MODULE 4 Securing a Company Portal

Contents

MODULE OVERVIEW

LESSON 1: EXPLAINING PERMISSIONS AND SECURITY IN SHAREPOINT

LESSON 2: CREATING SHAREPOINT GROUPS

LESSON 3: MANAGING PERMISSIONS WITHIN SHAREPOINT

LESSON 4: SHARING VERSUS TRADITIONAL SECURITY

LAB: MANAGING PERMISSIONS IN SHAREPOINT

Module Overview

This module explains how permissions work within a site collection, and how the tools within SharePoint 2016 are used to manage and maintain them. It is crucial that SharePoint 2016 site collection administrators and site administrators are able to create and manage permissions within SharePoint 2016.

After completing this module, students will be able to:

• Explain the concept of sharing

• Design and implement security

• Describe best practices around SharePoint 2016 security

Lesson 1: Explaining Permissions and Security in SharePoint

SharePoint uses an Access Control List security method for enforcing permissions throughout the farm. This security method answers the basic questions of who, what and where:

• Who: Those who have been given access

• What: The level of access granted

• Where: The object to which access has been granted

SharePoint security allows organizations to structure their information based on security levels to meet the needs of compliance or any security policies that are currently in place.

The Access Control List (ACL) is a property of each securable object within the SharePoint hierarchy. Securable objects are sites, lists, libraries, folders, items and documents. Permissions assigned at a higher level are inherited by lower levels. The site and site collection administrator can break this inheritance in order to customize the permissions for an individual subsite, list, library, item or document.
SharePoint uses Security Trimming. For example, if permissions on one document in a document library are removed, the SharePoint user will see all other documents except for that one document in that particular library.

The Access Control List is a collection of Access Control Entries. Each entry consists of two parts:

- **Security Principal**: This is the user or group to whom the permissions have been given. Groups may either be SharePoint groups (recommended) or Active Directory groups.
- **Permission Level**: This is the specifics of the access granted to the principal. Permission levels are pre-defined sets of permissions that can be granted as a unit, as opposed to assigning each permission individually. There are over 30 individual permissions that can be assigned in SharePoint.

**Security Principals**

As mentioned previously, a security principal is the who – a user or group to which permissions are granted for a specific object within SharePoint. A best practice is to avoid the direct assignment of permissions to an individual user. This management by exception often leads to messy and lengthy ACLs, which become difficult to manage and monitor. Moreover, each time the ACL is modified the object is flagged for backup, which increases the size of the incremental backup.

Best practices are to use groups for the assignment of permissions on an ACL. Both SharePoint groups and Active Directory groups can be added as security principals. Here are some considerations for both approaches.

**SharePoint Groups**

SharePoint groups allow for the site and site collection administrator to maintain specific access control to the site content. Each user that is to be given access must first be added to the SharePoint group. The permission level assigned to the group is then available to all members of the group. This allows for the site and site collection administrator to document the permissions granted through the name of the group. While the benefit of this approach is that the site and site collection administrator has direct control of granting access, it may be cumbersome to add a new user to each of several SharePoint groups.

**Active Directory Groups**

Active Directory groups leverage the existing Active Directory infrastructure and its grouping of users for securing SharePoint. The Active Directory administrators are responsible for creating and maintaining the group memberships. When a new user is added, the Active Directory administrators add that user to the required groups. While this takes access control out of the hands of the SharePoint administrator, it centralizes the administration of group memberships.

A best practice for security principals is a combination of the two. By nesting Active Directory groups within SharePoint Groups, the SharePoint administrator can leverage the groupings within Active Directory while specifically assigning permissions to that group. Moreover, when a new user is added, the Active Directory administrator can simply copy an existing user and all the Active Directory group assignments will be copied to the new user as well. Because SharePoint group memberships cannot be copied in this way, this blended approach offers the best of both.

One caveat to this two-layered approach: In some environments, Active Directory is managed by a separate team with strict operating procedures. It may be difficult to request the creation of Active Directory groups for use with SharePoint.
Permissions and Permission Levels

If security principals are the who, then permissions are the what – that is, what can they do? There are over 30 individual permissions that can be granted. These permissions fall into one of three different categories: list, site and personal. Following is a description of each permission:

List Permissions

List Permissions grant access to lists and libraries, and control the actions that can be performed there.

