VMware AirWatch Certificate Authentication for Cisco AnyConnect

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:
Workspace ONE UEM Certificate Authentication for Cisco AnyConnect

Workspace ONE UEM may be configured so that Apple and select Android devices can connect to an enterprise network through Cisco AnyConnect using a certificate for authentication.

You may be using other Secure Sockets Layer (SSL) Virtual Private Networks (VPN) hardware (e.g., Juniper, F5, etc.) or methods for certificate authentication. In this case, there is an explanation of the methodology so that you can understand the concepts and implement VPN within your enterprise.

Regardless of the method you choose, Workspace ONE UEM can provide your enterprise with MDM solutions for VPN. Workspace ONE UEM has many VPN features, including on-demand authentication. These features mean you can choose which domains your mobile device users have access to.

Every time a device user accesses the desired resources on your protected network, the device, without the user's knowledge, automatically handles the login and certificate authentication process. This makes their VPN log in experience simple and seamless.

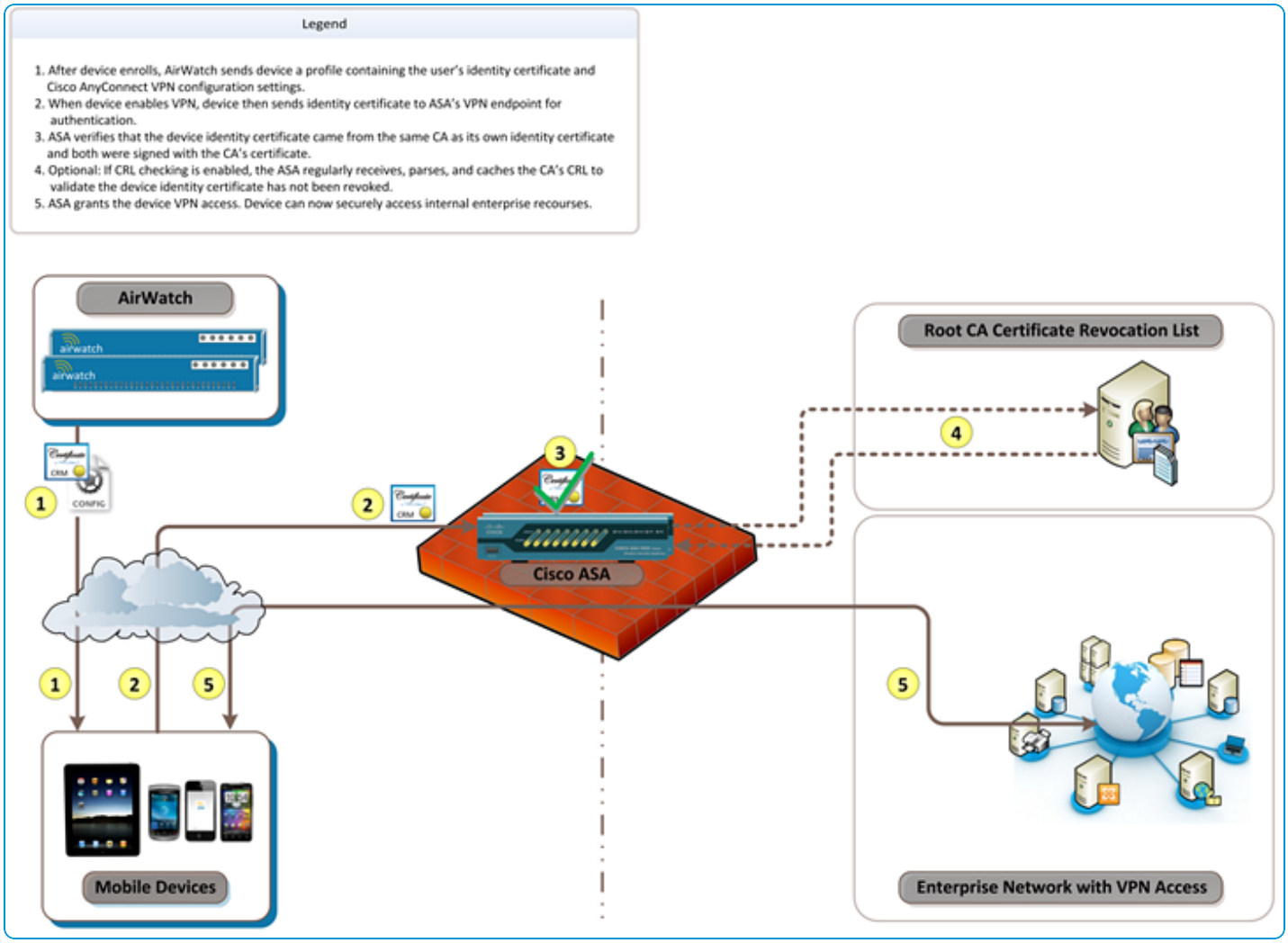
System Requirements for Cisco AnyConnect

