Permissions Required for Running the Parallels Configuration Manager Proxy Configuration Wizard

- Parallels Device Management

Information

A user that will be running the Parallels Configuration Manager Proxy Configuration Wizard must have specific permissions. This article lists these permissions and describes how to insure that the requirements are met.

The material presented here considers two possible scenarios:

- The Parallels Configuration Manager Proxy is configured for the first time;
- The Proxy has been previously configured and you want to reconfigure it using a different user account.

Some of the requirements described here apply to the first scenario only and some apply to both. Simply follow the instructions that correspond to your configuration and skip those that don't.

Note: *When creating (or choosing) a user that will configure the Proxy, 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.*

Create a Domain User

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

1. On the computer running Active Directory, click **Start > Administrative Tools > Server Manager**.
2. In the Server Manager window, navigate to **Roles / Active Directory Domain Services / Active Directory Users and Computers / `<domain-name>`**.
3. Right-click **Users** and select **New > User** in the context menu.
4. In the **New Object - User** dialog, type **Full name**, **User logon name**, and click **Next**.
5. Type the password in **Password** and **Confirm password** fields and click **Next**.
6. Click **Finish**.

Local Administrator Rights

The user must have administrative rights on the computer where the Parallels Configuration Manager Proxy will be installed:

1. Log into the computer that will run the Proxy.
2. Open **Server Manager** and navigate to **Configuration / Local Users and Groups / Groups**.
3. Right-click the **Administrators** group and select **Properties** in the context menu.
4. In the **Select Users** dialog, click **Add** and add the domain user you've created earlier. Click **OK** and click **OK** again.

DCOM Remote Activation Permission

The user must have the DCOM Remote Activation permission:

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

Administrative Rights in SCCM

The user must have **Full Administrator** rights in Configuration Manager:

1. Log into the computer running the Configuration Manager console.
2. In the Configuration Manager console, navigate to **Administration / Overview / Security**.
3. Right-click **Administrative Users** and click **Add User or Group** in the context menu.
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.
5. Click the **Add...** button in the **Assigned security roles** section.
6. In the **Available security roles** list, select **Full Administrator** and click **OK**.
7. Click **OK** to close the **Add User or Group** dialog.

Permissions in Active Directory

The user must have the necessary permissions in Active Directory. These permissions are required to create Parallels Mac Management-specific containers in AD and to manipulate data in these containers.

To grant the permissions:

1. Open **ADSI Edit** by clicking **Start > Administrative Tools > ADSI Edit**.
2. Verify that the following container exists: **DC=**`<domain>` **/ DC=**`<com>` **/ CN=System / CN=ParallelsServices**. Depending on the result, do one of the following:

    - If the container doesn't exist, grant the user the **Create All Child Objects** and **Read** permissions on the **CN=System** container. When granting these permissions to the user, apply it to **This object and all descendant object**.
    - If the container exists:

      a. Make sure the user have **Read**, **Write**, and **Create All Child Objects** permissions on it.

      b. Make sure the user has the **Full Control** permission on the **CN=ParallelsServices / PmaConfigMgrProxy-**`<site_code>` container.
3. Verify that the **DC=**`<domain>` **/ DC=**`<com>` **/ CN= Program Data / CN=Parallels** container exists:

- If the container doesn't exist, grant the user the **Create All Child Objects** and **Read** permissions on the **CN=Program Data** container. When granting these permissions to the user, apply it to **This object and all descendant object**.
- If the **CN=Parallels** container exists:

  a. Verify that the **CN=Parallels / CN=Parallels Management Suite** container exists. If it doesn't, grant the user the **Create All Child Objects** and **Read** permissions on **CN=Parallels** container.

  b. If the **CN=Parallels / CN=Parallels Management Suite** container exists, make sure that the user has **Read**, **Write**, and **Create All Child Objects** permissions on it.

Permissions to Read/Write Service Principle Name

The user must have permissions to read/write Service Principle Name. These permissions are required for the RBAC functionality. The Parallels Configuration Manager Proxy service account must have a registered Service Principle Name (SPN) for Kerberos connections. By default (with some exceptions) users are not permitted to register SPN to their own accounts.

To grant the permissions:

1. Open **ADSI Edit** by clicking **Start > Administrative Tools > ADSI Edit**.
2. Locate the required object:

   - If you specify a user as a service account during the configuration, you should locate this user object.