<table>
<thead>
<tr>
<th>List Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Lists</td>
<td>Creates and deletes lists, add or remove columns in a list, and add or remove public views of a list.</td>
</tr>
<tr>
<td>Override List Behaviors</td>
<td>Discards or checks in a document which is checked out to another user, and change or override settings which allow users to read/edit only their own items.</td>
</tr>
<tr>
<td>Add Items</td>
<td>Adds items to lists, add documents to document libraries, and add web discussion comments.</td>
</tr>
<tr>
<td>Edit Items</td>
<td>Edits items in lists, edit documents in document libraries, edit web discussion comments in documents and customize Web Part Pages in document libraries.</td>
</tr>
<tr>
<td>Delete Items</td>
<td>Deletes items from a list, delete documents from a document library, and delete web discussion comments in documents.</td>
</tr>
<tr>
<td>View Items</td>
<td>Views items in lists, view documents in document libraries and view web discussion comments.</td>
</tr>
<tr>
<td>Approve Items</td>
<td>Approves a minor version of a list item or document.</td>
</tr>
<tr>
<td>Open Items</td>
<td>Views the source of documents with server-side file handlers.</td>
</tr>
<tr>
<td>View Versions</td>
<td>Views past versions of a list item or document.</td>
</tr>
<tr>
<td>Delete Versions</td>
<td>Deletes past versions of a list item or document.</td>
</tr>
<tr>
<td>Create Alerts</td>
<td>Creates email alerts for users.</td>
</tr>
<tr>
<td>View Application Pages</td>
<td>Views forms, views, and application pages. Also, enumerate lists.</td>
</tr>
</tbody>
</table>

Site Permissions

Site Permissions grant access at the site level, and include management tasks above lists and libraries.

<table>
<thead>
<tr>
<th>Site Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Permissions</td>
<td>Creates and changes permission levels on the web site and assign permissions to users and groups.</td>
</tr>
<tr>
<td>View Web Analytics Data</td>
<td>Views reports on web site usage.</td>
</tr>
<tr>
<td>Create Subsites</td>
<td>Creates subsites such as team sites, meeting workspace sites and document workspace sites.</td>
</tr>
<tr>
<td>Manage Web Sites</td>
<td>Grants the ability to perform all administration tasks for the web site as well as manage content.</td>
</tr>
<tr>
<td>Add and Customize Pages</td>
<td>Adds, changes or deletes HTML pages or Web Part Pages, and edits the website using a Windows SharePoint Services-compatible editor.</td>
</tr>
<tr>
<td>Apply Themes and Borders</td>
<td>Applies a theme or borders to the entire website.</td>
</tr>
<tr>
<td>Apply Style Sheets</td>
<td>Applies a style sheet (.CSS file) to the website.</td>
</tr>
<tr>
<td>Create Groups</td>
<td>Creates a group of users that can be used anywhere within the site collection.</td>
</tr>
<tr>
<td>Browse Directories</td>
<td>Enumerates files and folders in a website using SharePoint Designer and Web DAV interfaces.</td>
</tr>
<tr>
<td>Use Self-Service Site Creation</td>
<td>Creates a website using Self-Service Site Creation.</td>
</tr>
<tr>
<td>View Pages</td>
<td>Views pages in a website.</td>
</tr>
<tr>
<td>Enumerate Permissions</td>
<td>Enumerates permissions on the website, list, folder, document or list item.</td>
</tr>
</tbody>
</table>
## Site Permission

<table>
<thead>
<tr>
<th>Site Permission</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse User Information</td>
<td>Views information about users of the website.</td>
</tr>
<tr>
<td>Manage Alerts</td>
<td>Manages alerts for all users of the website.</td>
</tr>
<tr>
<td>Use Remote Interfaces</td>
<td>Uses SOAP, Web DAV, Client Object Model or SharePoint Designer interfaces to access the website.</td>
</tr>
<tr>
<td>Use Client Integration Features</td>
<td>Uses features that launch client applications. Without this permission, users will have to work on documents locally and upload their changes.</td>
</tr>
<tr>
<td>Open</td>
<td>Allows a user to open a website, list or folder in order to access items inside that container.</td>
</tr>
<tr>
<td>Edit Personal User Information</td>
<td>Allows a user to change personal information, such as adding a picture.</td>
</tr>
</tbody>
</table>

## Personal Permissions

Personal Permissions grant access for users to customize SharePoint for their own purposes.

<table>
<thead>
<tr>
<th>Personal Permissions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Personal Views</td>
<td>Creates, changes and deletes personal views of lists.</td>
</tr>
<tr>
<td>Add/Remove Personal Web Parts</td>
<td>Adds or removes personal Web Parts on a Web Part Page.</td>
</tr>
<tr>
<td>Update Personal Web Parts</td>
<td>Updates Web Parts to display personalized information.</td>
</tr>
</tbody>
</table>

## Permission Levels

With over 30 different permissions from which to choose, assigning each permission individually would be a challenge. SharePoint allows for permission levels to be created. Permission levels are groups of permissions that can be assigned to a security principal as a block. This facilitates the assignment of permissions by allowing for all needed permissions to be applied in a single step.

SharePoint allows for the creation of custom permission levels. Following is a table the pre-defined permission levels. Based on the site template used to create the site, some of these permission levels may not be listed for that site.

