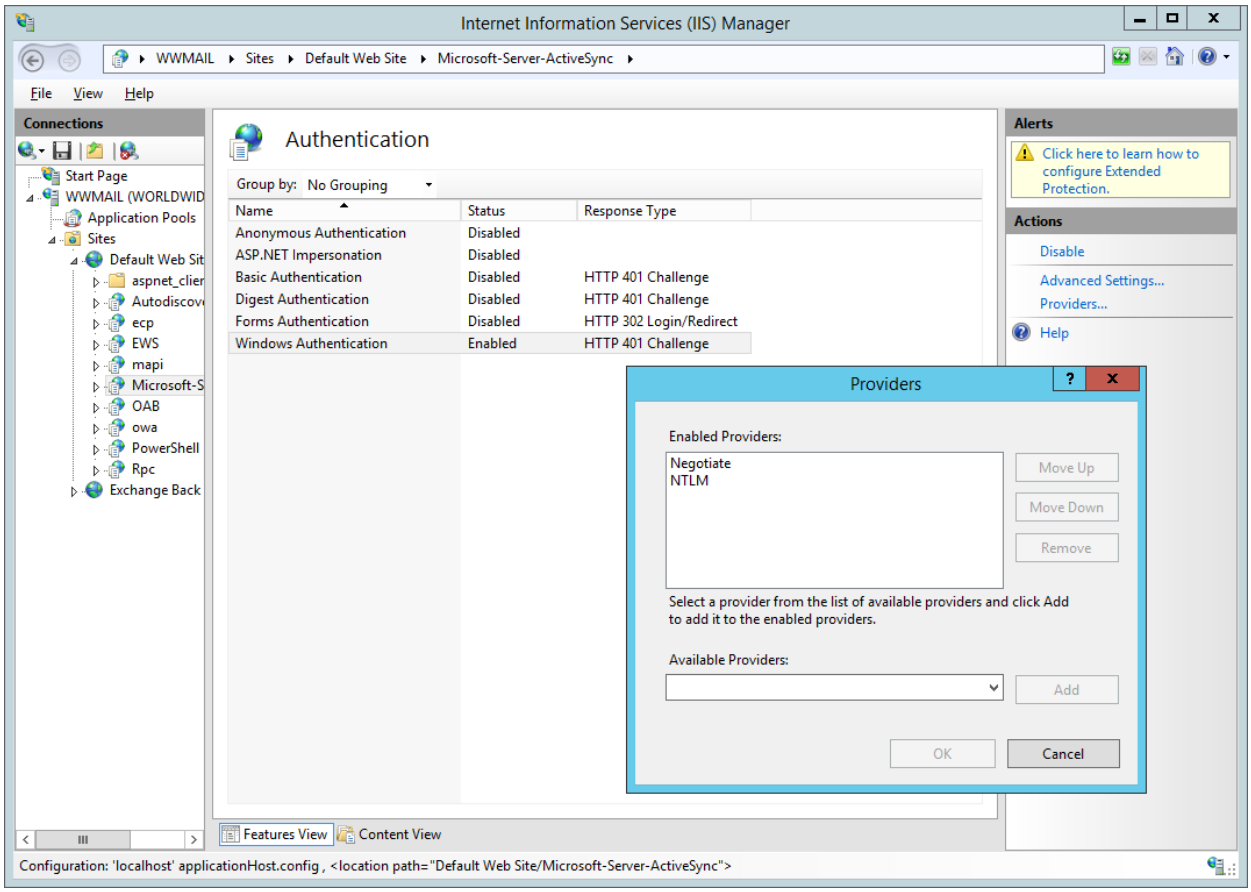
Enable Windows Authentication on the CAS/EAS

Configure Windows Authentication on CAS/EAS. If you configure SEG with KCD, and the EWS proxy is enabled, then you must perform the following procedure on the EWS Virtual Directory also.

