# AvePoint Perimeter Online

## User Guide

Issued June 2017

# Table of Contents


What's New in this Guide ..... 5

About AvePoint Perimeter Online ..... 6

- Site Collection Administrators ..... 6
- SharePoint Online Users ..... 7
- E-mail Users ..... 8

Integrating with AvePoint Online Services ..... 9

Site Collection Administrators ..... 10

- Managing User Settings in the AvePoint Perimeter Online Portal ..... 10
  - Role Management ..... 10
  - User and AD Group Management ..... 11
  - Managing File Sharing Groups ..... 12
- Configuring Secure Share Options in the AvePoint Perimeter Online Portal ..... 13
  - Configuring User Options ..... 13
  - Configuring File/Folder/Library Name Options ..... 14
  - Configuring File Type Options ..... 15
  - Configuring File Size Options ..... 16
  - Configuring File/Folder Attribute Options ..... 16
  - Configuring Country/Domain Options ..... 17
  - Configuring IP Address Options ..... 18
  - Configuring Classification Code Options ..... 18
- Managing E-mail Settings in the AvePoint Perimeter Online Portal ..... 19
  - Configuring SMTP Settings ..... 19
  - Managing E-mail Templates ..... 20
  - Creating an E-mail Template ..... 20
- License Management in AvePoint Perimeter Online Portal ..... 21
- Managing Security Settings in the AvePoint Perimeter Online Portal ..... 22
  - Configuring Encryption Deployment ..... 22
  - Managing a Security Profile ..... 22
  - Configuring Multi-Factor Authentication ..... 24

Customizing the Look and Feel in the AvePoint Perimeter Online Portal ..... 24
Viewing the Dashboard in the AvePoint Perimeter Online Portal ..... 24
Viewing Audit Records of All Shared Items ..... 25
Top 10 Secure Share Users ..... 25
Top 10 Most Accessed Items ..... 26
Top 10 External Visitors to Portal ..... 27
Top 10 Most Secure Shared Items ..... 28
Top 10 Recipient Domains ..... 29
Managing All Shared Files, Folders and Libraries in AvePoint Perimeter Online Portal ..... 30
Viewing All Shared Files, Folders, and Libraries ..... 30
Revoking Shared Files, Folders, or Libraries ..... 30
SharePoint Online Users ..... 32
Sharing Files, Folders or a library via the AvePoint Perimeter Online Secure Share Feature ..... 32
Logging into the AvePoint Perimeter Online Portal ..... 34
Viewing the Users with Whom You Shared Files, Folders or Libraries in SharePoint Online Sites ..... 35
Viewing the Dashboard in the AvePoint Perimeter Online Portal ..... 35
Recipients of My Shares ..... 36
My Shared Items ..... 37
Senders Who Shared With Me ..... 38
Items Shared With Me ..... 39
Managing My Shared Files, Folders, and Libraries in the AvePoint Perimeter Online Portal ..... 40
Viewing My Shared Files, Folders, or Libraries ..... 40
Editing My Shared Files ..... 40
Uploading a File ..... 41
Stopping Sharing of My Shared Files, Folders, or Libraries ..... 42
Managing the Files, Folders, and Libraries that have been Shared With You in the Perimeter Online Portal ..... 42
Viewing the Files or Folders that have been Shared with You ..... 42
Editing Files that have been Shared with You ..... 42
Uploading a File ..... 43
E-mail Users ..... 45
Registering an Account on the AvePoint Perimeter Online Portal ..... 45

Logging into the AvePoint Perimeter Online Portal ..... 46
Editing My Profile Settings..... 46
Resetting a Password in the AvePoint Perimeter Online Portal ..... 47
Viewing the Dashboard in the AvePoint Perimeter Online Portal ..... 48
Senders Who Shared With Me ..... 48
Items Shared With Me..... 49
Managing the Files, Folders, and Libraries that have been Shared with You in the Perimeter Online Portal..... 49
Viewing the Files, Folders and Libraries Shared with You ..... 50
Editing the Files Shared with You..... 50
Uploading a File..... 50
Using Message Center in the AvePoint Perimeter Online Portal..... 52
Notices and Copyright Information ..... 53

# What's New in this Guide

- Updated the User and AD Group Management section.
- Updated the Configuring Secure Share Options in the AvePoint Perimeter Online Portal section and added the Configuring Classification Code Options section.
- Updated the Logging into the AvePoint Perimeter Online Portal section.

# About AvePoint Perimeter Online

The AvePoint Perimeter Online add-in to SharePoint Online allows users to securely share files, folders, and libraries with other SharePoint Online users and e-mail users and enables users to view the history of files, folders and libraries that have been shared with others. The content of files, folders, or libraries shared via AvePoint Perimeter Online Secure Share feature can be viewed, downloaded, edited, or uploaded by the users with corresponding permissions.

SharePoint Online site collection administrators can log into the AvePoint Perimeter Online Portal to configure the settings in the **Settings** page, and view and manage all shared files, folders, and libraries. They can also view an overview of shared times, access times, and share times of the shared files within a certain period in the dashboard page. SharePoint Online users can go to the AvePoint Perimeter Online Portal to view and manage the files, folders, or libraries shared by them or shared with them. E-mail users with whom the files, folders, or libraries are shared can view, download, edit, or upload copies of the shared files or the files in shared folders, and libraries via the AvePoint Perimeter Online Portal. After logging into the AvePoint Perimeter Online Portal, all users can view their own user roles through **My Profile** and view an overview for what someone in this role can do.

AvePoint Perimeter Online is integrated with AvePoint Online Services. Users can access AvePoint Perimeter Online from the AvePoint Online Services page. For details, refer to Integrating with AvePoint Online Services.

## Site Collection Administrators

As a SharePoint Online site collection administrator, you can configure the settings of Secure Share in the AvePoint Perimeter Online Portal before users within the same tenant use the add-in. You can view the dashboard in Administrator View to get an overview on the rankings of the users who share items most, the items accessed most, the external users that access the Perimeter Online Portal most, the items shared most, and the domains of the recipients who were shared with most within a certain period.

***Note**: Site collection administrators can perform all of the same functions that SharePoint Online users can perform. For details, refer to SharePoint Online Users.

- Assign roles with different permissions to AD groups or SharePoint Online users within the same tenant, and create or manage **File Sharing Groups** to define the user groups with whom the files, folders, or libraries can be shared. For details, refer to Managing User Settings in the AvePoint Perimeter Online Portal.
- Configure the user filter, file name filter, file type filter, file size filter, country/domain filter, IP address filter, and classification code filter for sharing files and folders. For details, refer to Configuring Secure Share Options in the AvePoint Perimeter Online Portal.

- Configure the SMTP settings and e-mail templates. For details, refer to Managing E-mail Settings in the AvePoint Perimeter Online Portal.
- Control the usage of **AvePoint Perimeter Online** through assigning user seats to specific users. For details, refer to License Management in AvePoint Perimeter Online Portal.
- Configure the security settings to protect the shared content through **Azure Key Vault** encryption or the **Built-in Encryption**. For details, refer to Managing Security Settings in the AvePoint Perimeter Online Portal.
- Change the logo and the color for the **Perimeter Online Portal**. For details, refer to Customizing the Look and Feel in the AvePoint Perimeter Online Portal.
- Get an overview for the rankings of the users sharing items most, the items being shared most, the shared items being accessed most, the external users accessing the Perimeter Online Portal most, and the domains of the recipients being shared with most within a certain period. For details, refer to Viewing the Dashboard in the AvePoint Perimeter Online Portal.
- View, download, edit, upload, or revoke all of the files, or the files in folders or libraries shared via **AvePoint Perimeter Online Secure Share** feature within the managed site collections. For details, refer to Managing All Shared Files, Folders and Libraries in AvePoint Perimeter Online Portal.

## SharePoint Online Users

As a SharePoint Online user, you can share files, folders, or libraries and view the **Secure Shared With** information through the **AvePoint Perimeter Online Secure Share** feature on the SharePoint Online site collection. For details, refer to the introductions below:

- Share files, folders or libraries via **Perimeter Online Secure Share** feature in a SharePoint Online site. For details, refer to Sharing Files, Folders or a library via the AvePoint Perimeter Online Secure Share Feature.
- SharePoint Online users can log into the AvePoint Perimeter Online Portal for the first time by completing the following steps:
    i. Open the link to the shared content in the **AvePoint Perimeter Online Secure Share Notification** e-mail. The **Sign in** page for the AvePoint Perimeter Online Portal appears.
    ii. Log into the AvePoint Perimeter Online Portal with your Office 365 account.
    iii. Click **Sign in** to access the AvePoint Perimeter Online Portal.

    SharePoint Online users can also log into the AvePoint Perimeter Online Portal from the AvePoint Online Services page with an existing Office 365 account. For details, refer to the **Signing in with an Office 365 Account** section in the AvePoint Online Services User Guide.

- Check the users with whom the specific file, folder, or library is shared. For details, refer to Viewing the Users with Whom You Shared Files, Folders or Libraries in SharePoint Online Sites.

You can also view the dashboard and manage the files, folders, and libraries shared by or with you through the **AvePoint Perimeter Online Portal**. For details, refer to the introductions below:

- Get an overview on the rankings of recipients in your sharing, the items shared by you, the senders who shared items with you, and items shared with you within a certain period. For details, refer to Viewing the Dashboard in the AvePoint Perimeter Online Portal.
- View, download, edit, upload, or stop sharing the corresponding files, or the files in folders and libraries shared by you. For details, refer to Managing My Shared Files, Folders, and Libraries in the AvePoint Perimeter Online Portal.
- View or download the corresponding files, or files in folders and libraries that others have shared with you. For details, refer to Managing the Files, Folders, and Libraries that have been Shared With You in the Perimeter Online Portal.

## E-mail Users

As an e-mail user, you will receive an e-mail notification when anyone shares files, folders, or libraries with you via the **AvePoint Perimeter Online Secure Share** feature by selecting the **Send e-mail notifications to the users above** option. By clicking the link in the e-mail notification, you are directly led to the shared content that allows anonymous access or you may be required to log into the AvePoint Perimeter Online Portal before viewing the shared files, folders, and libraries.

You can perform the following actions:

- To register a new **Perimeter Online Portal** account, refer to Registering an Account on the AvePoint Perimeter Online Portal.
- To log into **Perimeter Online Portal**, refer to Logging into the AvePoint Perimeter Online Portal.
- To reset a password for a Perimeter Online Portal account, refer to Editing My Profile Settings or Resetting a Password in the AvePoint Perimeter Online Portal.
- Get an overview on the rankings of the senders who share items with you, and the items shared with you within a certain period. For details, refer to Viewing the Dashboard in the AvePoint Perimeter Online Portal.
- View and manage the sharing records of files, folders and libraries shared with you. For details, refer to Managing the Files, Folders, and Libraries that have been Shared with You in the Perimeter Online Portal.

# Integrating with AvePoint Online Services

AvePoint Perimeter Online is integrated with AvePoint Online Services. To access Ave Point Perimeter Online from the AvePoint Online Services page, you must sign in with an existing Office 365 account. For details, refer to the **Signing in with an Office 365 Account** section in the AvePoint Online Services User Guide.

# Site Collection Administrators

## Managing User Settings in the AvePoint Perimeter Online Portal

In the AvePoint Perimeter Online Portal, SharePoint Online site collection administrators and the SharePoint Online users who have the corresponding permissions can manage user roles and assign roles with different permissions to different users within the same tenant. They can also configure file sharing groups to share files, folders and libraries to the users in groups.

### Role Management

The **Role Management** page is used for managing user roles. By default, the **Administrator**, **Auditor**, **Business Manager**, **Quick Share User**, and **Collaborator** roles are created automatically, and they cannot be edited or deleted.

***Note**: External users that are outside of your organization will be automatically assigned an **External Collaborator** role and this role is not listed in **Role Management** page.

To access **Role Management**, open the **Settings** page, and click **Role Management** in the **User Settings** section. In the **Role Management** list, you can view the **Role Name** and **Description** for each role, and you can perform the following actions in the **Role Management** page:

- **Search** – Enter keywords of **Role Name** in the **Search** text box on the upper-right corner of the page, and press Enter on the keyboard to search.
- **Create** – Click **Create** in the command bar to create a new role. For details, refer to the Creating Roles section.
- **View** – Select a **Role Name** and click **View** on the command bar to access **View Details of the Role** page. The **Role Name**, **Description**, and **Permissions** of the selected role are displayed. You can view the information of all created roles.
- **Edit** – Select a **Role Name** and click **Edit** on the command bar. You can edit the **Role Name**, **Description**, and **Permissions** of the selected role**.**
- **Delete** – Select one or more **Role Names** and click **Delete** on the command bar. The selected roles will be deleted.

