

How to issue WSUS certificate from local Certificate Authority

- Parallels Device Management

Symptoms

- How to issue WSUS certificate from local Certificate Authority
- Unable to configure Parallels OS X Software Update Service: **The WSUS signing certificate must be deployed and accessible by <username>:**

Cause

WSUS certificate should be issued to configure Parallels OS X Software Update Service.

Resolution

Note: requirements to certificate can be found here: [System Center Updates Publisher Signing Certificate Requirements & Step-by-Step Guide](#).

1. In Certificate Authority Console right-click **Certificate Templates > Manage**:
2. In the opened **Certificate Templates Console** right-click **Code Signing > Duplicate Template**.
3. In **Compatibility** tab:
 - ◆ set **Certificate Authority** to **Windows Server 2003**
 - ◆ set **Certificate recipient** to **Windows XP / Server 2003**
4. In **General** tab set **Template display name**:
5. In **Request Handling** tab:
 - ◆ Check **Allow private key to be exported**
 - ◆ Check **Prompt the user during enrollment**
6. In **Subject Name** tab set **Subject name format** to **Common name**:
7. In **Extensions** tab double click on **Key Usage** and UN-check **Make this extension critical**:
8. In **Security** tab, select **Authenticated Users** and grant it **Read** and **Enroll** permissions:
9. Click **OK** and close **Certificate Template Console** window.
10. In Certificate Authority Console right-click **Certificate Templates > New > Certificate Template to Issue**:
11. Locate created template and click **OK**:
12. On Machine where WSUS is installed:

- ◆ click **WIN+R** combination to open **Run** dialog, enter **mmc** to open MMC Console.
- ◆ click **File > Add/Remove Snap-in...**
- ◆ in the left pane of **Add or Remove Snap-ins** window select **Certificates** and click **Add >** button:
- ◆ in the **Certificates snap-in** window select **My user account > Finish > OK**:
- ◆ expand **Certificates - Current User > right-click Personal > All Tasks > Request New Certificate...**:
- ◆ at **Before You Begin** window click **Next**:
- ◆ at **Select Certificate Enrollment Policy** click **Next** window:
- ◆ at **Request Certificates** window select template that you created and click **Enroll**:
- ◆ at **Certificate Installation Results** window click **Finish**:

13. Export enrolled certificate on machine with WSUS:

- ◆ in **Certificates - Current User > Personal > Certificates** right-click on issued certificate > **All Tasks > Export...**
- ◆ at **Welcome to the Certificate Export Wizard** window click **Next**:
- ◆ at **Export Private Key** window check **Yes, export the private key** and click **Next**:
- ◆ at **Export File Format** window check **Export all extended properties** and click **Next**:
- ◆ at **Security** window check **Password** and enter password and click **Next**:
- ◆ at **File to Export** window specify certificate location and click **Next**:
- ◆ at **Completing the Certificate Export Wizard** click **Finish**:
- ◆ at **The export was successful** dialog click **OK**:

14. Install generated certificate to WSUS by executing the following commands one by one in **Administrative PowerShell** on WSUS server:

```
[Reflection.Assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")
$updateServer = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer()
$config = $updateServer.GetConfiguration()
$config.SetSigningCertificate("<Path to pfxFile>", "<PFX file password>")
```

where *<Path to pfxFile>* and *<PFX file password>* should be changed to appropriate values.

```
$config.Save()
```

Note: see the following [article](#) for additional details.

15. Set up the update server and clients for locally-published updates:

On the WSUS server:

- ◆ click **Win+R** combination to open **Run** dialog, enter **mmc** to open MMC Console.
- ◆ click **File > Add/Remove Snap-in...**
- ◆ in the left pane of **Add or Remove Snap-ins** window select **Certificates** and click **Add >** button.
- ◆ in the **Certificates snap-in** window select **Local computer account > Finish > OK**.

- ◆ navigate to the **WSUS** node in the snap-in, and then find the certificate you added the previous step.
- ◆ right-click the certificate and select **All Tasks > Export**. For security reasons, you should export only the public key, not the private key.
- ◆ copy this certificate on the SCCM SMS Provider server and somewhere on the WSUS server.

The following steps should be done **on both WSUS and SCCM SMS Provider servers** (considering that WSUS and SCCM SMS Provider are running on different servers):

- ◆ click **Win+R** combination to open **Run** dialog, enter **mmc** to open MMC Console.
- ◆ click **File > Add/Remove Snap-in...**
- ◆ in the left pane of **Add or Remove Snap-ins** window select **Certificates** and click **Add >** button.
- ◆ in the **Certificates snap-in** window select **Local computer account > Finish > OK**.
- ◆ in the Certificates snap-in select **Trusted Root Certification Authorities >** right-click **Certificates > All Tasks > Import** and import the certificate you just exported.
- ◆ in the Certificates snap-in select **Trusted Publishers >** right-click **Certificates > All Tasks > Import** and import the same certificate.

NOTE: Import root CA certificate to Trusted Root Certification Authorities on machine with WSUS if it's installed separately from CA (if certificate for WSUS signed by CA)

NOTE: If WSUS installed separately from SCCM, WSUS certificate(s) must be imported to Trusted Root Certification Authorities and Trusted Publishers on machine with SCCM too. Otherwise, update downloading via SCCM (during deployment creation) will be failed with invalid certificate signature error.

16. **After** Parallels Software Update Point (PSUP) Configuration Utility has been launched and PSUP has been configured, execute Powershell script one more time on the WSUS server:

```
[Reflection.Assembly]::LoadWithPartialName("Microsoft.UpdateServices.Administration")
$updateServer = [Microsoft.UpdateServices.Administration.AdminProxy]::GetUpdateServer()
$config = $updateServer.GetConfiguration()
$config.SetSigningCertificate("<Path to pfxFile>", "<PFX file password>")
```

where *<Path to pfxFile>* and *<PFX file password>* should be changed to appropriate values.

```
$config.Save()
```