<table>
<thead>
<tr>
<th>Permission Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full Control</td>
<td>This permission contains all permissions.</td>
</tr>
<tr>
<td>Design</td>
<td>This permission allows the ability to create lists and libraries, apply themes, borders, style sheets and edit pages.</td>
</tr>
<tr>
<td>Edit</td>
<td>This permission set can add, edit and delete lists, view, update, delete list items and documents.</td>
</tr>
<tr>
<td>Contribute</td>
<td>This permission set can view, add, update and delete information in a library or list.</td>
</tr>
<tr>
<td>Read</td>
<td>This permission set offers a read-only view of SharePoint objects.</td>
</tr>
<tr>
<td>Limited Access</td>
<td>This permission set is used to give granular permissions to individual users or groups within a site, without giving rights to everything in that SharePoint site.</td>
</tr>
<tr>
<td>View Only</td>
<td>This set can view pages, list items and documents. Document types with server-side file handlers can be viewed in the browser but not downloaded.</td>
</tr>
<tr>
<td>Approve</td>
<td>This permission set can edit and approve pages, list items and documents.</td>
</tr>
<tr>
<td>Manage Hierarchy</td>
<td>This set can create sites and edit pages, list items and documents.</td>
</tr>
<tr>
<td>Restricted Read</td>
<td>This permission set can view pages and documents, but cannot view historical versions or user permissions.</td>
</tr>
<tr>
<td>Restricted Interfaces for Translation</td>
<td>Open lists and folders, and use remote interfaces with this permission set.</td>
</tr>
</tbody>
</table>
Lesson 2: Creating SharePoint Groups

SharePoint groups offer the best approach to assigning permissions within a site collection. SharePoint groups can be named in such a way as to document the purpose of the group, and the permissions that have been granted to it. All members of the SharePoint group then receive the permissions assigned to it. Members of a SharePoint group can include Active Directory users and groups, as well as external users if the farm is set up for other authentication.

Default SharePoint Groups

Upon creating a new SharePoint site collection, a set of SharePoint groups are automatically created. They use a specific syntax that looks like this:

- `<sitename> Visitors`: Assigned the Read permission level
- `<sitename> Members`: Assigned the Contribute permission level
- `<sitename> Owners`: Assigned the Full Control permission level

For example, a new top level site called Learning Lake would generate the following groups:

- Learning Lake Visitors
- Learning Lake Members
- Learning Lake Owners

Depending on the template on which the new site is based, SharePoint may also create other groups:

<table>
<thead>
<tr>
<th>Group</th>
<th>Permission Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approvers</td>
<td>Members can edit and approve pages, list items and documents.</td>
</tr>
<tr>
<td>Designers</td>
<td>Members can edit lists, libraries and pages in the site. They can also create master pages and page layouts as well as manage CSS files.</td>
</tr>
<tr>
<td>Hierarchy Managers</td>
<td>Users manage hierarchy.</td>
</tr>
<tr>
<td>Quick Deploy Users</td>
<td>Users can schedule quick deploy jobs.</td>
</tr>
<tr>
<td>Records Center Web Service Submitters</td>
<td>Records Center Web Service Submitters.</td>
</tr>
<tr>
<td>Style Resource Readers</td>
<td>This is restricted read permission to the Style Library.</td>
</tr>
<tr>
<td>Viewers</td>
<td>This is View Only.</td>
</tr>
</tbody>
</table>

If a new SharePoint group needs to be created, it is first necessary to determine the permission set, and to determine why the group needs to be unique. This is typically done because of governance principles followed by most organizations. It is best practice to provide only the permissions needed, and not more. There are three ways to accomplish this:

- Create a new SharePoint site with unique permissions
• Create new SharePoint groups for the non-inheriting permission site

• Create new groups within a site collection

Creating a New SharePoint Site with Unique Permissions

As covered in the section on Creating Unique Permissions, when creating a site there is an option to Use unique permissions. Once chosen, SharePoint will ask to configure unique permissions for the site, list, library, document, item or page.

1. After creating the site and choosing Use unique permissions, click Create.

2. SharePoint will refresh into the Set Up Groups for this Site page.

3. Leave the Visitors to the default that is already available, unless there needs to be a unique group.

4. Verify the name of the Members of this Site and Owners of this Site sections, as well as add members into the groups and click OK.

![Setting unique permissions on a site](https://skillpipe.com/#/reader/urn:uuid:9e691a33-42d3-4176-b322-412dee76a30f@2022-02-23T14:00:00Z/content)

Most organizations make everyone within the organization part of the Visitors group, giving them the ability to view information within SharePoint. To do this, be sure that the Visitors group contains NT Authority\authenticated users. This allows Visitors-level access to anyone who can log in to the domain as well as from trusted domains.

Create a New Group at the SharePoint Site Collection or Non-Inheriting Site

Creating a new group at the SharePoint site collection or site levels involves a similar approach. However, it is important to remember that if a SharePoint site is inheriting permissions from the site collection, then everything needs to take place there. Creating a new group at a SharePoint site level can only happen if non-inheriting permissions are in place.
1. In a SharePoint site that has non-inheriting permissions, click **Settings > Site Settings > Site Permissions**.

2. Click **Permissions > Create Group** from the **Grant** group.

![Permissions page](image)

3. Name the group. This name needs to be unique within the site or site collection and should always be preceded by the name of the site. An example is **Human Resources Owners**.

4. Provide a detailed description of the permissions this group will be given within SharePoint in the **About Me** section.

5. Review the account listed in the group owners for the group. Typically, the individual creating the group will be added as the owner. However, only one person can be added as the owner of the group.

6. In the **Group Settings** section, select who can view the membership of the group and who can edit the membership of the group.

