Kerberos Constrained Delegation (KCD) Authentication for SEG V2

VMware Workspace ONE UEM 1902

vmware®

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

https://docs.vmware.com/
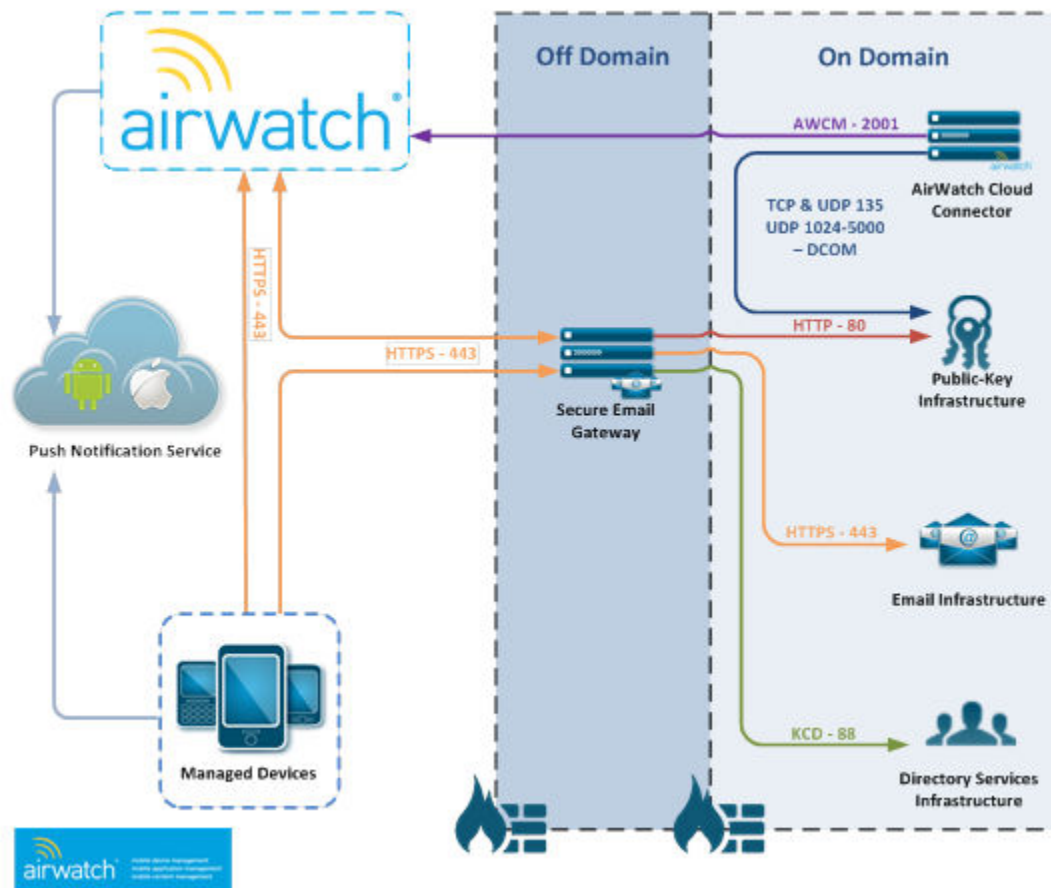
Contents

Introduction 1

Use Kerberos as the authentication method over username or password.

Kerberos Constrained Delegation (KCD) authentication eliminates the use of username or password authentication for email. Instead of username or password, 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 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:

- Prerequisites

Prerequisites

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 Configure Certificate Revocation List over HTTP for CA .