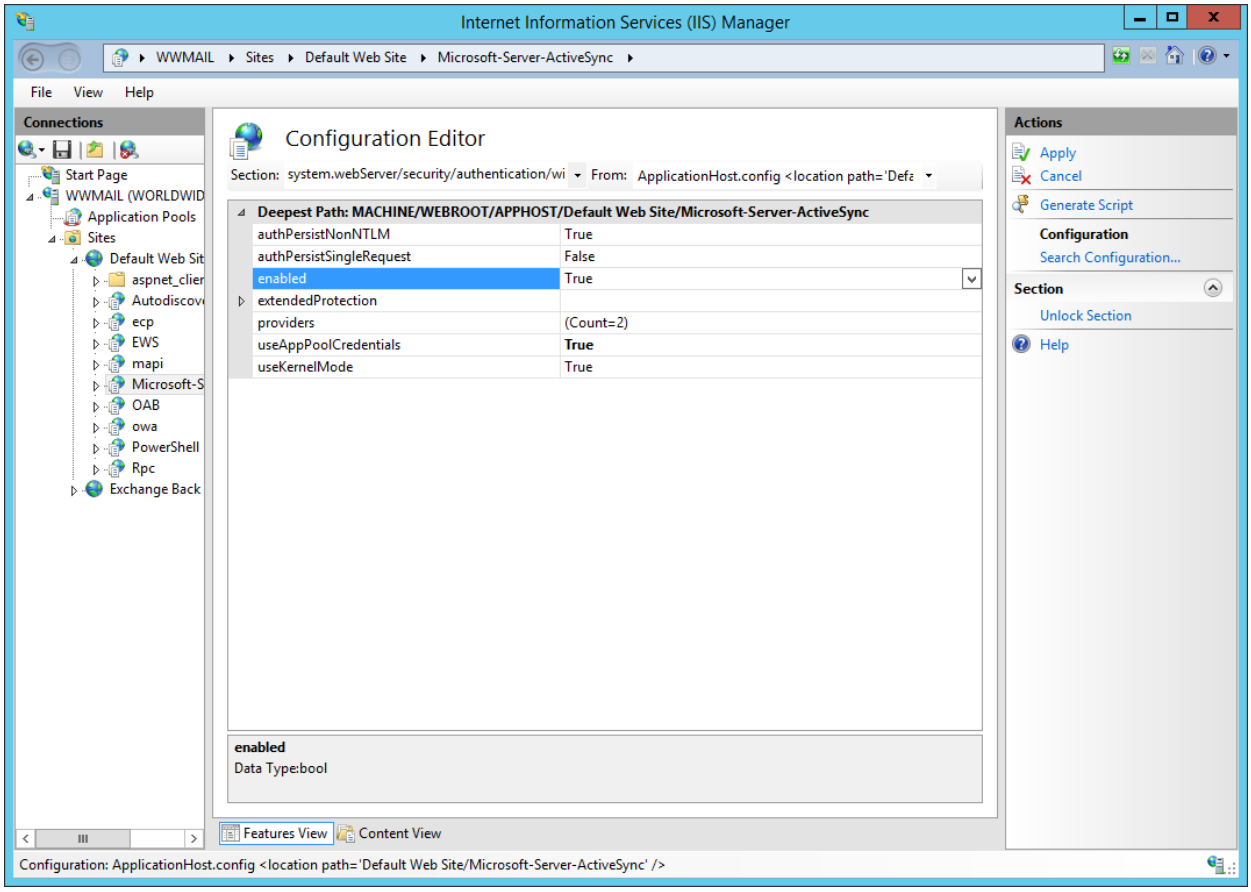
Procedure

1 On the Exchange Server, open IIS Manager and navigate to the **Microsoft-Server-ActiveSync** Virtual Directory.

2 Select **Authentication**, enable **Windows authentication**, and add **Negotiate** as a provider.



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**.



Leveraging an ASA Credential Type

Configure an alternate service account to represent the Exchange server. You can create a computer account or a user account for the Alternate Service Account (ASA).

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 Exchange server 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.

Create an Alternative Service Account

Create an Alternate Service Account (ASA) to represent the Exchange server. If an environment has multiple Client Access Server (CAS) or Exchange ActiveSync (EAS) servers, then the service registration procedure varies.