The following tasks must be completed before configuring certificate integration.

- An external CA server must be set up and configured. If you want guidance as to the methodology of setting up an external CA, refer to **Selecting Microsoft CA Deployment Models Overview**, which is available on docs.vmware.com. The CA must be an external Enterprise CA as opposed to a standalone CA since standalone does not allow for the configuration and customization of templates.
- For AnyConnect VPN, you must have a Cisco Adaptive Security Appliance (ASA) connected to your network.

High Level Design for Cisco AnyConnect

This diagram shows how certificate authentication is handled from the point where the user's device enrolls into Workspace ONE UEM to when the user has VPN access to the protected enterprise network.



Implementation Approach for Cisco AnyConnect

You can configure your enterprise network server to securely pass corporate information to the user's device over Cisco's AnyConnect VPN.

To do this, you must perform some steps so that your Adaptive Security Appliances (ASA) firewall recognizes the user's device and trusts it is the device belonging to an authorized user. This process is accomplished by authenticating the user and their device with an Identity Certificate provided from an external certificate authority (CA).

Regardless of the ASA firewall equipment or proprietary AnyConnect VPN being configured, the methodology is the same. Before proceeding, ensure you understand the methodology, have the technical expertise, and have a strong understanding of the hardware and software.

Integrate the Firewall with an External CA

First, your firewall must be integrated with an external CA. This step ensures it can trust that incoming Identity Certificates originated from a valid, trusted source and can be used for authentication. Specifically while configuring Cisco AnyConnect for certificate authentication, this process entails:

- Disabling the Local CA on the ASA firewall
- Generating a Certificate Signing Request (CSR) on the ASA firewall
- Installing the external CA's certificate on the ASA firewall
- Installing the Identity Certificate on the ASA firewall

Configure the Firewall for SSL VPN Using Certificate Authentication

The next step is to configure the remaining SSL VPN settings. For Cisco AnyConnect, this process entails:

- Enabling AnyConnect access (SSL VPN feature)
- Creating a Group Policy
- Creating a Connection Profile and Tunnel Group for the AnyConnect client connections

Configure Workspace ONE UEM to Deploy an Identity Certificate and VPN Profile to Devices

At this point, SSL VPN has been properly configured to allow devices to connect with certificates from an external CA. However, it requires a manual process of generating and deploying Identity Certificates to all devices, and also configuring the appropriate VPN settings on each. Automating this process with Workspace ONE UEM entails:

- Integrating Workspace ONE UEM with the external CA
- Deploying a VPN and certificate profile to devices
- Deploying the AnyConnect application to devices

