VMware AirWatch Certificate EOBO with ADCS via DCOM

For VMware AirWatch

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

Table of Contents

Chapter 1:
Overview

AirWatch Certificate EOBO with ADCS via DCOM

This document explains the installation and setup of the Enrollment Agent Signing Certificate for direct integration with AirWatch using ADCS over the DCOM protocol.

This setup allows AirWatch to take advantage of Microsoft's Certificate Enroll On Behalf Of Others function. By default, only domain administrators are granted permission to request a certificate on behalf of another user. However, a user or computer account other than a domain administrator can be granted permission to become an enrollment agent. A user becomes an enrollment agent by enrolling for an Enrollment Agent certificate. For integration with AirWatch, a computer account will be used.

Once someone has an Enrollment Agent certificate, that person can enroll for a certificate and generate a smart card on behalf of anyone in the organization. The resulting smart card could then be used to log on to the network and impersonate the real user. Because of the powerful capability of the Enrollment Agent certificate, AirWatch strongly recommends that your organization maintain very strong security policies for these certificates.

System Requirements

Software Requirements

- Microsoft Windows Server 2008 R2 Enterprise or later.

Other Requirements

- On-Premises AirWatch Environment.

- Server must be a member of the same domain as the AirWatch application server in order to install the Enterprise CA.

- Service Account with administrative access to the server.

Network Requirements

The AirWatch Console server, VMware Enterprise Systems Connector server (if you are using VMware Enterprise Systems Connector), must be able to communicate to the Microsoft CA over all configured DCOM ports. If using VMware Enterprise Systems Connector, the VMware Enterprise Systems Connector server must comply with the hardware sizing requirements mentioned in the **VMware AirWatch Recommended Architecture Guide**, which is available by name on the AirWatch Resource Portal. Refer to the guidelines described for the Admin Console server.

- Port 135: Microsoft DCOM Service Control Manager.

- Ports 1025 - 5000: Default ports DCOM processes.

- Ports 49152 - 65535: Dynamic Ports.

This port range can be configured to be any number of non-standard ports depending on your DCOM implementation. However, these ports are utilized by default.
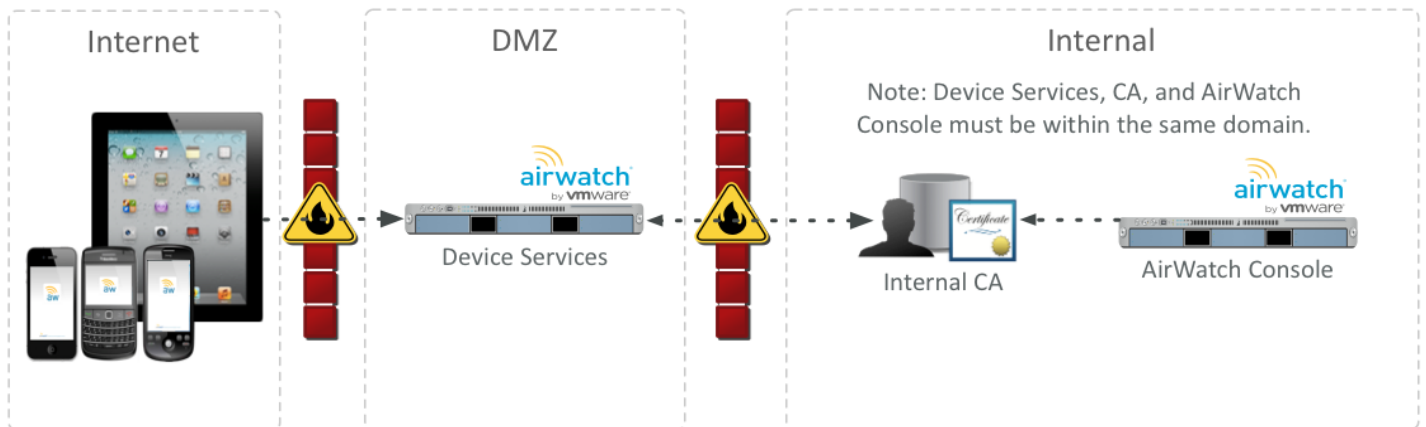
vmware airwatch

High Level Design

In order for AirWatch to use a certificate in a profile used to authenticate a user, an enterprise CA must be set up in the domain in an on-premises only environment. Additionally, the CA must be joined to the same domain as VMware Enterprise Systems Connector in order to successfully manage certificates within AirWatch. There are several methods for AirWatch to retrieve a certificate from the CA. Each method requires the basic installation and configuration described in this document.

Scenario #1 – On Premises: All AirWatch application servers internal. VMware Enterprise Systems Connector not installed.
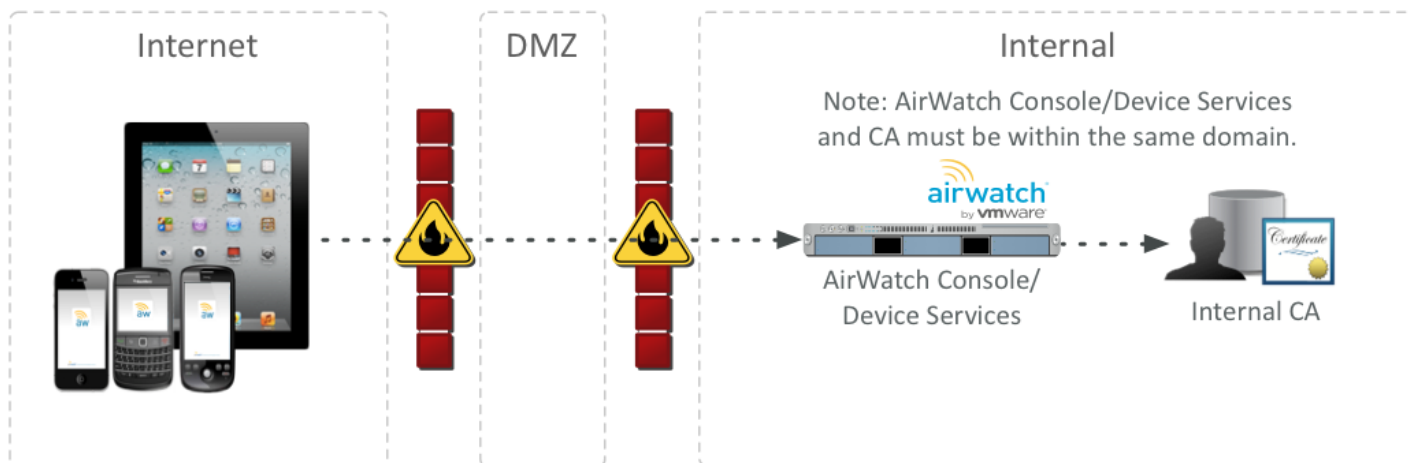
Scenario #2 – On Premises: Device Services located in the DMZ. CA and AirWatch servers internal. VMware Enterprise Systems Connector not installed.