   Note: *The user object you select in this step must be the object of the user that will be used to* ***run*** *the service, not of the user that will be used to* ***configure*** *it. If you'll be using the same user to configure and to run the Parallels Configuration Manager Proxy service, then select the domain user object that you created in previous steps.*

   - If you choose `LocalSystem` as a service account during the configuration, you should locate the computer object you are running Proxy on.
3. Right-click the object, select **Properties** in the context menu, and then click the **Security** tab in the user properties dialog.
4. Add the user that will be configuring the Parallels Configuration Manager Proxy to the **Group or user names** list and then click the **Advanced** button.
5. In the **Advanced Security Settings** dialog, select the user that you added to the list in the previous step and click the **Edit** button.
6. In the **Permission Entry** dialog, click the **Properties** tab.
7. In the **Apply to** drop-down list, select **This object only**.
8. In the **Permissions** list, select the following permissions:

   - **Read servicePrincipalName**
   - **Write servicePrincipalName**
9. Click **OK**, then **OK**, and then **OK** again to close all dialogs.

MS SQL Server Permissions

The user must have necessary permissions in MS SQL Server. These permissions are needed to create and use a database storing the Parallels Mac Management data.

Assign the user to the **dbcreator** and **securityadmin** role as follows:

1. Run SQL Server Management Studio by clicking **Start > All Programs > Microsoft SQL Server 2008 R2**.
2. Connect to the SQL server.
3. Verify that the user that will be configuring the Parallels Configuration Manager Proxy exists in **Security / Logins**. If the user doesn't exist, add the user to the **Logins** list. To do so, right-click **Logins** and then click

New Login. Select **Windows authentication** and specify the **Login name** as domain\username, or click **Search** to search for the user. Click **OK** when done.
4. Navigate to **Security / Logins**, right-click the user that will configure Parallels Configuration Manager Proxy, and then click **Properties** in the context menu.
5. In the left pane, click **Server Roles**.
6. In the right pane, select **dbcreator** and **securityadmin** server roles.
7. Click **OK** to apply changes and to close the dialog.

Grant permissions to the SCCM database(CM_<site_code>):

1. In Microsoft SQL Server Management Studio, navigate to **Security / Logins**.
2. Right-click the user that will configure the Proxy and click **Properties**.
3. In the left pane, click **User Mapping**.
4. In the right pane, select the "CM_<site_code>" database (select the **Map** checkbox) and then select the following roles in the **Database role membership** list:
   db_datareader
   db_owner

If you have previously configured Parallels Mac Management Proxy on this site, then the Parallels Mac Management database should already exist in this SQL Server instance. To verify this, connect to the SQL Server and look for a database named "PMM_<site_code>" (where <site_code> is your SCCM site code). If a database with such a name exists, then perform the steps below. If the database doesn't exist, skip to the next section.

Assuming that the "PMM_<site_code>" database exist, grant the user the necessary permissions on it as follows:

1. In Microsoft SQL Server Management Studio, navigate to **Security / Logins**.
2. Right-click the user that will configure the Proxy and click **Properties**.
3. In the left pane, click **User Mapping**.
4. In the right pane, select the "PMM_<site_code>" database (select the **Map** checkbox) and then select the following roles in the **Database role membership** list:

   - db_datareader
   - db_datawriter
   - db_ddladmin
   - db_owner
   - public
5. Click **OK**.

Administrative Rights in Authorization Manager

If the Parallels Configuration Manager Proxy has been configured previously and the Authorization Store exists, the user configuring the Proxy must be assigned to the Administrator role in Authorization Manager. To assign the user to the Administrator role:

1. Start Microsoft Management Console (run mmc.exe).
2. In the MMC, click **File > Add/Remove Snap-in...**
3. Select **Authorization Manager** in the **Available snap-ins** list and click **Add >**.
4. Click **OK**.
5. Right-click **Authorization Manager** and then click **Open Authorization Store...**
6. Select **Active Directory or Active Directory Application Mode (ADAM)** and click **Browse**.
7. Select **CN=Authorization Store,CN=Parallels Management Suite,CN=Parallels,CN=Program Data, DC=**<domain>,**DC=**<com>.
8. Click **OK** and **OK** again to close the dialogs.
9. Expand **Authorization Manager** in the left pane, right-click **Authorization Store**, and then click **Properties**.
10. Click the **Security** tab.

11. In the **Authorization Manager user role** drop-down list, select **Administrator**.
12. Click **Add** and add the user that will configure the Proxy to the **Users and groups that are assigned to this role** list.
13. Click **OK** to save the changes and close the dialog.

© 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.