![Group Settings](image)

7. In the **Membership Requests** section, select whether to allow requests to join/leave this group, and if requests should be auto-accepted.

---

If the Allows requests to join/leave this group option is enabled, an e-mail address needs to be added. Also, if the Auto-accept requests option is enabled, the SharePoint user will automatically be given the rights associated with that group.
Finally, select the appropriate permissions set for the group and click **Create**.

**Managing Users and Groups**

In some organizations, SharePoint site and site collection administrators will be managing the day-to-day activities of users and groups within SharePoint. As explained in the previous section, the administrator is able to create unique permissions and new groups. This section covers how to grant and remove permissions as well as edit permissions of an existing user or group.

**Grant Permissions to Users in Groups**

When granting permissions to users via group membership, it is important to remember that groups are present throughout the site collection. That is, it does not matter at which level in a site collection hierarchy a user is added to a group. Once a user is placed into a group, any access granted to that group at any point in the site collection is now immediately available to the newly added user.

For example, if a user is added into the Learning Lake Members group in the Projects site, and Projects is a subsite of Learning Lake, then when the user navigates up to the top level site that person should exist within the group. It does not matter where the user is added. It is the same group throughout the site collection. Here is how to add a user into a group at any level.

1. Navigate to the desired site.
2. Click **Settings > Site Settings > Users and Permissions > People and Groups**.
3. Click the appropriate group from the **Groups** quick launch.
4. Click **New > Add Users**.
5. In the **Share With** window, type the names, email address or ‘Everyone’ to add people to the group. Once
Sharing a site

6. Click **Share** to complete the assignment.

Lesson 3: Managing Permissions within SharePoint

To manage permissions within the SharePoint environment, administrators must understand SharePoint groups, how permissions are added within a SharePoint site collection or site, and how to control permission inheritance.

**Accessing Permissions within SharePoint**

Because there are multiple objects within SharePoint, there are multiple ways to apply permissions. The ability to manage SharePoint objects can be found easily at the following levels:

- **Site Collection**
- **Site**
- **Library or List**
- **Folder/Document or Item**

**Site Collection Level**

1. Navigate to the root site within the site collection and log in with the Site Collection administrator credentials.

2. Click **Settings > Site Settings > User Permissions.**
Accessing site settings

3. Click **Site Collection Administrators**.

The initial site collection administrators are defined by the server administrator when the top level site is created. Site collection administrators have full access to all content within the site collection. Their permissions cannot be stopped by blocking inheritance. Anyone who is added to the list of site collection administrators has complete access to all areas within the site collection.

This gives the SharePoint Site Collection administrator access to the entire site collection. Site Collection administrators have the ability to add other SharePoint users into this group.

The other two options under Users and Permissions allow Site Collection administrators the ability to configure Site permissions, Site app permissions, or People and Groups. Refer to the following table for more details:

<table>
<thead>
<tr>
<th>Users and Permissions</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Permissions</td>
<td>Assigns permission levels to users and groups that will be inherited down to all other inheriting SharePoint objects within the site collection.</td>
</tr>
<tr>
<td>Site App Permissions</td>
<td>This is a list of installed apps on the site; these permissions are not modified via the screen because app permissions are granted by the person installing the app at the time of installation.</td>
</tr>
<tr>
<td>People and Groups</td>
<td>Used to add individuals or groups into a SharePoint group; this permission routes to the Groups listing, specifically the Members group.</td>
</tr>
</tbody>
</table>

Additionally, **Site Permissions** can be accessed quickly by clicking **Settings > Shared With**. The window that appears shows the current Active Directory Accounts or Groups that have rights to the site as well as their level of access. The **Advanced** link redirects site owners to the Site Permissions page, where all of the permissions for the site are visible.

**Site Level**

1. Navigate to the desired SharePoint site.
2. Click **Settings > Shared With**.
3. Click **Advanced**.
Sharing a site

OR

Click Settings > Site Settings > Users and Permissions > People and groups or Site permissions.

Locating site permissions

If permission inheritance is still in place, Site Permissions cannot be modified.

Library or List Level

1. Navigate to the desired library or list.

2. Click List or Library > Shared With from the Settings group to view the current Active Directory groups or people with rights. The Advanced link within the Shared With window navigates to the permissions page for the list/library.

Sharing a list or library through the ribbon

OR
3. Click **List** or **Library > Shared With** from the **Settings** group > **Permissions and Management** > **Permissions for this document library** or list.

![Permissions and Management](image)

**Sharing a list or library through settings**

**Folder/Document/Item Level**

1. Within a SharePoint library or list, navigate to the desired folder.
2. Select the folder by clicking to the left of the folder.
3. Click **Files > Shared With** from the **Manage** group.

![Setting permissions on the folder or item level](image)

**OR**

4. Click the **Folder** menu to quickly view the list of Active Directory groups or accounts that have rights. If there are multiple users, the text **lots of people** will show. Click this link to view all accounts with permissions to the content.