Procedure

1. Open the **Active Directory User**, **Computers**, and create a new computer account. Create an ASA for the Exchange server in the domain. Enter a name for the ASA.
2. Create a service principal name (SPN) on the domain using the following command. See the Microsoft documentation on how to use the `setspn` command. The syntax for this command varies depending on your environment.

   ```
   setspn –s http/{MAIL–SERVER–FQDN} {ASA_ACCOUNT}$
   ```

   The `MAIL–SERVER–FQDN` must be the same mail server configured in the MEM configuration.
3. Run the following command in PowerShell and verify that all relevant SPNs are assigned.

   ```
   setspn –L {ASA_ACCOUNT}
   ```

4. To set the ASA to the Exchange servers, run the Alternate Service Account credential script in the Exchange Management Shell **RollAlternateserviceAccountPassword.ps1** based on the Exchange version.

   ```
   .\RollAlternateServiceAccountPassword.ps1 –ToSpecificServers {MAIL–SERVER–FQDN} –
   GenerateNewPasswordFor "{DOMAIN}{ASA_ACCOUNT}" –Verbose
   ```

   After you run the script, a **Success** message is displayed.
5. Verify if the ASA credentials are deployed.

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

6 Enable the SEG to delegate HTTP EAS traffic to the newly created ASA instead of the Exchange server FQDN.

For more information, see step 6 in Assign Delegation Rights to the Service Account.

Configure Secure Email Gateway (SEG) V2 for Kerberos Constrained Delegation (KCD)

3

Configure the SEG V2 for KCD using the UEM console.

Prerequisites

1 You must have installed and configured SEG.

2 Upload a single trust certificate for KCD using the UEM console. This certificate is used to validate the client certificate. If additional certificates are needed, then they must be added manually to the SEG configuration. See Update Secure Email Gateway v2 Configuration for Multiple Certificates Trust.

Note The supported certificate types are .p12, .pfx, and .cer.

Procedure

1 Navigate to **Email > Email Settings > Advanced**.

2 Deselect the **Use Recommended Settings** check box.

3 Select **Upload** from the **Client Certificate Chain** and then click **Choose File** to upload the certificate chain used to issue client certificates.

Note The result is a certificate chain that begins at the trusted root CA, through the intermediate and ending with the SSL certificate issued to you. The supported certificate types are .p12, .pfx, and .cer.

4 Click **Enable** from the **Require Client Certificate** to enable the client certificate if it is a security requirement.

5 Click **Enable** to enable KCD Authentication.

6 From the **KCD Authentication** menu, 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** and enter the name of your Service Account. For example, *SVC_awseg*.

8 Select **Service Account Password** 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.

Note The domain name is case-sensitive and must be entered in uppercase. For example, `DOMAIN-NAME.COM`.

b Select the **Domain Controller** text box and enter the domain controller server name. For example, `DC.DOMAIN-NAME.COM`.

The domain and domain controllers must be added in pairs and all domains must have trust with the primary domain.

10 Click **Save** and restart the SEG service.

Note If you modify these settings after the SEG installation, you must reinstall SEG.

Configure EAS and Credential Profile

Configure EAS and Credential profile using Workspace ONE UEM console.

Procedure

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.

Update Secure Email Gateway v2 Configuration for Multiple Certificates Trust

The Workspace ONE UEM console permits a single trust certificate for KCD to be uploaded although SEG v2 can support multiple certificates to trust. If additional certificates are required, you must add them manually to the SEG configuration.

The SEG v2 configuration must be updated for multiple certificates to trust if, for example, a profile is updated to switch to a new Certificate Authority (CA) or update the certificate therein. Then, both certificates must be trusted on the SEG to accommodate end users until the new certificate is absorbed by all devices.

You can upload a single certificate from the Workspace ONE UEM console while configuring SEG for KCD. See Chapter 3 Configure Secure Email Gateway (SEG) V2 for Kerberos Constrained Delegation (KCD).

Procedure

1 Export the full chain of certificates for the required CAs.

Note Ensure that this full chain contains both the root and intermediate certificates and only .pfx format certificate is supported.