Scenario #3 – On Premises: Devices Services, VMware Enterprise Systems Connector, AirWatch servers, and CA internal.
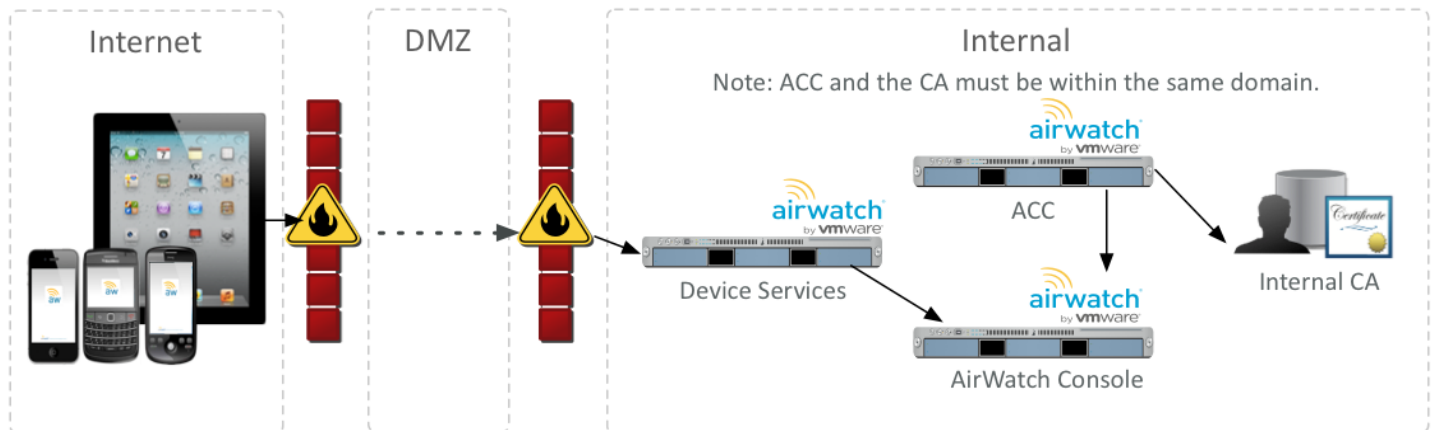
Scenario #4 – On Premises: Device Services located in the DMZ. VMware Enterprise Systems Connector, AirWatch servers, and CA internal.
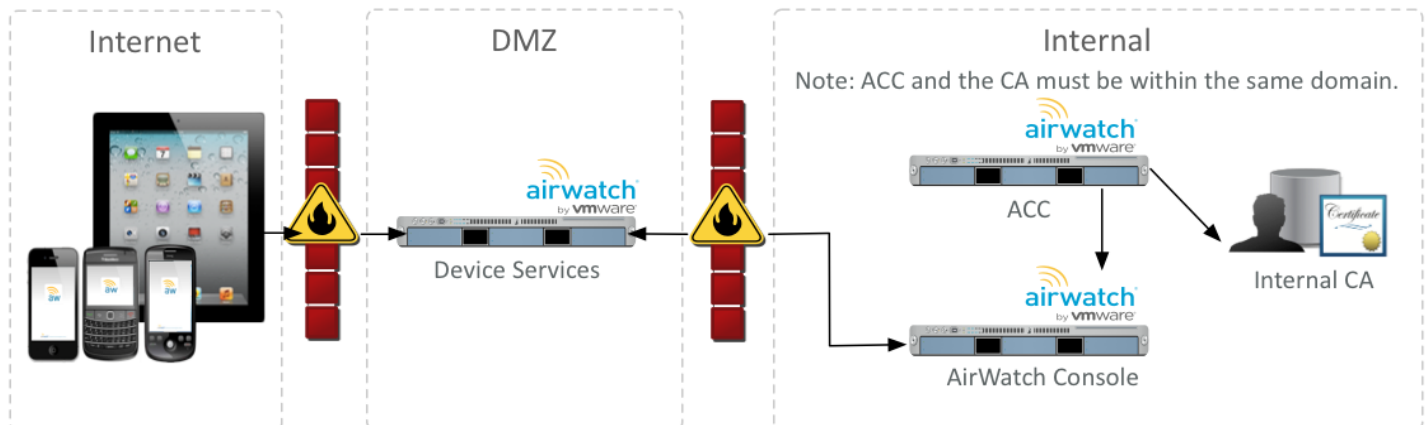
Scenario #5 – SaaS: AirWatch Servers and Device Services in the internet cloud, and the VMware Enterprise Systems Connector and Internal CA are Internal.
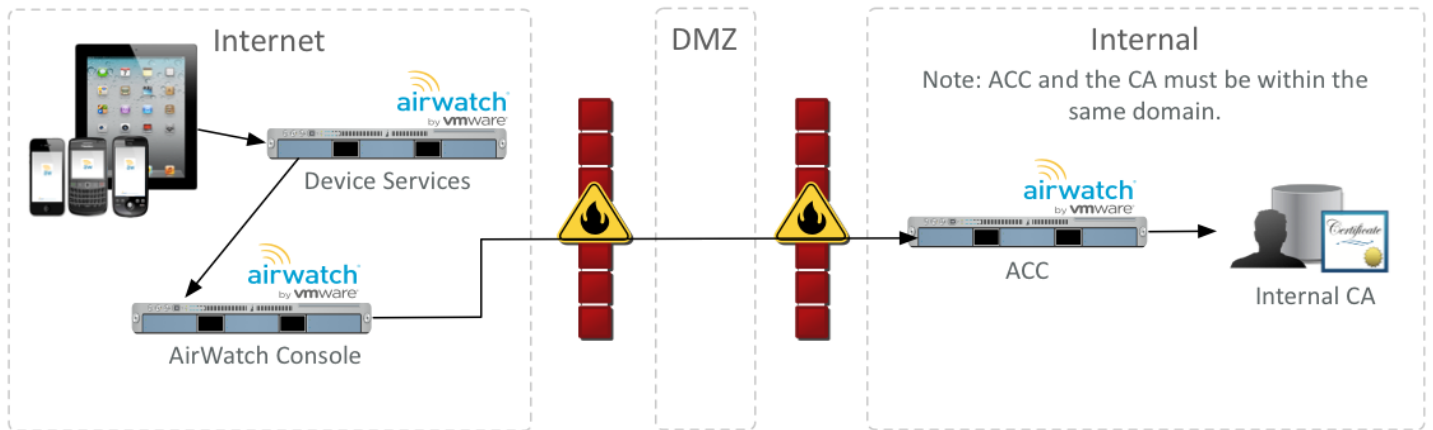
Chapter 2:
Microsoft Certificate Enroll On Behalf of Others with ADCS via DCOM Installation, Setup, and Configuration

vmware airwatch

Set up the Restricted Enrollment Agent Signing Certificate on the CA Server

Step 1: Enable LDAP Referrals

Run the following commands on the CA. This configuration is needed on ADCS CA since we are requesting certificates on behalf of some other user using service account.

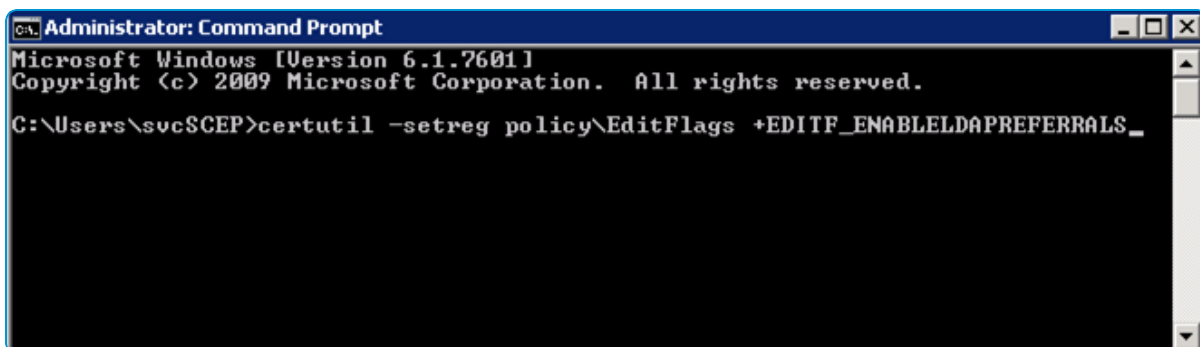This feature is only supported on Windows 2008 R2 Enterprise and later. See the link below for context and details: https://technet.microsoft.com/en-us/library/ff955842(v=ws.10).aspx

1. First stop certificate services by running the following command:

   ```
   net stop certsvc
   ```

2. Enable LDAP Referrals

   ```
   certutil -setreg policy\EditFlags +EDITF_ENABLELDAPREFERRALS
   ```

```
Administrator: Command Prompt                                    _ □ ×
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\svcSCEP>certutil -setreg policy\EditFlags +EDITF_ENABLELDAPREFERRALS_
```

3. Start certificate services by running the following command:

   ```
   net start certsvc
   ```

Step 2: Create the Restricted Enrollment Agent Certificate Template

1. Open the **Certificate Authority (CA)**.

2. Expand the CA Name, Right click **Certificate Templates**, and select **Manage**.

3. Right click the **Enrollment Agent (Computer)** template and select **Duplicate Template**. Name it per your preference.

4. Select **Windows Server 2008 Enterprise**.

5. On the **Request Handling** tab, select **Allow Private Key to be Exported**.

6. In the **Subject Name** tab, make sure **Build from this Active Directory Information** is activated and **Subject Name format** is set to **Fully distinguished name**.

