VMware AirWatch Certificate Authentication for Cisco IPSec VPN

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 IPSec VPN

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

For those who are using other Secure Sockets Layer (SSL) Virtual Private Networks (VPN) hardware (e.g., Juniper, F5, etc.) or methods for certificate authentication, 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. This means 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 making their VPN login experience very simple and seamless.

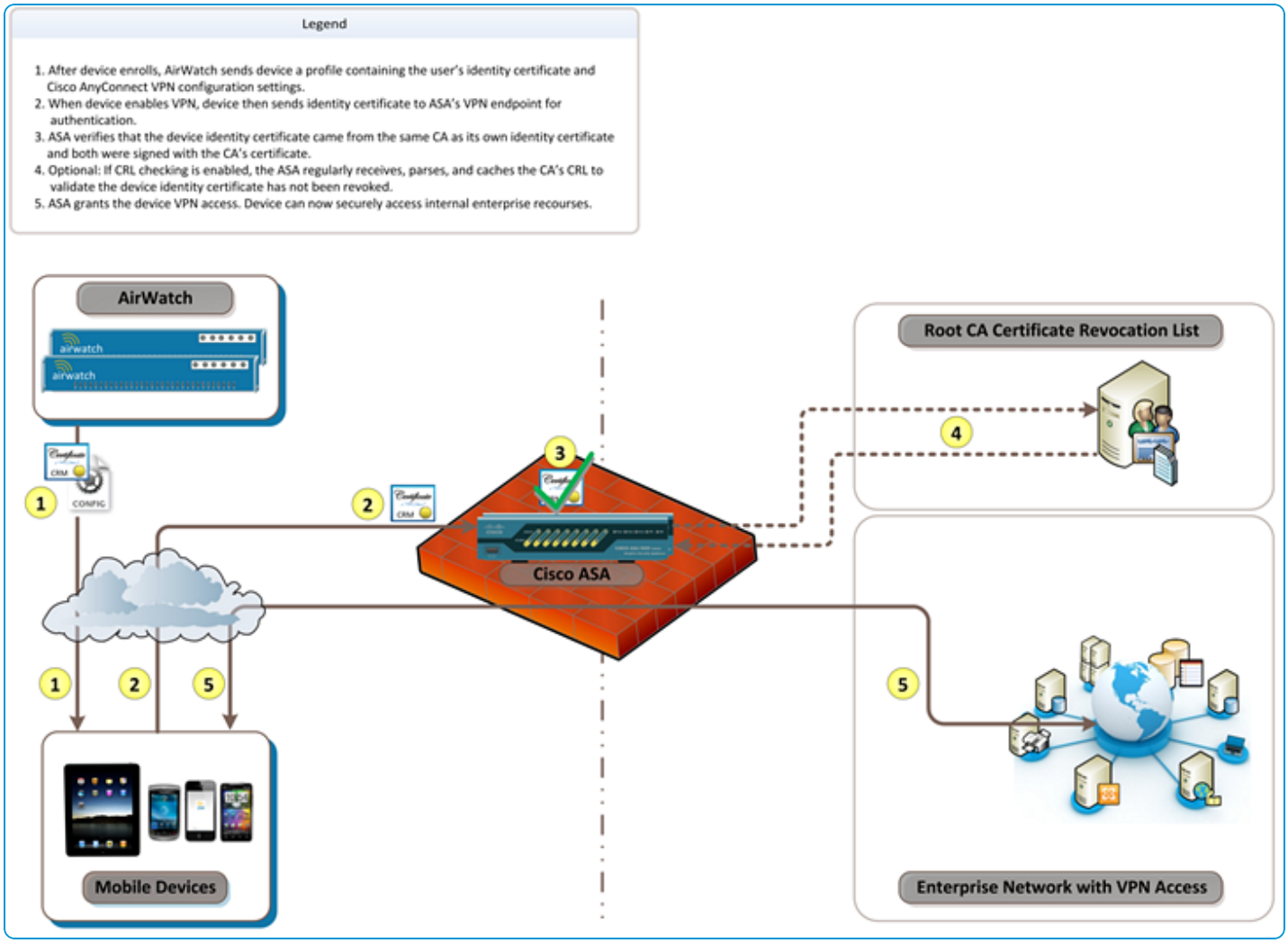
System Requirements for Cisco IPSec VPN

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 IPSec, you must have a Cisco Adaptive Security Appliance (ASA) connected to your network.