#### Creating Roles

To create new roles with the customized permissions of SharePoint Online users in **Role Management**, complete the following steps:

1. Navigate to **Settings** > **Role Management**. Click **Create** in the command bar.
2. **Role Name** – Enter a role name in the text box.
3. **Description** – Enter an optional description for the role.

4. **Permissions** – Customize the permissions for the role you are about to create by selecting permissions under the following tabs:

    - **Secure Share in SharePoint** – Configure the permissions of SharePoint Online users for using Secure Share features in SharePoint Online site. Select the options to grant permissions to SharePoint Online users in SharePoint Online site.
    - **Dashboard** – Configure the permissions of SharePoint Online users for viewing and exporting the content of the reports in dashboard. Select the options to grant permissions to SharePoint Online users in **Sharer/Collaborator View** and **Administrator View** of **Dashboard** page.
    - **Secure Share Files** – Configure the permissions of SharePoint Online users for managing the items shared by them and the items shared by others in **Secure Share Files** page. Select the options to grant permissions to SharePoint Online users in **My Shared Files**, **Files Shared with Me**, and **All Shared Files** tabs in **Secure Share Files** page. By default, all options of **My Shared Files** and **Files Shared with Me** tabs are selected, and they cannot be deselected.
    - **Settings** – Configure the permissions of SharePoint Online users for configuring **User Settings**, **Secure Share Settings**, **E-mail Settings**, **License Settings**, **Security Settings**, and **Personalization Settings** in **Settings** page. Select the options to grant permissions to SharePoint Online users in **User Settings**, **Secure Share Settings**, **E-mail Settings**, **License Settings**, **Security Settings**, and **Personalization Settings** of **Settings** page.

5. Click **Save** to save the role configurations, or click **Cancel** to return to the **Settings** page without saving any changes.

## User and AD Group Management

The **User/AD Group Management** interface is used for assigning roles with different permissions to different users or AD groups within the same tenant.

***Note**: The first SharePoint Online user who accesses the Perimeter Online Portal will be assigned the **Administrator** role automatically.

In the Perimeter Online Portal, go to the **Settings** page. Click **User/AD Group Management** in the **User Settings** section, and then the **Settings** > **User/AD Group Management** page appears. In the **User/AD Group Management** list, you can see the **Username/AD Group Name**, **E-mail Address**, **Description**, and **Role** fields for each user and AD group. You can perform the following actions in the **User/AD Group Management** interface:

- **Search** – Enter keywords of **Username/AD Group Name** or **E-mail Address** in the **Search** text box on the upper-right corner of the page, and press Enter on the keyboard to search for a user or an AD group who has been assigned a role.
- **Add** – Click **Add** on the command bar to add the users or AD groups to Perimeter Online Portal with roles assigned. For details, refer the Assigning Roles to AD Groups or SharePoint Online Users within the Same Tenant.

- **View** – Select a record and then click **View** on the command bar, or click the username or AD group name to access **View Details** page. You can view the type of the record, the roles assigned to the user or AD group, and the permission details. Additionally, you can click Edit on the bottom of the **View Details** page to edit the user or AD group.
- **Edit** – Select a record and click **Edit** on the command bar. You can edit the roles assigned to the user or AD group, and select whether or not to send e-mail notifications to administrators and this user or AD group to update about the changes. For details, refer to Assigning Roles to AD Groups or SharePoint Online Users within the Same Tenant.
- **Delete** – Select one or more records and click **Delete** on the command bar. The selected records will be deleted.

### Assigning Roles to AD Groups or SharePoint Online Users within the Same Tenant

To assign roles to users or AD groups within the same tenant, you can add a record in the **User/AD Group Management** interface. Complete the following steps to add a record:

1. Navigate to **Settings** > **User Management**. Click **Add** in the command bar.
2. **Username/AD Group Name** – Enter the usernames or e-mail addresses of the SharePoint Online users and AD groups to whom you are about to assign a role. When entering the usernames or e-mail addresses, Perimeter Online will search the SharePoint Online Active Directory for user's profiles with the entered characters, and provide the search results in the drop-down menu below the **Username/AD Group Name** text box.
3. **Description** – Enter an optional description for the user.
4. **Role** – Select at least one role to be assigned from the drop-down list, and the permissions of the selected roles are listed below in the **Permission Details** section.
5. **Send e-mail notifications to administrators and the users above** – Select whether or not to send an e-mail notifications to all of the administrators and the users or AD groups you entered above to inform them of the role that is assigned to the users.
6. Click **Save** to save the configurations or click **Cancel** to return to the **Settings** page without saving any changes.

***Note**: By default, the SharePoint Online users who are not added in the **User/AD Group Management** interface will be in the **Quick Share User** role.

## Managing File Sharing Groups

The **File Sharing Group** is a group of users with whom files, folders, and libraries are shared. When SharePoint Online users share files, folders, and libraries via **Perimeter Online Secure Share** feature, they can select the user groups that are configured in Perimeter Online Portal instead of selecting a large number of users.

In the Perimeter Online Portal, go to the **Settings** page. Click **File Sharing Groups** in the **User Settings** section, and the **Settings** > **File Sharing Groups** page appears. In the **File Sharing Groups** list, you can see the **Name**, **Description**, and **Number of User** fields for each group. You can perform the following actions on the **File Sharing Groups** interface:

- **Search** – Enter keywords of **Name** in the **Search** text box on the upper-right corner of the page, and press Enter on the keyboard to search a **File Sharing Group**.
- **Create** – Click **Create** on the command bar to create a new **File Sharing Group**. For the details, refer the Creating a File Sharing Group.
- **View** – Select a **File Sharing Group** and click **View** on the command bar to access **View the Shared With Group** page. The **Name**, **Description**, and **Users** of the selected **File Sharing Group** are displayed. You can view the information of a **File Sharing Group**.
- **Edit** – Select a **File Sharing Group** and click **Edit** on the command bar. **Name**, **Description**, and **Users** of the selected **File Sharing Groups** are displayed. You can edit the **File Sharing Group** settings.
- **Delete** – Select one or more **File Sharing Groups** and click **Delete** on the command bar. The selected **File Sharing Groups** will be deleted.

### Creating a File Sharing Group

To share files, folders, or libraries with a group you can create a **File Sharing Group**. Complete the following steps to create a **File Sharing Group**:

1. Navigate to **Settings** > **File Sharing Groups**. Click **Create** in the command bar.
2. **Name** – Enter a name for the group you are about to create.
3. **Description** – Enter an optional description for the group.
4. **Users** – Enter the e-mail addresses of the users you want to add. When entering the e-mail address of SharePoint Online users, Perimeter Online will search the SharePoint Online Active Directory for user's profiles with the entered characters, and provide the search result in the drop-down menu below the **Users** text box. You can also enter the e-mail users' e-mail addresses ending with a semicolon.
5. Click **Save** to save the group configurations or click **Cancel** to return to the **Settings** page without saving any changes.

# Configuring Secure Share Options in the AvePoint Perimeter Online Portal

In the AvePoint Perimeter Online Portal, SharePoint Online site collection administrators can configure the user filter, file name filter, file type filter, file size filter, country/domain filter, and IP address filter for sharing files and folders with users and groups via the **Perimeter Online Secure Share** feature.

***Note**: The Secure Share Options will also be checked when users view, download, edit, or upload the shared files or folders.

## Configuring User Options

To define the users who can share files, folders, and libraries with others using Secure Share, you can configure the **Blacklist** or **Whitelist** filter. Complete the following steps to configure the filters:

1. Navigate to **Settings** > **Secure Share Options**. Click **User Options** in the quick launch bar.
2. **Enable user filter** – Choose whether or not to enable the user filter. With this option selected, the **Blacklist** or **Whitelist** settings appear.
    - **Blacklist** – Select **Blacklist**, if you want to exclude the listed users from sharing files, folders, or libraries with others via the Secure Share feature.
    - **Whitelist** – Select **Whitelist**, if you want to allow the users from the list to share files, folders, or libraries with others via the Secure Share feature.

      ***Note**: The **Blacklist** and **Whitelist** cannot be enabled at the same time, and the settings of **Blacklist** or **Whitelist** will not be cleared when they are switched from each other. If the **Enable user filter** option is deselected, the user filter will be disabled.
3. **Add users to the selected list** –Adding users to the selected list by one of the methods listed below:
    - **Add users manually** – When you select this option, you must manually enter the names of users or Active Directory groups you want to add. When entering the name, **AvePoint Perimeter Online** will search for the users or Active Directory groups in SharePoint user profiles or Azure Active Directory Application with the entered characters, and provide the search result in the drop-down menu below.

      ***Note**: To add Active Directory groups in the text box for configuring the User Options, you must click the link in the prompt message on the top of this page to grant permissions to Perimeter Online for obtaining the Azure Active Directory Application data.
    - **Upload user list** – When you select this option, you must upload a user list in **CSV** file that contains the e-mail addresses of the users you want to add. You can download a user list template by clicking the **Download the User List Template** option.

      ***Note**: You can only upload one user list at a time. The previous user list will be replaced by the newly uploaded one.
4. Click **Save** to save the user filter or click **Cancel** to return to the **Settings** page without saving any changes.

## Configuring File/Folder/Library Name Options

To define which files, folders, or libraries can be shared via the **AvePoint Perimeter Secure Share** feature, you can configure the **Blacklist** or **Whitelist** file name filter by completing the following steps:

1. Navigate to **Settings** > **Secure Share Options**. Click **File/Folder/Library Name Options** in the quick launch bar.
2. Select a site to apply file name options in the field above **Enable a file/folder/library filter**.

***Note**: This field only appears when you access the AvePoint Perimeter Online portal from AvePoint Online Services page, and all site collections are listed as long as you are the site collection administrator.

***Note**: You must select a site in which AvePoint Perimeter Online has been installed. Otherwise, the configured file name options will not take effect.

3. **Enable a file/folder/library name filter** – Choose whether or not to enable the file/folder/library name filter. With this option selected, the **Blacklist** or **Whitelist** settings appear.
    - **Blacklist** – Select **Blacklist**, if you want to exclude the listed files, folders, or libraries from being shared via the Secure Share.
    - **Whitelist** – Select **Whitelist**, if you want to share the files, folders, or libraries in the list via the Secure Share.

      ***Note**: The **Blacklist** and **Whitelist** cannot be enabled at the same time, and the settings of **Blacklist** or **Whitelist** will not be cleared when they are switched from each other. If the **Enable file/folder/library name filter** option is deselected, the file/folder/library name filter will be disabled.
4. **Add file/folder/library names to the list** – Enter the names of files, folders, or libraries that you want to add. When entering the file/folder/library name, **AvePoint Perimeter Online** will search for the files, folders, or libraries in the SharePoint online site collection with the entered characters, and provide the search result in the drop-down menu below.
5. Click **Save** to save the file/folder/library name filter or click **Cancel** to return to the **Settings** page without saving any changes.

## Configuring File Type Options

To define the file types that can be shared via the **AvePoint Perimeter Secure Share** feature, you can configure the **Blacklist** or **Whitelist** file type filter by completing the following steps:

1. Navigate to **Settings > Secure Share Options**. Click **File Type Options** in the quick launch bar.
2. **Enable file type filter** – Choose whether or not to enable the file type filter. With this option selected, the **Blacklist** or **Whitelist** settings appear.
    - **Blacklist** – Select **Blacklist**, if you want to exclude the listed file types from being shared via the Secure Share.
    - **Whitelist** – Select **Whitelist**, if you want to share files of the listed file types via the Secure Share.

      ***Note**: The **Blacklist** and **Whitelist** cannot be enabled at the same time, and the settings of **Blacklist** or **Whitelist** will not be cleared when they are switched from each other. If the **Enable file type filter** option is deselected, the file type filter will be disabled.
3. **Add file types to the selected list** – Enter the extension of the file type you want to add, and separate them with a semicolon.

4. Click **Save** to save the file type filters or click **Cancel** to return to the **Settings** page without saving any changes.

## Configuring File Size Options

To define the maximum file size for the specific file types that can be shared via the **AvePoint Perimeter Secure Share** feature, you can configure the file size filter by completing the following steps:

1. Navigate to **Settings** > **Secure Share Options**. Click **File Size Options** in the quick launch bar.
2. **Add a File Size Filter** – Click **Add a File Size Filter** under the configuration table to add a new row.
    - **File Type** – Enter the extension of the file type to define the maximum file size.
    - **Maximum Size** – With selecting **MB** as the unit, you can enter a number to a precision of one decimal place between 0 and 2047.9 as the maximum size; with selecting **KB** as the unit, you can enter a number between 0 and 1024 as the maximum size. The files in the corresponding file type whose file size exceeds the defined maximum size cannot be shared via Secure Share.
3. You can click **Clear All Fields** to clear all the file size filters that you added, and reconfigure the file size filters by clicking **Add a File Size Filter**.
4. Click **Save** to save the file size filters or click **Cancel** to return to the **Settings** page without saving any changes.