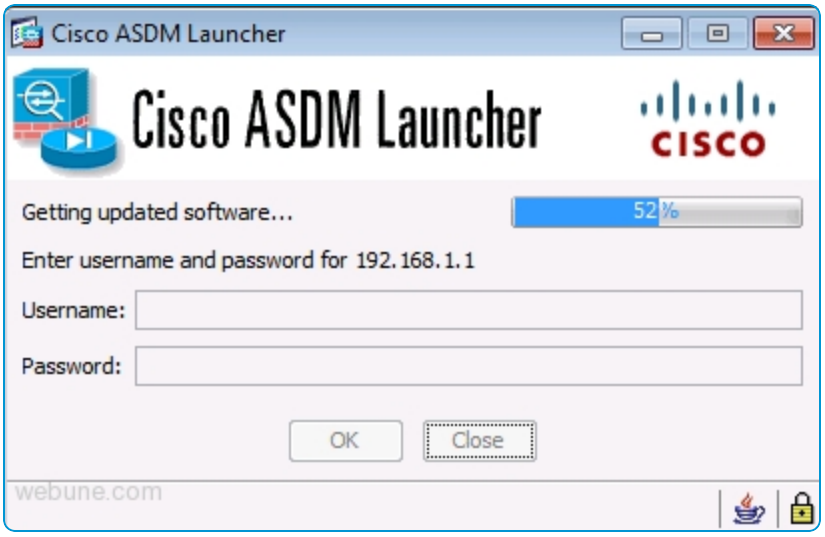
Chapter 2:
Install, Set Up, Configure Certificate

This section provides instructions to configure the certificate authority (CA) of your choice to work with the Workspace ONE ™ UEM console. Take the following steps and procedures to integrate the certificate.

Disable the Local CA on the ASA Firewall for AnyConnect

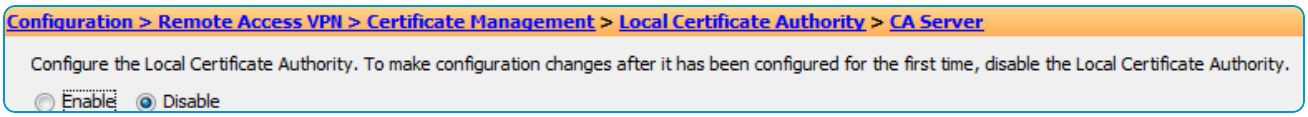
Before configuring the ASA firewall for AnyConnect VPN using an external certificate authority, you must disable the local CA on the ASA firewall. This ensures that certificates are authenticated against the external CA.

1. Log in to the Cisco Adaptive Security Device Manager (ASDM) to configure your ASA firewall.



2. Navigate to **Configuration > Remote Access VPN > Certificate Management > Local Certificate Authority > CA Server**.
3. Select **Disable**.

4. Select **OK**.



Next, you must **Configure the ASA Firewall and AnyConnect Clients**.

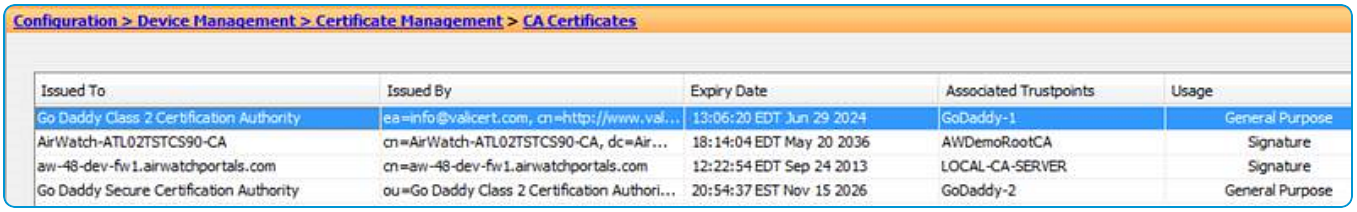
Configure the ASA Firewall and AnyConnect Clients

Once you have disabled the local CA, you are now free to configure the ASA firewall with a properly-signed identity certificate.

1. Create a CSR on the ASA firewall and send it to the external CA. The ASA needs an Identity Certificate signed by the external CA. For assistance, follow Cisco's instructions for Generating a CSR on the ASA firewall.

   After you have completed all the steps, a *CER file (for example, cert_client_id.cer) downloaded to your local machine that was obtained from the external CA.

2. Download the certificate from the external CA and install it on the ASA firewall to authenticate that the external CA is a trusted source. For assistance, follow Cisco's instructions on how to install the external CA's certificate.