High Level Design for Cisco IPSec VPN

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 IPSec VPN

Before your enterprise network server can securely pass corporate information to the user's device over IPSec VPN, you need to perform some steps so that your Adaptive Security Appliances (ASA) firewall recognizes the user's device and trusts it belongs to an authorized user.

This 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 IPSec VPN being configured, the methodology is basically the same. If you understand the methodology, have the technical expertise, and have a strong understanding of the hardware and software needed to perform this, then it becomes much easier to configure and it ensures the user having a seamless experience using Remote Access VPN.

Integrate the Firewall with an External CA

First, your firewall must be integrated with an external CA so that it can trust that incoming Identity Certificates originated from a valid, trusted source that can be leveraged for authentication. Specifically, when configuring IPSec VPN for certificate authentication, the process includes:

- 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 IPSec VPN Using Certificate Authentication

Once your firewall has been configured with an external CA and both the CA's certificate and a corresponding firewall Identity Certificate have been added to the firewall, the remaining IPSec VPN settings can be configured. For IPSec VPN, the process includes:

- Configuring Internet Key Exchange (IKE) policies
- Selecting the mode of encryption
- Configuring the tunnel properties and policies
- Creating a new group policy
- Defining IP addresses (pool) available VPN clients
- Creating user accounts and group assignments
- Associating all attributes to create an IPSec profile

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

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

- Integrating Workspace ONE UEM with the external CA
- Deploying an IPSec VPN and certificate profile to devices

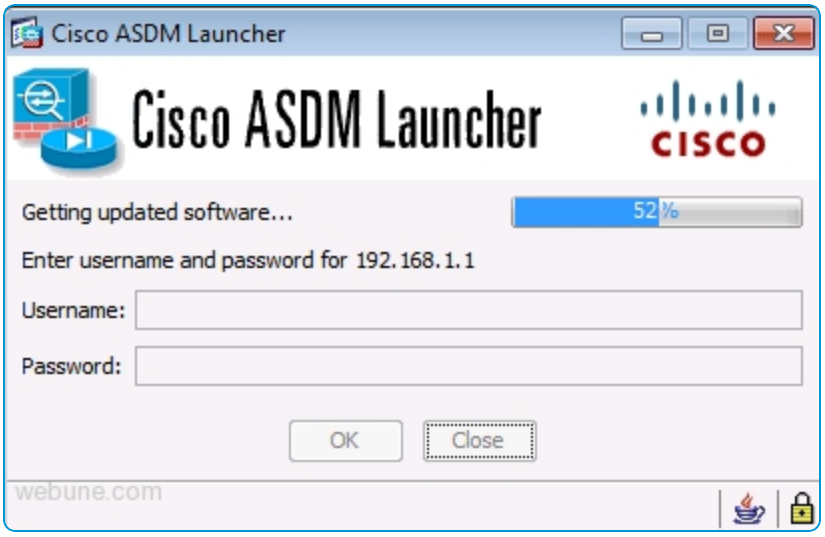
Chapter 2:
Install, Set Up, Configure Certificate

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 Cisco IPSec VPN

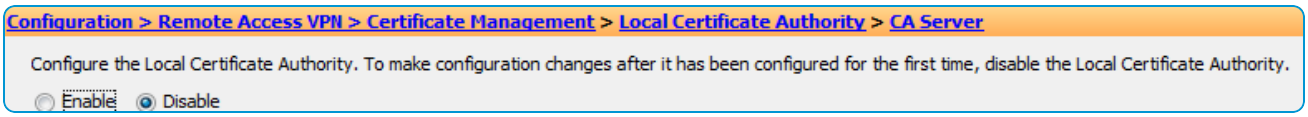
Before configuring the ASA firewall for IPSec using an external certificate authority, you must disable the local CA on the ASA firewall to ensure that certificates are authenticated against the external CA.