7. Click **OK**.

8. Navigate back to the **CA**, right click **Certificate Templates**, select **New**, and select **Certificate Template to Issue**.
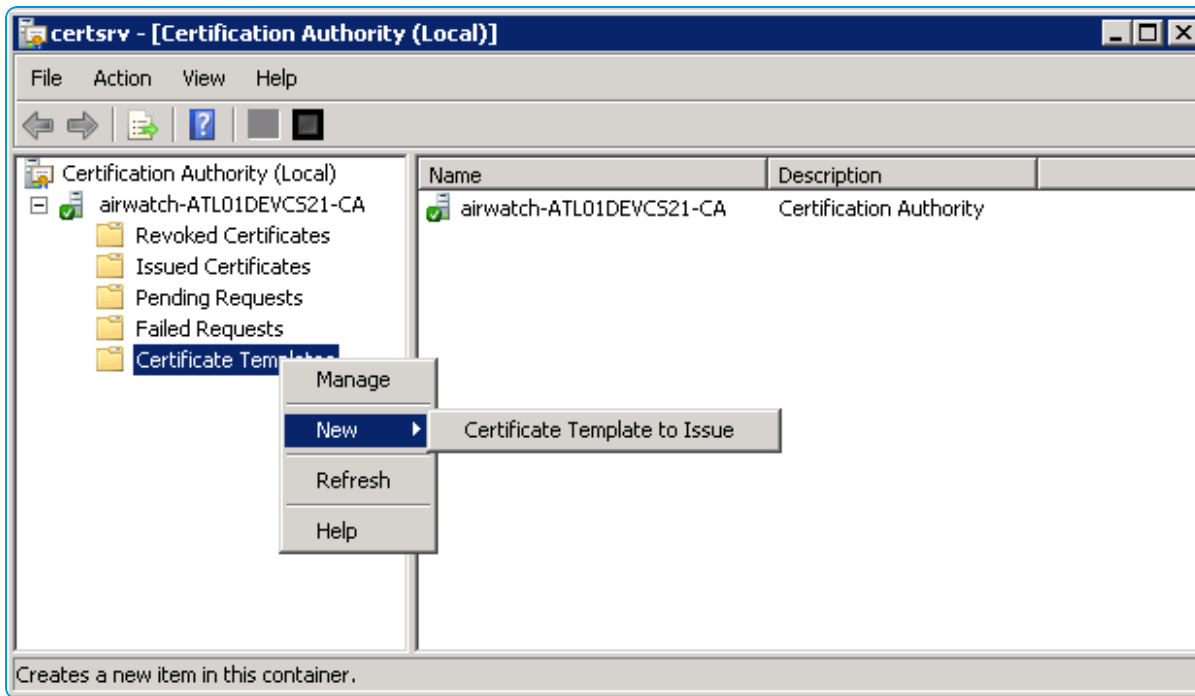
9. Select the duplicate copy of the template created in the previous step.
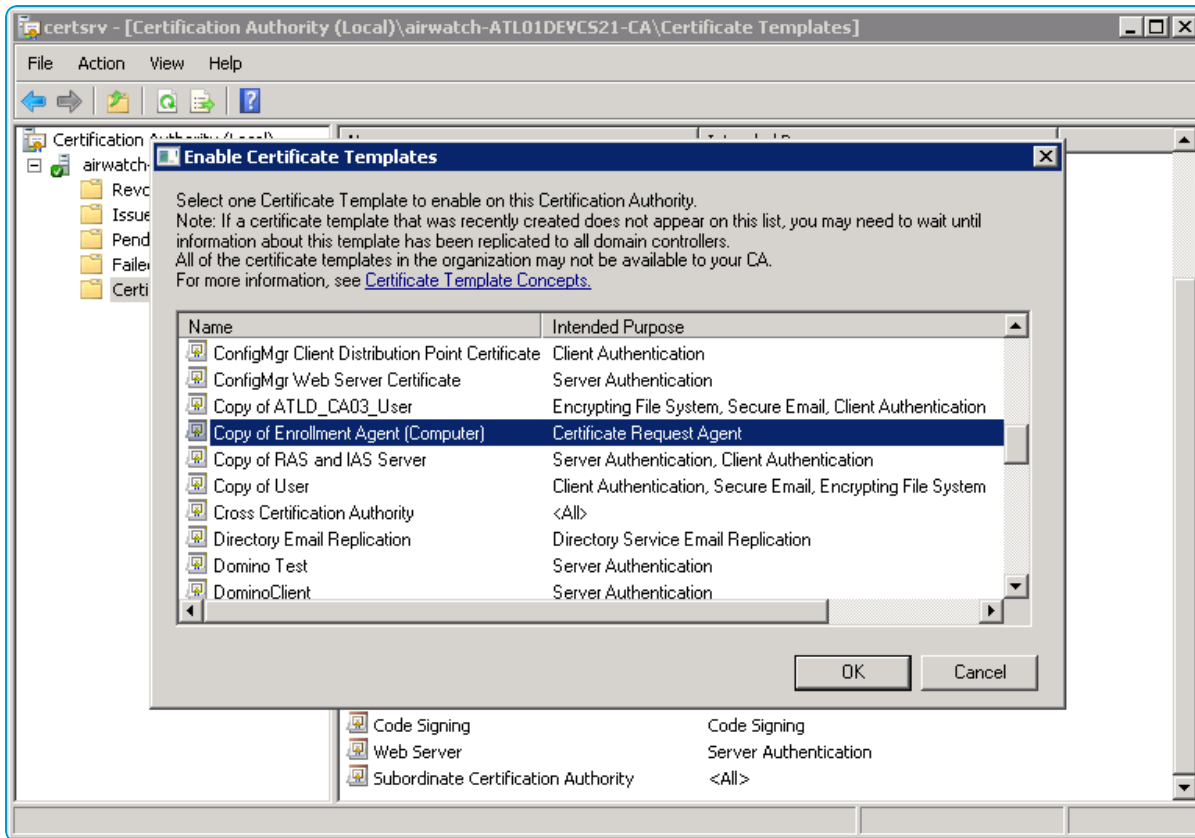
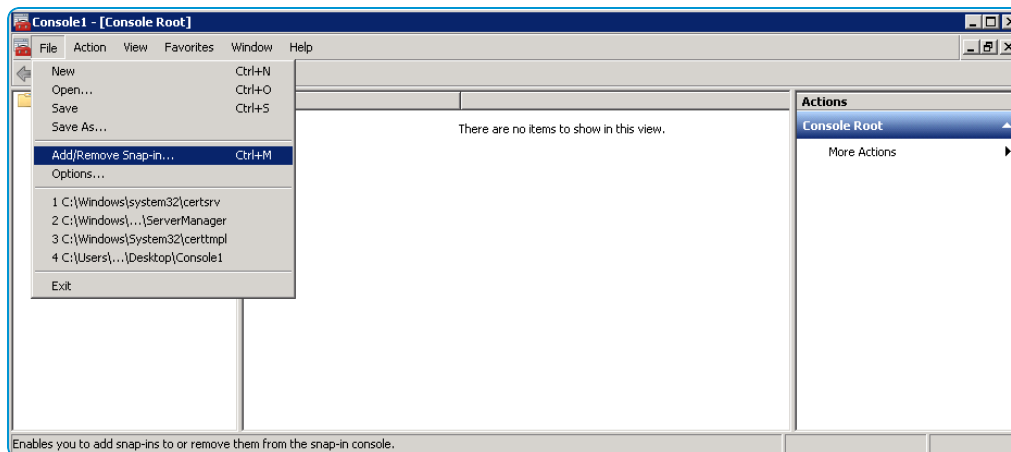10. Click **OK**.

Enroll a computer for the Signer Certificate

Step 1: Generate a new Restricted Enrollment Agent Signer Certificate

The following actions in this step can be done on any server that can connect to the Certificate Authority.

1. Open **MMC**.

2. Click **File** and select **Add/Remove Snap in**.

vmware airwatch

3. Select **Certificates**.

4. Select **Computer Account**.

5. Select **Local Computer** and select **Finish**.

6. Click **OK**.

7. Expand **Certificates (Local Computer)**, double click **Personal**, right click **Certificates**, select **All Tasks**, and select **Request New Certificate**.

8. Click **Next**.

9. Select **Active Directory Enrollment Policy** and select **Next**.
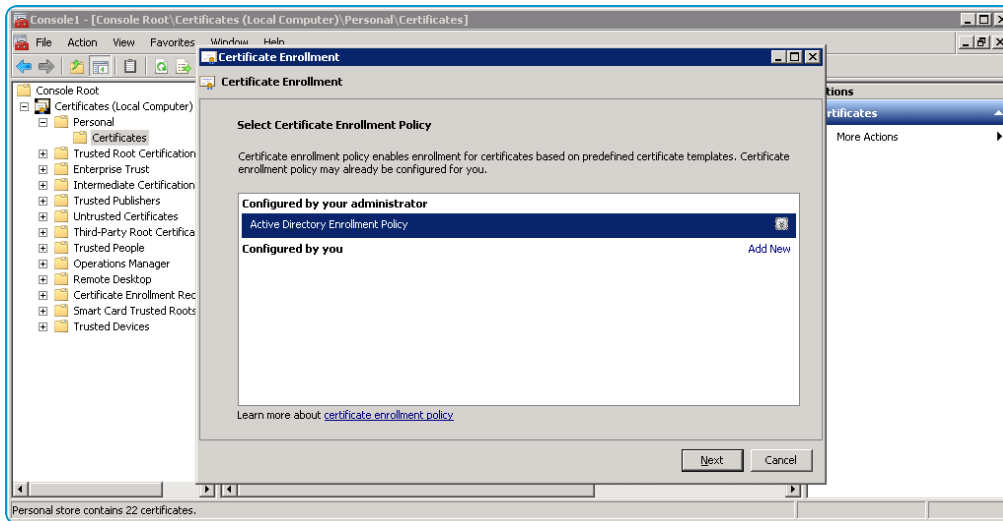
10. Check the duplicate template created in earlier steps and select **Enroll**.
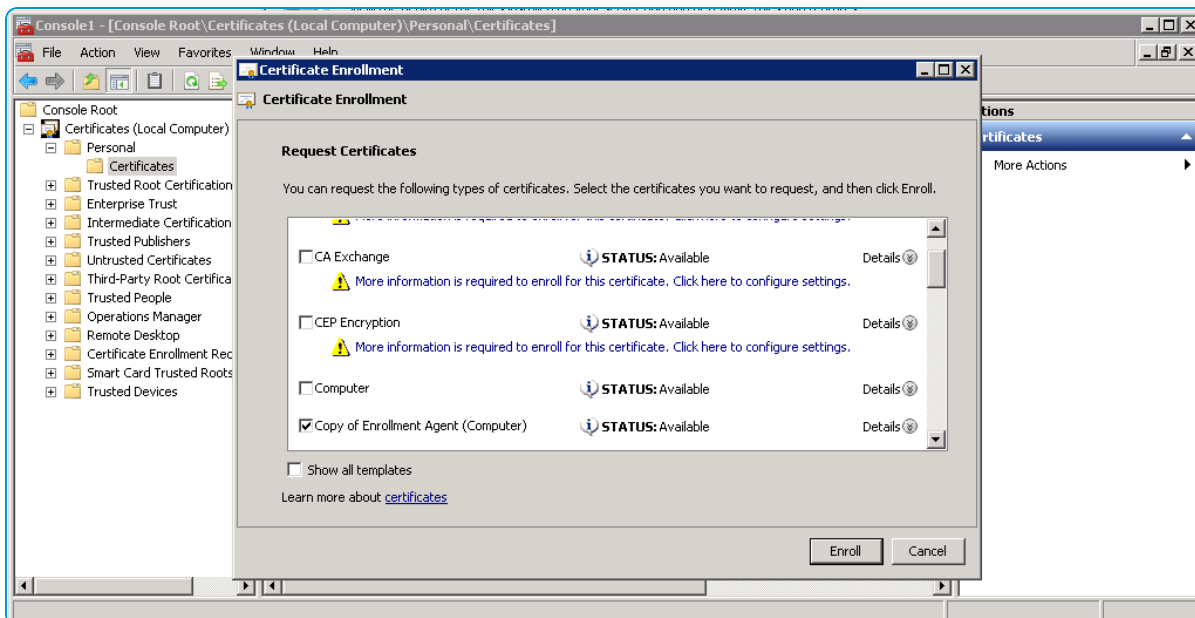
11. Once completed, select **Finish**.