## Configuring File/Folder Attribute Options

To filter the files or folders that can be shared via the **AvePoint Perimeter Secure Share** feature by their attributes, complete the following steps:

1. Navigate to **Settings** > **Secure Share Options**. Click **File/Folder Attribute Options** in the quick launch bar.
2. **Enable file/folder attribute filter** – Choose whether or not to enable the file or folder attribute filter. With this option selected, the **Blacklist** or **Whitelist** settings appear.
    - **Blacklist** – Select **Blacklist**, if you want to exclude the files or folders with the listed attribute from being shared via the Secure Share.
    - **Whitelist** – Select **Whitelist**, if you want to share the files or folders with the listed attribute via the Secure Share.

      ***Note**: The **Blacklist** and **Whitelist** cannot be enabled at the same time, but the settings of **Blacklist** or **Whitelist** will not be cleared when they are switched from each other. If **Enable file/folder attribute filter** option is deselected, the file/folder attribute filter will be disabled.
3. **Add a File or Folder Attribute Filter** – Click **Add a File or Folder Attribute Filter** under the configuration table to add a new row.

- **File/Folder Attribute** – Select an attribute from the drop-down list.
- **Conditions** – Select Equal or Does Not Equals from the drop-down list.
- **Value** – Enter a value of file or folder's attribute to filter the files or folders which can or cannot be shared.

4. You can click **Clear All Fields** to clear all of the file or folder attribute filters, and then you can reset the file or folder attribute filters by clicking **Add a File or Folder Attribute Filter.**
5. Click **Save** to save the file or folder attribute filters, or click **Cancel** to return to the **Settings** page without saving any changes.

## Configuring Country/Domain Options

To define the users from which countries or domains the files, folders, or libraries can or cannot be shared with via the **AvePoint Perimeter Secure Share** feature, you can configure the country/domain filter by completing the following steps:

1. Navigate to **Settings** > **Secure Share Options**. Click **Country/Domain Options** in the quick launch bar.
2. **Enable country/domain filter** – Choose whether or not to enable the country or domain filter. With this option selected, the **Blacklist** or **Whitelist** settings appear.
   - **Blacklist** – Select **Blacklist**, if you want to exclude the users who are from the listed countries and domains from being shared with files, folders, or libraries via the Secure Share.
   - **Whitelist** – Select **Whitelist**, if you want to share files, folders, or libraries with the users who are from the listed countries and domains via the Secure Share.

     ***Note**: The **Blacklist** and **Whitelist** cannot be enabled at the same time, but the settings of **Blacklist** or **Whitelist** will not be cleared when they are switched from each other. If **Enable country/domain filter** option is deselected, the country/domain filter will be disabled.
3. **Add a Country or Domain Filter** – Click **Add a Country or Domain Filter** under the configuration table to add a new row.
   - **Type** – Select **Country** or **Domain** from the drop-down list.
   - **Name** – Select the country from this drop-down menu, or enter the domain name in this text box according to the type you selected.
4. You can click **Clear All Fields** to clear all of the country or domain filters, and then you can reset the country or domain filters by clicking **Add a Country or Domain Filter**.
5. Click **Save** to save the country or domain filters or click **Cancel** to return to the **Settings** page without saving any changes.

## Configuring IP Address Options

To define the IP addresses that can access the files, folders, or libraries shared via the **AvePoint Perimeter Secure Share** feature, you can configure the IP address filter by completing the following steps:

1. Navigate to **Settings** > **Secure Share Options**. Click **IP Address Options** in the quick launch bar.
2. Enable IP address filter – Choose whether or not to enable the IP address filter. With this option selected, the **Blacklist** or **Whitelist** settings appear.
    - **Blacklist** – Select **Blacklist**, if you do not want the servers whose IP addresses included in the list to access the shared files, folders, or libraries.
    - **Whitelist** – Select **Whitelist**, if you want the servers whose IP addresses included in the list to access the shared files, folders, or libraries.

      ***Note**: The **Blacklist** and **Whitelist** cannot be enabled at the same time, but the settings of **Blacklist** or **Whitelist** will not be cleared when they are switched from each other. If **Enable IP address filter** option is deselected, the IP address filter will be disabled.
3. **Add an IP Address Filter** – Click **Add an IP Address Filter** under the configuration table to add a new row.
    - **Starting IP Address** – Enter a starting IP address between 0.0.0.0 and 255.255.255.255 to configure the range of IP addresses.
    - **Ending IP Address** – Enter an ending IP address between 0.0.0.0 to 255.255.255.255 to configure the range of IP addresses.
4. You can click **Clear All Fields** to clear the filters, and then you can reconfigure the IP address filter by clicking **Add an IP Address Filter**.
5. Click **Save** to save the filters or click **Cancel** to return to the **Settings** page without saving any changes.

## Configuring Classification Code Options

If you have installed AvePoint Compliance Guardian 4.2.1 or later in your environment, you can integrate the Compliance Guardian with Perimeter Online Secure Share feature to control the files to be shared. You can configure the **Classification Code Options** to define the classification codes of the files for filtering the files that can be shared through **AvePoint Perimeter Secure Share** feature. The shared files will be scanned by AvePoint Compliance Guardian, and the files with the classification codes in blacklist or out of whitelist cannot be shared.

Complete the steps below to configure the **Classification Code Options**:

1. Navigate to **Settings** > **Secure Share Options**. Click **Classification Code Options** in the quick launch bar.

2. **Enable classification code filter** – Choose whether or not to enable the classification code filter. With this option selected, configure the following settings:

    - **AvePoint Compliance Guardian URL** – Enter the host URL of the AvePoint Compliance Guardian. The Compliance Guardian will be connected for scanning the shared files. Click **Validation Test** to test the connection.
    - **Blacklist** – Select **Blacklist**, if you do not want the files whose classification codes are included in the list to be shared.
    - **Whitelist** – Select **Whitelist**, if you want to allow the files whose classification codes are included in the list to be shared.

      ***Note**: The **Blacklist** and **Whitelist** cannot be enabled at the same time, but the settings of **Blacklist** or **Whitelist** will not be cleared when they are switched from each other. If **Enable classification code filter** option is deselected, the classification code filter will be disabled.

3. Click **Add a Classification Code Filter** under the configuration table to add a new row, and then add the classification code into the text box. You can click the Delete ( ) button under the **Action** column to delete a filter, or you can click **Clear All Fields** to delete all of the filters, and then you can reconfigure the filter by clicking **Add an IP Address Filter**.
4. Click **Save** to save the filters or click **Cancel** to return to the **Settings** page without saving any changes.

# Managing E-mail Settings in the AvePoint Perimeter Online Portal

After the files, folders, or libraries are shared via Secure Share, **AvePoint Perimeter Online** sends an e-mail notification to the users that the files, folders, or libraries have been shared with. As a SharePoint Online site collection administrator, you must configure the customizable e-mail template in the SMTP settings.

## Configuring SMTP Settings

Complete the following steps to configure the SMTP Settings:

1. Navigate to **Settings** > **E-mail Settings** > **SMTP Settings** to access the **SMTP Settings** page.
2. **SMTP Server** – Enter the address of the SMTP e-mail server.

   ***Note**: Optionally, you can choose to use secure password authentication by selecting the **Use secure password authentication** option under the **SMTP Server** text box.

3. **Port** – Enter the port of the SMTP server. The default SMTP port is 443.
4. **Sender** – Enter the e-mail address that is used to send the e-mail notification.
5. **Username on SMTP** – Enter the sender's username on the SMTP server.
6. **Password on SMTP** – Enter the sender's password to log into the SMTP server.

7. **SSL authentication** – Select this option according to your SMTP server settings.
8. Click **Save** to save your configurations and the sender will receives the **SMTP Settings Test** e-mail, or click **Cancel** to exit the page without saving any configurations.

   ***Note**: If the configurations are successfully saved, the **SMTP Settings** are tested successfully; otherwise, you must check each configuration again.

## Managing E-mail Templates

In the **Settings** page, clicking **E-mail Templates** in the **E-mail Settings** section allows you to access the **Settings** > **E-mail Templates** page. In the **E-mail Templates** list, you will view the **Name**, **Description**, and **Type** of each e-mail template. You can perform the following actions:

- **Search** – Enter keywords of **Name** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.
- **Create** – Click **Create** in the command bar to create a new e-mail template. For details, refer to Creating an E-mail Template.
- **View** – Select an e-mail template and click **View** in the command bar to access the **Settings** > **E-mail Templates** > **View the E-mail Template** page. The **Name**, **Subject**, **Description**, **Type**, **Status**, and **E-mail Template** of the selected e-mail template are displayed. You can view the information of an e-mail template.
- **Edit** – Select an e-mail template and click **Edit** in the command bar. **Name**, **Subject**, **Description**, **Type**, **Status**, and **E-mail Template** of the selected e-mail template are displayed. You can edit the e-mail template settings. For details on configuring an e-mail template, refer to Creating an E-mail Template.
- **Delete** – Select one or more e-mail templates and click **Delete** in the command bar. The selected e-mail templates will be deleted.

## Creating an E-mail Template

Complete the steps below to create a new e-mail template:

1. Navigate to **Settings** > **E-mail Settings** > **E-mail Template**. Click **Create** in the command bar to access the **Create an E-mail Template** page.
2. **Name** – Enter a name for the e-mail template you are about to create.
3. **Subject** – Enter a subject for the e-mail template.
4. **Description** – Enter an optional description for the e-mail template.
5. **Type** – The type of the e-mail template is **For Secure Share**. This value cannot be changed.
6. **Status** – Select the **Enable this e-mail template** option to enable this e-mail template.

7. **Body** – You can customize the e-mail body in the text box below.

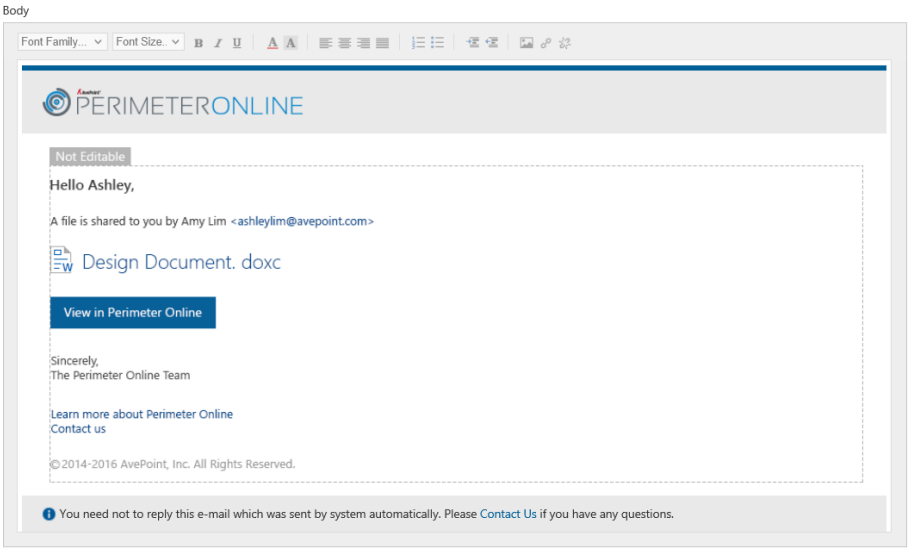


**Figure 1: The text box to customize an e-mail template.**

8. Click **Save** to save the e-mail template or click **Cancel** to exit the page without saving any configurations.

# License Management in AvePoint Perimeter Online Portal

SharePoint Online site collection administrators can control the usage of **AvePoint Perimeter Online** through assigning user seats of the license to specific users. Manage the license of **AvePoint Perimeter Online** by completing the following steps:

1. Navigate to **Settings** > **License Management**. In this page, you can see the following information of the license:
    - **License Type** – Displays the license type information.
        - **Trial** – The validity period is 30 days.
        - **Free** – The validity period is unlimited.
        - **Enterprise** – The validity period for this license depends upon the type of license purchased.
    - **Expiration Date** – Displays the license expiration date.
    - **User Seat Quantity** – Displays the remaining number and the total number of the available user seats of the license.
2. **User Seat Assignment** – If you want to automatically assign the user seats to the SharePoint Online users according to the time order using the Secure Share feature, deselect the **Assign user seats manually** option; otherwise, select this option and continue with the following settings to manually assign user seats.

