How to Create Certificate Template for Parallels Configuration Manager Proxy 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 its communication 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 certificate for the Parallels CM Proxy** by its configuration utility. This PKI certificate will secure the communication between the Parallels CM Proxy 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 CM Proxy.

Note: The article was created for Windows Server 2016, steps and screenshots may look differently on older systems.

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.

Create Certificate Template for Parallels Configuration Manager Proxy

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 **Web Server** certificate template:
    1. Scroll down to find the **Web Server** 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,**
    2. and **Certificate recipient** is set to **Windows 7/ Server 2008**:

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

4. 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. In **Subject Name** options:
    1. Ensure **Supply in the request** radio button is selected.
    2. Turn **ON** the **Use subject information from existing certificates for autoenrollment renewal requests** checkbox:

9. In the **Extensions** options add **Client Authentication** to the **description of Application Policies**:
    1. Select **Application Policies** in the list of **Extensions included in the template**, and click **Edit...** button:

2. In the **Edit Application Policies Extension** dialog press **Add...** button:

3. Choose **Client Authentication** item and press **OK** button:

4. **Client Authentication** policy will be added to the **Description of Application Policies:**

5. Now press **OK** button to apply changes and close the Properties dialog.

10. In the **Security** options grant **Enroll** and **Autoenroll** permissions to following accounts:
    1. Press **Add...** button:

2. Find the following accounts:
    1. **User** account, which will be used for **configuring CM Proxy;**
    2. Account of the **computer**, where **CM Proxy will be installed;**
    3. **User** account, which will be used for **running CM Proxy,** if CM Proxy will **not** be running under **LocalSystem account**!

4. then press **OK**.

3. Grant **Enroll** and **Autoenroll** permissions to added accounts:

11. Press **OK** in the **Properties of New Template** dialog to finish the creation of new template:

12. **Issue the certificate template** you have just created:
    1. Get back to the **Certification Authority** console.
    2. Right click on **Certificate Templates** item, located 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**.

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.