Step 2: Configure the issued certificate

1. Once the certificate has been issued, right click it and select **All Tasks** followed by **Manage Private Keys**.

2. Click **Add**.

3. Type **Network Service** and select **Check Names**. Once added, select **OK** twice.
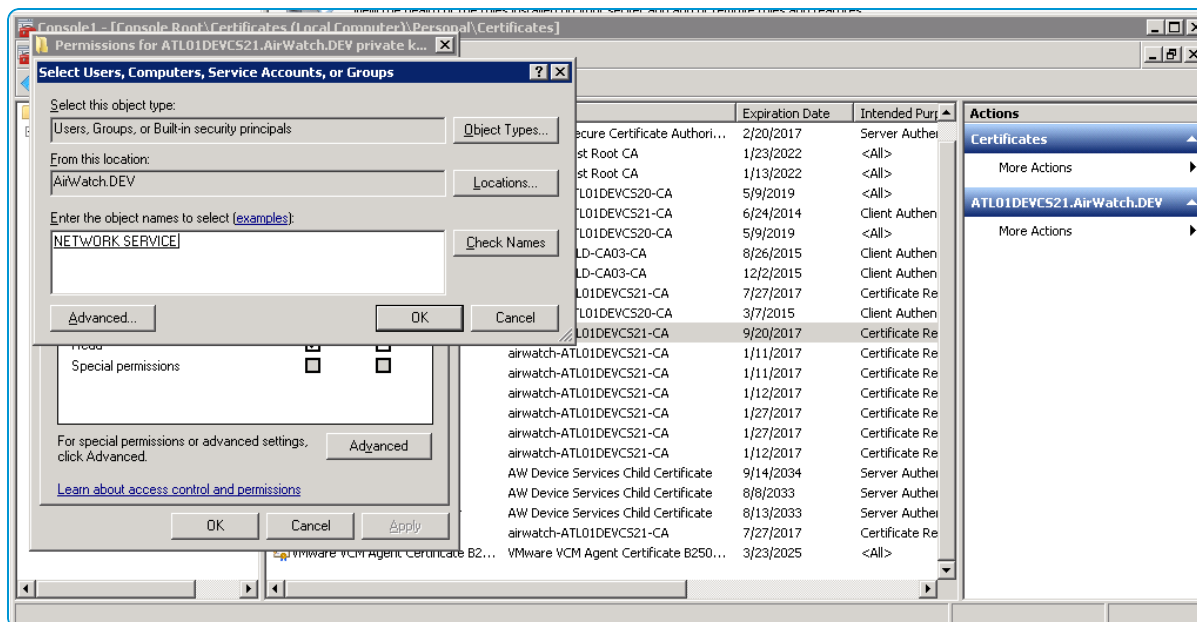
Step 3: Export the Certificate

If the certificate needs to be installed on multiple Device Services servers or AirWatch Cloud Connector servers, export with the private key. If not, skip to exporting just the public key.

Export public and private key to a .pfx file

1. Right click the issued certificate, select **All Tasks** followed by **Export**.

2. Click **Next**.

13

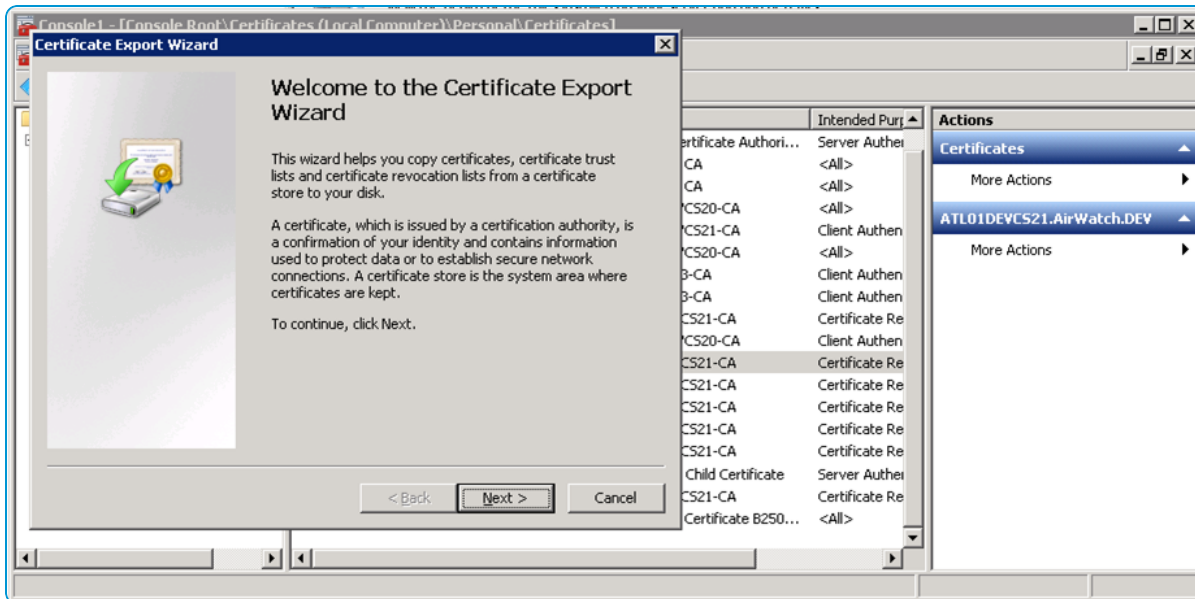3. Select **Yes, export the private key** and select **Next**.

4. Select **Include all certificates in the certification path if possible** as well as **Export all extended properties**. Click **Next**.

5. Set a password and select **Next**.

6. Select a folder in which to save the exported certificate.

7. Click **Finish**.

Export the public key to .cer file

Only the public key needs to be exported for upload to the console:

1. Right click the issued certificate, select **All Tasks** followed by **Export**.

2. Select **No, do not export the private key**, select **Next**.

3. Select **DER encoded binary X.509 (.CER)**, select **Next**.

4. Select a destination for the exported certificate and select **Next**.

5. Click **Finish**.

Step 4: (If required) Import the certificate for other Device Services servers or AirWatch Cloud Connector servers

On any other servers DS servers or AirWatch Cloud Connector servers, the certificate that was exported in previous steps will need to be imported. Skip this section if no other DS or ACC servers are involved.