3. Click **Add** in the command bar of **User List**. The **Add Users** window appears.
4. Enter the name of the user you want to add. AvePoint Perimeter Online will search for the users in the SharePoint user profiles with the entered characters, and provide the search result in the drop-down menu below. Select the desired result.
5. Click **Add** to add users in **User List** or click **Cancel** to close the pop-up window without adding any users.
6. Click **Save** to save your configurations, or click **Cancel** to return to the **Settings** page without saving the configurations. If you want to purchase additional user seats or extend the license, you can click the **Buy More** button on the upper-right corner of the page.

# Managing Security Settings in the AvePoint Perimeter Online Portal

The SharePoint Online site collection administrators can configure the security settings to protect the shared content through the **Azure Key Vault** encryption or the **Built-in Encryption**.

## Configuring Encryption Deployment

As a SharePoint Online site collection administrator, you can deploy the file level encryption using the custom security profile to enhance the security of sharing. Complete the following steps to enable file level encryption:

1. Navigate to **Settings** > **Encryption Deployment** to access the **Encryption Deployment** page.
2. Select the **Enable File Level Encryption** option. A drop-down menu to select a security profile appears.
3. Select a security profile from the **Select a Security Profile** drop-down menu. If you want to create a new security profile, you can select the **New Security Profile** option. For the details on creating a new security profile, refer to Creating a Security Profile. If you select the **Built-in Encryption**, the Master Encryption Key will be used for the file level encryption.
4. Click **Save** to save your configurations, or click **Cancel** to return to the **Settings** page without saving the configurations.

## Managing a Security Profile

Security Profile contains the encryption settings that can be used to protect your shared content.

In the Settings page, clicking **Security Profile** in the **Security Settings** section allows you to access the **Settings** > **Security Profile** page. In the Security Profile list, you can see **Name**, **Profile Type**, **Client ID**, **Key Name**, **Key Version**, and **Create Time** of each security profile. You can perform the following actions on security profile:

- **Search** – Enter keywords of **Profile Name** in the search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search. The security profiles whose names include the keywords will be shown in the security profile list.
- **Create** – Click **Create** in the command bar to create a security profile. For details, refer to Creating a Security Profile.
- **View** – Select a security profile and click **View** in the command bar to access the **Settings** > **Security Profile** > **View Security Profile** page. The **Name**, **Profile Type**, **Encryption Type**, **Client ID**, **Client Secret**, **Key Vault Name**, **Key Name**, **Version**, **Key Type**, and **Key Operation** of the selected security profile are displayed.
- **Edit** – Select a security profile and click **Edit** in the command bar. The **Name**, **Profile Type**, **Encryption Type**, **Client ID**, **Client Secret**, **Key Vault Name**, **Key Name**, **Version**, **Key Type**, and **Key Operation** of the selected security profile are displayed. You can edit the security profile settings. The **Profile Type**, **Encryption Type**, **Key Type**, and **Key Operation** fields cannot be edited. For details, refer to Creating a Security Profile.
- **Delete** – Select one or more security profiles and click **Delete** in the command bar. The selected security profiles will be deleted.
- **Show Rows** – To change the number of users displayed per page, select the desired number from the **Show Rows** drop-down menu on the lower-right corner.

## Creating a Security Profile

SharePoint Online site collection administrators can create a security profile to choose the encryption method for protecting shared files or folders. Complete the following steps to create a security profile:

1. Navigate to **Settings** > **Security Profile**. Click **Create** to create a security profile.
2. **Profile Name** – Enter a profile name. When configuring encryption options while creating scans, security profile names are listed for you to select.
3. **Profile Type** – The profile type is **File Level Encryption**. This value cannot be changed.
4. **Encryption Type** – The encryption type is **Azure Key Vault**. This value cannot be changed.
5. **Active Directory Application Client ID** – Enter the client ID.
6. **Active Directory Application Client Secret** – Enter the client secret.
7. **Key Vault Name** – Enter the key vault name.
8. **Key Name** – Enter the key name.
9. **Key Version** – You can select a version from the drop-down list, if you have entered the correct information for the settings above. The corresponding **Key Type** and **Key Operation** will be displayed under the selected **Version**.

   ***Note**: For the details of applying for an **Azure Key Vault**, refer to Get started with Azure Key Vault.
10. Click **Save** to save the security profile or click **Cancel** to return to the **Security Profile** page without saving the configurations.

### Configuring Multi-Factor Authentication

As a SharePoint Online site collection administrator, you can enable the multi-factor authentication function for further account verification when users log into Perimeter Online Portal via external links. Complete the following steps to enable the multi-factor authentication:

1. Navigate to **Settings** > **Multi-Factor Authentication** to access the **Multi-Factor Authentication** page.
2. Select the **Enable multi-factor authentication for login via external links** option.
3. With the **Enable multi-factor authentication for login via external links** option selected, the **Sending Authentication E-mail** option is automatically selected. When users log into Perimeter Online via external links, they will receive an authentication e-mail for further account verification via verification code.
4. Click **Save** to save your configurations, or click **Cancel** to return to the **Settings** page without saving the configurations.

## Customizing the Look and Feel in the AvePoint Perimeter Online Portal

SharePoint Online site collection administrators can change the look and feel of the AvePoint Perimeter Online Portal through completing the following steps:

1. Navigate to **Settings** > **Change Look and Feel** to access the **Change Look and Feel** page.
2. **Logo** – An optional setting for you to customize your Perimeter Online logo.
    - **Browse** – Click **Browse** to upload a picture to be the logo of **AvePoint Perimeter Online**.
    - **Reset** – Click **Reset**, the logo will revert back to the default picture.
3. **Color** – Click the color boxes in the color banner to select your desired color.
4. Click **Save** to save your configurations, or click **Cancel** to return to the **Settings** page without saving the configurations.

## Viewing the Dashboard in the AvePoint Perimeter Online Portal

In the **Dashboard** page, you can view the dashboard and change the views by clicking the following tabs on the command bar:

- **Sharer/Collaborator View** – This view of **Dashboard** is available to all of the SharePoint Online users. For details, refer to the Viewing the Dashboard in the AvePoint Perimeter Online Portal.
- **Administrator View** – This view of **Dashboard** is only available for SharePoint site collection administrators. In **Administrator View**, you can get an overview on the rankings of the users who share items most, the items accessed most, the external users

access the Perimeter Online Portal most, the items shared most, and the domains of the recipients who shared with most within a certain period. See the sections below for detailed instructions on viewing each ranking in the **Administrator View** of dashboard page. See the sections below for detailed instructions on viewing each ranking of the charts in the **Administrator View** of dashboard.

## Viewing Audit Records of All Shared Items

In the **Administrator View** of dashboard, you can view all audit records of the shared items by clicking the **View Audit Records** on the upper-right corner of the chart to access the **Dashboard** > **View Audit Records** page. You can perform the following actions in this page:

- **Search** – Enter keywords of **Username**, **E-mail Address**, or **Item Name** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to search.
- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Activity** – To customize the activities of the audit records that you want to view, select the activities from the **Activity** drop-down list.
- **Export** – Click **Export** on the upper-right corner of the table, you can export all searched audit records within a certain period into a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu on the lower-right corner of this page. You can view more audit records in each page.

## Top 10 Secure Share Users

The following chart displays the users ranked by the number of shared times within a certain period:

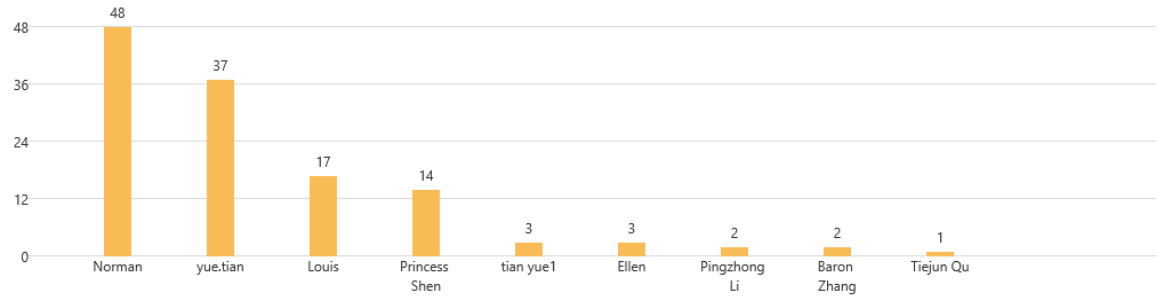


**Figure 2: The Top 10 Secure Share Users chart.**

By default, the chart can display the data for up to ten users. The Y-axis of the chart represents the number of shared times. The X-axis of the chart represents the name of users who shared files within a certain period. If desired, you can view all users who used secure share by clicking the **View All Users Who Secure Shared** on the upper-right corner of the chart to access the **Dashboard** > **View All Users Who Secure Shared** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all users who used to secure share within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu on the lower-right corner of this page. You can view more users on each page.
- **Search** – Enter keywords of **Username** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

## Top 10 Most Accessed Items

The following chart displays the shared files, folders, and libraries ranked by the number of accessed times within a certain period:

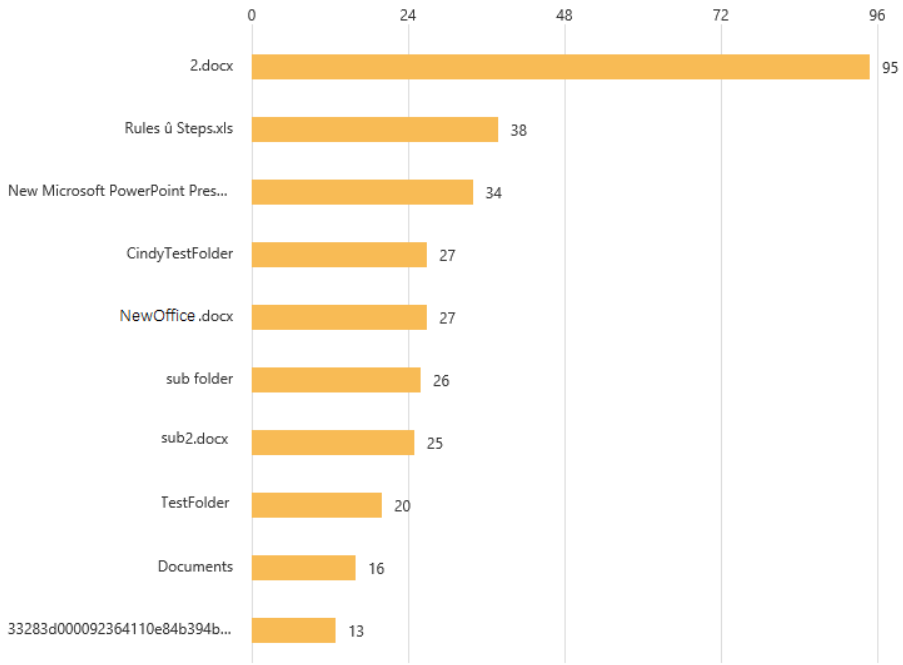


**Figure 3: The Top 10 Most Accessed Items chart.**

By default, the chart will display the data for up to ten shared items. The Y-axis of the chart represents the name of the shared items. The X-axis of the chart represents the number of accessed times within a certain period. If desired, you can view all shared items accessed by recipients by clicking the **View All Shared Items Accessed by Users** on the upper-right corner of the chart to access the **Dashboard** > **View All Shared Items Accessed by Recipients** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all shared items which used to be accessed within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more shared files, folders, and libraries on each page.
- **Search** – Enter keywords of **Item Name** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.
- **View Additional Details** – Click **View Additional Details** in each row, and the page of displaying the additional shared records' information of **Accessed Time**, **E-mail Address**, **IP Address**, and the **Location** of the corresponding shared file, folder or library appears. You can perform the following actions in this page:
    - **Export** – Click **Export** on the upper-right corner of this page, you can export the shared records' data of **Accessed Time**, **E-mail Address**, **IP Address**, and the **Location** of the corresponding shared file, folder or library within a certain period in a **CSV** file to a custom location.
    - **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more shared files, folders, and libraries on each page.
    - **Search** – Enter keywords of **Item Name**, **E-mail Address**, **IP Address** or **Location** in the **Search** text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

## Top 10 External Visitors to Portal

The following chart displays the external visitors ranked by the number of times of accessing Perimeter Online Portal within a certain period:

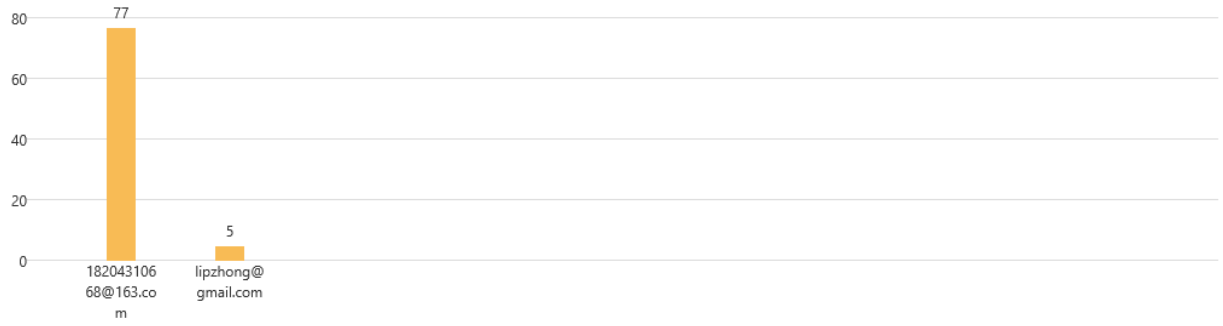


**Figure 4: The Top 10 External Visitors to Portal chart.**

By default, the chart will display the data for up to ten external users. The Y-axis of the chart represents the number of accessed times. The X-axis of the chart represents the name of external users who accessed the Perimeter Online Portal within a certain period. If desired, you can view all external users who accessed the Perimeter Online Portal by clicking the **View All External Users Who Accessed the Portal** on the upper-right corner of the chart to access the **Dashboard** > **View External Users Who Accessed the Portal** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all external users who accessed the Perimeter Online Portal within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more external users on each page.
- **Search** – Enter keywords of **E-mail Address** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

## Top 10 Most Secure Shared Items

The following chart displays the files, folders, and libraries ranked by the number of shared times within a certain period:

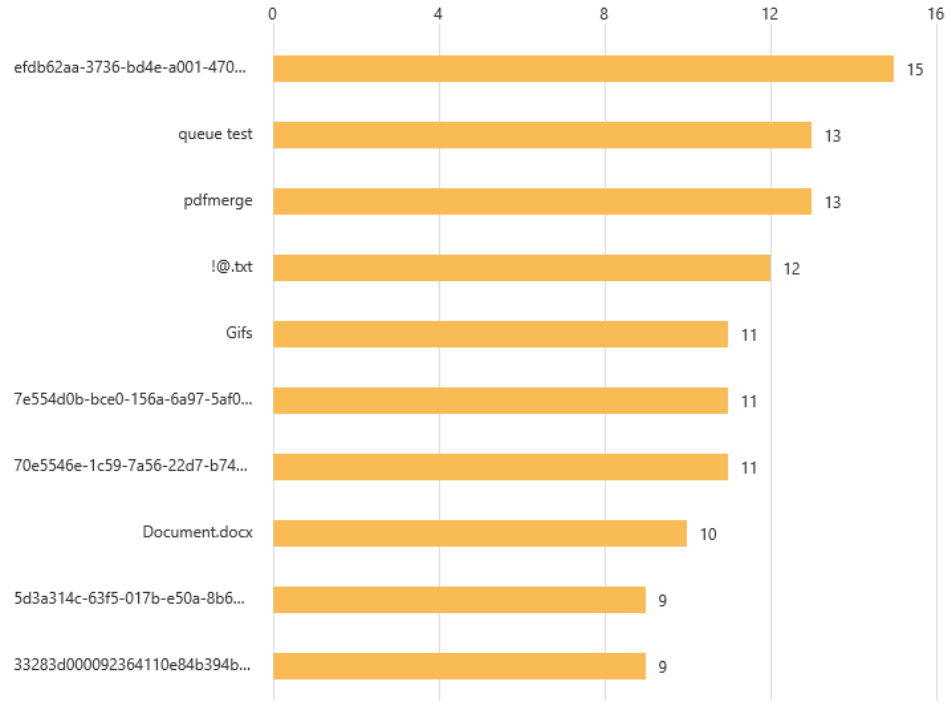


**Figure 5: The Top 10 Most Secure Shared Items chart.**

By default, the chart can display the data for up to ten shared items. The Y-axis of the chart represents the name of shared items. The X-axis of the chart represents the number of shared times within a certain period. If desired, you can view all shared items by clicking the **View All Secure Shared Items** on the upper-right corner of the chart to access the **Dashboard** > **View All Secure Shared Items** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all shared items within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more shared files, folders, and libraries on each page.
- **Search** – Enter keywords of **Item Name** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

## Top 10 Recipient Domains

The following chart displays the recipients' domains ranked by the number of times of receiving shared items within a certain period:


**Figure 6: The Top 10 Recipient Domains chart.**

By default, the chart can display the data for up to ten recipient domains. The Y-axis of the chart represents the times of receiving shared items. The X-axis of the chart represents the name of recipients' domains within a certain period. If desired, you can view all recipients' domains by clicking the **View All Recipient Domains** on the upper-right corner of the chart to access the **Dashboard** > **View All Recipient Domains** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all recipients' domains within a certain period in a **CSV** file to a custom location.

- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more recipients' domains on each page.
- **Search** – Enter keywords of **Domain** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

# Managing All Shared Files, Folders and Libraries in AvePoint Perimeter Online Portal

SharePoint Online site collection administrators can view the sharing records' information of all shared items and revoke all of the files, or files in folders, and libraries shared via the **AvePoint Perimeter Online Secure Share** feature.

In the **Secure Share Files** page, clicking **All Shared Files** in the quick launch bar allows you to access the **Secure Share Files** > **All Shared Files** page.

## Viewing All Shared Files, Folders, and Libraries

In the **All Shared Files** page, you can only view detailed information of all sharing records' information of shared files, folders, and libraries in **All Shared Files** list. Complete the steps below:

***Note**: The SharePoint Online site collection administrators cannot view the content of all shared items. They cannot download or upload items in this page as well.

1. Navigate to **Secure Share Files** > **All Shared Files**, or the shared folder or library where the file resides.
2. Click the setting ( ) button in the same row with the shared item to view its detailed information, and a drop-down list appears.
3. Select **View Share Details** option from the drop-down list, and then you can view the detailed information of **Item Name**, **File Size**, **Version**, **File Path**, and the **Share Details** of the corresponding shared item. In the **Share Details** table, all sharing records of this shared item are listed. You can select one or more sharing records, and click **Delete** on the command bar to delete them.

   ***Note**: When the sharing records are deleted, this shared item in corresponding sharing records is revoked at the same time.

## Revoking Shared Files, Folders, or Libraries

SharePoint Online site collection administrators can revoke all of the sharing records of each shared file, folder or library in the **All Shared Files** page. Refer to the following steps to revoke sharing:

1. Navigate to **Secure Shared Files** > **All Shared Files**. The **All Shared Files** list appears.

2. Search the desired files, folders, or libraries by entering keywords of the **Item Name** in the **Search** text box on the upper-right corner of the **All Shared Files** page, and then press Enter on the keyboard to perform the search.
3. Select one or more desired files, folders, or libraries in the search results.
4. Click **Revoke** on the command bar. The sharing of the selected shared files, folders, and libraries will be revoked. The sharing records of the selected files, folders and libraries will not be deleted.

   ***Note**: When the sharing of a folder is revoked, the sharing events of each file within this folder will not be impacted.

After the sharing of the files, folders, or libraries is revoked, both the users who shared them and the users who they have been shared with will receive a message that the files, folders, or libraries have been revoked in the Message Center. For detailed instructions on the Message Center, refer to Using Message Center in the AvePoint Perimeter Online Portal.

# SharePoint Online Users

## Sharing Files, Folders or a library via the AvePoint Perimeter Online Secure Share Feature

To share files, folders, or a library through the **AvePoint Perimeter Online Secure Share** feature in a SharePoint Online site, complete the steps below:

1. Navigate to the library you want to share, or the library containing the files or folders you want to share.
2. If you share a file or folder, select one or more files or folders and then click **Secure Share** on the ribbon of the **FILES** tab, or click ··· to select the **Secure Share** from the drop-down list; If you share a library, click **Secure Share** on the ribbon of the **FILES** tab without selecting any file or folder, or you can also click **Secure Share** on the ribbon of the **LIBRARY** tab.
3. The **Secure Share** pop-up window appears. Complete the settings below in the **Secure Share** window:
4. **Enter users** – To share files, folders, or a library with other users, enter their e-mail addresses or shared groups' names in the text box, and select the search result in the drop-down menu below this text box. You can also enter or copy valid e-mail addresses.
5. Select a permission for the selected users from the drop-down list under the **Enter users** text box. For detailed permissions on each permission level, you can click the **Do you have questions about permission assignment?** link under the drop-down list, and the permission table appears.

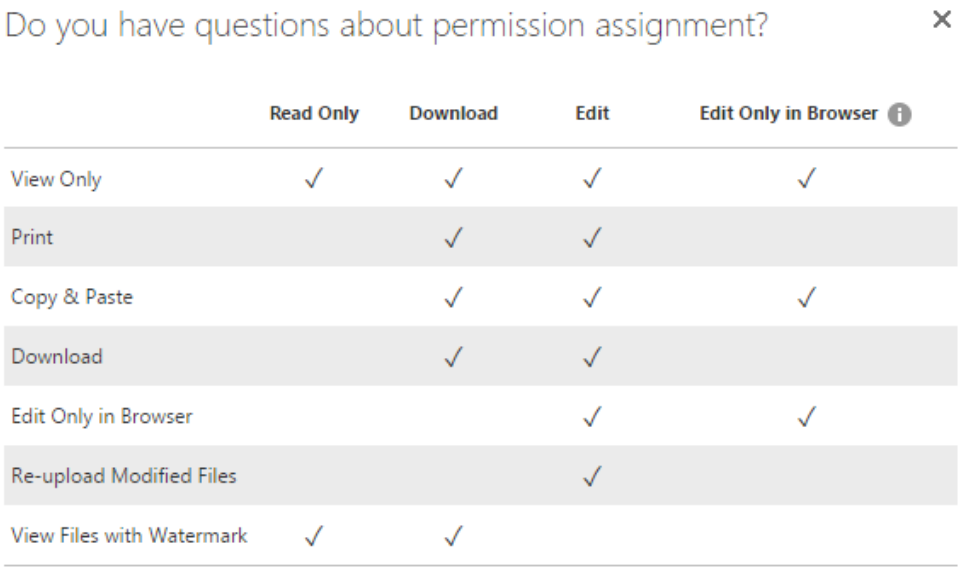


**Figure 7: The permissions table.**

- **Read Only** – Select the **Read Only** permission so that the selected users can only view the shared files, folders, and libraries.
- **Download** – Select the **Download** permission to allow the selected users to view, download and print a copy of the shared files, folders, and libraries.
- **Edit** – Select the **Edit** permission to allow the selected users to view, download, edit on local device, upload a new file to a shared folder or library, and upload a copy of a modified file to a shared file or library. If the selected users are Office 365 users, they can also directly edit or print the shared files in browser.
- **Edit Only in Browser** – Select the **Edit Only in Browser** permission to allow the selected Office 365 users to view and edit the shared files in an internet browser. This permission supports only the following file types: .pptx, .xlsx, and .docx.

***Note**: SharePoint Online site will record the revision history of the shared with users that have edited the shared files by logging into Perimeter Online Portal in the **Modified By (AvePoint Perimeter)** column.

6. **Send e-mail notifications to the users above** – Select whether or not to send an e-mail notification to the users you are sharing the files, folders, or library with. By default, this option is selected.

   ***Note**: Optionally, you can enter a custom message within the e-mail notifications in the text box. The entered message will be displayed before the pre-defined message in the e-mail notifications.

7. **Require sign in** – If the **Require sign in** option is selected, the selected users must log into the AvePoint Perimeter Online Portal to view, download or edit shared files, folders or libraries, or upload files to a shared folder or library. If the **Require sign in** option is deselected, you will grant the e-mail users anonymous access to the shared files, folders, or libraries. This means anyone that has the link in the Secure Share e-mail can view, download, edit, or upload the shared files.

   ***Note**: When the permission of **Edit** or **Edit Only in Browser** is selected, the **Require sign in** option is selected by default.

8. **Enable watermark** – Add a watermark in the shared files, folders, or library to protect their copyrights by checking the **Enable watermark** option. You can customize the content of the watermark by entering the watermark text in the text box. You can also select the font and size for the watermark text.

   ***Note**: If you add a watermark to a folder or library, the watermark will appear in every file within this folder or library.