- ■ 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 Chapter 4 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 CAS or 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}
   ```
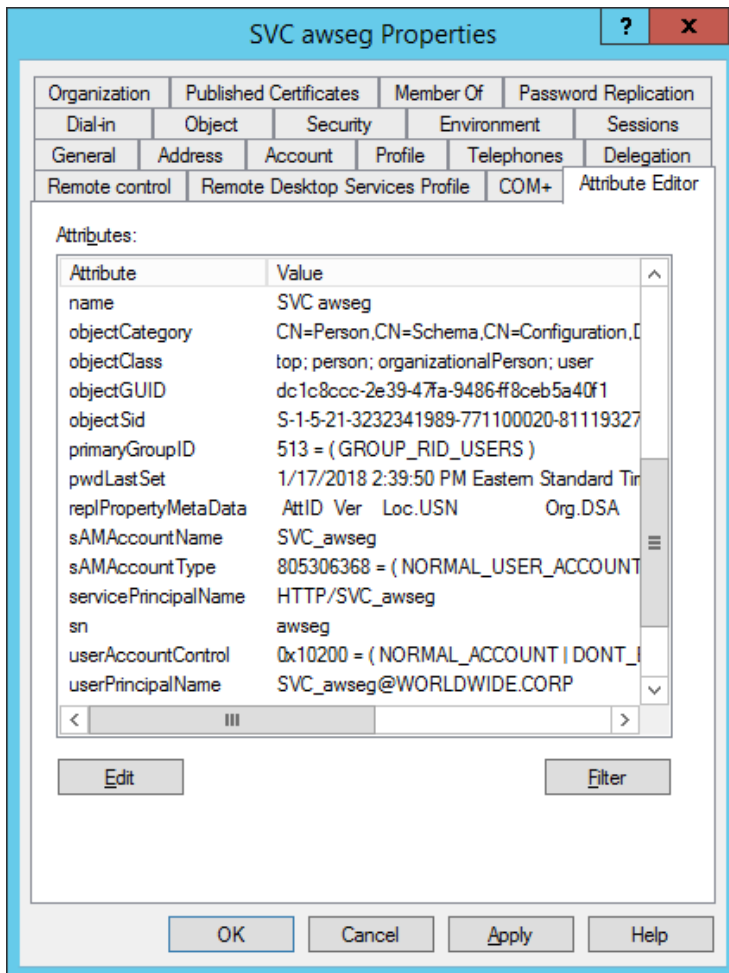
   Wherever **{EX_DNS_NAME}** is the name, the SEG uses it to refer to the Exchange server and {EX_MACHINE_NAME} is the actual machine name of the Exchange server, you must select this SPN when assigning delegation rights to the Service Account.
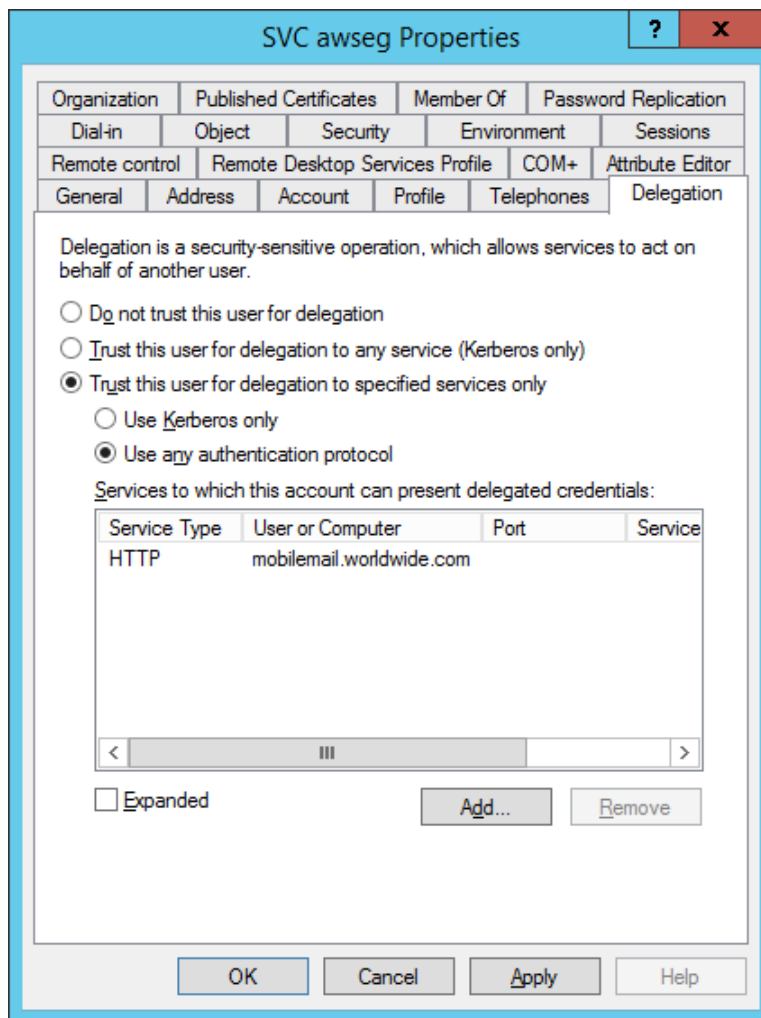
Assign Delegation Rights to the Service Account

Configure delegation rights for the service account.

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**.
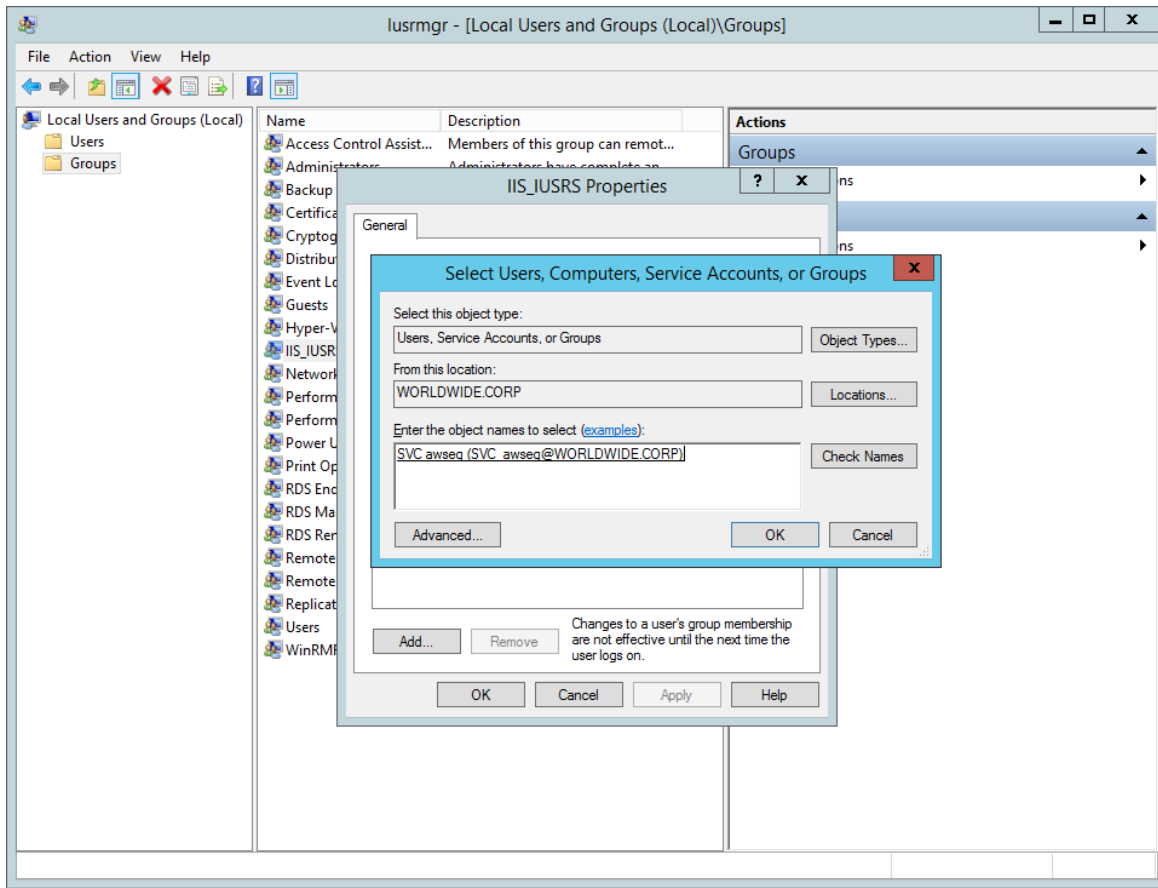

5   After setting up the SPN for the user account, close the **Properties** window and reopen it to access the **Delegation** tab. Delegation cannot be set for a user account until an SPN is set.

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 Chapter 4 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

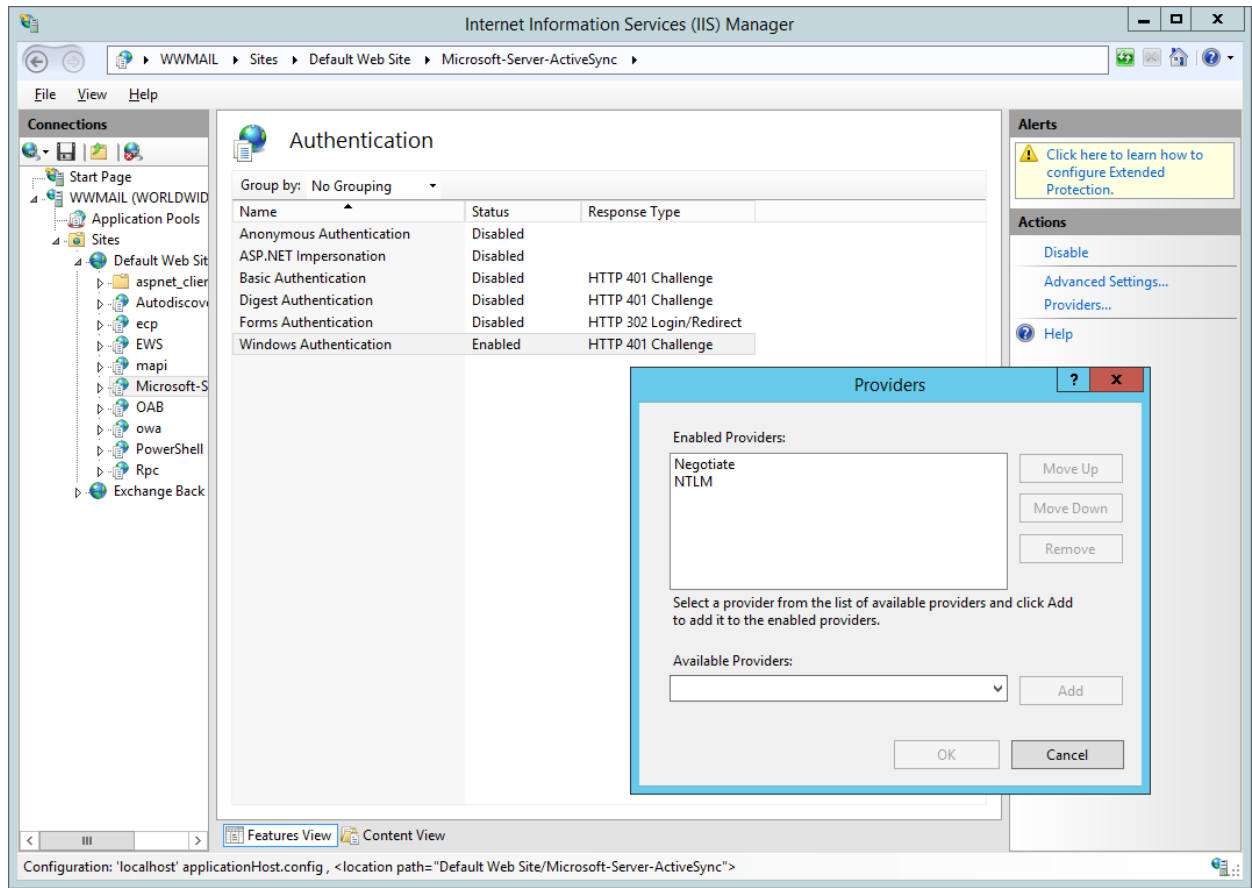Add a service account to the IIS user groups of the ActiveSync server.

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.

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.

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**.

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 You can only upload a single certificate using the UEM console. 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.

