How to configure Mac computers to request digital certificates from a certificate authority using SCCM compliance settings

- Parallels Device Management

How to configure Mac computers to request digital certificates from a certificate authority using SCCM compliance settings

Many organizations use certificate-based network authentication. For example, a certificate may be required for a computer to join a Wi-Fi network or to establish a VPN connection. This article describes how to use SCCM compliance settings (OS X configuration profiles) to configure Mac computers to request a digital certificate from a certificate authority (CA).

To set up and use this functionality, you need the following:

1. A Mac computer running OS X Server to create an OS X configuration profile. You will create a configuration profile using the OS X Server?s Profile Manager. Note that the Profile Manager must have Device Management enabled in order to create a device profile with the **Directory** payload. To verify, in OS X Server, go to **Services > Profile** Manager and make sure that the **Device Management** option is enabled. Please note that you cannot use a user profile because it does not include the **Directory** payload.
2. Install a root certificate on each Mac computer to establish a chain of trust. This can be accomplished by using the **Certificates** payload of the OS X configuration profile.
3. Create a certificate template from which a certificate will be issued. You will specify the template in the **AD Certificate** payload of the OS X configuration profile.
4. Each target Mac computer must be a member of a domain. A Mac computer can be joined to a domain using the **Directory** payload of the OS X configuration profile.

Network and System Requirements

The following requirements must be met in order for Mac computers to be able to request certificates from the CA:

1. A valid Active Directory (AD) domain must exist.
2. Active Directory Certificate Services (AD CS) must be configured and running.
3. Mac computers on which the OS X configuration profile will be deployed must run OS X Mountain Lion (or later) and must be members of a domain.

Export a Root CA Certificate

First, you need to export a root CA certificate to a file, so you can later install it on Mac computers by including it in the Certificates payload of the OS X configuration profile.

To export a root certificate, do the following on a domain joined Windows computer:

1. Run **certmgr.msc** from the command prompt.
2. In the **certmgr** console, navigate to **Trusted Root Certification Authorities / Certificates**.
3. Find the root CA certificate in the list of certificates, right click it and then click **All Tasks > Export**.
4. The **Certificate Export Wizard** opens. Click **Next** on the **Welcome** page.
5. On the **Export File Format** page, select the **DER encoded binary X.509 (.CER)** option and click **Next**.
6. On the **File to Export** page, specify the target file name and path.
7. Click **Next**.
8. On the **Completing the Certificate Export Wizard** page, click **Finish**.
9. Click **OK** to close the wizard.

10. Copy the exported certificate file to the Mac running OS X Server where you?ll be creating an OS X configuration profile for your Mac computers.

Create and Issue a Certificate Template

Certificates for Mac computers will be issued using a certificate template, which you need to create and configure according to your needs. The following steps demonstrate how to create a certificate template. You may have additional requirements, so you should configure your template accordingly.

To create a certificate template:

1. Click **Start > Administrative Tools > Certification Authority**.
2. In the **certsrv** console, right click on **Certificate Templates** and then click **Manage** in the context menu.
3. In the **Certificate Templates** list, find a template named "Computer", right click on it, and then click **Duplicate Template** in the context menu.
4. In the **Properties of New Template** dialog, click the **General** tab and type a name in the **Template display name** field.
5. Click the **Subject Name** tab and make the following changes:

    - In the **Subject name format** drop-down list, select **Common name**.
    - In the **Include this information in alternate subject name** section, select the **User principal name (UPN)** option.
6. Click the **Security** tab and ensure that the **Domain Computers** group is granted the **Enroll** permission.
7. Click **OK** to save the changes and create a template.

You now need to issue the template that you just created. To do so:

1. In the **certsrv** console, right click on the **Certificate Template** node in the left pane and then click **New > Certificate Template** to Issue in the context menu.
2. In the **Enable Certificate Templates** dialog, select the template that you created earlier and click **OK**.
3. Back in the **certsrv** console, click on the **Certificate Templates** node in the left pane and then verify that the new template appears in the template list in the right pane.

Create an OS X Configuration Profile

For a Mac computer to request a certificate from the CA, it must be configured to do so. This task can be accomplished by creating a device configuration profile with the following payloads:

1. **Directory** ? for binding Mac to a domain.
2. **Certificates** ? for installing the root CA certificate on a Mac.
3. **AD Certificate** ? with proper settings for requesting a certificate from the CA.
4. **Network and/or VPN** ? [optional] for joining a corporate Wi-Fi network or configuring a VPN connection using a digital certificate for authentication.

To create a device configuration profile:

1. Log into the Mac computer running OS X Server.
2. Open the **Profile Manager**. If you haven't done so already, please verify that Device Management is enabled. To do so, go to **Services > Profile Manager** and make sure that the **Device Management** option is enabled.
3. In the **Profile Manager** window, select **Device Groups** in the left pane and then click the **Add Device Group** button in the right pane.
4. Type a device group name (e.g. "New Active Directory Group").
5. Click the **Settings** tab.
6. Click the **Edit** button in the **Settings for New Active Directory Group** section.
7. The **Settings for New Active Directory Group** window opens. Read on to learn how to configure the necessary payloads on this window.