9. **Date range settings** – Select an expiration time from the calendar for how long you would like to share the files, folders, or library with these users. You can set expiration date only or set start and expiration dates. If you want this sharing to never expire, deselect this option.

   ***Note**: The links for accessing expired sharing items are unavailable in AvePoint Perimeter Online Portal.

10. **Notify all collaborators if the file is updated** – With this option selected, an e-mail notification will be sent to all collaborators with whom this file is currently shared once anyone updates this file.
11. **Notify me if the file is downloaded by anyone** – With this option selected, you will receive an e-mail notification once this file is downloaded by anyone else.
12. Click **Share** to share files, folders, or a library. If the **Send e-mail notifications to the users above** option is selected, and your Office 365 Mail application is not available, a prompt message will appear asking for whether or not to send the e-mail notifications via your e-mail account. If you want to send the e-mail notifications via your e-mail account, click **Learn More** to view the details of this message, and get Office 365 Mail application service token by clicking the corresponding link in the message. If you do not have an Office 365 Mail account or do not want to send e-mail notifications via your e-mail account, you can click **Share** again, and the e-mail notifications will be sent from an administrator specified account or from perimeteronline@avepointonlineservices.com.

***Note**: The data of shared items will be temporarily stored in Azure BLOB storage for 7 days, and the data will be automatically deleted after 7 days.

***Note**: When this sharing event is going to expire, **AvePoint Perimeter Online** will send a message to the users with whom the files, folders, or library is shared to remind them to check the shared items on time. For detailed instructions on Message Center, refer to Using Message Center in the AvePoint Perimeter Online Portal.

## Logging into the AvePoint Perimeter Online Portal

SharePoint Online users can log into the AvePoint Perimeter Online Portal via the following four methods:

- In the SharePoint Online site where the AvePoint Perimeter Online is added, click **AvePoint Perimeter Online** on the quick launch pane to open the AvePoint Perimeter Online Portal. You will automatically log into the portal with your Office 365 account.
- In the SharePoint Online site where the AvePoint Perimeter Online is added, click **Manage Shared Files** on the ribbon of **Files** tab. The AvePoint Perimeter Online Portal will be opened and you will automatically log into the portal with your Office 365 account.
- Click the link of the shared content in the AvePoint Perimeter Online Secure Share notification e-mail. The **Sign In** page for the AvePoint Perimeter Online Portal appears. Log into the AvePoint Perimeter Online Portal with your Office 365 account.
- Since AvePoint Perimeter Online is integrated with AvePoint Online Services, SharePoint Online users can also log into the AvePoint Perimeter Online Portal from AvePoint Online Services page with an existing Office 365 account. For details, refer to the **Signing in with an Office 365 Account** section in AvePoint Online Services User Guide.

***Note**: If the user logged into the AvePoint Perimeter Online Portal from the SharePoint Online site or AvePoint Online Services interface, the user profile of this user in the AvePoint Perimeter Online Portal will display the picture of the user's Office 365 account.

## Viewing the Users with Whom You Shared Files, Folders or Libraries in SharePoint Online Sites

When you share a file, folder, or library through the **AvePoint Perimeter Online Secure Share** feature in a SharePoint Online site, you may want to check the users with whom you previously shared the specific file, folder or library. You can view the user list by completing the following steps:

1. Navigate to the library that contains the files or folders that you have shared with others.
2. To check the users with whom you used to share the specific file or folder, select the file or folder, and then click **Secure Shared With** on the ribbon of the **FILES** tab, or click ··· to select the **Secure Shared With** from the drop-down list; to check the users with whom you used to share the library, click **Secure Shared With** on the ribbon of the **FILES** tab without selecting any files or folders, or click **Secure Shared With** on the ribbon of the **LIBRARY** tab. The **Secure Shared With** pop-up window appears.

   ***Note**: When you select a file in a shared folder, and click **Secure Shared With** on the ribbon of the **FILES** tab, the records displayed in the **Secure Shared With** pop-up window are the users with whom you used to share the folder.
3. View the users with whom you shared this file, folder or library. You can click **Stop Sharing** in each row to stop sharing the selected file with the corresponding user. For more details on stopping sharing, refer to Stopping Sharing of My Shared Files, Folders.
4. Click **Close** to close the **Secure Shared With** pop-up window

## Viewing the Dashboard in the AvePoint Perimeter Online Portal

In the **Dashboard** page, you can get an overview on the rankings of recipients in your sharing, the items shared by you, the senders who shared items with you, and items shared with you within a certain period. See the sections below for detailed instructions on viewing each ranking in the charts of the dashboard.

## Recipients of My Shares

The following chart displays the recipients ranked by the number of your shares within a certain period:

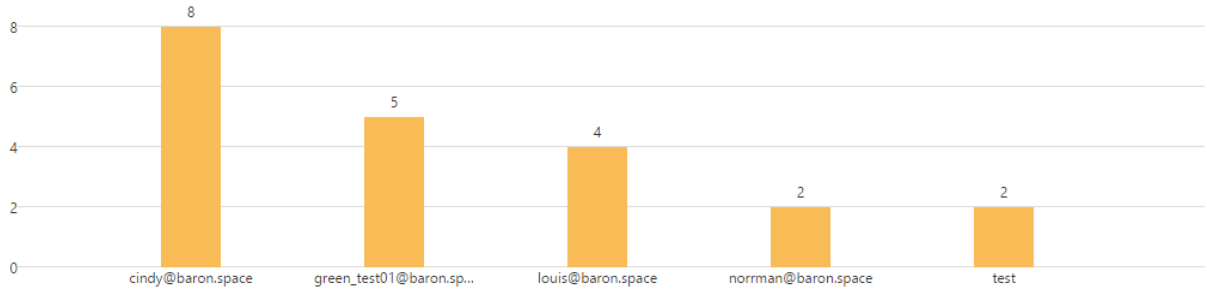


**Figure 8: The Recipients of My Shares chart.**

By default, the chart can display the data for up to five recipients. The Y-axis of the chart represents the number of my shares. The X-axis of the chart represents the number of my shares within a certain period. If desired, you can view all recipients of my shares by clicking the **View All Recipients of My Shares** on the upper-right corner of the chart to access the **Dashboard** > **View All Recipients of My Shares** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all recipients of my shares within a certain period in a **CSV** file to a custom location.
- **Show Rows** –Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more recipients with more details.
- **Search** – Enter keywords of **Recipient Name** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

## My Shared Items

The following chart displays your shared items ranked by the number of shared times within a certain period:

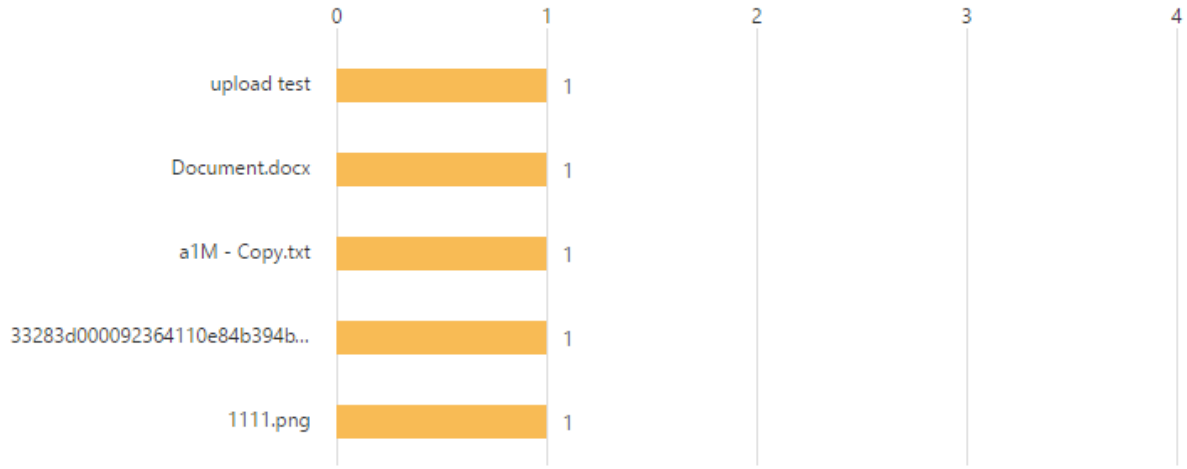


**Figure 9: The My Shared Items chart.**

By default, the chart can display the data for up to five shared items. The Y-axis of the chart represents the names of shared items. The X-axis of the chart represents the number of my shares within a certain period. If desired, you can view all your shared items within a certain period by clicking the **View All My Shared Items** on the upper-right corner of the chart to access the **Dashboard** > **View All My Shared Items** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all your shared items within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more shared files, folders, and libraries with more details.
- **Search** – Enter keywords of **Item Name** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

## Senders Who Shared With Me

The following chart displays the senders ranked by the number of times items have been shared with you within a certain period, as the screenshot below shows:

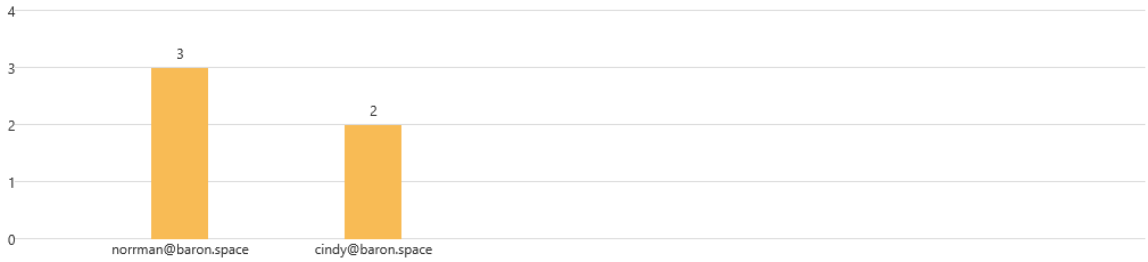


**Figure 10: The Senders Who Shared With Me chart.**

By default, the chart can display the data for up to five senders. The Y-axis of the chart represents the number of shared times of the items shared with you. The X-axis of the chart represents the name of senders who shared with you within a certain period. If desired, you can view all senders who shared with you by clicking the **View All Senders Who Shared With Me** on the upper-right corner of the chart to access the **Dashboard** > **View All Senders Who Shared With Me** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all senders who shared with you within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more senders with more details.
- **Search** – Enter keywords of **E-mail Address** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

## Items Shared With Me

The following chart displays the shared items ranked by the number of times of being shared with you within a certain period:

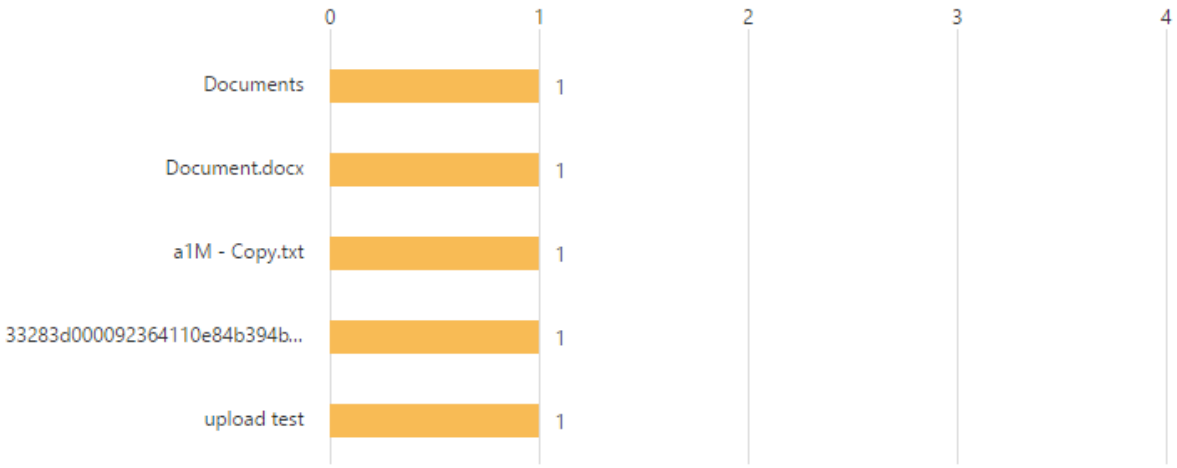


**Figure 11: The Items Shared With Me chart.**

By default, the chart can display the data for up to five shared items. The Y-axis of the chart represents the names of shared items. The X-axis of the chart represents the number of times of items shared with you within a certain period. If desired, you can view all items shared with you by clicking the **View All Items Shared With Me** on the upper-right corner of the chart to access the **Dashboard** > **View All Items Shared With Me** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all items shared with you within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more shared files, folders, and libraries with more details.
- **Search** – Enter keywords of **Item Name** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

# Managing My Shared Files, Folders, and Libraries in the AvePoint Perimeter Online Portal

As a SharePoint Online user, you can view, download, edit, upload, or stop sharing the corresponding files, or files in the folders and libraries that are shared by you via **AvePoint Perimeter Online Secure Share**.