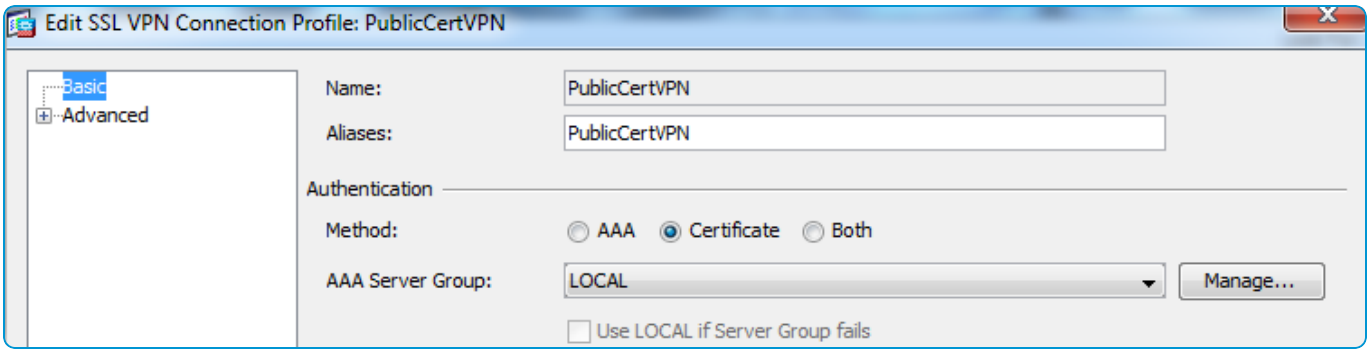
3. Install the Identity Certificate that you previously downloaded from the external CA. This certificate is used to verify that the Identity Certificate users authenticate with the same parameters and are coming from the same external CA as the Identity Certificate on the ASA firewall. For assistance, follow Cisco's instructions on how to install ASA's Identity Certificate. After completing these steps, the Identity Certificate that the external CA created is now installed on your ASA firewall.

4. Configure the VPN settings on the ASA. To begin, you must enable AnyConnect access on the appropriate VPN interface. Follow instructions on the Cisco Web site on how to enable the AnyConnect client access to the ASA.

5. Specify the group policy that is applied to AnyConnect clients and devices that connect to SSL VPN through the ASA firewall. Follow instructions on the Cisco Web site on how to create a SSL VPN Group Policy that is used by the ASA firewall.

6. Set up the connection profile and tunnel group to define the connection parameters of the SSL VPN session used by AnyConnect clients. For assistance, follow instructions on the Cisco Web site.

While creating a connection profile and tunnel group on the ASA for SSL VPN clients, a screen similar to the image here appears so that you can configure the **PublicCertVPN** SSL VPN Connection Profile. When this screen appears, make sure that you select **Certificate** instead of **AAA** authentication.



Next Steps

You have completed all the steps necessary to configure the external CA and ASA firewall to create a trust using certificates. You have enabled access, created a group policy, and created a connection profile so that SSL VPN certificate authentication can now be used with Cisco AnyConnect clients to gain access into your enterprise network.

Now, you can connect a device to your network using SSL VPN. The last step is to configure Workspace ONE UEM to manage devices. Continue to the following steps to integrate Workspace ONE UEM.

Integrate Workspace ONE UEM with the External CA, Cisco AnyConnect

After you configure the ASA firewall for AnyConnect VPN with external CA authentication, Workspace ONE UEM can be used to automate the deployment process of Identity Certificates and VPN settings to each device.

To accomplish this process, you must first integrate Workspace ONE UEM with the external CA so that Workspace ONE UEM can request and deploy Identity Certificates.