Procedure

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

2 Deselect the **Use Recommended Settings** checkbox.

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

4 From the **Require Client Certificate**, click **Enable** 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. 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   Click **Save** and restart the SEG service to apply the KCD settings.

Configure EAS and Credential Profile

Configure EAS and Credential profile using Workpsace ONE UEM console.

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

Although SEG v2 is capable of supporting multiple certificates to trust, the UEM Console only allows for a single certificate to be uploaded. If additional certificates are required, you must add them manually to the SEG configuration.

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

You can upload a single certificate from the 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.

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.

Leveraging an ASA Credential Type

4

Configure an alternate service account to represent the Client Access Server (CAS) array. 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 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.

This chapter includes the following topics:

- Create an Alternative Service Account

- Configure Certificate Revocation List over HTTP for CA
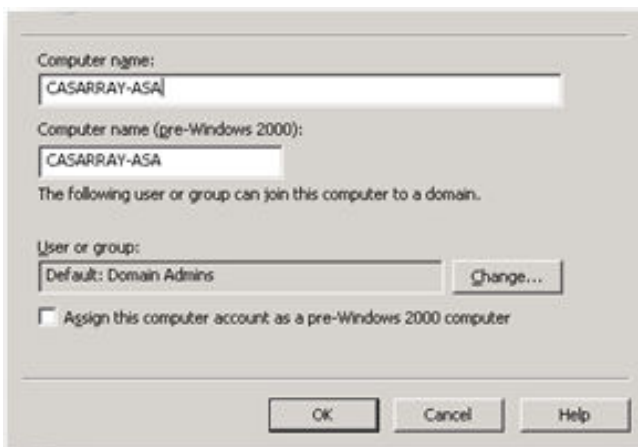
- Upgrade from Classic SEG with KCD

Create an Alternative Service Account

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.

Procedure

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 CASARRAY- ASA, verify the account has replicated to all Domain Controllers before proceeding.

2 Verify the CAS array's FQDN by running the command in PowerShell.

```
Get-ClientAccessArray
```

The FQDN is used for the SPN that is attached to the ASA.

3 Create the SPN using the following command. To create a service principal name (SPN) on the domain, see the Microsoft documentation on how to use the SETSPN command. The syntax for this command will vary depending on your environment.

```
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** based on the Exchange version.

```
.\RollAlternateServiceAccountPassword.ps1 —ToSpecificServers {CAS—FQDN} —GenerateNewPasswordFor
"{DOMAIN}{ASA_ACCOUNT}" —Verbose
```

For more information, see the Microsoft technet document *How to Deploy the ASA Credentials to the CAS Servers.*

After the script is run, a **Success** message is displayed.

6   Verify if the ASA credentials is deployed.

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

7   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 Certificate Revocation List over HTTP for CA

Configure CA for CRL over HTTP.

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.

Upgrade from Classic SEG with KCD

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 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).