![View permissions](image)
Sharing through the edit menu

OR

5. Click the Folder > Open > Advanced > Shared With.

Sharing using the Shared With feature

Stop Inheriting Permissions

Permissions begin at the top and flow down the hierarchy, passing from top level site to subsite, list and library and on to the items and documents themselves. This allows for a single point of management for permissions within the site collection. Changes made at the top will be inherited by all subordinate objects.

When a site collection administrator or site owner wants to create unique permissions for a SharePoint site, list, library, document or item, the inheritance can be stopped. Once inheritance is stopped, all objects below that point will inherit the new set of permissions.

Editing Permissions – Unique Permissions

1. Navigate to a site, list, library, folder or item and access the Permissions window.

For the SharePoint site, this needs to be the Site Permissions window in order to manage the inheritance.

2. Notice the Permissions window and the message currently available for this SharePoint site. As an example, it should say, This website inherits permissions from its parent. The site administrator does not have the ability to edit these permissions at this point.
**Inheritance message**

3. On the **Permissions** screen, click **Permissions > Stop Inheriting Permissions** from the **Inheritance** group.

**Stop inheriting permissions**

SharePoint will prompt for confirmation if this is an action that is desired with the following statement: **You are about to create unique permissions for this web site. Changes made to the parent web site permissions will no longer affect this web site. To manage changes in permissions across multiple web sites, using groups is recommended.**

4. Click **OK**.

Stopping the inheritance for a site will then prompt to create new SharePoint security groups or reuse existing groups for the site.

Notice that permissions can now be edited in this SharePoint site by the included check boxes as well as the message, **This site has unique permissions.**

---

**Create Unique Permissions for a Site**

When creating a SharePoint site, the site and site collection administrators will also be able to create a unique permission structure right from the **Create New Site** window.

1. Create a new SharePoint site.
2. In the Permissions section, choose Use unique permissions to break inheritance between the site and child site.

![Permissions settings]

Setting unique permissions on a site

When creating sites, it is best practice to use the same permissions as the parent site, contrary to what is shown above. This site will then start out with the same permissions and groups as the parent site. The site owner can then break inheritance and work with the existing groups or create new ones. This decreases the creation of duplicate groups.

Inherit Permissions

If a SharePoint object needs to re-inherit permissions from the parent, perform the following steps:

1. Within the permissions of the SharePoint object, click Permissions > Delete unique permissions in the Inheritance group.

![Permissions settings]

Deleting unique permissions

2. The user will be prompted with the message, Hold on. This site includes things that have been shared with specific people. Those people will lose access. Click OK.

Notice that permissions should be set to inherit from the parent SharePoint object as well as the message stating, This library inherits permissions from its parent.

![Permissions settings]

Deleting unique permissions does not delete the previously created SharePoint groups created for the site. They can still be accessed at the root of the site collection. Additionally, if
individuals belong to other SharePoint groups that have access to the parent site/list/library they will have access to the site/list/library via that permissions level.

**Edit User Permissions**

To edit an entry in an Access Control List:

1. Navigate to either the top level site or a SharePoint object with unique permissions.
2. If the object is a site, then click **Settings > Site Settings > Site Permissions**. For other objects, click **Shared With** from the ribbon.
3. Click **Advanced** from the **Shared With** window.
4. Click **Permissions > Edit User Permissions** from the **Modify** group.

![Editing user permissions](image)

5. In the **Edit Permissions** page adjust the permissions for the user or group and then click **OK**.

**Remove User Permissions**

To remove a user or group from an Access Control List:

1. Navigate to the SharePoint site, list, library, document or item.
2. Click **Shared With**. If the object is a site click **Settings > Shared With**.
3. Click the **Advanced** link.
4. Select the checkbox next to the user or groups.
5. Click **Permission > Remove User Permissions** from the **Modify** group.
Removing user permissions

6. SharePoint will request confirmation with the following window, **You are about to remove all permissions for the following user or group to...** Click OK.

Confirm removing permissions

Other Permission Management Tools

These are other options that can help when working with permissions at the site or site collection levels.

Custom Permission Levels

1. From the top level site within the Site Collection, click **Settings > Site settings > Site Permissions**.

2. Once in **Site Permissions**, click **Permissions > Permission Levels** from the **Manage** group.

Setting a custom permission level

3. Click **Add a Permission Level** command to create a custom permission level.

4. Name the new **Site Owner Permission** appropriately (e.g. **Site Owner Adjusted**).

5. Make sure to include a **Description** with details as to why this group was created and what permissions they do or do not have.

6. Click the **Select All** checkbox and then selectively remove the necessary permissions:
   - **Create Subsites**: Creates subsites such as team sites, Meeting Workspace sites and Document Workspace sites.
- **Manage Permissions**: Creates and changes permission levels on the website and assign permissions to users and groups.

- **Apply Style Sheets**: Applies a style sheet (.CSS file) to the website.

- **Apply Themes and Boards**: Modifies the look and feel of a site.

7. Click the **Create** button.

Now that a new permission level has been created, it can be added to an existing group, or a new group needs to be created using the new level. It has now been added to the web page as an option for group permissions.

![List of permission levels with newly created custom permission level](image)

**View Group Permissions**

Understanding where SharePoint Groups are used and what permissions they have can often be a struggle for site administrations. Within the permissions settings of a site, site administrators can view the permissions assigned to a particular SharePoint group as well as see where the group is currently used.