In the **Secure Share Files** page, clicking **My Shared Files** in the quick launch bar allows you to access the **Secure Share Files** > **My Shared Files** page.

## Viewing My Shared Files, Folders, or Libraries

In the **My Shared Files** page, you can view detailed information of all your shared files, folders, and libraries in **My Shared Files** list. Complete the steps below:

1. Navigate to **Secure Share Files** > **My Shared Files**, or the shared folder or library where the file resides.
2. Click the setting ( ) button in the same row with the shared item to view its detailed information, and a drop-down list appears.
3. Select **View Share Details** option from the drop-down list, and then you can view the detailed information of **Item Name**, **File Size**, **Version**, **File Path**, and the **Share Details** of the corresponding shared item. In the **Share Details** table, all sharing records of this shared item are listed. You can select one or more sharing records, and click **Delete** on the command bar to delete them.

   ***Note**: When a sharing record is deleted, the shared item in the corresponding sharing record is also deleted at the same time.

## Editing My Shared Files

In the **My Shared Files** page, you can edit the files shared by you by completing the following steps:

1. Navigate to **Secure Share Files** > **My Shared Files**, or the shared folder or library where the file resides.
2. You can edit the file via an internet browser by directly clicking the file name; you can edit the copy of a shared file on your local device by selecting the file, and then clicking **Download** on the command bar to download a copy of the file; you can also click the setting ( ) button in the same row with the selected file, and select the **Lock & Download for Editing** option to lock and download the shared file for editing.

   ***Note**: When a shared file is locked or being edited in a browser by another user, you cannot lock and download it for editing.

3. After you finish editing the copy of a file, follow the instructions on Uploading a File to upload the modified file to the **My Shared Files page** to overwrite the existing shared file.

The changes made to the shared file in AvePoint Perimeter Online Portal will be synchronized to the original file in SharePoint Online.

## Uploading a File

The sections below provide detailed instructions on using the **Upload** feature in AvePoint Perimeter Online Portal.

### Uploading a New File to a Shared Folder

To upload a new file into a shared folder or library, completing the following steps:

1. Open the shared folder or library where you want to upload a new file in AvePoint Perimeter Online Portal. Make sure no file with the same name exists in the shared folder or library.
2. Click **Upload** on the command bar, and an **Upload** window appears.
3. Click **Browse**, and select a file that you want to upload by clicking **Open**.
4. The **Overwrite the existing file** option is deselected. If the same file exists in the shared folder, the upload will fail.
5. Click **Upload** in the **Upload** window to upload the selected file, and then the file will be scanned for viruses and checked for its file size. If the file contains viruses, or the file size exceeds the maximum limit, the upload will fail.

   ***Note**: If you upload the file in Perimeter Online Portal via Internet Explorer, the maximum upload size is 2 GB. For other browsers, the maximum upload size is 10 GB.

The uploaded file will be added to the shared folder or library in Perimeter Online Portal and then synchronized to the original folder or library in SharePoint Online. In this way, the newly uploaded file is shared with all of the users with whom the folder or library has been shared.

### Overwriting an Existing Shared File

To overwrite an existing shared file, complete the following steps:

1. Navigate to **Secure Share Files** > **My Shared Files**, or the shared folder or library that contains the shared file you want to overwrite.
2. Select a shared file that you want to overwrite.
3. Click **Upload** on the command bar, or you can also click the setting ( ) button in the same row with the selected file, and select the **Replace Edited File** option. An **Upload** window appears.
4. Click **Browse**, and select the modified file in the same name with the shared file that you want to overwrite.
5. The **Overwrite the existing file** option is selected by default and you cannot deselect it. If the name of the file you selected to upload is not the same as the file you selected in the shared folder or library, the upload will fail.
6. Click **Upload** in the **Upload** window to upload the selected file.

The existing shared file will be overwritten by the uploaded file, and the changes will by synchronized to the original file in SharePoint.

### Stopping Sharing of My Shared Files, Folders, or Libraries

SharePoint Online users can stop sharing the shared files, folders and libraries in the **My Shared Files** list. Refer to the following steps to stop sharing:

1. Navigate to **Secure Shared Files** > **My Shared Files** page. The **My Shared Files** list appears.
2. Search the files, folders, or libraries by entering keywords of **Item Name** in the search text box on the upper-right corner of the **My Shared Files** page, and press Enter on the keyboard to perform the search.
3. Select one or more desired files, folders, or libraries in the search results.
4. Click **Stop Sharing** on the command bar. The selected files, folders, and libraries will no longer be shared with all of the users with whom you ever shared. The sharing records of selected files or folders will be deleted.

## Managing the Files, Folders, and Libraries that have been Shared With You in the Perimeter Online Portal

As a SharePoint Online user, you can view, download, edit, or upload the corresponding files, or the files in the folders and libraries that others have shared with you.

In the **Secure Share Files** page, clicking **Files Shared with Me** in the quick launch bar allows you to access the **Secure Share Files** > **Files Shared with Me** page.

### Viewing the Files or Folders that have been Shared with You

In the **Files Shared with Me** page, you can view detailed information of all shared files, folders, and libraries that are shared with you in **Files Shared with Me** list. Complete the steps below:

1. Navigate to **Secure Share Files** > **Files Shared with Me**, or the shared folder or library where the file resides.
2. Click the setting ( ) button in the same row with the shared item to view its detailed information, and a drop-down list appears.
3. Select **View Share Details** option from the drop-down list, and then you can view the detailed information of **Item Name**, **File Size**, **Version**, and the **Share Details** of the corresponding shared item. In the **Share Details** table, all sharing records of this shared item are listed.

### Editing Files that have been Shared with You

In the **Files Shared with Me** page, you can edit the files shared with you by completing the following steps:

1. Navigate to **Secure Share Files** > **Files Shared with Me**, or the shared folder or library where the file resides.
2. You can edit the file via an internet browser or on your local device.
    - **Edit** – If you have the **Edit** permission, you can directly edit the shared files in browser by clicking the file name; you can edit the copy of a shared file on your local device by selecting the file, and then clicking **Download** on the command bar to download a copy of the file; you can also click the setting ( ) button in the same row with the selected file, and select the **Lock & Download for Editing** option to lock and download for editing the shared file. After you finish editing the copy of a file, follow the instructions on Uploading a File to upload the modified file to the **My Shared Files** page or shared folder to overwrite the existing shared file.

      ***Note**: When a shared file is locked or being edited in browser by another user, you cannot lock and download it for editing.

    - **Edit Only in Browser** – If you have the **Edit Only in Browser** permission, you can edit a file in your internet browser by directly clicking the file name.

The changes made to the shared file in Perimeter Online Portal will be synchronized to the original file in SharePoint Online.

## Uploading a File

The sections below provide detailed instructions on using the **Upload** feature in the Perimeter Online Portal if you have **Edit** permission.

### Uploading a New File to a Shared Folder

To upload a new file into a shared folder or library, complete the following steps:

1. Open the shared folder or library where you want to upload a new file in AvePoint Perimeter Online Portal. Make sure no file with the same name exists in the shared folder or library.
2. Click **Upload** on the command bar, and an **Upload** window appears.
3. Click **Browse**, and select a file that you want to upload by clicking **Open**.
4. The **Overwrite the existing file** option is deselected. If the same file exists in the shared folder, the upload will fail.
5. Click **Upload** in the **Upload** window to upload the selected file, and then the file will be scanned for viruses and checked for its file size. If the file contains viruses, or the file size exceeds the maximum limit, the upload will fail.

    ***Note**: If you upload the file in Perimeter Online Portal via Internet Explorer, the maximum upload size is 2 GB. For other browsers, the maximum upload size is 10 GB.

The uploaded file will be added to the shared folder or library in Perimeter Online Portal and then synchronized to the original folder or library in SharePoint Online. In this way, the newly uploaded file is shared with all of the users who are shared with the folder or library.

### Overwriting an Existing Shared File

To overwrite an existing shared file, complete the following steps:

1. Navigate to **Secure Share Files** > **Files Shared with Me**, or the shared folder or library that contains the shared file you want to overwrite.
2. Select a shared file that you want to overwrite.
3. Click **Upload** on the command bar, or you can also click the setting ( ) button in the same row with the selected file, and select the **Replace Edited File** option. An **Upload** window appears.
4. Click **Browse**, and select the modified file in the same name with the shared file that you want to overwrite.
5. The **Overwrite the existing file** option is selected by default and you cannot deselect it. If the name of the file you selected to upload is not the same as the file you selected in the shared folder or library, the upload will fail.
6. Click **Upload** in the **Upload** window to upload the selected file.

The existing shared file will be overwritten by the uploaded file, and the changes will by synchronized to the original file in SharePoint.

# E-mail Users

As an e-mail user, if another user shares files, folders, or a library with you and selects the **Send e-mail notifications to the users above** option, you will receive an e-mail notification that includes the links to the shared content on the AvePoint Perimeter Online Portal.

After clicking the link in the e-mail, you will be immediately directed to the shared content if you are not required to log into the AvePoint Perimeter Online Portal; if you are required to log into the AvePoint Perimeter Online Portal and you have not registered an account, the **Account Registration** page will appear; if you are required to log into the AvePoint Perimeter Online Portal and you have registered an account, the **Sign In** page will appear.

## Registering an Account on the AvePoint Perimeter Online Portal

E-mail users can register a new AvePoint Perimeter Online Portal account by completing the following steps:

1. Click the link of the shared content in the AvePoint Perimeter Online secure share notification e-mail. If you are required to register, the **Account Registration** page of the AvePoint Perimeter Online Portal will appear.
2. Configure the following user profile settings for the new account:
    - **Name** – Enter the first name and last name into the corresponding text box.
    - **E-mail Address** – Your e-mail address will be displayed. This e-mail address will become your login ID for accessing the AvePoint Perimeter Online Portal.
    - Select the **Country** and **Gender** information from the drop-down lists.
    - **Password** – Enter the password for this login ID in the **Password** text box. Your password strength will be indicated in different colors. For details, click the information ( ) button.
    - **Confirm Password** – Enter the password again to confirm the password in the **Confirm Password** text box
    - **Verification Code** – Enter the verification code into the text box. Click **Refresh** to refresh the verification code.
3. You can click **UPLOAD PICTURE** to upload your picture to your user profile.
4. Click **Register** to register a new user account. Upon registering, a registration confirmation e-mail is sent to the e-mail entered in the **E-mail Address** section. Once you receive the e-mail message, click the supplied link to activate your account. After clicking the link, you will be redirected to the **Sign In** page.

# Logging into the AvePoint Perimeter Online Portal

E-mail users can log into AvePoint Perimeter Online Portal by completing the following steps:

1. Open the link for the shared content in the AvePoint Perimeter Online secure share notification e-mail using the browser. The **Sign In** page for the AvePoint Perimeter Online Portal appears.
2. Enter your login information:
    - If you have registered an AvePoint Perimeter Online Portal account, the user ID is automatically populated in the **Username** field. Enter the password into the **Password** field to log into the AvePoint Perimeter Online Portal.

      ***Note**: Click the **Forgot password?** link for the following conditions:

        - If you already registered a user account for AvePoint Perimeter Online Portal but forget your password, click the **Forgot password?** to reset your password. For detailed instructions, refer to Resetting a Password in the AvePoint Perimeter Online Portal.
        - If you already registered a user account for AvePoint Perimeter Online Portal but want to change your password, refer to the Editing My Profile Settings section to reset your password.
3. Click **Login** to access the AvePoint Perimeter Online Portal; if the multi-factor authentication function is enabled, the **Further Account Verification** page appears, and you must process the further account verification by completing the following steps:
    a. Click the **Sending Verification Code** button, and you will receive an authentication e-mail including a verification code.
    b. Enter the verification code in the corresponding text box on the **Further Account Verification** page.

      ***Note**: The verification code will expire in 2 minutes.

    c. Click Login to access the AvePoint Perimeter Online Portal.

# Editing My Profile Settings

To edit **My Profile** settings, complete the steps below:

1. Log into the AvePoint Perimeter Online portal.
2. Click the down arrow ( ) button next to the username on the upper-right corner of the page. A drop-down list appears.
3. Select the My Profile option from the drop-down list, and the **My Profile** page appears.
4. You can configuring the following settings in this page:
    - To change your profile picture, you can click **Change Picture** under your picture.