1. Log into 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 IPSec VPN**.

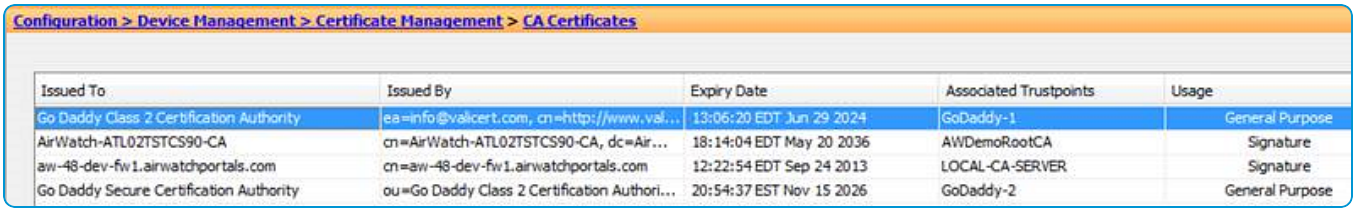
Configure IPsec VPN

Once you have disabled the local CA on the ASA firewall, you are now free to configure the IPSec VPN.

1. Create a CSR on the ASA firewall and send it to the external CA. This is because 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 (e.g., 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 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 was created by the external CA is now installed on your ASA firewall as shown below:

4. Configure the IKE policies, tunnel properties and policies, group policies, available VPN client IP addresses (pool), user accounts and group assignments, and associate these configurations to create an IPSec profile used by the VPN clients.

   Visit the Cisco website for instructions on creating a remote access connection profile and tunnel group on the ASA for IPSec VPN clients. Complete the steps necessary to configure the external CA and ASA firewall to create a trust using certificates and configure a remote access connection profile and tunnel group so that IPSec VPN certificate authentication can be used by your VPN clients to gain access into your enterprise network.

   At this time, you should be able to connect a device to your network using IPSec VPN. The last step is to configure Workspace ONE UEM to manage devices. Continue to the following steps to integrate Workspace ONE UEM.

   Next, you must **Integrate Workspace ONE UEM with the External CA**.

Integrate Workspace ONE UEM with the External CA for Cisco IPSec VPN

After configuring the ASA firewall for IPSec 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.

You can now integrate Workspace ONE UEM with the external CA so that Workspace ONE UEM can request and deploy Identity Certificates. First, you must provide Workspace ONE UEM with information about the external CA.

1. Log in to the Workspace ONE UEM console as a user with Workspace ONE UEM Administrator privileges, at minimum.
2. Navigate to **Devices > Certificates > Certificate Authorities**.
3. Select **Add**.
4. Select from the **Microsoft ADCS** from the Authority Type drop-down menu prior to completing any other configuration settings for the certificate authority.
5. Enter the information about the **Certificate Authority**.

- Enter a name for the new **Certificate Authority**.
- Enter a brief **Description** for the new certificate authority.
- Microsoft ADCS should already be selected for the **Authority Type** as described previously.
- Select **ADCS** radio button for the **Protocol**.
- Enter the URL of the server in the **Server Hostname** field. The server hostname must be entered in the following format: `https://{servername}/certsrv/adcs/`. The site can be `http` or `https` depending on how the site is set up. The URL must include the trailing /.
- Enter the **Authority Name**. This is the name of the certificate authority that the ADCS endpoint is connected to. This can be found by launching the **Certification Authority** application on the certificate authority server.
- Verify the **Service Account** radio button is selected for **Authentication**.
- Enter the **Username** and **Password**. This is the username and password of the ADCS Admin Account with sufficient access to allow Workspace ONE UEM to request and issue certificates.

6. Select **Save**.
7. Select the **Request Templates** tab at the top of the page and then select **Add**.
8. Complete the certificate template information.

- Enter a name for the new **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 field is the “Subject” of the certificate, which can be used by the network administrator to determine who or what device received the certificate.

