



How to Create Certificate Template for Parallels Mac Clients for PKI Infrastructure

- Parallels Device Management

Introduction

If your SCCM infrastructure is configured in **HTTPs (PKI)** then you also need to configure the **Parallels Configuration Manager Proxy (CM Proxy) in PKI mode** to enable **Parallels Mac Clients** to communicate with SCCM.

To do this you will need to prepare a **certificate template** in your Certificate Authority (CA), trusted by SCCM. This certificate template will then be used for issuing a **PKI certificates for Parallels Mac Clients** by the **CM Proxy**. This PKI certificate will secure the communication between the Parallels Mac Clients and the Configuration Manager site by using mutual authentication and encrypted data transfers.

This article will provide you with a step-by-step guidance for preparing a certificate template for Parallels Mac Clients.

Notes

1. You can create the certificate template **manually**, as described below.
2. Or you can use [Parallels Mac Management Server Tools](#) to **automate** this task.

Creating Certificate Template for Parallels Mac Clients for PKI Infrastructure

1. Open **Certification Authority** console:
 1. Open the **Start** menu and click on **Certification Authority**:

2. Certification authority console will show up:

2. Open **Certificate Templates** console:

1. Right click on **Certificate Templates** item, located in **Certification Authority (Local)** *<name-of-your-ca>* and click **Manage:**

2. Certificate Templates Console will show up:

3. Duplicate **Workstation Authentication** certificate template:

1. Scroll down to find the **Workstation Authentication** certificate template, right-click on this template, and then click **Duplicate Template**:

4. Configure **Compatibility** options:

1. Ensure that **Certification Authority** is set to **Windows Server 2008**, and **Certificate recipient** is set to **Windows 7/ Server 2008**:

2. When changing **Certificate recipient** you will be informed that the necessary changes will effectively happen in the template options:

3. Press **OK** button to apply these changes.
5. In **General** options, provide a distinctive **name** for the new certificate template:

6. In **Cryptography** options ensure **minimum key size is set to 2048**:

7. In **Request Handling** options, ensure that **Allow private key to be exported** is turned **ON**:

8. Open **Subject Name** tab:
 1. Select the **Supply in the request** radio button:

2. **Certificate Templates** warning will be displayed, press **OK** button to proceed:

3. Turn **ON** the **Use subject information from existing certificates for autoenrollment renewal requests** checkbox:

9. In the **Extensions** options ensure that **Client Authentication** is listed in the **Description of Application Policies**:

10. In the **Security** options grant **Enroll** and **Autoenroll** permissions to following accounts:
 1. Add the **computer**, where **CM Proxy will be installed** to the **Group or user names** list, and grant it **Enroll** and **Autoenroll** permissions.
 2. Press **Add...** button:

3. Find the **computer** account and press **OK** button:

4. Choose the **computer** account you have just added, and grant it **Enroll** and **Autoenroll** permissions:

5. If **CM Proxy** will be running under a **domain user account** (not *LocalSystem*), then also **add this user account** to the **Group or user names** list, and grant it **Enroll** and **Autoenroll** permissions.
 1. *Note*: Skip the step if CM Proxy will be running under *LocalSystem* account!
 2. Press **Add...** button:

3. Find the **user** account for running CM Proxy, and press **OK** button:

4. Choose the **user** account you have just added, and grant it **Enroll** and **Autoenroll** permissions:

11. Press **OK** in the **Properties of New Template** dialog, and the new template will be created:

12. **Issue the certificate template** you have just created:

1. Get back to the **Certification Authority** console.
2. Right click on **Certificate Templates** in **Certification Authority (Local)** *<name-of-your-ca>* and click **New Certificate Template to Issue** in opened context menu:

3. Enable Certificate Templates dialog will pop up:

4. Choose the certificate template you have just created, and press **OK** button.

13. Now you have the **certificate template** ready to be used during the **configuration of Parallels Configuration Manager Proxy in PKI mode**.
