Permissions Required for Running the Parallels Configuration Manager Proxy Service

- Parallels Device Management

Information

Parallels Configuration Manager Proxy runs as a service in Windows. The user account under which it runs must have specific permissions. This article describes these permissions.

Note: *When creating (or choosing) a user account that will be used to run the Proxy service, consider the following. If Parallel Configuration Manager Proxy and Active Directory will run on different computers, permissions must be granted directly to the user or to a custom group (not a built-in group, like Administrators) to which the user belongs. If the Proxy and AD will run on the same server, you can add the user to a built-in group.*

1. Create a Domain User

The user configuring Parallels Configuration Manager Proxy must be a domain user. To create a domain user:

1.1. On the computer running Active Directory, click **Start > Administrative Tools > Server Manager**.

1.2. In the Server Manager window, navigate to **Roles / Active Directory Domain Services / Active Directory Users and Computers / `<domain-name>`**.

1.3. Right-click **Users** and select **New > User** in the context menu.

1.4. In the **New Object** - **User** dialog, type **Full name**, **User logon name**, and click **Next**.

1.5. Type the password in **Password** and **Confirm password** fields and click **Next**.

1.6. Click **Finish**.

2. Local administrator rights on the computer running the Parallels Configuration Manager Proxy.

2.1. Log into the computer that will run the Proxy.

2.2. Open **Server Manager** and navigate to **Configuration / Local Users and Groups / Groups**.

2.3. Right-click the **Administrators** group and select **Properties** in the context menu.

2.4. In the **Select Users** dialog, click **Add** and add the domain user you've created earlier. Click **OK** and click **OK** again.

3. The DCOM Remote Activation permission.

3.1. On the computer where the SMS Provider is installed, click **Start > Administrative Tools > Component Services**.

3.2. In the **Component Services** window, navigate to **Console Root / Component Services / Computers / My Computer / DCOM Config**. Scroll down to **Windows Management and Instrumentation**, right-click it, and then click **Properties** in the context menu.

3.3. Click the **Security** tab. The **Launch and Activation Permissions** section will have either the **Use Default** or the **Customize** option selected depending on your server configuration. Set the DCOM Remote Activation permission for the user as follows:

- If the **Customize** option is selected, click the **Edit** button, then add the user to the list and grant the user the **Remote Activation** permission.
- If the **Use Default** option is selected, close this window and do the following:

  a. In the **Component Services** window, navigate to **Console Root / Component Services / Computers**. Right-click **My Computer** and click **Properties** in the context menu.

  b. Click the **COM Security** tab.

  c. In the **Launch and Activation Permissions** section, click **Edit Default**.

  d. Add the user to the list and grant the user **Remote Activation** permission.

4. Full Administrator rights in Configuration Manager.

4.1. Log into the computer running the Configuration Manager console.

4.2. In the Configuration Manager console, navigate to **Administration / Overview / Security**.

4.3. Right-click **Administrative Users** and click **Add User or Group** in the context menu.

4.4. In the **Add User or Group** dialog, click **Browse**, find the domain user that you created earlier, and then click **OK**. The user will appear in the **User or group name** field in the **Add User or Group** dialog.

4.5. Click the **Add...** button in the **Assigned security roles** section.

4.6. In the **Available security roles** list, select **Full Administrator** and click **OK**.

4.7. Click **OK** to close the **Add User or Group** dialog.

5. Permissions in Active Directory.

If the **CN=System / CN=ParallelsServices / CN=PmaConfigMgrProxy-**`<site-code>` container exists in Active Directory, the user must have **Read**, **Write**, and **Create All Child Objects** permissions on it.

6. Permissions on SCCM Network Share.

Service account must have read and write permission on the \\sccm-server\SMS_site-code\inboxes\ddm.box share:

1. Open *sccm-server* in a file browser.
2. Right click the *SMS_site-code* folder and choose **Properties**.
3. Click the **Sharing** tab.
4. Click the **Advanced Sharing...** button.
5. In the **Advanced Sharing** dialog, click the **Permissions** button.
6. In the **Permissions** for *SMS_site-code* dialog, click the **Add...** button.
7. Select a user that will be used to run the service and click **OK**.
8. Select the user that you?ve added in the previous step (if it's not selected automatically) in the **Group or user names** list.
9. Select **Full Control** for the selected user in the **Permissions** for *user-name* section.
10. Click **OK** in **Permissions** for *SMS_site-code*.

11. Click **OK** in **Advanced Sharing**.
12. Click Close in *SMS_site-code* properties.
13. Go to *\\sccm-server\SMS_site-code\inboxes* in a file browser.
14. Right click on *ddm.box* and choose **Properties**.
15. In the **ddm.box Properties** dialog, click the **Security** tab.
16. Click the **Edit...** button under **Group or user names**.
17. In **Permissions for ddm.box**, click the **Add...** button.
18. Select the user that will be used to run the service and click **OK**.
19. Select the user that you?ve added in the previous step (if it's not selected automatically) in the **Group or user names** list.
20. Select the following permissions in the **Permissions** for *user-name* section:

    - Read & execute
    - List folder contents
    - Read
    - Write
21. Click **OK** in the **Permissions for ddm.box** dialog.
22. Click **OK** in the **ddm.box Properties** dialog.