1. Navigate to the top level site within the Site Collection.

2. Click **Settings > Site settings > People and Groups**.

3. Click a group to view the members.

4. From within the group, click **Settings > View Group Permissions**.

![Viewing group permissions](image)
List of group permissions

Check Permissions for Accounts

Another challenge presented to site administrators is understanding which rights an individual account has throughout the site collection.

1. **Click** Settings > Site Settings > Site Permissions > Check Permissions.
2. **Type or click** Browse to select a user or group.

Check permissions on the ribbon

Checking effective permissions
Edit Group Quick Launch

By default, only a small set of groups are listed in the Quick Launch menu within a site. In some cases, the groups lists are not used; therefore, they could be hidden or removed from the Quick Launch menu. Site collection administrators can control which groups are visible within a site or site collection.

1. Click Settings > Site Settings > People and Groups.

2. In the Quick Launch menu, click the More link at the bottom of the navigation.

3. Click Settings > Edit Group Quick Launch.

4. In the Groups box, add or remove the groups that should be visible in the menu.

Lists that have Unique Permissions

When working with lists or libraries, site or site collection administrators can quickly determine if a list or library is inheriting permissions from the parent site, or has been configured to use unique permissions.

1. Navigate to a site.

2. Click Settings > Site Settings > Site Permissions. If content within a site contains unique permissions, a yellow information box appears.
Lesson 4: Sharing versus Traditional Security

SharePoint 2016 introduces the concept of sharing as a means to give users the ability to share content with others. This new approach is a quick way to grant permissions to a site, a document or list item. Using the Share command modifies the underlying permissions within the site granting access to the account(s) invited to the site, list, library or item. The default level of access granted at the time of sharing is set to Edit/Contribute. However, this permission level is adjustable to any of the permission level available within the site.

Users that do not have rights to modify permissions on an item will have their request to share content automatically routed to the administrator for approval prior to the underlying security being modified. In order for site administrators to receive notification, the sites access request settings must be configured to include an email address for the person responsible for approving access requests.

Enabling Access Request

Access request allows non-authorized users the ability to request access to a SharePoint site, library/list or item. Administrators of a site receive email messages to either accept or reject these requests.

1. Navigate to the top level site within the site collection.
2. Click Settings > Site Settings.
3. Click Site Permissions.
4. Click Access Request Settings.
Access request settings

5. Confirm the box is marked next to **Allow access requests**.

6. Confirm the email address in the box is a person that has proper rights to modify security. Typically, this is the site administrator.

7. Click **OK** to confirm.

---

**In order to have different email addresses for various areas of the site, inheritance must be blocked. Then the Access Request Settings are available at each new point of inheritance.**

---

**This feature is turned off if outgoing e-mail has not been configured by the SharePoint administrator.**

---

**Sharing a SharePoint Object**

Sometimes it may be necessary to add a single user to a site or a SharePoint object, even though this is against best practices. For example, a unique document that is only to be seen by the CEO would require unique permissions for that individual, without creating a group.

**Sharing a Site**

1. Navigate to the SharePoint site.

2. Click **Share** in the ribbon to invite individuals to the site.
Sharing an object

3. Enter the names or email addresses in the **Invite** box.

4. Click **Show Options** to view a list of available permissions levels for the individuals entered in the **Invite** box.

5. Select the appropriate **SharePoint Group** from the box and to determine whether to send an email invitation.

6. Click **Share** to send an invitation.

---

When sharing a site, the individuals listed in the Invite box are automatically added to the SharePoint group that is selected from the Show Options section. If the default security setting remains at **Edit**, users are added to the Members group for that site.

---

**Sharing a List or Library**

1. Navigate to the SharePoint list or library.

2. Click **List or Library > Shared With** from the **Settings** group to view the current Active Directory Groups or People with rights.

---

**Sharing through the ribbon**
3. Click **Invite People** to open the **Share** window.

![Share dialog box](image)

**Granting permissions through the Share dialog**

4. Enter the names or email addresses in the **Invite** box.

5. Click **Show Options** to view a list of available permissions levels for the individuals entered in the **Invite** box.

6. Select the appropriate permission level from the box and determine whether to send an email invitation.

7. Click **Share** to send an invitation.

---

**When sharing a list or library, the individuals listed in the Invite box are automatically added to the library as an individual account and are granted the selected permissions level. If the default security setting Edit is used, users are added as individuals with edit rights only.**

---

**Sharing an Item or File**

1. Navigate to the SharePoint document or item.

2. Place a checkmark next to the items to be shared with other individuals.

3. Click **Items** or **Files > Shared With** from the **Manage** group to view the current Active Directory Groups or
People with rights.

Sharing a folder:

The Share dialog box.

4. Click **Invite People** to open the **Share** window.

Granting permissions through the Share dialog box

OR

5. Click **Share** in the ribbon to invite individuals to a file or item.
Share on the ribbon

Share dialog box

6. Enter the names or email addresses in the Invite box.

7. Select the level of rights from either Can Edit or Can View.

8. Click Show Options to review the options to send an email invitation.

9. Click Share to send them an invitation.

When sharing an item or file, the individuals listed in the Invite box are automatically added as an individual account and are granted edit or view rights.