1. Open **MMC**.

2. Click **File** and select **Add/Remove Snap in**.
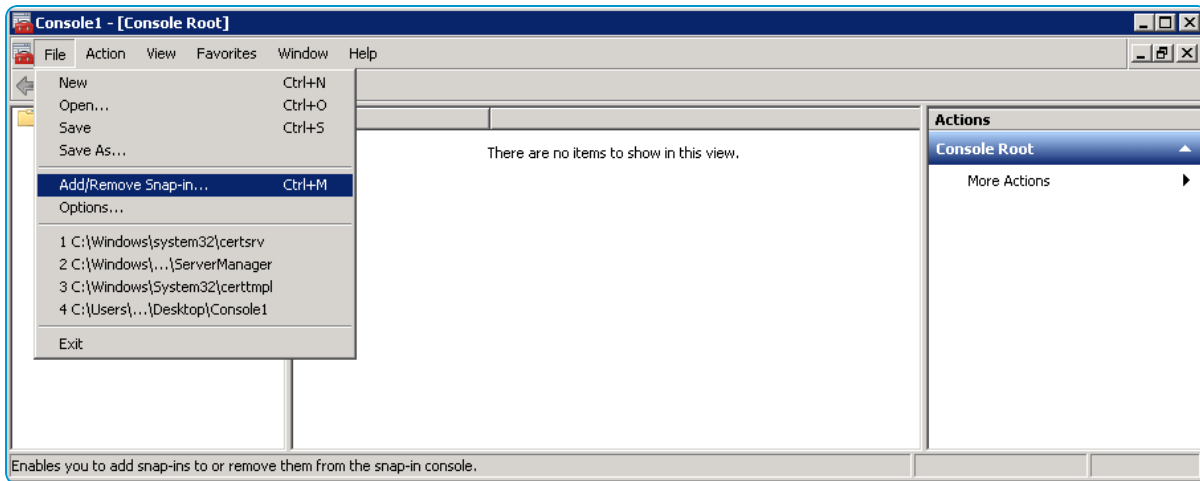
3. Select **Certificates**.

4. Select **Computer Account** and select **Next**.

5. Select **Local Computer** and select **Finish**.

6. Click **OK**.

7. Expand **Certificates (Local Computer)** and select **Personal**. Right click **Certificates**, select **All Tasks** and select **Import…**

8. Select the .pfx file exported in previous steps and select **Next**.

9. Enter the password created for this file in previous steps, make sure **Include all extended properties** is checked and select **Next**.

10. Ensure **Place all certificate in the following store** is set to **Personal** and select **Next**.

11. Click **Finish**.

vmware airwatch

Make Custom User Templates

The default Microsoft Certificate template can be used to issue certificates to the end user. If using such a default, you may skip this section. AirWatch recommends the User Template for client authentication certificates.

1. On the CA server, under the **Certificate Authority Name**, right click **Certificate Templates** and select **Manage**.

2. Right click a default template that is closest to your needs and select **Duplicate Template**.
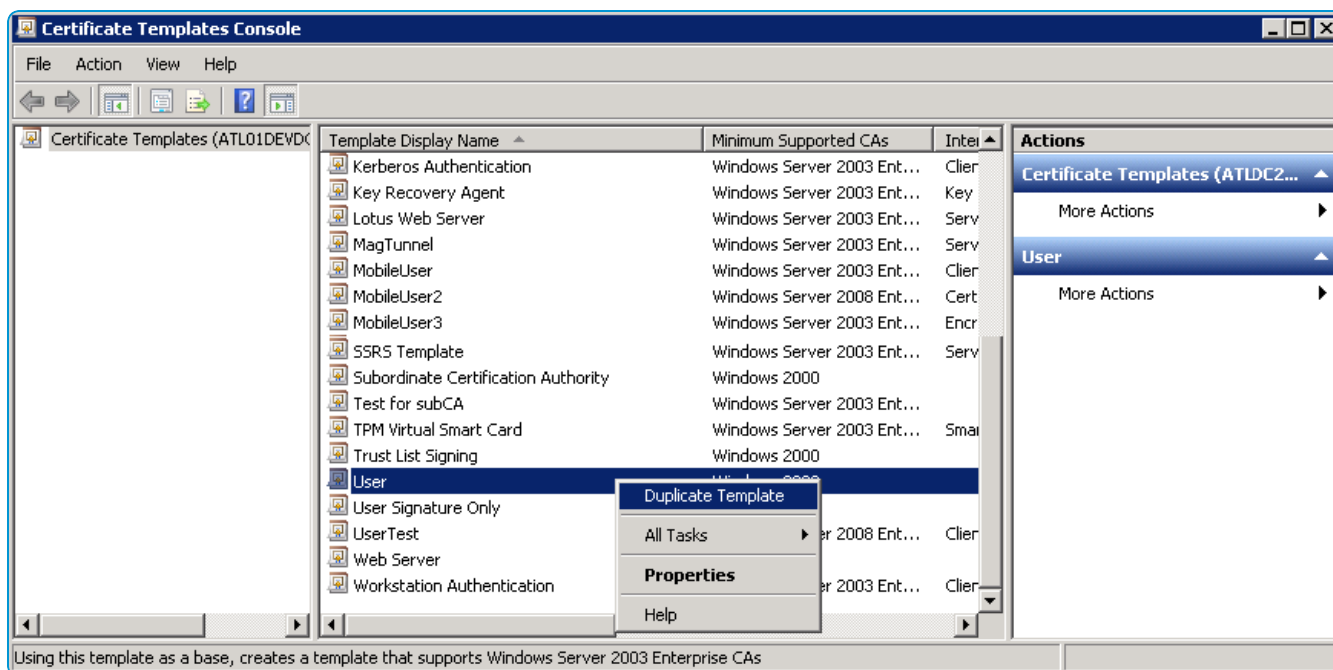
3. Select **Windows Server 2008 Enterprise** and select **OK**

4. Enter the **Template display name** and select **Apply**.
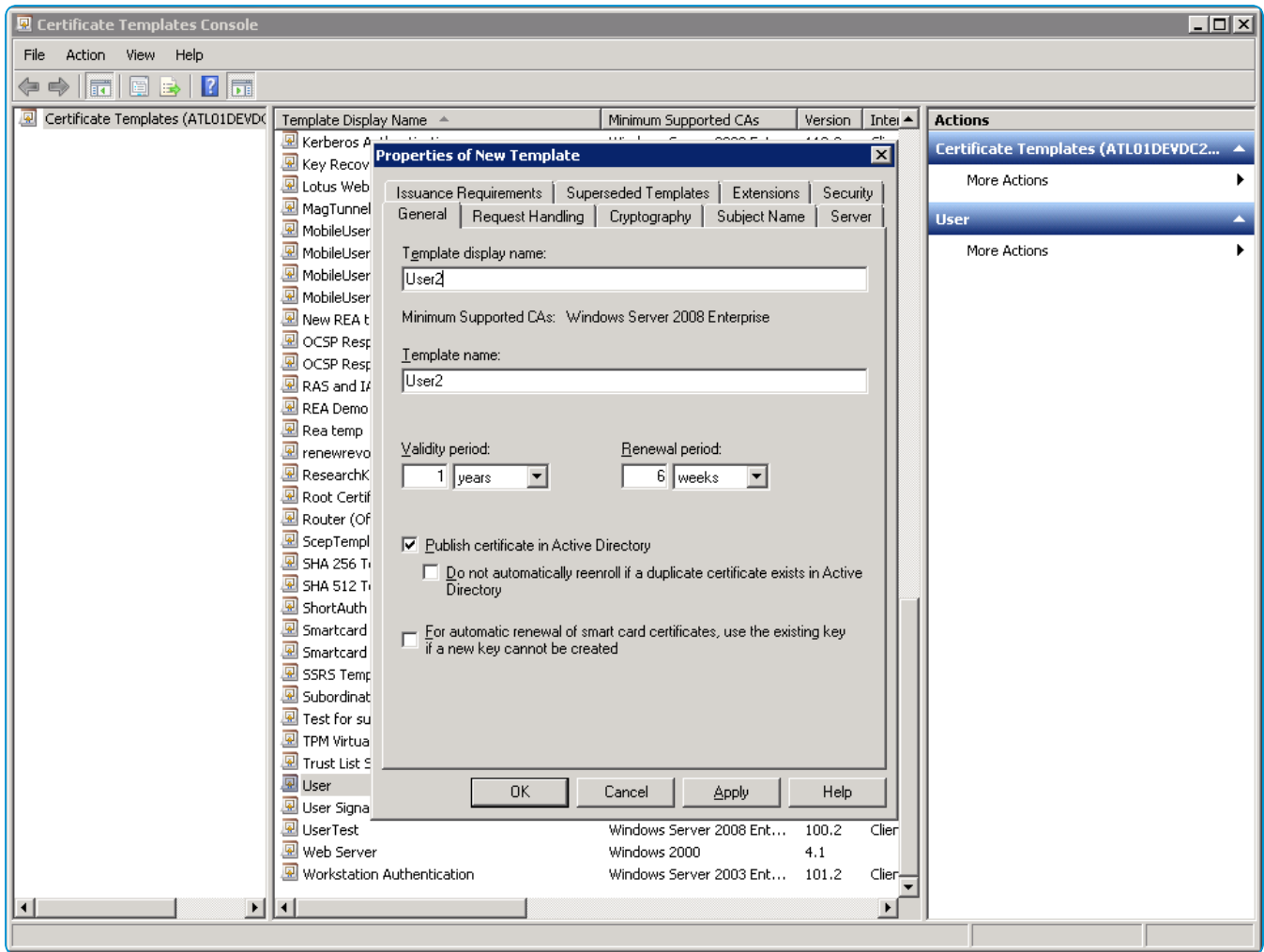
5. Select the **Issuance Requirements** tab and select **This number of authorized signatures**. Under the **Application policy** drop-down field, select **Certificate Request Agent** and select **Apply**.