1. Log in to the Workspace ONE UEM console as an Administrator.
2. Navigate to **Devices > Certificates > Certificate Authorities**.
3. Select **Add**.
4. Select the appropriate PKI type from the **Authority Type** drop-down menu. This value is typically **Microsoft ADCS** (Active Directory Certificate Services). Make your Authority Type selection before configuring any other settings as the available options change depending on the Authority Type selected.
5. Enter the following details about the CA in the remaining text boxes.
   - Enter a name for the CA in the **Certificate Authority** text box. This value is how the CA is displayed within the Workspace ONE UEM console.
   - Enter a brief **Description** for the new CA.
   - Select **ADCS** radio button in the **Protocol** section. If you select SCEP, then there are different text boxes and selections available not covered by this document.

- Enter the host name of the CA server in the **Server Hostname** text box.
- Enter the actual CA Name in the **Authority Name** text box. This value is the name of the CA to which the ADCS endpoint is connected. This value can be found by launching the **Certification Authority** application on the CA server.
- Select the type of service account in the **Authentication** section. **Service Account** causes the device user to enter credentials. **Self-Service Portal** authenticates the device without the user having to enter their credentials.
- Enter the Admin **Username** and **Password**. This value is the user name and password of the ADCS Admin Account which has sufficient access to allow Workspace ONE UEM to request and issue certificates.

6. Select **Save**. Next, enter in information about the Identity Certificate template that Workspace ONE UEM deploys to devices for VPN certificate authentication.
7. Select the **Request Templates** tab.
8. Select **Add**.
9. Complete the certificate template Information.
   - Enter a name for the Request Template.
   - Enter a brief Description for the new certificate template.
   - Select the certificate authority that was just created from the certificate authority drop-down menu.
   - Enter the Subject Name or Distinguished Name (DN) for the template. The text entered in this text box is the Subject of the certificate, which a network administrator can use to determine who or what device received the certificate.

     A typical entry in this text box is “CN=WorkspaceONEUEM.{EnrollmentUser}” or “CN={DeviceUid}” where the {} entries are Workspace ONE UEM lookup values.
   - Select the private key length from the Private Key Length drop-down menu.

     This value is typically 2048 and must match the setting on the certificate template that is being used by DCOM.
   - Select the Private Key Type using the applicable check box.

     This value must match the setting on the certificate template that is being used by DCOM.
   - Select Add to the right of San Type to include one or more Subject Alternate Names with the template. This value is used for extra unique certificate identification. Usually, this value needs to match the certificate template on the server. Use the drop-down menu to select the San Type and enter the subject alternate name in the corresponding data entry text box. Each text box supports lookup values.
   - Select the Automatic Certificate Renewal check box to have certificates using this template automatically renewed before their expiration date. If enabled, specify the Auto Renewal Period in days.
   - Select the Enable Certificate Revocation check box to have certificates automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.
   - Select the Publish Private Key check box to publish the private key to the specified Web service endpoint (directory services or custom Web service).
10. Select **Save**.

Next, you must **Deploy a VPN and Certificate Profile to Devices**.

Deploy an AnyConnect VPN and Certificate Profile to Devices

After you configure the certificate authority and certificate template settings in Workspace ONE UEM, you can deploy an Identity Certificate and AnyConnect VPN settings to configure all assigned devices.

This process can be accomplished by creating a VPN and Certificate Profile.

1. Navigate to **Devices > Profiles > List View** from the Workspace ONE UEM console main menu.
2. Select **Add**.
3. Select the applicable device platform to open the **Add a New Profile**screen.
4. Configure the General settings for the profile. The **General** settings determine how the profile is deployed and who receives it and other overall settings.
5. Select **Credentials** from the profile options at left and then select **Configure**.
6. Select **Defined Certificate Authority** from the **Credential Source** drop-down menu.
7. Select the external CA created previously from the **Certificate Authority** drop-down menu.
8. Select the certificate template created previously from the **Certificate Template** drop-down menu.
9. Select **VPN** from the profile options at left and then select **Configure**.