Best Practices for SharePoint Permissions

The following list summarizes best practices for working with SharePoint permissions. Administrators should:

- Use Active Directory groups and then add these into SharePoint groups whenever possible.
- Always make sure to retain site administrators when breaking inheritance and removing groups from the SharePoint object. In other words, do not remove permissions of the site collection administrators.
- Whenever possible, assign permissions at the parent level and use permission inheritance to populate through the rest of the site collection.
- Use the default SharePoint groups such as Owners, Members and Visitors.
- Not give more permissions than necessary to an individual or group.
- Limit the use of granular permissions since this will cause permission issues in the future.
- Always document when in doubt.

Lab: Managing Permissions in SharePoint
The Learning Lake organization has a security policy based on roles within the organization. This policy can be applied at the site, library or list, and item levels. Because of the SharePoint structure, the ability to inherit permissions or break inheritance affects the ability for an individual to access the different areas within SharePoint.

After completing this lab, you will be able to:

• View permissions of SharePoint objects
• Add users and groups to SharePoint objects
• Create a new SharePoint managers group with customized permissions
• Stop inheriting permissions between SharePoint objects

Estimated time to complete this lab: 45 minutes

Exercise 1: Viewing Permissions of SharePoint Objects

Let us look at how permissions are currently established for the Human Resources site.

1. If necessary, navigate to the Human Resources site below Departments.

2. Click Settings > Shared with to see the groups and users that have access to the site.

3. Click Advanced to browse to the Site Permissions page.
4. Click the Learning Lake Intranet Owners group to see who is within that group—Jerome Clark.

The site administrator has the ability to change Group Settings, such as giving an individual the ability to request to join or leave a group.

5. Click Settings > Group Settings to change the group settings.

6. Within the Group Settings window, in the Membership Requests section, click Yes for Allow request to join/leave this group. Notice the ability to type an email address. This user will receive an email whenever another user requests membership to the group.

7. Click OK.

8. Click Settings > View Group Permissions to see what permissions are set for the members group. This window shows permission assignments across the site collection.

9. Click OK to close the window.

10. At the top of the screen, click Settings > Site settings > Site permissions from the Users and Permissions section.

11. On the ribbon, click Permissions > Stop Inheriting Permissions from the Inheritance group.

12. Click OK in the message box. This will break inheritance from the parent site.
13. Click the radio buttons next to each of the options to create a new visitors group, new members group and new owners group.

14. Keep the group names set to their default values of:

   a. Human Resources Visitors
   b. Human Resources Members
   c. Human Resources Owners

15. Click **OK** to create the groups. Now, these three groups have permission to access the Human Resources site and subsites.

Exercise 2: Adding Users and Groups to SharePoint Objects

Now that unique permissions have been created for the Human Resources site, you can share the Human Resources department site with other employees without giving them blanket rights to the entire site collection.

1. Navigate to the Human Resources – Home page.

2. From the SharePoint ribbon, click **Share**.

3. In the Share ‘Human Resources’ box start typing **Irene Ward** and then click the result found for **Irene Ward** in the box that appears.

4. Click **Show Options** to expand the list of available permissions for this site.
Exercise 3: Creating a New SharePoint Group with Custom Permissions

It has been determined that there needs to be a subset of the Learning Lake Site Owners group that is more restrictive. The current site collection has been configured with all permissions inheriting from the top level site. You will need to be a Site Collection Administrator or have Full Control permissions to complete these tasks.

2. Click Settings > Site Settings.
3. In the Users and Permissions section, click Site permissions. This will show you all the groups that have permissions within the root Learning Lake Intranet site.
4. To create a new permission level, click Permissions > Permission Levels in the Manage group on the ribbon. Notice all the different built-in permission levels.
5. Click Add a Permission Level.
6. Use the following information to create this new permission level called **Site Owner Limited**:
   
   a. **Name**: Site Owner Limited
   
   b. **Description**: This permission level has all of the same permissions as Full Control except for Manage Permissions and Create Subsites permissions.
   
   c. Click Select All.
   
   d. In the **Site Permissions** section, deselect Manage Permissions and Create Subsites.

   e. Scroll to the bottom and click **Create**.

7. Click **Permissions** in the page title breadcrumb to navigate back to site permissions.

8. To create a new group, click **Permissions > Grant > Create Group** on the ribbon.

9. Use the following information to create this new group called **Limited Site Owners**:
   
   a. **Name**: Limited Site Owners
   
   b. **About Me**: Members of this group have all the permissions of the Team Site Owners group except for managing permissions or creating subsites within the site collection.
   
   c. **Give Group Permission to this Site** section: Site Owner Limited (near bottom of the page)

   d. **Everything else**: Leave defaults.