6. Under the **Subject Name** tab, configure subject alternate name Including **Email name** and **User Principal Name**. AirWatch recommends this practice for Wi-Fi, VPN, and Email authentication. Click **OK**.

7. Right click **Certificate Templates** under the CA name, select **New**, and select **Certificate Template to Issue**.
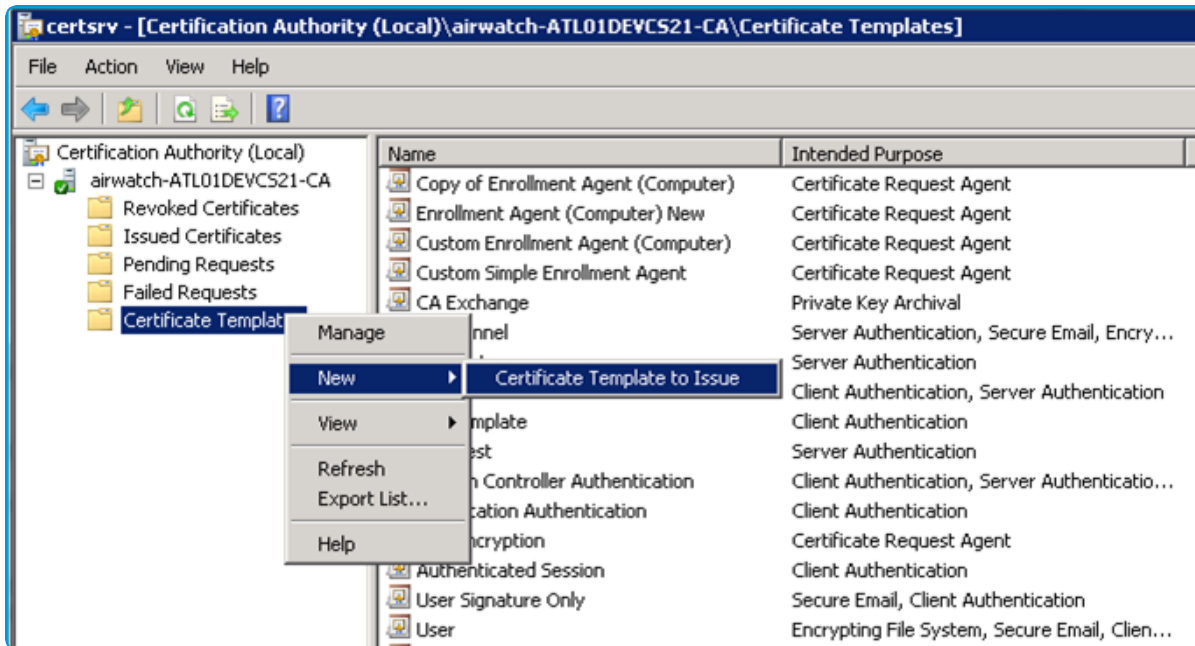
8. Select the template that was just created and select **OK**.
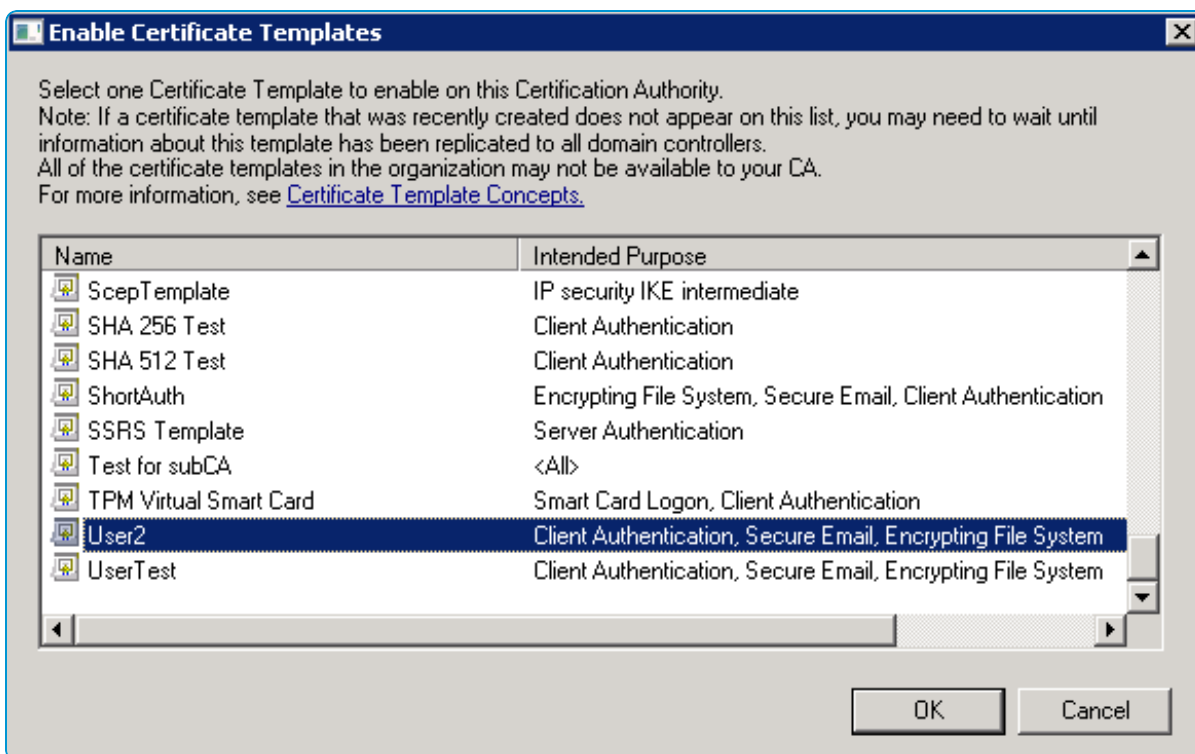
Configure the VMware Enterprise Systems Connector

Enrollment On Behalf Of (EOBO) with ADCS on Microsoft's Distributed Component Object Model (DCOM) substrate can be deployed on the VMware Enterprise Systems Connector in a SaaS environment and as such, additional configuration steps are required.

If using VMware Enterprise Systems Connector, the VMware Enterprise Systems Connector server must comply with the hardware sizing requirements mentioned in the **VMware AirWatch Recommended Architecture Guide**, which is available by name on the AirWatch Resource Portal. Refer to the guidelines described for the Admin Console server.

VMware Enterprise Systems Connector Configuration Steps

If your AirWatch deployment is strictly on-premises, then you may skip ahead to Configuring the AirWatch Console, otherwise, configure the VMware Enterprise Systems Connector by completing the following steps.

1. On the VMware Enterprise Systems Connector server, run `services.msc`

2. Stop the **VMware Enterprise Systems Connector** service.

3. Right-click the **VMware Enterprise Systems Connector** service.

4. Select **Properties**.

5. Select the **Log On** tab.

6. Under **Log on as:**, choose **Local System account** and enable the check box **Allow Service to Interact with Desktop**.

7. Click **OK** to save settings and close the **Properties** page.

If necessary, see Troubleshooting the VMware Enterprise Systems Connector Configuration for additional information.

Connect to the CA

1. Select **Microsoft ADCS** as the **Authority Type** and enable **Restricted Enrollment Agent**.

   The **Username** and **Password** entered here require administrative access to the certificate authority server as mentioned in the pre-requisites.

2. Upload the public key file (.cer) exported in previous steps.

3. Click **Save**.

Configure the Request Template

1. Set the **Issuing Template** to either a default template or the template configured in "Configuring a Custom User Template."

2. Set the **Requester Name** to {**EmailDomain**}\{**EnrollmentUser**} for best results. AD configuration in AirWatch is required to populate these look up values accurately.

   Only user-specific look up values are configurable in the requester name. Device-specific look up values are not supported.

3. Click **Save**.

   This CA and template combination can be used in any profile in the credentials payload and associated with wifi, email, or vpn payloads.

Chapter 3:
Testing and Troubleshooting

vmware airwatch

Troubleshooting Additional Settings

The system cannot find the file specified. 0x80070002 (WIN32: 2)

The REA signing certificate might not be present on the console/DS server's certificate store. You might have added it using your awsso AD user. These AD user-uploaded mmc certificates remain specific to that instance since they are not Network Admin users. Therefore, the private key of REA certificate uploaded using awsso\shwethan cannot be accessed by airwatchdev\svcscep (network admin).

When adding REA signing certificate to mmc, make sure you login as network admin (airwatchdev\svcscep) and then add it to certificate store and give proper network service access to it so that other network admin users can also access it. When you provide Service Account credentials on CA configuration page in airwatch console, you are asking console/DS server to do 'remote call' to the server hostname (atl01devcs21 in this case) using these service account credentials.