   Credentials profile settings must be configured before the VPN profile settings because the VPN configuration refers to the Credential that was created in the previous step. Also, some of the configuration settings described here are not applicable to all device platforms.
10. Configure the following VPN profile settings:

- Enter a **Connection Name** used to identify this specific VPN connection on the device.
- Select **Cisco AnyConnect** as the VPN **Connection Type**.
- Enter the VPN **Server**. This value is the URL that users connect to for establishing their VPN connection.
- If your VPN has been configured to apply user credentials in addition to a certificate for authentication, then specify a **User Account** to pass to the VPN endpoint. To pass Workspace ONE UEM User Account names to the VPN endpoint, use the {EnrollmentUser} lookup value.
- To send all device traffic through the VPN connections, check the **Send All Traffic** check box. Alternatively, only traffic destined for the internal enterprise network uses the VPN connection, and public traffic continues to use 3G or other external connections to communicate.
- Next, select **Certificate** as the **User Authentication** type.
- Specify the AnyConnect VPN **Group Name** used to establish the connection.
- Select the credential you created previously from the **Identity Certificate** drop-down menu.

11. Select **Save** or **Save & Publish** to push the profile to a device.

And finally, you must **Deploy the AnyConnect application to Devices**.

Deploy the AnyConnect application to Devices

For devices to use the Cisco AnyConnect VPN settings you deploy, the Cisco AnyConnect application must be installed on the device.

This deployment can be completed manually, by asking each device user to download the application from the App Store, or you can use Workspace ONE UEM to prompt each user to install the Cisco AnyConnect app.

1. Navigate to **Apps & Books > Applications > Native**.
2. Select the **Public** tab.
3. Select **Add Application**.
4. Ensure that the correct organization group is displayed in the **Managed By** text box.
5. Select the appropriate platform from the **Platform** drop-down menu.
6. Enter **Cisco AnyConnect** in the **Name** text box.
7. Select **Next**.
8. Locate Cisco AnyConnect in the Search window.

   Please note that **Cisco Legacy AnyConnect** represents all versions up to 4.0.05069 and that **Cisco AnyConnect** represents all versions afterward. Ensure you select the correct version for your needs by clicking the appropriate **Select** button.
9. All required configuration settings populate automatically in the **Add Application** window. Specify any additional parameters.
10. Select **Save & Publish**.

Chapter 3:
Troubleshooting for Cisco AnyConnect

You can confirm that the VPN certificate is operational by pushing a profile to the device. Then, test whether or not the device can connect and sync to the configured ASA firewall.

If the device is not connecting, it may show a message that the certificate cannot be authenticated or the account cannot connect to the ASA firewall. In this case, there is a problem in the configuration.

Listed here are some helpful troubleshooting checks.

- Make sure that a certificate is issued by the external CA to the device by checking the following information:
  - Go to the external CA's server, start the certification authority application, and browse to the "issued certificates" section.
  - Find the last certificate that was issued. Ensure it has a subject that matches the one created in the certificate template section earlier in this document.

    If there is no certificate, then there is an issue with the external CA, client access server (for example, ADCS), or with the Workspace ONE UEM connection to the client access server.
  - Check that the permissions of the client access server (for example, ADCS) Admin Account are applied correctly to the external CA and the template on the external CA.
  - Check that the account information is entered correctly in the Workspace ONE UEM configuration.
- If the certificate is being issued, make sure that it is in the **Profile** payload and on the device.
  - Navigate to **Devices > Profiles > List View**. In the **Device Profiles** screen for the user's device, select **Actions** and then, select **</> View XML** to view the profile XML. There is certificate information that appears as a large section of text in the payload.
  - On the device, go to the profiles list, select details, and see if the certificate is present.
- If the certificate is on the device and contains the correct information, then the problem is most likely with the security settings on the ASA firewall.
  - Confirm that the address of the VPN endpoint is correct in the Workspace ONE UEM profile. Also confirm that all the security settings have been adjusted for allowing certificate authentication on the firewall.

- A good test to run is to configure a single device to connect to AnyConnect VPN using certificate authentication. Ensure this test works outside of Workspace ONE UEM, as until this works properly, Workspace ONE UEM is not able to configure a device to connect to AnyConnect VPN with a certificate.