A typical entry in this field is “CN=WorkspaceONEUEM.{EnrollmentUser}” or “CN={DeviceUid}” where the {} fields are Workspace ONE UEM lookup values.

- Select the private key length from the **Private Key Length** drop-down box.

  This is typically 2048 and should match the setting on the certificate template that is being used by ADCS.

- Select the private key type from the **Private Key Type** drop-down box.

  This is typically “Signing & Encryption” and should match the certificate template that is being used by ADCS. For use with Exchange Active Sync it should be “Signing & Encryption.”

- Select **Add** to the right of **San Type** to include one or more Subject Alternate Names with the template. This is used for additional unique certificate identification. In most cases, this 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 field. Each field supports lookup values.

- Select the **Automatic Certificate Renewal** checkbox to have certificates using this template automatically renewed prior to their expiration date. If enabled, specify the **Auto Renewal Period** in days.

  The auto-renewal period is the amount of time (in days) before the current certificate expires that the certificate will be renewed and pushed to devices.

- Select the **Enable Certificate Revocation** checkbox to have certificates automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.

- Select the **Publish Private Key** checkbox to publish the private key to the specified web service endpoint (directory services or custom web service).

9. Select **Save**.

Now you can proceed to the final step, **Deploy an IPSec VPN and Certificate Profile to Devices**.

Deploy an IPSec VPN and Certificate Profile to Devices

After configuring the certificate authority and certificate template settings in Workspace ONE UEM, deploy an Identity Certificate and IPSec VPN settings to be automatically configured on all of your devices.

1. Navigate to **Devices > Profiles > List View**.
2. Select **Add**.
3. Select the applicable device platform to launch 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 as well as other overall settings.
5. Select **Credentials** from the profile options at left and then select **Configure**.
6. Select **Define Certificate Authority** from the **Credential Source** drop-down menu.
7. Select the **Certificate Authority** you created previously from the **Certificate Authority** drop-down menu.
8. Select the **Certificate Template** you created previously from the **Certificate Template** drop-down menu.
9. Select **VPN** from the profile options at left.

10. Select **Configure**.

    You must configure the **Credentials** payload settings before the **VPN** payload settings.

11. Configure the **VPN** settings.

    - Enter in the **Connection Name** field a descriptive name that identifies the VPN connection on the device.
    - Select **IPSec (Cisco)** from the **Connection Type** drop-down menu.
    - Enter the VPN Endpoint URL or VPN Server in the **Server** field. This is the URL that users connect to in order to establish their VPN connection.
    - If your VPN has been configured to leverage user credentials in addition to a certificate for authentication, then enter in the **Account** field the User Account to pass to the VPN endpoint. To pass Workspace ONE UEM User Account names to the VPN endpoint, leverage the {enrollmentUser} lookup value.
    - Select **Certificate** as the type of **Machine Authentication**.
    - Select the **Identity Certificate** credentials that you created previously.
    - Verify the **Include User PIN** and **Enable VPN On Demand** checkboxes are not checked.

12. Select **Save** or **Save & Publish** to publish this profile to a device.

Chapter 3:
Troubleshooting for Cisco IPSec VPN

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

If the device is not connecting and shows a message that the certificate cannot be authenticated or the account cannot connect to the ASA firewall, then there is a problem in the configuration.

Chapter 4:
Troubleshooting Checks

- Make sure that a certificate is being issued by the external CA to the device by checking the following information.
  - Go to the external CA's server, launch the certification authority application, and browse to the "issued certificates" section.
  - Find the last certificate that was issued and it should have 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 (e.g., ADCS), or with the Workspace ONE UEM connection to the client access server.
  - Check that the permissions of the client access server (e.g., 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 and that all the security settings have been adjusted for allowing certificate authentication on the firewall.
- A very good test to run is to manually configure a single device to connect to IPSec VPN using certificate authentication. This should work outside of Workspace ONE UEM and until this works properly, Workspace ONE UEM will not be able to configure a device to connect to IPSec VPN with a certificate.