Object reference not set to an instance of an object

In this case, CA server was receiving the certificate request (you can always check this by login to CA server and check its Failed requests), but it failed due to policy module denying the request. This happens either because the LDAP forest referrals are not set (Step 1 of CA server) OR the user domain used is not correct/not associated with the CA server.

Looking at 'Issued certificates' on CA server, it was clear that requests only from Airwatchdev domain are processed and awsso domain requests are rejected (atl01devcs21 CA is synced only with Airwatchdev AD, not with awsso). Therefore, we changed the directory mapping on the LGs to Airwatchdev and users from this domain for enrolling devices. Profile lands on the device with correct client certificate for REA.

Troubleshooting the VMware Enterprise Systems Connector Configuration

In some cases, the above steps used to configure the VMware Enterprise Systems Connector may not be sufficient to establish the proper permissions required to log in to the server. To ensure adequate permissions are set, the following steps need to be taken on the VMware Enterprise Systems Connector.

Step 1: Create Service Account with Full Permissions

A service account will be required to run the VMware Enterprise Systems Connector service. Current service account permissions are as follows but are subject to change if the permission levels can be successfully lowered.
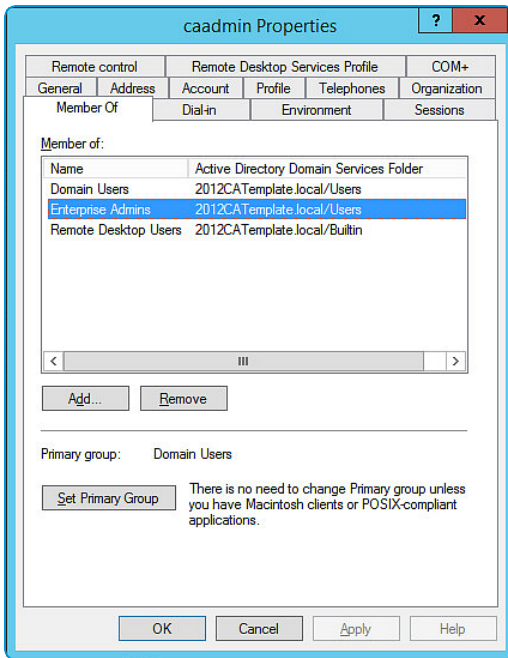
1. Member of the following groups in AD

    - Domain Users

    - Enterprise Admins

    - Remote Desktop Users

    For example, the screen to the right displays the permissions for the Service Account 'caadmin'. This can be the same Service Account mentioned in Other System Requirements.
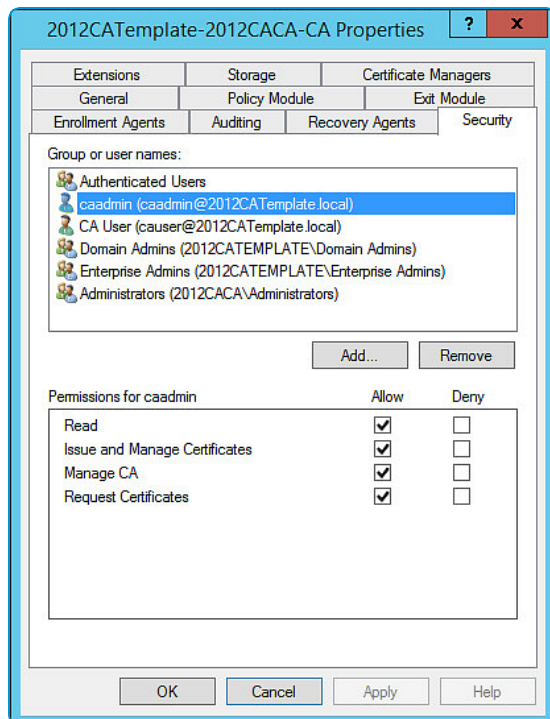
2. On the CA Server

- Member of Local Administrator Group

   For example, the screen to the right displays Local Administrator Group permissions on the CA Server.
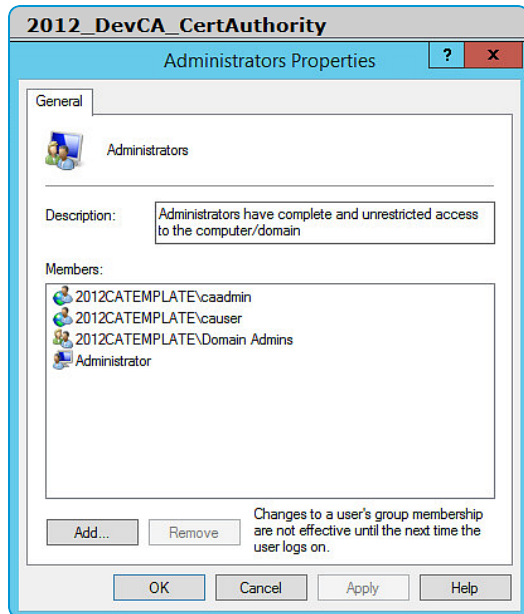
- Full permissions on the Certification Authority

- For example, the screen below displays the full compliment of available permissions for 'caadmin'.
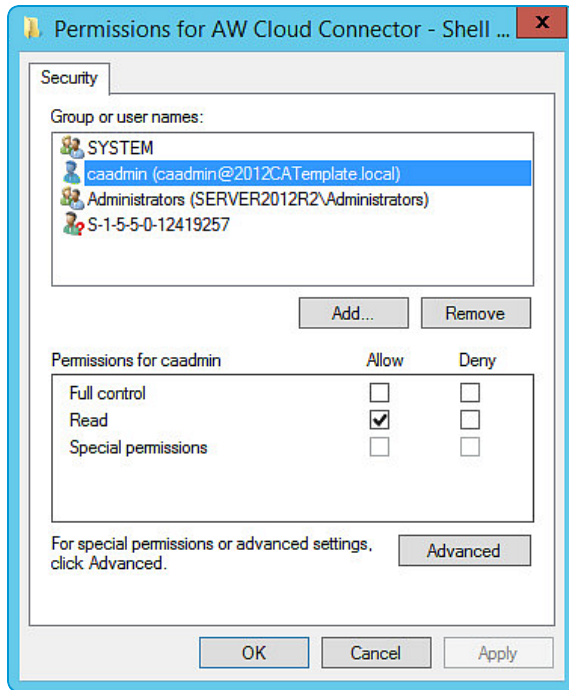
Step 2: Use Alternate VMware Enterprise Systems Connector Configuration

1. On the VMware Enterprise Systems Connector server, run `services.msc`

2. Locate and stop the **VMware Enterprise Systems Connector** service.

3. Right-click the **VMware Enterprise Systems Connector** service.

4. Select **Properties**.

5. Select the **Log On** tab.

6. Under **Log on as:**, choose **This account** and **Browse** for the Service Account you created in Step 1.

7. Enter and confirm the password.
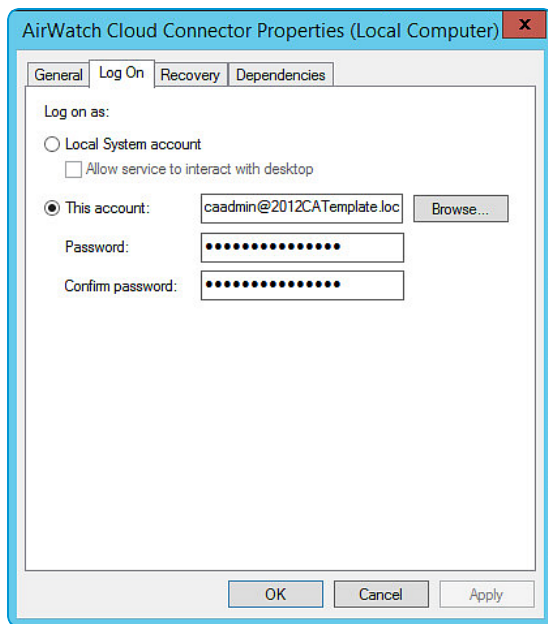
8. Launch the Microsoft Management Console (mmc.exe) and open the personal certificate store of the local computer.

   Ensure you are logged in with an account that has admin permissions for both the VMware Enterprise Systems Connector server and the domain, otherwise you may not be able to access MMC and also add a domain user to manager the private key.

9. Select the Restricted Enrollment Agent created and installed earlier in Step 4 of this guide.

10. In MMC, right-click the Restricted Enrollment Certificate you added and select **All Tasks** and then **Manage Private Keys**.

11. Add the Service Account created in Step 1 and set read permissions.

12. Click **OK** to save settings and close the Properties page.

13. Repeat steps 10-12 for both the VMware Enterprise Systems Connector and the Secure Channel Certificates.

- Both these certificates will be issued by the **Device Services Child Certificate**.