2 Move the certificates to the `/config/ssl-certs` path within the install directory of the SEG.

3 Navigate to the `config.json` file within the config folder of the SEG directory.

4 Modify the `clientCertTrustStorePath` file to include the certificate's absolute paths as comma-separated values within quotes and save the file. For example:

```
"C:/SecureEmailGateway/config/ssl-certs/Example1.cer,C:/SecureEmailGateway/config/ssl-certs/Example2.cer"
```

5 Restart the SEG service.

SEG Client Certificate Mapping for Kerberos Authentication

You can configure SEG to use client certificate mapping when the certificate either does not have a user principal name (UPN), or the available user principal name does not match the user principal name value in the Active Directory.

Typically, during a certificate-based authentication, SEG extracts the UPN from the client certificate received from the device. The UPN is used to request a Kerberos token from the Kerberos Domain Controller (KDC) server. This token is then used for authenticating the email request at the Exchange server.

SEG cannot acquire a Kerberos token when a UPN is unavailable due to the following reasons:

- When a client certificate does not have a user principal name.
- If the user principal name on the certificate does not match the user principal name in the Active Directory.
- The certificate generation template cannot be modified to include the user principal name attribute.

In such cases, you can configure SEG to retrieve the UPN from the Active Directory using certificate mapping and use the retrieved UPN to obtain the Kerberos token.

When certificate mapping is enabled, certificate mapping takes precedence over any UPN in the certificate. In case the certificate mapping does not fetch a valid UPN, SEG might fall back to the UPN in the certificate, if any, to request for a Kerberos token.

To enable client certificate mapping, you must adhere to the following prerequisites:

- Enable Kerberos authentication.
- SEG uses the same service account user credentials that are configured under the Kerberos authentication settings for certificate mapping. The service account user must have the permissions to fetch the user details through the LDAP query.
- Publish the client authentication certificate generated from the CA server to the respective user object in the Active Directory server.
- Enable the **Attribute Indexing** and the **Replication to Global Catalog** settings in the Active Directory for the attributes listed in the following table.

Attribute Name	Attribute Indexing Default Setting	Replication to Global Catalog Default Setting
userCertificate	Not Enabled	Enabled
userPrincipalName	Enabled	Enabled
objectClass	Enabled	Enabled
objectCategory	Enabled	Enabled

Note **Attribute indexing** for the **userCertificate** attribute is not enabled by default in the Active Directory. You must explicitly enable the same.

Enabling **Attribute indexing** might consume additional storage space on the Active Directory servers.

To enable or verify the **Attribute Indexing** and **Replication to Global Catalog** settings, see the *Active Directory Settings to Enable Attribute Indexing and Replication* section.

For improving the overall security of the system, enable LDAP over TLS (LDAPS) between the SEG and the Active Directory. When you enable LDAPS, the communication between the SEG and LDAP server is encrypted.

When the **Attribute Indexing** and **Replication to Global Catalog** settings are enabled, running the query against the Global Catalog port (generally port 3269 with TLS) instead of the LDAP port (generally port 636 with TLS) might perform better.

Certificate Mapping in SEG

To perform certificate mapping in SEG, update the following configuration properties in the **application-override.properties** file of the SEG.

Note For SEG version 2.17.0 or later, with the Workspace ONE UEM console version 20.10 and later, perform the SEG configuration using the custom gateway settings. To understand the SEG custom gateway settings, see the *SEG Custom Gateway Settings* topic in the *Secure Email Gateway (SEG V2)* guide.

For SEG version before 2.17.0, SEG continues to use the default configuration (pre-defined configuration). If the custom settings feature is not available, manually update the respective files at the individual node and modify the SEG configuration.

Key	Description	Supported Values/ Format	Default Value	Mandatory
cert.mapping.ldap.enabled	Indicates if the certificate mapping feature is enabled for SEG. This setting is ignored and considered as false if the KCD authentication is disabled in the email configuration.	True/False	False	Yes
cert.mapping.ldap.host	Specify the remote LDAP host information in a URL format.	protocol://host:port/dc=whatever For example, ldap://ldap-remote:3268, ldaps://ldap-remote:3269, and ldaps://ldap-remote:3269/dc=memldap,dc=org	None	Yes