***Note**: The picture must be a JPG, JPEG, or PNG file and the file size cannot exceed 5 MB.

- To change your password, you can click the **Change Password** button on the lower-right corner of this page. The **Change Password** page appears. Change your password by completing the following steps:
    i. **Old Password** – Enter your old password in this textbox.
    ii. **New Password** – Enter a new password.
    iii. **Confirm Password** – Enter the new password again for confirmation.
    iv. **Verification Code** – Enter the verification code. Click **Refresh** to refresh the verification graphic.
    v. Click **Save** to save your new password, or click **Cancel** to go back to the **My Profile** page.

## Resetting a Password in the AvePoint Perimeter Online Portal

To reset a password for an AvePoint Perimeter Online Portal account, complete the steps below:

1. Go to the **Sign In** page of AvePoint Perimeter Online Portal and click **Forgot password?**. The **Forgot Password** page appears.
2. Enter the following information:
    - **E-mail Address** – Enter the e-mail address used as your AvePoint Perimeter Online Portal user ID to receive **Reset Password Confirmation** e-mail.
        - If you already registered an AvePoint Perimeter Online Portal account, enter the **E-mail Address** you configured in the **Account Registration** page.
    - **Verification** – Enter the verification code. Click **Refresh** to refresh the verification graphic.
3. Click **Submit**. After submitting, a **Reset Password Confirmation** e-mail is sent to the e-mail address you entered.
4. Retrieve the e-mail message and click the supplied link to set a new password. After clicking the link, you will be redirected to the **New Password** page. Enter the following information in this page:
    - **New Password** – Enter a new password.
    - **Confirm Password** – Enter the new password again for confirmation.
    - **Verification** – Enter the verification code. Click **Refresh** to refresh the verification graphic.

5. After setting up the new password, click **Submit** to save your new password, and then click **Back to sign in** in the new page. You are redirected to the **Sign In** page. Log into the AvePoint Perimeter Online Portal with the new password.

# Viewing the Dashboard in the AvePoint Perimeter Online Portal

In the **Dashboard** page, you can get an overview on the rankings of the senders who share items with you, and the items shared with you within a certain period. See the sections below for detailed instructions on viewing each ranking in the charts of the dashboard.

## Senders Who Shared With Me

The following chart displays the senders ranked by the number of times items have been shared with you within a certain period:

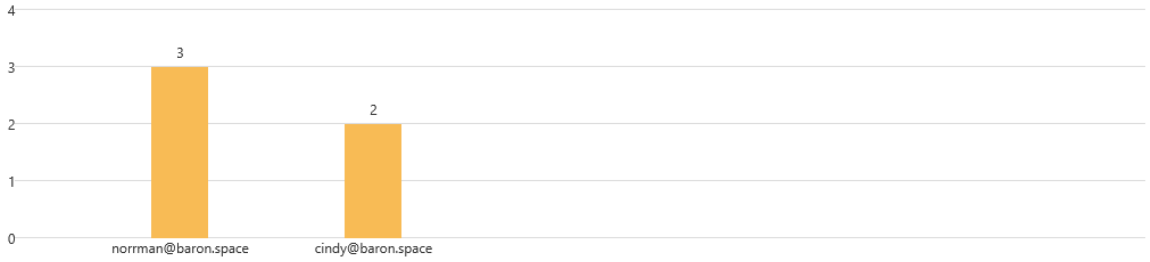


**Figure 12: The Senders Who Shared With Me chart.**

By default, the chart can display the data for up to five senders. The Y-axis of the chart represents the number of times that the sender shared items with you. The X-axis of the chart represents the name of senders who shared with you within a certain period. If desired, you can view all senders who shared with you by clicking the **View All Senders Who Shared With Me** on the upper-right corner of the chart to access the **Dashboard** > **View All Senders Who Shared With Me** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all senders who shared with you within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more senders with more details.
- **Search** – Enter keywords of **E-mail Address** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search.

## Items Shared With Me

The following chart shows the shared items ranked by the number of times they were shared with you within a certain period:

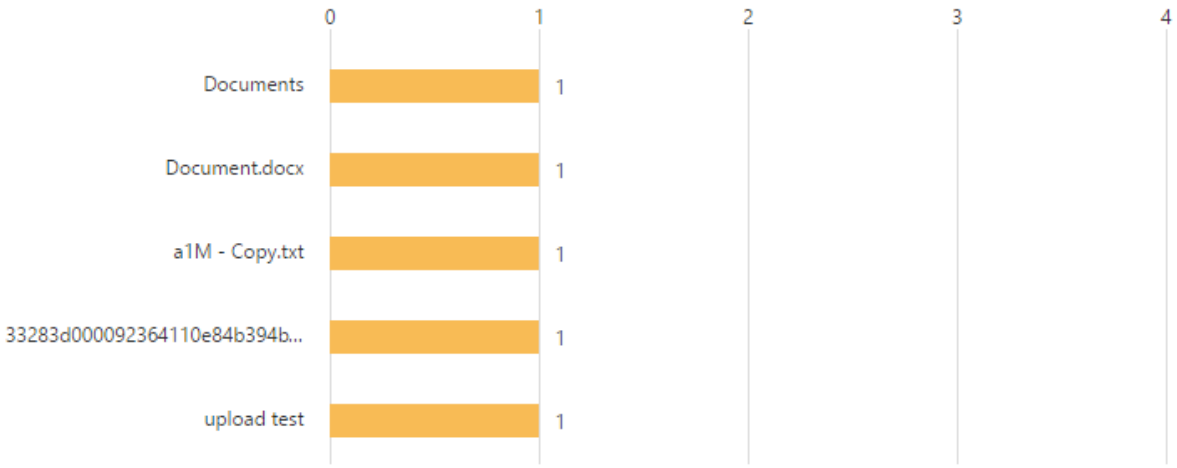


**Figure 13: The Items Shared With Me chart.**

By default, the chart can display the data for up to five shared items. The Y-axis of the chart represents the names of shared items. The X-axis of the chart represents the number of times items were shared with you within a certain period. If desired, you can view all items shared with you by clicking the **View All Items Shared With Me** on the upper-right corner of the chart to access the **Dashboard** > **View All Items Shared With Me** page. You can perform the following actions in this page:

- **Time Range** – To customize the time range for this chart, click the box next to **Time Range**. Select the start date and end date of your time range from the calendar, and then click **OK** to save your configuration.
- **Export** – Click **Export** on the upper-right corner of this chart, you can export the data of all items shared with you within a certain period in a **CSV** file to a custom location.
- **Show Rows** – Select the desired number from the **Show Rows** drop-down menu in the lower-right corner of this page. You can view more shared files, folders, and libraries with more details.
- **Search** – Enter keywords of **Item Name** in the Search text box on the upper-right corner of the page, and press Enter on the keyboard to perform the search

# Managing the Files, Folders, and Libraries that have been Shared with You in the Perimeter Online Portal

E-mail users can view, download, edit, or upload the corresponding files, or the files in folders and libraries that others have shared with you.

## Viewing the Files, Folders and Libraries Shared with You

In the **Files Shared with Me** page, you can view detailed information of all shared files, folders, and libraries that are shared with you in **Files Shared with Me** list. Complete the steps below:

1. Navigate to **Secure Share Files** > **Files Shared with Me**, or the shared folder or library where the file resides.
2. Click the setting ( ) button in the same row with the shared item to view its detailed information, and a drop-down list appears.
3. Select **View Share Details** option from the drop-down list, and then you can view the detailed information of **Item Name**, **File Size**, **Version**, and the **Share Details** of the corresponding shared item. In the **Share Details** table, all sharing records of this shared item are listed.

## Editing the Files Shared with You

In the **Files Shared with Me** page, if you have the **Edit** permission, you can edit the files shared with you by completing the following steps:

1. Navigate to **Secure Share Files** > **My Shared Files**, or the shared folder or library where the file resides.
2. You can edit the file on your local device.
    - **Edit** – If you have the **Edit** permission, you can edit the copy of a shared file on your local device by selecting the file, and then clicking **Download** in the command bar to download a copy of the file; you can also click the setting ( ) button in the same row with the selected file, and select the **Lock & Download for Editing** option to lock and download for editing the shared file. After you finish editing the copy of a file, follow the instructions on Uploading a File to upload the modified file to the **My Shared Files** page or shared folder to overwrite the existing shared file.

      ***Note**: When a shared file is locked or being edited in browser by another user, you cannot lock and download it for editing.

The changes made to the shared file in Perimeter Online Portal will be synchronized to the original file in SharePoint Online.

## Uploading a File

The sections below provide detailed instructions on using the **Upload** feature in the Perimeter Online Portal if you have **Edit** permission.

### Uploading a New File to a Shared Folder

To upload a new file into a shared folder or library, complete the following steps:

1. Open the shared folder or library where you want to upload a new file in the AvePoint Perimeter Online Portal. Make sure no file with the same name exists in the shared folder or library.

2. Click **Upload** on the command bar, and an **Upload** window appears
3. Click **Browse**, and select a file that you want to upload by clicking **Open**.
4. The **Overwrite the existing file** option is deselected. If the same file exists in the shared folder, the upload will fail.
5. Click **Upload** in the **Upload** window to upload the selected file, and then the file will be scanned for viruses and checked for its file size. If the file contains viruses, or the file size exceeds the maximum limit, the upload will fail.

   ***Note**: If you upload the file in Perimeter Online Portal via Internet Explorer, the maximum upload size is 2 GB. For other browsers, the maximum upload size is 10 GB.

The uploaded file will be added to the shared folder or library in Perimeter Online Portal and then synchronized to the original folder or library in SharePoint Online. In this way, the newly uploaded file is shared with all of the users who the folder or library are shared with.

### Overwriting an Existing Shared File

To overwrite an existing shared file, complete the following steps:

1. Navigate to **Secure Share Files** > **Files Shared with Me**, or the shared folder or library that contains the shared file you want to overwrite.
2. Select a shared file that you want to overwrite.
3. Click **Upload** on the command bar, or you can also click the setting ( ) button in the same row with the selected file, and select the **Replace Edited File** option. An **Upload** window appears.
4. Click **Browse**, and select the modified file in the same name with the shared file that you want to overwrite.
5. The **Overwrite the existing file** option is selected by default and you cannot deselect it. If the name of the file you selected to upload is not the same as the file you selected in the shared folder or library, the upload will fail.
6. Click **Upload** in the **Upload** window to upload the selected file.

The existing shared file will be overwritten by the uploaded file, and the changes will by synchronized to the original file in SharePoint.

# Using Message Center in the AvePoint Perimeter Online Portal

The messages sent by AvePoint Perimeter Online are stored in the Message Center. AvePoint Perimeter Online will send messages in the following situations:

- If some files, folders, or a library is secure shared successfully and the **Send e-mail notifications to the users above** option is selected, AvePoint Perimeter Online will send a message to the shared users to remind the corresponding users to check the shared files, folders, or library.
- If some shared files, folders, or libraries are about to expire, AvePoint Perimeter Online will send a message to the shared users to remind the corresponding users of checking the shared files, folders, or libraries.
- If some shared files, folders, or libraries are expired, AvePoint Perimeter Online will send a message to the shared users to remind the corresponding users that the expiration date has come.
- If shared files, folders, or libraries are revoked, AvePoint Perimeter Online will send a message to the users who shared them and the users who are shared with.

After logging into the AvePoint Perimeter Online Portal, you can see a Message Center icon ( ) in the upper-right corner. To view and manage the messages, complete the following steps:

1. Click the icon ( ) in the upper-right corner. The **Message Center** pop-up window appears.
2. Click the **View all message** option in the bottom of the pop-up window to access the **Message Center** page.
3. In the **Message Center** page, you can see a **Message Center** list and the messages are listed according to their **Sending Time** in descending order.
    - **Show Rows** – To change the number of messages displayed per page, select the desired number from the **Show Rows** drop-down menu in the lower-right corner.
    - **Delete** – Select one or more messages that you want to delete, and click **Delete** on the command bar to delete them.
    - **Delete All** – Click **Delete All** to clear all the messages in **Message Center**.
4. Click **Close** to exit the **Message Center** and go back to the previous page in the AvePoint Perimeter Online Portal.

# Notices and Copyright Information

**Notice**
The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

**Copyright**


**Trademarks**
AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Office, Office 365, SharePoint, Windows PowerShell, SQL Server, Outlook, Windows Server, Active Directory, and Dynamics CRM 2013 are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

**Changes**
The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
Harborside Financial Center, Plaza 10
3 Second Street, 9th Floor
Jersey City, New Jersey 07311
USA