- Issued to **AW Cloud Connector - VMware Enterprise Systems Connector** and **AW Cloud Connector - [OG Name]**.

14. From `services.msc`, manually start the **VMware Enterprise Systems Connector** service.

Appendix:
Additional Settings

Additional Settings Overview

In certain networks and environments, additional permissions and settings are required. Please follow the steps below and refer to the troubleshooting list if required.

Settings and Configuration

A service account will be required to run the VMware Enterprise Systems Connector service. Current service account permissions are as follows but are subject to change if the permissions can be successfully lowered.

- Member of the following groups in AD
  - Domain Users
  - Enterprise Admins
  - Remote Desktop Users
- On the CA Server
  - Member of Local Administrator Group
  - Full permissions on the Certification Authority
- On the VMware Enterprise Systems Connector Server
  - Logon User for the VMware Enterprise Systems Connector Service
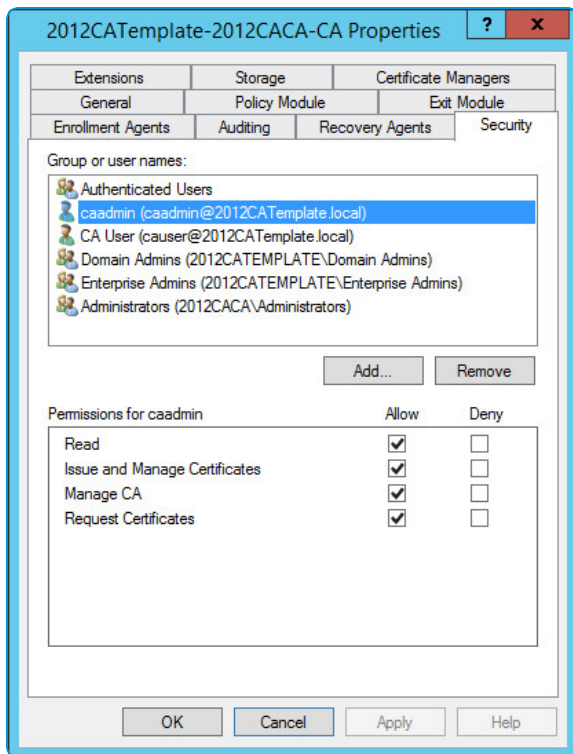
Permissions Settings

The following permissions have been set for the service account 'caadmin'.
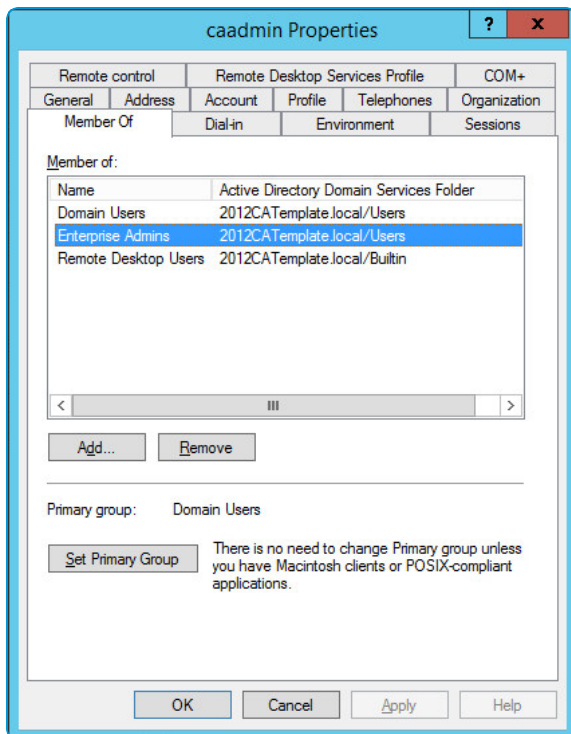
CA Server Local Administrator Group Permissions

vmware airwatch
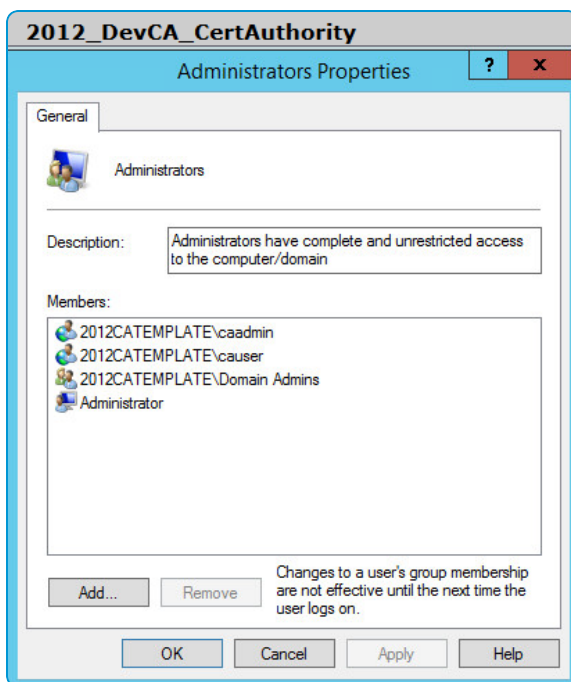
Certification Authority Permissions

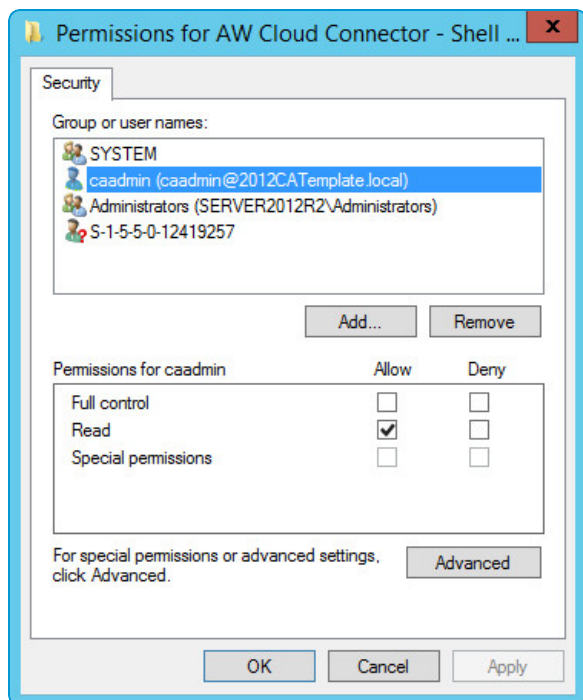## VMware Enterprise Systems Connector Configuration

1. Run Services.msc

2. Stop VMware Enterprise Systems Connector Service

3. Right Click VMware Enterprise Systems Connector service.

4. Select Properties

5. Click on Log On

- For 2008 R2 Enterprise

  - Logon as Local System account

  - Select Allow Service to Interact with Desktop

- For 2012 R2 Standard:

  - Logon as This Account

  - Browse for the user of the service account created

○ Enter and confirm the password
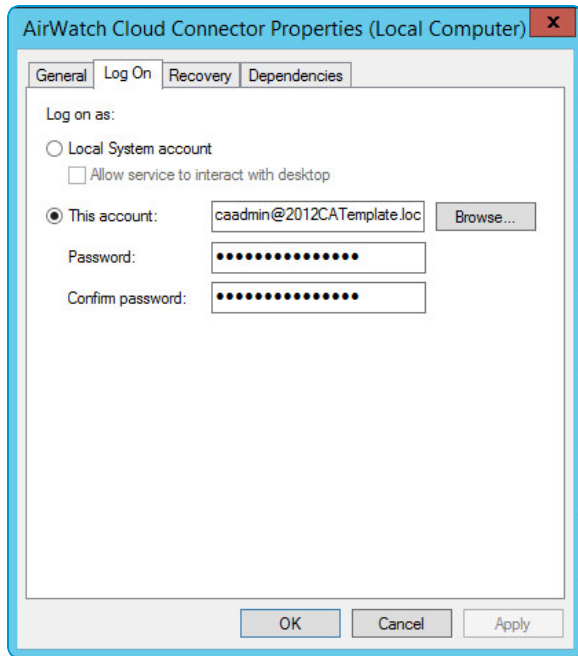
6. Open the personal certificate store of the local computer

   • Make sure you are logged in with an account that has admin permissions both on the VMware Enterprise Systems Connector server and on the domain, or you may not be able to access the computer store and also add a domain user to manage the private keys.

7. Select the Certificate Request Agent certificate created and installed in the original set up guide.

   • Refer Chapter 4 of the Setting up Certificate Enrollment on-Behalf-of with ADCS with DCOM guide.

8. Right Click, select All Tasks, select Manage Private Keys

9. Add the service account and set read permissions

10. Repeat Steps 8-9 for both the VMware Enterprise Systems Connector and Secure Channel Certificates

   - Both these certificates will be issued by Device Services Child Certificate

   - Issued to AW Cloud Connector – VMware Enterprise Systems Connector and AW Cloud Connector – [OG Name]

11. Start the VMware Enterprise Systems Connector service