Key	Description	Supported Values/ Format	Default Value	Mandatory
cert.mapping.ldap.user	Used for authenticating the LDAP query. SEG uses the same service account credential that is configured as part of the Kerberos authentication settings. However for the LDAP query, the user name must be provided in the Distinguished Name (DN) format.	LDAP recognizable Distinguished Name (DN) of the Kerberos service user account. For example, CN=servKCD,CN=Users,DC=memldap,DC=org.	None	Yes
cert.mapping.ldap.lookup.base	Specify the distinguished name of the base domain configured for running the LDAP query. The query fetches the matching results from the domain. By default, the LDAP query indicates the rootDSE of the LDAP setup. In cases, with **userCertificate** and **userPrincipalName** attributes indexed and replicated to the Global Catalog, these fields need not be modified.	Distinguished name of the base domain. For example, DC=memldap, DC=org	None	No

Active Directory Settings to Enable Attribute Indexing and Replication

You must first register the dynamic-link library (DLL) that is required for the Active Directory schema snap-in. You can then add the snap-in to Microsoft Management Console (MMC).

The membership in the **Domain Admins**, or equivalent, is the minimum required to complete the procedure. You can check the details about using the appropriate accounts and group memberships at Local and Domain Default Groups.

To configure the Active Directory settings, perform the following steps:

1 Open a command prompt, type `regsvr32 schmmgmt.dll` and press **Enter** to install the Active Directory schema snap-in.

2 Click **Start > Run**, type `mmc`, and then click **OK**.

3 On the **File** menu, click **Add/Remove Snap-in**.

4 In the **Available snap-ins** option, click the **Active Directory Schema > Add** and click **OK**.

5 Expand the **Active Directory Schema > Attributes**.

6 Select the **userCertificate** attribute to be updated and click the **Properties** of the attribute.

7 Select the **Index** check box and verify that the **Replicate this attribute to the Global Catalog** check box is selected.

8 Click **Apply** to save the changes.

Configure Certificate Revocation List over HTTP

4

Configure the certificate authority (CA) for the Certificate Revocation List (CRL) over HTTP.

The SEG requires that the client certificate CRLs are reachable over HTTP. By default, Microsoft CAs 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 the *Creating a Certificate Revocation List Distribution Point for Your Internal Certification Authority* topic available at Archived MSDN and TechNet Blogs.

The following table lists the configuration keys to enable the certificate revocation validation in SEG:

Configuration Key	Description	Default Value
enable.cert.revocation.validation	Flag to enable the certificate revocation check using the CRL. This flag is used only when the Kerberos authentication or the **RequireClientCertificate** flag is enabled.	False
remote.crl.fetch.interval.in.minutes	Interval in minutes for a periodic timer that attempts to update the SEG with the latest CRL data.	1440 (1day)
remote.crl.distribution.http.uris	Comma-separated list of HTTP URLs of the CRL Distribution Points (CDP).	
fail.hard.on.crl.download.failure.during.server.startup	Flag to determine how to handle the failure to fetch CRLs during the SEG startup. If this flag is set to true and you are unable to fetch the CRL, then the SEG fails to start, else SEG ignores the error and starts.	True

Note For SEG version 2.17.0 or later, the configuration keys must be configured using the custom gateway settings. For earlier versions of SEG, that is, for SEG versions before 2.17.0, the configuration keys must be configured using the **application-override.properties** file.

Configuration Updates when Migrating from Classic SEG to SEG V2

5

Upgrade from Classic SEG with KCD to SEGV2 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 advaced settings.
- The certificate chain of trust is provided in the configuration and is not stored in the Microsoft Management Console. The .pfx certificate type is supported.
- 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).

Disable LLMNR with Active Directory GPO

6

The Link-Local Multicast Name Resolution (LLMNR) protocol is enabled by default. The active directory has a Group Policy Object (GPO) you can configure to prevent its domain workstations from using LLMNR.

To disable LLMNR through the GPO, perform the following steps:

Procedure

1. Open gpedit.msc file.
2. Navigate to **Local Computer Policy > Computer Configuration > Administrative Templates > Network > DNS Client**.
3. Click **Turn Off Multicast Name Resolution** and set the value to **Enabled**.