**Manage permissions for a web application in SharePoint Server**

**To manage permissions for a web application**

1. Start SharePoint 2019 Central Administration.
2. On the SharePoint Central Administration website, in the **Application Management** section, click **Manage web applications**.
3. In the web applications list, click the web application for which you want to manage permissions.
4. In the **Security** group of the ribbon, click **User Permissions**.
5. In the **User Permissions for Web Application** dialog, select the check boxes next to the permissions that you want to enable, and clear the check boxes next to those permissions that you want to disable.

You can select all permissions by selecting the **Select All** check box. You can clear all permissions by clearing the **Select All** check box.

1. Click **Save**.

**Manage permission policies for a web application in SharePoint Server**

**Add a permission policy level**

Use the following procedure to create a permission policy level.

**To add a permission policy level**

1. Start SharePoint 2019 Central Administration.
2. On the SharePoint Central Administration website, in the **Application Management** section, click **Manage web applications**.
3. Click to highlight the line for the web application whose permission policy level that you want to manage.
4. In the **Policy** group of the ribbon, click **Permission Policy**.
5. In the Manage permission policy levels dialog, click **Add Permission Policy Level**.
6. In the Add permission policy level dialog, in the **Name and Description** section, type the name and description for the policy that you want to create.
7. In the **Site Collection Permissions** section, select the site collection permissions for this policy.
8. In the **Permissions** section, select the permissions to grant or deny for this permission level.

* Select the **Grant All** check box to include all available permissions in this policy.
* Select the **Deny All** check box to deny all available permissions in this policy.
* Select either the **Grant** or **Deny** check boxes to include or exclude individual List, Site, and Personal permissions from this policy.

Do not click either **Grant** or **Deny** if you want access to be controlled through regular site or site collection permissions.

1. Click **Save.**

**Edit a permission policy level**

Use the following procedure to edit a permission policy level.

**To edit a permission policy level**

1. Start SharePoint 2019 Central Administration.
2. On the SharePoint Central Administration website, in the **Application Management** section, click **Manage web applications**.
3. Click to highlight the web application whose permission policy level that you want to manage.
4. In the **Policy** group of the ribbon, click **Permission Policy**.
5. In the Manage permission policy levels dialog, click the link for the permission policy level that you want to edit.
6. On the Edit permission policy level page, edit the settings, and then click **Save**.

**Delete a permission policy level**

You might want to delete a permission policy level if the users or groups for which you created it are no longer required to use it. It is a good practice to review all existing permission policy levels to ensure that they are still required.

**To delete a permission policy level**

1. Start SharePoint 2019 Central Administration.
2. On the SharePoint Central Administration website, in the **Application Management** section, click **Manage web applications**.
3. Click to highlight the web application whose permission policy level that you want to manage.
4. In the **Policy** group of the ribbon, click **Permission Policy**.
5. In the Manage permission policy levels dialog, select the check box of the permission policy level that you want to delete, and then click **Delete Selected Permission Policy Levels**.
6. Click **OK** to confirm the deletion.

**Add users to or remove users from a permission policy level**

You can add users to a permission policy level, edit the policy level settings, and delete users from a permission policy level. The following settings can be specified or changed:

* **Zone:** If a website has multiple zones, you can choose the zone that you want the permission policy level to apply to. The default is all zones, which can be specified for Windows users only.
* **Permissions:** You can specify a default policy level of Full Control, Full Read, Deny Write, and Deny All permissions, or you can specify a custom permission level that you created.
* **System**: This setting enables SharePoint to display **SHAREPOINT\System** for system-related activity regardless of the Windows user accounts that have been configured for the hosting application pool and the SharePoint farm service account. You might want to specify this setting to prevent unnecessary information disclosure to end-users and potential malicious users who would be interested in knowing more about the SharePoint deployment in the enterprise.

**Add users to a permission policy level**

Use the following procedure to add users to a permission policy level.

**To add users to a permission policy level**

1. Start SharePoint 2019 Central Administration.
2. On the SharePoint Central Administration website, in the **Application Management** section, click **Manage web applications**.
3. Click to highlight the web application whose permission policy level that you want to manage.
4. In the Policy group of the ribbon, click **User Policy**.
5. In the Policy for Web Application dialog, click **Add Users**.
6. In the Add Users dialog, in the **Zone** list, click the zone to which you want the permission policy level to apply and then click **Next**.
7. In the Add Users dialog, in the **Choose Users** section, type the user names, group names, or e-mail addresses that you want to add to the permission policy level.
8. In the **Choose Permissions** section, select the permissions that you want the users to have.
9. In the **Choose System Settings** section, check **Account operates as System** if you want to specify whether a user account should be displayed as SHAREPOINT\System instead of the actual accounts that perform specific tasks within the SharePoint environment.
10. Click **Finish**.

**Edit a permissions policy**

Use the following procedure to edit the permissions granted by a permission policy level.

**To edit a user permissions policy**

1. Start SharePoint 2019 Central Administration.
2. On the SharePoint Central Administration website, in the **Application Management** section, click **Manage web applications**.
3. Click to highlight the web application whose permission policy level that you want to edit.
4. In the **Policy** group of the ribbon, click **User Policy**.
5. In the Policy for Web Application dialog, select the check box next to the user or group that you want to manage, and then click **Edit Permissions of Selected Users**.
6. On the Edit Users page, in the **Permission Policy Levels** section, select the permissions that you want the users to have.
7. In the **Choose System Settings** section, click **Account operates as System** to specify whether a user account should be displayed as SHAREPOINT\System instead of the actual accounts that perform specific tasks within the SharePoint environment.
8. Click **Save**.

**Delete users from a permission policy level**

Use the following procedure to delete a user from a permission policy level.

**To delete users from a permission policy level**

1. Start SharePoint 2019 Central Administration.
2. On the SharePoint Central Administration website, in the **Application Management** section, click **Manage web applications**.
3. Click to highlight the web application whose permission policy level that you want to manage.
4. In the **Policy** group of the ribbon, click **User Policy**.
5. In the Policy for Web Application dialog, select the check box next to the user or group that you want to delete, click **Delete Selected Users**, and then click **OK**.