Configure the Certificates Payload

1. In the **Settings for New Active Directory Group** window, select **Certificates** in the left pane.
2. Click **Configure** in the right pane.
3. Click the **Add Certificate...** button and select the root CA certificate file that you exported earlier.
4. The **Certificates** payload should now look as shown on the screenshot below:

Configure the AD Certificate Payload

1. In the **Settings for New Active Directory Group** window, select the **AD Certificate** payload in the left pane and then click **Configure** in the right pane. The payload properties are displayed in the right pane.

2. Type a description for the payload in the **Description** field.
3. Type the fully qualified host name of the CA in the **Certificate Server** field.
4. Type the short name of the CA in the **Certificate Authority** field.
5. Specify a certificate template name in the **Certificate Template** field. This should be the name of the template that you created earlier (see the **Create and Issue a Certificate Template** section above).
6. Leave the **User name** and **Password** fields empty.

Configure the Directory Payload

1. In the **Settings for New Active Directory Group** window, select the **Directory** payload.
2. Click the **Configure** button in the right pane.
3. Select **Active Directory** in the **Directory Type** drop-down list.
4. The **Directory** payload properties are displayed in the right pane.

5. In the **Server Hostname** field, type the hostname of the directory server.
6. In the **User name** and **Password** fields, type the credentials of the user that has rights to add a computer to **Active Directory**.
7. Type a value in the **Client ID** field. To make it work for any client, you can use (as an example) the *%SerialNumber%* variable. The value of this variable will be resolved to the serial number of a computer on which the configuration profile is applied.
8. Leave other settings unchanged or modify them according to your needs if you wish.

Configure Wi-Fi and VPN for Certificate-Based Authentication

This step is optional. You need to complete it if your Mac computers will be connecting to a Wi-Fi network or establishing a VPN connection using a certificate-based authentication.

To make the necessary configuration changes:

1. In the **Settings for New Active Directory Group** window, select the **Network** payload.
2. In the **Identity Certificate** drop-down list, select the AD certificate payload configured earlier.

3. Select the **VPN** payload.
4. In the **Machine Authentication** drop-down list, select **Certificate**.
5. In the **Credentials** field, select the AD certificate payload configured earlier.

- Certificate-based machine authentication is only supported for IPsec (Cisco) VPN tunnels. Other VPN types require different authentication methods.
- The account name field can be populated with a placeholder string.

You are nearly done crating the OS X configuration profile. To save the profile and close all windows:

1. Click **OK** on the **Settings for New Active Directory Group** window to save the changes and close the window.

2. Click the **Save** button at the bottom of the **Profile Manager** window.
3. Click the **Download** button near the **Settings for New Active Directory Group** window to download the configuration profile that you just created.
4. You can find the downloaded profile in */Users//Downloads*. A file containing the profile has the **.mobileconfig** extension.

Apply OS X Configuration Profile on Mac Computers

Once you've created an OS X configuration profile with a certificate request function configured, you can deploy it to Mac computers. To do so:

1. Log into the computer where the Configuration Manager console (with Parallels Mac Management extensions) is installed.
2. In the console, navigate to **Assets and Compliance / Overview / Compliance Settings / Configuration Items**.
3. Right click on **Configuration Items** and then click **Create Parallels Configuration Item > Mac OS X Configuration Profile from File** in the context menu.
4. In the **Mac OS X Configuration Profile** dialog, type a name for the configuration item, then select System profile as the profile type and specify the configuration profile that you created earlier (the one with the ".mobileconfig" extension).
5. Create a configuration baseline containing just the configuration item that you created in the previous step.
6. Deploy the baseline to a collection containing your Mac computers.

Note: It would make sense to set a custom schedule without recurrence for this configuration baseline because otherwise a certificate will be issued for a Mac every single time the baseline is applied on it. To avoid issuing multiple certificates for a given Mac, the baseline should be executed only once, when needed.

Troubleshooting

If a certificate request fails (the configuration profile isn?t installed), do the following to find out why:

1. Log into a Mac computer.
2. View the */var/log/system.log* records about certificate requests. Search for the *GetCertificateFromCAServer* text. A record will contain the request ID which can be checked for on the CA for more information.

3. Log into the server hosting the CA.
4. Open the **Certification Authority** console (**Start > Administrative Tools > Certification Authority**).
5. Select the **Failed Requests** node in the console.
6. Find an item with a **Request ID** matching the request ID from the log file on a Mac and see error details in the **Request Status Code field**.

7. Additional information can be found in the Event Viewer (Start > Administrative Tools > Event Viewer > Windows Logs > Application).