10. Click **Create**. You are now inside the **Limited Site Owners** group.

11. Click **New > Add Users**.

12. Use the Share ‘Learning Lake Intranet’ box to type names of individuals. As you begin to type the following names, a box will appear where you can easily select their full name to add them to the invite box.

   a. **Linus Evans**
b. Ali Roth  
c. Irene Ward  
d. Natasha Patton

Exercise 4: Test New Permission Level

1. Switch account to Irene Ward. To do this, click the Windows icon in lower left of the screen.
2. In the top left corner, click Jerome Clark and select Switch account.
3. In the lower left, select Other User.
4. Log in using the following credentials:
   a. Username: IreneW  
   b. Password: Passw0rd1
5. On the taskbar, click your browser.
   If the Adobe Helper add-on message bar displays at the bottom, click Enable.
7. When your browser is available, navigate to the Human Resources site by going to Departments > Human Resources on the global navigation.
8. Click Settings > Site Contents. Notice the New Site option is not available under the Subsite section for Irene even though you can still add an app.
9. Click **Settings > Site Settings** and notice how limited Irene is with managing the site.

10. Close the browser window with which Irene has been working.

**Exercise 5: Creating New SharePoint Objects with Unique Permissions**

The Human Resources team would like a secure document library to house files that should only be accessed by HR. Only those who are in the Human Resources department should be able to access the library.

1. Switch account to Jerome Clark. To do this, click the Windows icon in lower left of screen.

2. In the top left corner, click **Irene Ward** and choose **LEARNINGLAKE\JeromeC**.

3. Type the password **Passw0rd1** and then press **[Enter]**. (Your browser should still be open.)

4. On the global navigation, click **Departments > Human Resources** to navigate to the **Human Resources** site.

5. Click **Settings > Add an app**.

6. Click **Document Library**.

7. Type **SecureHRDocs** in the **Name** box for the new library.

   ![Reminder](image)

   Remember that the name of the library or list, given here, is used for the URL. You will create a title that is more user friendly in the next steps.

8. Click **Create**.

9. From the Quick Launch toolbar, click **SecureHRDocs**.

10. From the ribbon, click **Library > Library Settings** in the **Settings** group.

11. Under **General Settings**, click **List name, description and navigation**.
12. In the Name field, type **Secure HR Documents** and click Save.

13. From the Quick Launch toolbar, click **Secure HR Documents**.

14. From within the document library, click **Library > Shared With** from the **Settings** group on the ribbon. (Look for an icon with two people and a gold key.)

15. Click **Advanced**.

16. On the ribbon, click **Permissions > Stop Inheriting Permissions** from the **Inheritance** section to break the inheritance from the Learning Lake Human Resources site.

17. A SharePoint dialogue box will appear to remind you what is going to happen when stopping inheritance. Click **OK**.

18. Select everybody except for the following group: **Learning Lake Intranet Owners**.

19. Click **Permissions > Remove User Permissions** from the **Modify** section.

20. Click **OK** on the pop-up window.

21. Click **Permission > Grant Permission** from the **Grant** section.

22. Type individuals in the **Invite people** box. As you begin to type their name, a box will appear showing a list of matching names. Click the names as they appear in the box to add them to the invite box.
a. **Linus Evans**

b. **Ali Roth**

c. **Terry Vanderbilt**

23. Under **Show Options**, leave the **Select a permission level** set to **Edit**.

24. Click **Share** after the users have been added.

25. To ensure that nothing is left from the parent site, you need to remove the Learning Lake Intranet Owners group. To do this, select the **Learning Lake Intranet Owners** group.

26. On the ribbon, click **Permissions > Remove User Permissions** from the **Modify** group.

27. On the pop-up window, click **OK** (if applicable).

28. Click **Home** on the Quick Launch toolbar to navigate to the Human Resources site.

29. Click **Setting > Site Contents** and **Secure HR Documents** should be displayed.

![Secure HR Documents](image)

Next, you will see what happens when Irene Ward tries to access the Secure HR Documents.

30. Switch account to Irene Ward. To do this, click the Windows icon in lower left of screen.

31. In the top left corner, click **Jerome Clark** and choose **LEARNINGLAKE\IreneW**.

32. Type the password **Passw0rd1** and press **[Enter]**.

33. On the taskbar, click your browser.

34. Navigate to the Human Resources site.

Notice that the **Secure HR Documents** library does not appear on the Quick Launch toolbar.

35. In the address bar, type **http://intranet.learninglake.com/dept/hr/SecureHRDocs** and press **[Enter]**.

Irene should receive the **Sorry, this site hasn’t been shared with you** window.

36. Close the browser window with which Irene has been working.

37. Switch account to Jerome Clark. To do this, click the Windows icon in the lower left of screen.

38. In the top left corner, click **Irene Ward** and select **Sign out**.

39. In the **Virtual Machine Connection** window, click **Action > Ctrl+Alt+Delete**. (If you click anywhere on your screen instead, you should have the same effect.)

40. Click **Jerome Clark**.

41. Sign in with password **Passw0rd1** and press **[Enter]**.

https://skillpipe.com/#/reader/urn:uuid:9e691a33-42d3-4176-b322-412dee76a30f@2022-02-23T14:00:00Z/content
42. If your browser is not open on the taskbar, click your browser.